Jan Kolouch, Pavel Bašta a kol.

# CyberSecurity

Edice CZ.NIC

**CYBERSECURITY**

doc. JUDr. Jan Kolouch, Ph.D.
Bc. Pavel Bašta
Andrea Kropáčová
Bc. Martin Kunc

Vydavatel:
CZ.NIC, z. s. p. o.
Milešovská 5, 130 00 Praha 3
Edice CZ.NIC
www.nic.cz

1. vydání, Praha 2019
Kniha vyšla jako 20. publikace v Edici CZ.NIC.
ISBN 978-80-88168-34-8

© 2019 Jan Kolouch, Pavel Bašta a kol.
Toto autorské dílo podléhá licenci Creative Commons BY ND 3.0 (http://creativecommons.org/licenses/by-nd/3.0/cz/), jeho sdílení je tedy možné za předpokladu, že zůstane zachováno označení autora díla a prvního vydavatele díla, sdružení CZ.NIC, z. s. p. o. Dílo může být překládáno a následně šířeno v písemné či elektronické formě, na území kteréhokoliv státu.

CZ.NIC | SPRÁVCE DOMÉNY CZ

Právní stav byl zohledněn ke dni 1. 7. 2018.

**Autorský kolektiv**
**doc. JUDr. Jan Kolouch, Ph.D.,** autor kapitol:
předmluva autorů, 1, 2, 3, 4, závěr, seznam literatury; spoluautor kapitol: 5, 6
**Bc. Pavel Bašta,** autor kapitol: 5, 6; spoluautor kapitol: 1, 1.3.3, 1.4.
**Andrea Kropáčová,** autorka kapitoly 7
**Bc. Martin Kunc,** autor kapitol: 6.4, 6.5

ISBN 978-80-88168-34-8

— Jan Kolouch, Pavel Bašta a kol.

# CyberSecurity

— Edice CZ.NIC

# Předmluva vydavatele

**Vážení čtenáři,**

pokaždé, když vidím novou knihu v naší edici, mám pocit dobře vykonané práce. Ne, nejsem autorem, editorem nebo grafikem těchto knih, na jejich vzniku se nepodílím prakticky žádnou činností, ale i tak ten pocit mám. Jsem rád, že Edice CZ.NIC existuje a pomáhá spatřit světlo světa spoustě výborných knih, které by to (možná) bez nás měly s cestou ke čtenáři složitější.

Speciálně mám ale radost vždy, když jde o knihu z oblasti bezpečnosti. Měl jsem tu čest psát již předmluvu ke knize CyberCrime, kterou jsme v naší edici vydávali v roce 2016. V letošním roce jsme se pokusili na tuto knihu volně navázat – s rozšířeným týmem autorů a novým, z trochu jiného úhlu pohledu pojatým obsahem.

K osvědčenému autorovi, vysokoškolskému pedagogovi a ostřílenému odborníkovi na kybernetickou kriminalitu Janu Kolouchovi se připojili moji kolegové z prostředí bezpečnostních týmů, kteří dali knize další rozměr.

Kniha se tak z mého pohledu ještě více posunula z oné pomyslné knihovny na pracovní stůl (jak jsem o tom psal před dvěma lety) a já věřím, že bude užitečná jak pro běžné uživatele, kteří budou potřebovat radu, návod nebo vhodný postup při řešení každodenních problémů bezpečnosti, tak i pro odborníky, kteří v ní najdou inspiraci pro své další vzdělávání.

Ostatně udělejte si obrázek sami – přeji příjemně a užitečně strávené chvíle při práci s knihou.

**Martin Peterka, CZ.NIC**
*Praha, 23. října 2018*

# Předmluva autorů

## Předmluva autorů

*„Život bez informačních a komunikačních technologií je pro naši společnost již nemyslitelný, respektive nemožný.“* [1]

Dnešní společnost se v průběhu posledních 20 let stala na informačních a komunikačních technologiích[2] natolik závislá, že okamžitý kolaps těchto technologií a služeb na ně navázaných by pro značnou část lidstva byl spojen s téměř apokalyptickými následky, ne nepodobnými těm uvedeným v románu Ondřeje Neffa - Tma.[3]

V tomto románu je apokalypsa spojena s masivním a dlouhotrvajícím výpadkem, respektive zdánlivým koncem elektrické energie. Co by však pro lidstvo znamenal okamžitý a nečekaný výpadek ICT?

Jsme přesvědčeni, že ještě před deseti či patnácti lety by nemožnost připojení se k Internetu a dalším ICT službám znamenala pouze to, že bychom se věnovali jiné práci, či udělali víc „skutečné práce“.

V současné době je otázkou, co bychom mohli dělat? Nezapnuli bychom počítač ani textový editor, ve kterém píšeme tuto knihu, nikomu bychom se nedovolali, nebyli bychom schopni si užitečné odkazy dohledat na Internetu (ok… na https://www.google.com/), nedomluvili bychom se se svým editorem a rozhodně bychom Vám nijak nebyli schopni předat informace, které se do této knihy snažíme zachytit.

Další otázkou je, zda by vůbec byly poskytovány služby, na které jsme zvyklí a bez kterých si svůj život už neumíme představit. Mezi tyto služby je zcela bezpochyby možné zařadit distribuci elektřiny, vody, telekomunikační služby, zdravotní péči, zajištění bezpečnosti občanů a státu, dopravu (řízení provozu, ale i hromadnou dopravu), finanční transakce (včetně běžných plateb, výběru z bankomatů atd.), přístup k informacím (televizní zpravodajství, ale samozřejmě i Seznam.cz, Google.com) aj.

Nedávné útoky ransomwarem[4] WannaCry, Petya (respektive mutací tohoto malware – Petrwap či Win32/Diskcoder.C Trojan) ukázaly zranitelnost a zejména závislost „vyspělého a moderního“

1: KOLOUCH, Jan. *CyberCrime.* Praha: CZ.NIC, 2016, s. 474

2: Dále jen: **ICT** či informační a komunikační technologie, **IT** či informační technologie, **IS** či informační systémy. Pojem **ICT** v sobě zahrnuje jednak počítačové systémy (viz dále), tak i technologie (např. optické, metalické kabely aj.) umožňující vzájemnou interakci těchto systémů.

3: NEFF, Ondřej. *Tma.* Praha: Plus. ISBN 978-80-259-0279-0

4: Blíže k pojmu ransomware viz KOLOUCH, Jan. *CyberCrime.* Praha: CZ.NIC, 2016, s. 221 a násl. Dostupné z: https://knihy.nic.cz/files/edice/cybercrime.pdf

světa na ICT a zároveň prezentovaly nedostatečnost zabezpečení vitálních systémů před kybernetickými útoky. Právě WannaCry, byť se jednalo o klasický ransomware útok, kterých jsou denně desítky, dokázal zcela zastavit provoz 16 nemocnic ve Velké Británii.[5] Petrwap pak způsobil značné problémy zejména na Ukrajině, kdy řada ukrajinských společností (mimo jiné se jednalo o energetické společnosti, letiště v Kyjevě, banky aj.) nemohla vykonávat svoji běžnou činnost či ji musela zcela zastavit. *„V důsledku tohoto útoku mají některé banky problémy s prováděním bankovních operací"*, oznámila ukrajinská centrální banka. Různé antivirové společnosti pak oznamovaly země, jež byly tímto útokem přímo dotčeny. Podle antivirové společnosti ESET byly mezi nejvíce napadenými zeměmi vedle Ukrajiny i Itálie, Izrael, Srbsko, ale také Česká republika.[6] Společnost Kaspersky Lab pak tento okruh zemí dále rozšířila o Polsko, Německo, Francii, USA, Velkou Británii, Austrálii, Rusko aj.[7]

Otázkou pak zůstává, jestli jsme skutečně „vyspělí a moderní"? Možná by bylo lepší nás označit za „trendy a in" a především **neustále připojené**. Velmi rychle jsme si začali zvykat na nové a nové technologie, jejich vylepšení a nadstavby v podobě Internet of Things[8] (do budoucna Internet of Everything), které vlastně ani v řadě případů skutečně nepotřebujeme.

---

5: Viz např.: *UK hospitals hit with massive ransomware attack*. [online]. [cit. 27. 6. 2076]. Dostupné z: https://www.theverge.com/2017/5/12/15630354/nhs-hospitals-ransomware-hack-wannacry-bitcoin
*U.K. Hospitals Hit in Widespread Ransomware Attack.* [online]. [cit. 27. 6. 2017]. Dostupné z: https://krebsonsecurity.com/2017/05/u-k-hospitals-hit-in-widespread-ransomware-attack/
*Masivní kyberútok zasáhl ve stovce zemí. Ochromil nemocnice i Telefóniku.* [online]. [cit. 27. 6. 2017]. Dostupné z: https://www.cnews.cz/ransomware-wanacryptor-wcry-wannacry

6: *Šíří se staronový vir vyděrač. Výkupné neplaťte, adresa je nefunkční.* [online]. [cit. 28. 6. 2017]. Dostupné z: https://technet.idnes.cz/kyberneticky-hackersky-utok-ve-svete-ransomware-fbq-/sw_internet.aspx?c=A170627_172510_tec-kratke-zpravy_pka

7: *RANSOMWARE IS ONE OF THE WORLD'S FASTEST GROWING TYPES OF MALWARE.* [online]. [cit. 28. 6. 2017]. Dostupné z: https://go.kaspersky.com/Anti-ransomware-tool.html

8: Dále jen **IoT**, či Internet věcí. Typicky se jedná o zařízení (počítačové systémy), které sbírají a vyměňují si data s jinými počítačovými systémy. Předpokladem je, že jsou tato zařízení připojena k počítačovému systému, či počítačové síti. Příkladem může být:

- komunikace mezi televizí a žárovkou - pokud bude televize schopna navázat kontakt se žárovkou, bude možné zajistit optimální nastavení světla žárovky ve vztahu k aktuálnímu nastavení jasu televize;
- předávání informací z osobní váhy do telefonu či přímo lékaři;
- předání informací z wearables („nositelná" elektronika, čidla aj.) umístěného v oblečení, botách do počítačového systému pro výpočet ušlých kroků, spálených kalorií aj.
- sledování pozice GPS a předávání této informace;
- sledování množství potravin v lednici a případný automatický nákup chybějících potravin aj.

Bližší informace naleznete např. na:
*What is Internet of Things.* [online]. [cit. 15. 7. 2016]. Dostupné z: https://www.microsoft.com/en-us/cloud-platform/internet-of-things

*„Ještě než jsem se přestěhoval do své vily na šesti kolech, byl můj byt ten nejlepší kamarád. Lednička vždycky věděla, na co mám právě chuť. Šampaňské bylo pokaždé vychlazené na tu správnou teplotu s přesností na desetinu stupně. Sama vyhazovala prošlé potraviny a sama nakupovala čerstvé. Pračka hlásila šatní skříni, kdy má pořídit nové oblečení podle poslední módy. Postel mě sama uspávala i budila podle mozkových vln. Záchodová mísa průběžně analyzovala tělesný odpad, a když něco nebylo v pořádku, přivolala lékařského medibota a nařídila ledničce, co mám jíst a pít pro zdraví. Všechno bylo tak propojené a perfektní, že jsem si nakonec začal připadat jako další domácí spotřebič. A tak jsem oprášil starý vojenský kufr po tátovi ukrývající skoro zapomenuté nářadí. Z útrob jsem vytáhl kladivo a všem těm chytrým přístrojům vymlátil wi-fi anténky.“*

**Být nad věcí internetu věcí**[9]

Informace a data představují značný ekonomický i politický potenciál. Informace a jejich obsah mohou rozhodovat nejen o bytí či nebytí jednotlivce či firmy, ale ve své podstatě jsou schopny ovlivnit celosvětový vývoj.[10]

Je třeba si uvědomit, že čím více budeme závislí na ICT a čím více dat o nás tyto technologie budou sbírat a sdílet, tím se staneme zranitelnějšími.

Řadě následků, které jsou způsobeny kybernetickými útoky, lidskou hloupostí či neznalostí, je přitom možné se vyhnout, pokud budou respektovány základní principy kybernetické bezpečnosti.[11]

V této souvislosti je třeba připomenout citát ***Scientia est potentia*** (***vědění je moc, v poznání a znalostech je síla, vědění je síla***). V případě ICT a služeb s nimi spojených je třeba poznat, co tyto technologie a služby představují, co činí a k čemu slouží.[12]

---

*Internet of Things (IoT).* [online]. [cit. 15. 7. 2016]. Dostupné z: http://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT

9: STANČÍK, Petr. *100 miliard neuronů.* [online]. [cit. 16. 8. 2018]. Dostupné z: https://backendstories.skoda-kariera.cz/assets/files/library/b01/100_MILIARD_NEURONU_-_PETR_STANCIK.pdf s. 133

10: Viz informace o ovlivnění prezidentských voleb v USA (2016) a Francii (2017). Blíže viz např.: *Tajné služby: Kampaň, která měla ovlivnit prezidentské volby v USA, nařídil Putin.* [online]. [cit. 29. 6. 2017]. Dostupné z: http://www.ceskatelevize.cz/ct24/svet/2005207-tajne-sluzby-kampan-ktera-mela-ovlivnit-prezidentske-volby-v-usa-naridil-putin

*Macronův volební štáb napadli hackeři, tvrdí japonská protivirová firma.* [online]. [cit. 29. 6. 2017]. Dostupné z: http://zpravy.idnes.cz/macron-utok-hackeri-trend-micro-d3b-/zahranicni.aspx?c=A170425_071554_zahranicni_san

11: *WannaCry se neměl vůbec rozšířit. Stačilo, abychom používali Windows Update.* [online]. [cit. 27. 6. 2017]. Dostupné z: https://www.zive.cz/clanky/wannacry-se-nemel-vubec-rozsirit-stacilo-abychom-pouzivali-windows-update/sc-3-a-187740/default.aspx

12: KOLOUCH, Jan. *CyberCrime.* Praha: CZ.NIC, 2016, s. 474

V současnosti by rezignace na využívání ICT znamenala izolaci jedince či organizace od zbytku společnosti, v řadě případů i nemožnost „fungování“ tohoto jedince ve společnosti či státě, který tyto technologie využívá, případně vyžaduje, aby jej využívaly i osoby, které se v jeho teritoriu nacházejí (např. datové schránky, které jsou povinné pro určité subjekty; různé formy e-identit aj.).

Pokud chceme v současné společnosti žít a využívat její benefity, není možné se od ICT oprostit a rozhodně nemá smysl tyto technologie přestat využívat.

Informační a komunikační technologie jsou oborem, který se nejdynamičtěji a nejmasivněji vyvíjí, avšak otázkám bezpečnosti či zabezpečení není věnována taková pozornost jako například tomu, jaký bude design výrobků, kapacita úložného prostoru, možnosti telekomunikace s dalšími zařízeními aj.

Kniha, kterou právě čtete, se primárně snaží věnovat problematice kybernetické bezpečnosti. Ale tak, jako nebylo možné se při řešení problematiky kyberkriminality vyhnout kybernetické bezpečnosti, ani u kybernetické bezpečnosti nelze opomenout problematiku kyberkriminality. Tyto dvě oblasti jsou bezprostředně spjaty a bezpečnostní opatření v řadě případů odráží útoky, které mají ve své podstatě kriminální povahu.

Naší snahou je v této knize představit základní principy, které by každá osoba, která využívá ICT, měla respektovat a případně si je měla modifikovat v závislosti na činnosti či účelu, za kterým tyto technologie využívá. Dále pak načerpat informace o činnosti bezpečnostních týmů typu CERT, CSIRT[13] v kyberprostoru, jejich možnostech a limitech.

Samostatná pozornost je také věnována výkladu některých právních norem, které s problematikou kybernetické bezpečnosti bezprostředně souvisejí. Půjde především o novelizovaný zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)[14], ve znění pozdějších předpisů; Nařízení Evropského parlamentu a Rady (EU) 2016/697 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů[15] a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) aj.

Výklad zákona o kybernetické bezpečnosti a prováděcích vyhlášek k tomuto zákonu je podán formou komentáře.

---

13: **CERT** (**C**omputer **E**mergency **R**esponse **T**eam) či **CSIRT** (**C**omputer **S**ecurity **I**ncident **R**esponse **T**eam). Dále jen **CERT** a **CSIRT**. Blíže viz kap. 7 CERT/CSIRT týmy

14: Dále jen zákon o kybernetické bezpečnosti či **ZoKB**

15: Také známé jako GDPR (**G**eneral **D**ata **P**rotection **R**egulation) či Obecné nařízení o ochraně osobních údajů. Dále jen **GDPR**.

Tato kniha byla pro autory skutečným oříškem, neboť je mnohem složitější psát knihu o kybernetické bezpečnosti, respektive o tom, jak byste si měli zabezpečit svoje prvky ICT, jak se chovat bezpečně on-line aj. než psát knihu o kybernetických útocích a právní odpovědnosti za ně.[16] Ten zásadní problém totiž spočívá v tom, že kybernetická bezpečnost je de facto něco, co je možné popsat jako neustále se vyvíjející a měnící se proces, který je závislý na řadě proměnných. Těmito proměnnými samozřejmě mohou být data či samotné prvky ICT, jež jsou předmětem ochrany, vlastní nastavené procesy a jejich revize aj. Tím nejvýznamnějším prvkem je však uživatel (ať již koncový uživatel či administrátor), který vlastní prvky kybernetické bezpečnosti aplikuje.

Právě zde se nachází onen pomyslný kámen úrazu spočívající v tom, že vám budou v dobré víře předány informace, návody a postupy, které jsme si osvojili a otestovali. To co bude prezentováno, je náš náhled na problematiku kybernetické bezpečnosti a procesů s ní spojených. Tyto návody, postupy a doporučení fungují u nás, ale nemusí fungovat u vás, neboť při vlastní implementaci jakýchkoliv bezpečnostních postupů je dobré vycházet z určitých ověřených doporučení, ale především je vhodné individualizovat, modifikovat či měnit tyto postupy v závislosti na specifických podmínkách ať už uživatele samotného, či organizace.

Na základě výše uvedeného jsme se rozhodli tuto knihu koncipovat tak, aby informace v ní obsažené mohli využít jak běžní uživatelé (např. při tvorbě a správě hesel; nastavování VPN aj.), tak IT odborníci, kteří se chtějí vzdělat i v problematice kybernetické bezpečnosti. Nedílnou součástí této publikace jsou i doporučení, rady, postupy, případně nástroje využitelné jak uživateli, tak právě i správci jednotlivých ICT systémů. Tyto rady a doporučení vycházejí zejména ze zkušeností pracovníků CSIRT.CZ a CZ.NIC-CSIRT při řešení kybernetických útoků.

Tato kniha shrnuje naše názory a zkušenosti, které jsme získali v oblasti kybernetické bezpečnosti, kybernetické kriminality a edukace uživatelů.

Identifikační údaje osob použité v příkladech (IP adresy, e-mailové schránky apod.) byly v některých případech pozměněny, na druhou stranu monografie obsahuje celou řadu reálných případů z praxe, u nichž z důvodu objektivnosti byly zachovány informace o skutečných aktérech či detailech útoku.

Kdykoli rádi přivítáme jakoukoli zpětnou vazbu od čtenářů této knihy. Vy jste totiž ti, kteří dokáží odhalit chyby a prohřešky, které jsme přehlédli. Také budeme rádi, pokud nás upozorníte na témata, která vás zajímají více.

Za jakoukoli Vaši zpětnou vazbu jsme vděční.

16: Viz KOLOUCH, Jan. *CyberCrime.* Praha: CZ.NIC, 2016. ISBN 978-80-88168-18-8 [online]. Dostupné z: https://knihy.nic.cz/files/edice/cybercrime.pdf

Tuto knihu jsme se rozhodli vydat pod Creative Commons licencí: CC BY ND.[17]

Závěrem bychom chtěli poděkovat všem těm, kdo se o výslednou podobu této knihy zasloužili. Náš dík patří Evě Cvrkové, Martinu Peterkovi, JUDr. Josefu Součkovi, CSc., Mgr. Janu Nejedlému, všem kolegům z CESNET CERTS a CSIRT.CZ jakož i dalším odborníkům, s nimiž jsme měli tu čest spolupracovat a diskutovat.

Děkujeme všem, kdo byli ochotni číst a připomínkovat rukopis této knihy. Díky za Vaše připomínky a náměty.

Poslední a největší dík patří našim rodinám, které nám umožnily a umožňují dělat to, co nás baví.

Za autory

**Jan Kolouch**
jan.kolouch@cesnet.cz

17: Bližší informace o creative commons licencích dále naleznete např. na:
https://creativecommons.org/licenses/by-nd/3.0/cz/
https://cs.wikipedia.org/wiki/Creative_Commons

# Obsah

**Předmluva vydavatele** **5**

**Předmluva autorů** **9**

**Seznam zkratek** **25**

**I Základní terminologie** **33**

**1 Kyberprostor (Cyberspace)** **35**

**2 Pojem kybernetické bezpečnosti a pojmy související** **39**
2.1 Kybernetická bezpečnost 39
2.2 Principy kybernetické bezpečnosti 45
2.2.1 Triáda CIA 45
2.2.2 Prvky kybernetické bezpečnosti 56
2.2.3 Životní cyklus kybernetické bezpečnosti 63
2.3 Riziko, aktivum, zranitelnost 68
2.3.1 Riziko 68
2.3.2 Aktivum 72
2.3.3 Zranitelnost 72
2.4 Kybernetické hrozby, události, incidenty a útoky 73
2.4.1 Kybernetická hrozba 74
2.4.2 Kybernetická bezpečnostní událost 80
2.4.3 Kybernetický (bezpečnostní) incident 81
2.4.4 Kybernetický útok (Cyber Attack) 82
2.4.5 Kyberkriminalita (Cybercrime) 83

**II Legislativa** **85**

**3 Legislativní základ kybernetické bezpečnosti** **87**
3.1 Legislativní vývoj kybernetické bezpečnosti v ČR 87
3.2 Právní normy vztahující se ke kybernetické bezpečnosti 94
3.2.1 Dokumenty EU/ES sloužící k harmonizaci právních úprav při řešení problematiky kybernetické bezpečnosti 95
3.2.2 Právní normy ČR 98
3.3 Exkurze do práv a povinností vyplývajících z některých právních norem 99
3.3.1 GDPR 101
3.3.1.1 Místní působnost GDPR 104
3.3.1.2 Osobní údaj 104

3.3.1.3 Zpracování osobních údajů 109
3.3.1.4 Zabezpečení osobních údajů 111
3.3.1.5 Posouzení vlivu na ochranu osobních údajů (DPIA) 112
3.3.2 ePrivacy 113
3.3.2.1 Působnost ePrivacy 114
3.3.2.2 Základní terminologie ePrivacy 115
3.3.2.3 Zpracování dat 118
3.3.3 Občanský zákoník 120
3.3.3.1 Ochrana soukromí 121
3.3.3.2 Právní jednání 123
3.3.3.3 Náhrada škody 123
3.3.4 Trestní zákoník 124

**4 Zákon o kybernetické bezpečnosti 129**
4.1 Příčiny vzniku ZoKB 130
4.2 Základní cíle a principy ZoKB 133
4.3 Komentář k ZoKB 138
§ 1 Předmět úpravy 138
§ 2 Vymezení pojmů 142
Kybernetický prostor 148
Kritická informační infrastruktura 150
Bezpečnost informací 154
Významný informační systém 154
Správce informačního systému 164
Správce komunikačního systému 164
Provozovatel informačního nebo komunikačního systému 164
Významná síť elektronických komunikací 167
Základní služba. Informační systém základní služby.
Provozovatel základní služby 167
Digitální služba 189
Příslušný orgán 197
§ 3 198
Poskytovatel služby elektronických komunikací a subjekt zajišťující síť elektronických komunikací 200
Orgán nebo osoba zajišťující významnou síť 205
Správce a provozovatel informačního systému kritické informační infrastruktury 208
Správce a provozovatel komunikačního systému kritické informační infrastruktury 208
Správce a provozovatel významného informačního systému 216
Správce a provozovatel informačního systému základní služby 222

Provozovatel základní služby 228
Poskytovatel digitální služby 233
§ 3a Zástupce poskytovatele digitálních služeb 237
§ 4 Bezpečnostní opatření 241
§ 4a 248
§ 5 250

**Organizační opatření 253**
Systém řízení bezpečnosti informací 253
Řízení rizik 259
Bezpečnostní politika 264
Organizační bezpečnost 266
Stanovení bezpečnostních požadavků pro dodavatele 274
Řízení aktiv 275
Bezpečnost lidských zdrojů 276
Řízení provozu a komunikací kritické informační infrastruktury nebo významného informačního systému 277
Řízení přístupu osob ke kritické informační infrastruktuře nebo k významnému informačnímu systému 277
Akvizice, vývoj a údržba kritické informační infrastruktury a významných informačních systémů 278
Zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů 279
Řízení kontinuity činností 280
Kontrola a audit kritické informační infrastruktury a významných informačních systémů 281

**Technická opatření 281**
Fyzická bezpečnost 282
Nástroj pro ochranu integrity komunikačních sítí 285
Nástroj pro ověřování identity uživatelů 285
Nástroj pro řízení přístupových oprávnění 287
Nástroj pro ochranu před škodlivým kódem 288
Nástroj pro zaznamenávání činnosti kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů 289
Nástroj pro detekci kybernetických bezpečnostních událostí 290
Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí 291
Aplikační bezpečnost 292
Kryptografické prostředky 292
Nástroj pro zajišťování úrovně dostupnosti informací 293
Bezpečnost průmyslových a řídicích systémů 294

§ 6 294
§ 6a 295
§ 7 Kybernetická bezpečnostní událost a kybernetický bezpečnostní incident 299
§ 8 Hlášení kybernetického bezpečnostního incidentu 302
§ 9 Evidence 311
§ 10 314
§ 10a 316
§ 11 Opatření 319
§ 12 Varování 323
§ 13 Reaktivní a ochranné opatření 325
§ 14 330
§ 15 331
§ 15a 334
§ 16 Kontaktní údaje 335
§ 17 Národní CERT 340
§ 18 Provozovatel národního CERT 348
§ 19 Veřejnoprávní smlouva 353
§ 20 Vládní CERT 356
§ 21 Stav kybernetického nebezpečí 361
§ 21a Úřad 367
§ 22 367
§ 22a Určení provozovatele základní služby a informačního systému základní služby 374
§ 22b 379
§ 23 Kontrola 381
§ 24 Nápravná opatření 384
§ 24a Kontrola činnosti Úřadu 386
§ 24b 388
§ 24c 388
§ 25 Přestupky 389
§ 26 393
§ 27 Společné ustanovení k přestupkům 394
§ 28 Zmocňovací ustanovení 394
§ 29 Přechodná ustanovení 395
§ 30 396
§ 31 397
§ 32 398
§ 33 Společná ustanovení 399
§ 35 Změna zákona o elektronických komunikacích 401
§ 37 Změna zákona o provozování rozhlasového a televizního vysílání 402
§ 38 Účinnost 402

**III Kyberbezpečnost prakticky** **405**

**5 Fyzická bezpečnost** **411**
5.1 Zajištění perimetru 411
5.2 Kontrola přístupu 412
5.3 Vnitřní bezpečnost 415
5.4 Ochrana počítačových systémů 416
5.4.1 Opatření proti krádeži počítačových systémů 417
5.4.2 Ochrana před rozebráním a úpravou počítačových systémů 418
5.4.3 Ochrana před připojením cizích periferií k počítačovým systémům 420

**6 Bezpečnost sítí a služeb** **425**
6.1 Ochrana sítí 425
6.1.1 Rozdělení sítě jako základní prvek zajištění bezpečnosti 426
6.1.1.1 DMZ 426
6.1.1.2 VLAN 427
6.1.2 Ochrana sítě LAN 429
6.1.2.1 DHCP protokol 429
6.1.2.2 ARP protokol 431
6.1.2.3 DNS 435
6.1.2.4 IEEE 802.1X 438
6.1.2.5 Bezdrátové sítě 439
6.1.2.6 IPv6 451
6.1.3 Ochrana na rozhraní sítí 455
6.1.3.1 Access Control List (ACL) 455
6.1.3.2 Firewall 455
6.1.3.3 Proxy server 458
6.1.3.4 Intrusion Detection System (IDS) a Intrusion Prevention System (IPS) 460
6.1.3.5 Security Information and Event Management (SIEM) 461
6.1.3.6 Antivir, Antispam 462
6.2 Aplikační bezpečnost 462
6.2.1 Řízení přístupů 462
6.2.2 Ověřování uživatelů 463
6.2.3 Hesla 464
6.2.4 Logy a logování 475
6.2.5 Zabezpečení důvěrnosti a integrity přenášených dat 476
6.2.6 Zranitelnosti 478
6.3 Ochrana koncových počítačových systémů 480
6.4 Vzdálený přístup k počítačovým systémům 481
6.5 Paměťová média 484
6.6 Správa a dohled nad počítačovou sítí 485

6.7 Přenosné počítačové systémy 487
6.8 Bezpečnost lidských zdrojů 489
6.9 Reakce na incident 490
6.9.1 Hlášení bezpečnostních incidentů 492
6.9.2 Interní hlášení bezpečnostních incidentů 492
6.9.3 Řešení bezpečnostních incidentů 493
6.10 Možnosti využití dalších informačních zdrojů o incidentech 495
6.10.1 Malicious Domain Manager 496
6.10.2 Cyber Threat Intelligence Project - PROKI 497

**7 CERT/CSIRT týmy 505**
7.1 Historie 505
7.2 CERT a CSIRT týmy 506
7.3 Jak vzniká CERT/CSIRT tým 508
7.4 Spolupráce CERT/CSIRT infrastruktury 510
7.5 Hierarchie CERT/CSIRT týmů? 512
7.6 Národní a vládní CERT/CSIRT týmy 513
7.7 Situace v ČR a ve světě 514
7.8 Národní CSIRT České republiky 515
7.9 Vládní CERT České republiky 516
7.10 Na který CERT/CSIRT tým se obrátit? 516

**Závěr 519**

**Seznam použitých pramenů a dalších zdrojů 523**

**Rejstřík 541**

**Summary 560**

# Seznam zkratek

## Seznam zkratek

| Zkratka | Význam |
|---|---|
| **AES** | Advanced Encryption Standard |
| **API** | Application Programming Interface |
| **APT** | Advanced Persistent Threat |
| **BYOD** | Bring Your Own Device |
| **C&C** | Command-and-Control |
| **CCMP** | Counter Mode Cipher Block Chaining Message Authentication Code Protocol |
| **CCTV** | Closed Circuit Television |
| **CERT** | Computer Emergency Response Team |
| **CSIRT** | Computer Security Incident Response Team |
| **Data retention** | plošné ukládání provozních a lokalizačních údajů u poskytovatelů připojení |
| **DHCP** | Dynamic Host Configuration Protocol |
| **DMZ** | Demilitarized zone |
| **DNS** | Domain Name System (hierarchický systém doménových jmen) |
| **Dodatkový protokol** | Dodatkový protokol Rady Evropy č. 189 k Úmluvě o kybernetické kriminalitě |
| **DoS, DDoS** | Denial of Service, Distributed Denial of Service |
| **DPIA** | Data Protection Impact Assessment (posouzení vlivu na ochranu osobních údajů) |
| **eIdas** | Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES |
| **ENISA** | The European Union Agency for Network and Information Security (Evropská agentura pro bezpečnost sítí a informací) |
| **EULA** | End User Licence Agreement (smlouva uzavřená typicky mezi uživatelem a ISP) |
| **EZS** | elektronický zabezpečovací systém či elektronická zabezpečovací signalizace |

| | |
|---|---|
| **GDPR** | Nařízení Evropského parlamentu a Rady (EU) 2016/697 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) |
| **HIDS** | Host-based Intrusion Detection System |
| **HMAC** | Hashed Message Authentication Mode |
| **HTML** | Hyper Text Markup Language |
| **HTTP** | Hypertext Transfer Protocol (internetový protokol určený pro výměnu hypertextových dokumentů ve formátu HTML) |
| **IaaS** | Infrastructure as a Service |
| **IAP** | Internet Access Provider |
| **ICANN** | Internet Corporation for Assigned Names and Numbers |
| **ICT** | informační a komunikační technologie |
| **IDS** | Intrusion Detection System |
| **IoE** | Internet of Everything (Internet všeho) |
| **IoT** | Internet of Things (Internet věcí) |
| **IP** | Internet Protocol |
| **IPS** | Intrusion Prevention System |
| **Ipv4, IPv6** | Internet Protocol verze 4, 6 |
| **IS** | informační systém / systémy |
| **ISMS** | Information Security Management System |
| **ISP** | Internet Service Provider (specificky k českému právu je využíván pojem poskytovatel služeb informační společnosti) |
| **IT** | informační technologie |
| **KZ, krizový zákon** | Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů |
| **LAN** | Local Area Network |
| **LDAP** | Lightweight Directory Access Protocol (protokol definovaný pro ukládání a přístup k datům na adresářovém serveru) |
| **LIR** | Local Internet Registry |
| **Listina** | Zákon č. 2/1993 Sb., ve znění ústavního zákona č. 162/1998 Sb., Listina základních práv a svobod |
| **NBÚ** | Národní bezpečnostní úřad |
| **NIDS** | Network Intrusion Detection System |

| | |
|---|---|
| **NIS** | Směrnice Evropského parlamentu a Rady (EU) 2016/1148 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii |
| **NIST** | National Institute of Standards and Technology |
| **NTP** | Network Time Protocol |
| **NÚKIB** | Národní úřad pro kybernetickou a informační bezpečnost |
| **OS** | operační systém |
| **OZ, občanský zákoník** | Zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů |
| **PaaS** | Platform as a Service |
| **PC** | Personal Computer (osobní počítač) |
| **PCO** | pult centralizované ochrany |
| **PROKI** | PRedikce a Ochrana Před Kybernetickými Incidenty |
| **PTK** | Pairwise Transient Key |
| **RDP** | Remote Desktop Protokol |
| **RIR** | Regional Internet Registry |
| **SaaS** | Software as a Service |
| **SAE** | Simultaneous Authentication of Equal |
| **SIEM** | Security Incident and Event Management (nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí) |
| **SLA** | Service-Level Agreement |
| **SMTP** | Simple Mail Transfer Protocol (internetový protokol určený pro přenos zpráv elektronické pošty) |
| **SMTP** | Simple Mail Transfer Protocol |
| **SOHO** | Small Office/Home Office |
| **SQL** | Structured Query Language |
| **SŘ, správní řád** | Zákon č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů |
| **SSH** | Secure Shell |
| **SSID** | Service Set Identifier |
| **TCP** | Transmission Control Protocol |
| **TI** | Trusted Introducer |
| **TKIP** | Temporal Key Integrity Protocol |
| **TLP** | Traffic Light Protocol |
| **TLS** | Transport Layer Security |

| | |
|---|---|
| **TOPO, zákon o trestní odpovědnosti právnických osob** | Zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob, ve znění pozdějších předpisů |
| **TŘ, trestní řád** | Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů |
| **TZK, trestní zákoník** | Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů |
| **UDP** | User Datagram Protocol |
| **UEFI** | Unified Extensible Firmware Interface |
| **Úmluva o kyberkriminalitě** | Úmluva Rady Evropy č. 185 o kybernetické kriminalitě ze dne 23. listopadu 2001 |
| **UPS** | Uninterruptible Power Supply (záložní zdroj elektrického napájení) |
| **URL** | Uniform Resource Locator (jednotná adresa zdroje) |
| **Úřad** | V kap. 4 a násl. je v textu zákona používán pojem Úřad pro označení NBÚ či NÚKIB (v závislosti na době) |
| **Ústava** | Ústava České republiky ze dne 16. 12. 1992 jako součást ústavního pořádku České republiky pod č. 1/1993 Sb., ve znění ústavních zákonů č. 347/1997 Sb., č. 300/2000 Sb., č. 395/2001 Sb., č. 448/2001 Sb. a č. 515/2002 Sb. |
| **VLAN** | Virtual LAN |
| **VoIP** | Voice over Internet Protocol |
| **VPN** | Virtual Private Network |
| **WAN** | Wide Area Network |
| **WEP** | Wired Equivalent Privacy |
| **WPA, WPA2** | Wi-Fi Protected Access |
| **WPA-PSK** | Wi-Fi Protected Access - Pre-Shared Key |
| **WPS** | Wi-Fi Protected Setup |
| **XML** | eXtensible Markup Language |
| **XSS** | Cross-Site Scripting |
| **ZoBČR** | Ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky |
| **ZoEK, zákon o elektronických komunikacích** | Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně dalších zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů |

| | |
|---|---|
| **ZoKB, zákon o kybernetické bezpečnosti** | Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů |
| **ZoOU, zákon o ochraně osobních údajů** | Zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů |
| **ZoOUI, zákon o ochraně utajovaných informací** | Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů |
| **ZoP, zákony o přestupcích** | Zákon č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich<br>Zákon č. 251/2016 Sb., o některých přestupcích |
| **ZoS** | Zákon č. 634/1992 Sb., o ochraně spotřebitele, ve znění pozdějších předpisů |
| **ZoZT, zákon o znalcích a tlumočnících** | Zákon č. 36/1967 Sb., o znalcích a tlumočnících, ve znění pozdějších předpisů |
| **ZSIS, zákon o některých službách informační společnosti** | Zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů, ve znění pozdějších předpisů |

# 1 Základní terminologie

# I Základní terminologie

## 1 Kyberprostor (Cyberspace)

Chceme-li se věnovat problematice kybernetické bezpečnosti, kybernetických útoků, incidentů, ochrany digitálních dat aj., je nezbytně nutné nejprve vymezit ono pomyslné hrací pole, ve kterém se tyto „útočné a obranné" akce odehrávají.

Vlastní pojem kyberprostor (cyberspace) poprvé použil v roce 1982 v povídce „*Jak vypálit Chrom*"[18] William Gibson. Ten následně v románu Neuromancer uvedl, že kyberprostor je:

„*Konsensuální halucinace každý den zakoušená miliardami oprávněných operátorů všech národů, dětmi, které se učí základy matematiky… Grafická reprezentace dat abstrahovaných z bank všech počítačů lidského systému. Nedomyslitelná komplexnost. Linie světla seřazené v neprostoru mysli, shluky a souhvězdí dat. Jako světla města, …*"

William Gibson: Neuromancer (1984)

Do obecného povědomí se ale pojem kyberprostor začíná dostávat až po vydání deklarace Johna Barlowa (zakladatele Electronic Frontier Foundation): **„A Declaration of the Independence of Cyberspace."**[19]

Pokud bychom chtěli nalézt definici kyberprostoru v některém ze slovníků, pak Oxford dictionary k termínu cyberspace uvádí, že jde o „*fiktivní prostředí, ve kterém dochází ke komunikaci skrze počítačové sítě.*"[20] Český Výkladový slovník kybernetické bezpečnosti nedefinuje pojem kyberprostor, ale specificky uvádí pouze pojem „*Český kyberprostor*"[21], kterým se rozumí „*kyberprostor pod jurisdikcí České republiky*".

Jsme přesvědčeni o tom, že ani jeden z výše uvedených slovníků nedefinuje kyberprostor tak, aby bylo možné pochopit komplexnost tohoto prostředí.

---

18: v originále: Burning Chrome (1982)

19: Blíže viz BARLOW, Perry John. *A Declaration of the Independence of Cyberspace.* [online]. [cit. 23. 9. 2014]. Dostupné z: https://www.eff.org/cyberspace-independence.

Český zdroj: http://www.piratskelisty.cz/clanek-1476-deklarace-nezavislosti-kyberprostoru

20: *Cyberspace.* [online]. [cit. 6. 7. 2018]. Dostupné z:
https://en.oxforddictionaries.com/definition/cyberspace Překlad autora.

21: JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. 3. aktualiz. vyd. Praha: AFCEA, 2015, s. 37. [online]. [cit. 10. 7. 2018]. Dostupné z:
https://www.govcert.cz/download/slovnik/vykladovy_slovnik_KB_3_vydani.pdf

**Kyberprostor** je tvořen prvky informačních a komunikačních technologií, které vytvářejí pomocí protokolu TCP/IP celosvětovou, globální počítačovou síť, a jednotlivými počítačovými systémy[22], které jsou do této sítě připojeny a které v ní interagují. Vlastní interakce uvedených systémů samozřejmě není možná bez zásahu jednotlivých uživatelů (administrátorů či koncových uživatelů).

Tím je vytvořen dynamický, neustále se měnící a vyvíjející systém vázaný na hardware, avšak zároveň vytvářející těžko definovatelný a prakticky neomezený kyberprostor.

**Kyberprostor je virtuální realitou, nemající konec ani začátek. Tato virtuální realita je však zcela závislá na materiální podstatě, tedy technologiích nacházejících se ve světě reálném.** Vzniká tak zajímavý paradox, který sice umožňuje existenci nehmotného média (kyberprostoru), schopného, díky distribuovanosti hmotného média (prvků sítě, jednotlivých počítačových systémů, cloudových úložišť, propojených služeb, atd.), se adaptovat a měnit v případě poškození materiálního média, avšak v případě úplného kolapsu materiálního média (respektive všech jeho součástí) dojde k nevratnému poškození či zániku kyberprostoru jako takového.

Kyberprostor je také možné definovat jako prostor kybernetických aktivit, či jako prostor vytvořený informačními a komunikačními technologiemi. Tento prostor, oproti světu reálnému, je značně specifický a rozhodně je mylné se domnívat, že v něm budou fungovat stejná pravidla, jako ve světě reálném. Obecně je sice možné konstatovat, že na kyberprostor lze aplikovat standardní kritéria[23], která jsou uplatňována v návaznosti na skutečnou fyzickou lokalizaci dat či informací. Druhou možností je vytvoření nových kritérií, pro aplikaci principu místní působnosti (jedná se o virtuální lokalizaci právních vztahů).[24]

Kyberprostor je dnes mnohými státy považován za pátou doménu či sféru (a to ne jen pro účely války) po zemi, vodě, vzduchu a vesmíru. Tomuto prostoru je nejen ze strany státních organizací věnována stále větší a vetší pozornost.

Mezi **znaky kyberprostoru** je možné zařadit jeho **decentralizovanost**, **globálnost**, **otevřenost**, **bohatost na informace**, **interaktivnost** a možnost ovlivňování mínění skrze uživatele. Podstatným rysem kyberprostoru je, že primární roli v něm zaujímají technologie a na ně navázané služby. V poslední době se čím dál víc ukazuje, že projev světa virtuálního může mít a má dopady ve světě reálném.

Pokud jde o legální definici kyberprostoru, je možné využít například znění § 2 písm. a) zákona o kybernetické bezpečnosti, kde je uvedeno, že „***kybernetickým prostorem je digitální prostředí***

22: Blíže viz § 2 odst. 2 ZoKB, případně: KOLOUCH, Jan. *CyberCrime.* Praha: CZ.NIC, 2016, s. 57 a násl.

23: Viz např. kap. 3.3.4 Trestní zákoník

24: Blíže viz REED, Chris. *Internet Law*. Cambridge: Cambridge University Press, 2004, str. 218

***umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací.***"

Dle našeho názoru jednu z velmi zdařilých definic kyberprostoru přináší dokument Cyberspace Operations: Concept Capability Plan 2016–2028, který definuje **kyberprostor jako prostor složený ze tří vrstev:**[25]

1) **fyzické**,
2) **logické** a
3) **sociální**.

Tyto vrstvy se pak skládají z celkem pěti komponent.

**Ad 1) Fyzická vrstva**
Tato vrstva zahrnuje pojem „**geographic component**" a pojem **fyzické síťové komponenty**. Pojem „geographic component" nemá v našem jazyce přesný ekvivalent, nicméně je jím myšleno přesné umístění síťových prvků ve fyzickém světě. Pojem fyzické síťové komponenty pak zahrnuje infrastrukturu v podobě kabelů, řídících prvků sítě (switch, router) a dalšího zařízení.

Toto rozdělení fyzické vrstvy má svou logiku. Zatímco geopolitické hranice mezi státy mohou být v kyberprostoru snadno překročeny, v reálném světě zde stále existují omezení, která vyplývají z podstaty našeho fyzického světa.

Pokud tuto myšlenku převedeme do světa kyberútoků a incidentů, znamená to, že mohu jako útočník poškodit prvek fyzické vrstvy buď vzdáleně, například tím, že znám jeho konkrétní zranitelnost, kterou lze vzdáleně napadnout, nebo jej mohu poškodit přímo v reálném světě, pokud se mi k němu podaří fyzicky dostat a zaútočit na něj například s použitím fyzické síly. Dopad v kyberprostoru bude stejný, ale provedení samotného útoku je značně odlišné.

**Ad 2) Logická vrstva**
Tato vrstva obsahuje **logické síťové komponenty**, čímž jsou myšlena logická propojení mezi síťovými uzly. Ta jsou realizována prostřednictvím síťových komunikačních protokolů. Uzly mohou být počítače, telefony a další síťová zařízení.

**Ad 3) Sociální vrstva**
Tato vrstva se skládá z komponent nazvaných „**kyberosobnost**" a **osobnost**.

25: *Cyberspace Operations: Concept Capability Plan 2016–2028*. [online]. [cit. 18. 2. 2018], s. 8–9 Dostupné z: www.fas.org/irp/doddir/army/pam525-7-8.pdf?

Komponenta „kyberosobnost“ zahrnuje identifikaci osoby na síti, jako je e-mailová adresa, IP adresa, číslo telefonu a další. Komponenta osobnost se skládá ze skutečných osob připojených k síti. Jedna individualita pak může mít více „kyberosobností“, například různé e-maily na různých zařízeních, a jedna „kyberosobnost“ může být ve skutečnosti více různých skutečných osob, využívajících například jeden společný sdílený účet.

**Kyberprostor je také možné definovat podle dostupnosti a dohledatelnosti dat pro běžného uživatele.** Podle tohoto dělení lze kyberprostor rozdělit na služby a data dostupná pomocí Internetu, na služby a data dostupná pouze v rámci konkrétních sítí a zařízení a na služby a data záměrně skrytá a dostupná s využitím speciálních nástrojů.

Obvykle se pro tyto kategorie používají názvy:

1) **Surface Web**,
2) **Deep Web** a
3) **Dark Web**.

Deep a Dark Weby jsou také souhrnně označovány jako **D4rkN3ts – Darknets**. Všechny tyto součásti pak společně vytváří skutečný kyberprostor.[26]

Na terminologii, která používá k rozdělení kyberprostoru pojem *web,* se bohužel podepsal fakt, že pro většinu laické veřejnosti platí jednoduchá rovnice:

KYBERPROSTOR = INTERNET = **WEB**

Nicméně kyberprostor se netýká pouze webových stránek, ale všech počítačových systémů, služeb, uživatelů a dat, jež se v tomto prostoru pohybují.

26: Srov. Např. *The dark Web explained.* [online]. [cit. 20. 7. 2016]. Dostupné z:
https://www.yahoo.com/katiecouric/now-i-get-it-the-dark-web-explained-214431034.html
či *Surface Web, Deep Web, Dark Web – What's the Difference.* [online]. [cit. 20. 7. 2016]. Dostupné z:
https://www.cambiaresearch.com/articles/85/surface-web-deep-web-dark-web----whats-the-difference

## 2 Pojem kybernetické bezpečnosti a pojmy související

*„Objev jaderné energie nepřinesl nové problémy. Pouze učinil naléhavějším nutnost vyřešit existující problémy."*

Albert Einstein

V této kapitole se pokusíme vymezit některé základní pojmy, které jsou důležité pro pochopení problematiky kybernetické bezpečnosti. Záměrně jsme si pro úvod do této kapitoly vybrali citát Alberta Einsteina, neboť právě tento citát vystihuje základní problém kybernetické bezpečnosti, kterým je samotné pochopení tohoto relativně nového fenoménu a aplikování „starých bezpečnostních pravidel" na tento „nový" jev, jakož i vytvoření podmínek a prostředků pro řešení problémů, které je možné označit jako kybernetické útoky.

Vzhledem k zaměření a rozsahu knihy není možné vysvětlit veškeré pojmosloví související s kybernetickou bezpečností a ICT, k tomuto účelu slouží specializované slovníky.[27] Na tomto místě budou vysvětleny základní pojmy, které budou v dalších částech této monografie využívány. Další pojmy pak jsou samostatně vymezeny v kapitole 4.3, která se věnuje výkladu zákona o kybernetické bezpečnosti.

### 2.1 Kybernetická bezpečnost

*„Kybernetická bezpečnost v posledním desetiletí získala na významu a stala se tak jednou z hlavních priorit v mnoha národních politikách. Je tomu zejména díky přesahu do jiných bezpečnostních sfér a taktéž díky incidentům, které tento pojem nechvalně proslavily a přiměly i širokou veřejnost přemýšlet o potřebě zabezpečení v kyberprostoru. S tím souvisí potřeba chránit kyberprostor tak, aby v nejvyšší možné míře byla zachována komplexní bezpečnost České republiky a zároveň práva jedinců na informační sebeurčení."* [28]

Vymezení pojmu kybernetická bezpečnost může být do určité míry problematické. Pro řadu lidí představuje kybernetická bezpečnost oblast, kterou se zabývají de facto výhradně oddělení informačních a komunikačních technologií.

---

27: Jedná se například o:
HAVELKA, Jiří a kol. *Výkladový slovník výpočetní techniky a komunikací.* 1. Vyd. Praha: Computer Press, 1997. 456 s. či JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. 3. aktualiz. vyd. Praha: AFCEA, 2015. ISBN 978-80-7251-436-6. Dostupné z:
https://nukib.cz/download/aktuality/container-nodeid-665/slovnikkb-cz-en-1505.pdf

28: *Zpráva o stavu kybernetické bezpečnosti za rok 2017.* [online]. [cit. 29. 6. 2018]. Dostupné z:
https://nukib.cz/download/Zpravy-KB-vCR/Zprava-stavu-KB-2017-fin.pdf

Tato premisa je od počátku chybná, neboť kybernetická bezpečnost se týká každého z nás, kdo využívá jakékoliv prvky ICT ve svém každodenním životě. Pokud si sami neuvědomíme, že jsme klíčovým, a v mnoha případech stěžejním prvkem kybernetické bezpečnosti (ať už ve svém soukromí či v práci), tak vlastně zvyšujeme pravděpodobnost úspěchu kybernetických útoků.[29]

Kybernetickou bezpečnost nelze v současné době ani podceňovat ani bagatelizovat. Je to oblast, která je pro řadu organizací, ale i jedinců samotných klíčová, a proto by měla být řešena dlouhodobě a systematicky.

*„Management organizací by měl pochopit a akceptovat, že řízení kybernetické bezpečnosti spadá mnohem více k dalším oblastem bezpečnosti a krizového managementu. Vždyť i dnešní sofistikované útoky jsou často multidisciplinární a kombinují v sobě oblasti ICT, sociálního inženýrství, personální a objektové bezpečnosti."* [30]

Vrátíme-li se k vlastnímu pojmu kybernetická bezpečnost, je vhodné vyjít z rozboru tohoto sousloví. Slovo **kyber** reprezentuje provázanost s prvky informačních a komunikačních technologií a kyberprostorem[31] jako takovým.

## Bezpečnost

Definic pojmu **bezpečnost (security)**[32] existuje celá řada, avšak neexistuje žádná jednotná, obecně akceptovaná definice. Většina definic pojmu bezpečnost je uváděna spíše v odborné literatuře, než v legislativě samotné.[33]

Mareš definuje bezpečnost jako *„stav, kdy jsou na nejnižší možnou míru limitovány hrozby pro objekt (zpravidla národní stát, popř. i mezinárodní organizace) a jeho zájmy a tento objekt je k eliminaci stávajících i potenciálních hrozeb efektivně vybaven a ochoten při ní spolupracovat."* [34]

29: Viz kap. 2.4 Kybernetické hrozby, události, incidenty a útoky

30: *Kybernetická bezpečnost: Co s tím?* [online]. [cit. 29. 6. 2018]. Dostupné z: http://www.businessinfo.cz/cs/clanky/kyberneticka-bezpecnost-co-s-tim-84467.html

31: Viz kap. 1 Kyberprostor (Cyberspace)

32: Z pohledu výkladu vlastního pojmu je nutné zmínit relativní nepřesnost češtiny oproti angličtině, která pro pojem bezpečnost využívá typicky dva pojmy: **security** a **safety**. Pojem **security** je využíván ve smyslu aktivní ochrany i aktivního zabezpečení, zajištění či ochrany a pojem **safety** je využíván zpravidla k vyjádření pasivní bezpečnosti, bezpečí, charakteristice stavu či vlastnosti určitého objektu.

33: Viz např. Ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky; zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon); zákon o kybernetické bezpečnosti aj.

34: ZEMAN, Petr a kol. *Česká bezpečnostní terminologie: Výklad základních pojmů.* [online]. [cit. 10. 7. 2018]. Dostupné z: http://www.defenceandstrategy.eu/filemanager/files/file.php?file=16048. s. 13

Požár definuje *„bezpečnost jako vlastnost nějakého objektu nebo subjektu, která určuje stupeň, míru jeho ochrany proti možným škodám a hrozbám.“* [35]

Tato definice pak byla dále upřesněna ve Výkladovém slovníku kybernetické bezpečnosti:

***Bezpečnost (Security)***
*Vlastnost prvku (např. informační systém), který je na určité úrovni chráněn proti ztrátám, nebo také stav ochrany (na určité úrovni) proti ztrátám. Bezpečnost IT zahrnuje ochranu důvěrnosti, integrity a dosažitelnosti při zpracování, úschově, distribuci a prezentaci informací.*[36]

Je třeba si uvědomit, že bezpečnost není v současné době jen otázkou státu, který však v oblasti zajištění bezpečnosti stále hraje primární roli, ale že jde o proces realizovaný i jinými subjekty (právnické a fyzické osoby), které byly v poslední době nuceny se stále více zabývat právě otázkou bezpečnosti, respektive zabezpečení svých aktivit před útoky.

Díky tomuto rozšiřování okruhu bezpečnosti, je nezbytné se zabývat mimo jiné následujícími otázkami:

- **O čí bezpečnost se jedná** (mezinárodní organizace, stát, organizace, jednotlivec aj.)**?**
- **Jaké hodnoty jsou chráněny** (organizace, osoby, data aj.)**?**
- **Před čím jsou (mají být) tyto hodnoty chráněny** (fyzické, kybernetické, kombinované útoky aj.)**?**
- **Jaké prostředky je třeba vynaložit k ochraně těchto hodnot?**[37]

Ideálním cílem bezpečnosti je vytvoření stavu „absolutního bezpečí“. Tento stav je ale utopií, protože jej není možné reálně dosáhnout,[38] neboť vždy bude existovat hrozba či riziko, které nebylo do konceptu tvorby bezpečnosti zahrnuto, nebo bylo záměrně opomenuto.

Smyslem bezpečnosti však není za všech okolností postihnout všechna reálná, méně reálná či zcela nepředpokládatelná a nepravděpodobná rizika, neboť by takovouto implementací vznikl

35: POŽÁR, Josef. *Informační bezpečnost*. Plzeň: Aleš Čeněk, 2005, s. 37.

36: JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. 3. aktualiz. vyd. Praha: AFCEA, 2015, s. 23. [online]. [cit. 10. 7. 2018]. Dostupné z: https://www.govcert.cz/download/slovnik/vykladovy_slovnik_KB_3_vydani.pdf

37: Blíže viz např. MAREŠ, Miroslav. *Bezpečnost.* [online]. [cit. 10. 7. 2018]. Dostupné z: https://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=69511
WAISOVÁ, Šárka. *Bezpečnost: vývoj a proměny konceptu.* Plzeň: Aleš Čeněk, s.r.o., 2005. ISBN 80-86898-21-0
FRANK, Libor. *Bezpečnostní studia.* [online]. [cit. 10. 7. 2018]. Dostupné z: https://moodle.unob.cz/pluginfile.php/35788/mod_page/content/23/Bezpe%C4%8Dnostn%C3%AD%20studia.pdf

38: Viz WAISOVÁ, Šárka. *Bezpečnost: vyvoj a proměny konceptu*. Plzeň: Aleš Čeněk, 2005. 159 s. ISBN 80-86898-2-10

zcela nefunkční moloch, který by ve své podstatě aplikaci a implementaci bezpečnosti popíral, nebo i zcela eliminoval.

**Příklad:** *Také se vám v běžném životě stane, že si například zabouchnete klíče uvnitř bytu. Pokud jste s touto variantou počítali, máte nejspíš náhradní klíče u rodiny, známých, či jinde. Pokud však nemáte náhradní klíče, zavoláte zřejmě zámečníka, nebo vyrazíte dveře.*

### Kybernetická bezpečnost

Stejně jako u pojmu bezpečnost, ani kybernetická bezpečnost nemá jednotnou obecně uznávanou definici. Kybernetická bezpečnost představuje podmnožinu bezpečnosti jako takové.

Při vlastním definování kybernetické bezpečnosti je vhodné vycházet z již ustálených definic. Uvedu několik takto ustálených definic:

1) **Kybernetická bezpečnost** představuje **soubor opatření, která jsou přijata, aby byl ochráněn počítačový systém před neoprávněným přístupem či útokem**.[39]

2) Oxford dictionary uvádí, že **kybernetická bezpečnost** představuje **stav, kdy dochází k ochraně před kriminálním či neautorizovaným užitím elektronických dat**. Do kybernetické bezpečnosti je pak třeba zahrnout i opatření, která je třeba přijmout k dosažení tohoto stavu.[40]

3) Dle Jiráska a kol. představuje **kybernetická bezpečnost (Cyber Security)** „***souhrn** právních, organizačních, technických a vzdělávacích **prostředků směřujících k zajištění ochrany kybernetického prostoru.***“ [41]

4) Relativně obdobně je kybernetická bezpečnost definována i v Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020. V této strategii je uvedeno, že: *„Kybernetická bezpečnost představuje **souhrn** organizačních, politických, právních, technických a vzdělávacích **opatření a nástrojů směřujících k zajištění zabezpečeného, chráněného***

39: *Cybersecurity.* [online]. [cit. 6. 7. 2018]. Dostupné z: https://www.merriam-webster.com/dictionary/cybersecurity Překlad autora.

40: *Cybersecurity.* [online]. [cit. 6. 7. 2018]. Dostupné z: https://en.oxforddictionaries.com/definition/cybersecurity Překlad autora.

41: JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. 3. aktualiz. vyd. Praha: AFCEA, 2015, s. 69. [online]. [cit. 10. 7. 2018]. Dostupné z: https://www.govcert.cz/download/slovnik/vykladovy_slovnik_KB_3_vydani.pdf

***a odolného kyberprostoru v České republice**, a to jak pro subjekty veřejného a soukromého sektoru, tak pro širokou českou veřejnost.*“ [42]

Tyto definice se sice snaží vymezit pojem kybernetické bezpečnosti, ale dopouští se určitých nepřesností.

První definice se zaměřuje jen na počítač a počítačový systém a jejich ochranu před dvěma typy kybernetických útoků, přičemž spektrum jak cílů útoků, tak především útoků samotných je značně rozmanitější.[43]

Druhá definice pak chrání pouze elektronická data, a ne počítačové systémy jako takové.

Třetí definice se zaměřuje na přijetí prostředků, které mají sloužit k ochraně prvků ICT v rámci kyberprostoru. Tato definice je relativně přesná, avšak její omezení pouze na kyberprostor může být zavádějící, neboť kybernetickou bezpečnost lze aplikovat i na prvky ICT, které nejsou zapojeny do kyberprostoru, či si vytváří svůj vlastní „off-line kyberprostor“.[44]

Poslední z definic se pak explicitně omezuje pouze na kyberprostor v České republice, přičemž zcela pomíjí možnost ochrany zájmů občanů ČR či dalších subjektů, kteří nejsou usídleni v ČR. Domníváme se, že zúžení kybernetické bezpečnosti pouze na kyberprostor ČR je sice z pohledu implementace zákona o kybernetické bezpečnosti pochopitelné, avšak z pohledu implementace kybernetické bezpečnosti nevhodné.

Další definici kybernetické bezpečnosti je možné nalézt například v dokumentu **Definition of Cybersecurity - Gaps and overlaps in standardisation**[45] Evropské agentury ENISA[46]: „*Kyberbezpečnost se vztahuje na bezpečnost kyberprostoru, kde samotný kybernetický prostor odkazuje na soubor vazeb a vztahů mezi objekty, které jsou přístupné prostřednictvím všeobecné telekomunikační sítě, a na samotnou sadu objektů, jejichž rozhraní umožňující jejich dálkové ovládání, vzdálený přístup k datům, anebo jejich zapojení do řídících akcí v rámci kyberprostoru. Kyberbezpečnost bude zahrnovat*

42: *Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020.* [online]. [cit. 1. 7. 2018]. Dostupné z: https://www.govcert.cz/download/gov-cert/container-nodeid-998/nskb-150216-final.pdf s. 5

43: Napadány mohou být i aplikace, účty uživatelů aj. Pokud se jedná o vlastní útoky, pak jednotlivé útoky jsou popsány např v: KOLOUCH, Jan. *CyberCrime.* Praha: CZ.NIC, 2016, s. 181 a násl.

44: Blíže viz např. *Příchod hackerů: příběh Stuxnetu.* [online]. [cit. 1. 7. 2018]. Dostupné z: https://www.root.cz/clanky/prichod-hackeru-pribeh-stuxnetu/ či FRUHLINGER, Josh. *What is Stuxnet, who created it and how does it work?* [online]. [cit. 1. 7. 2018]. Dostupné z: https://www.csoonline.com/article/3218104/malware/what-is-stuxnet-who-created-it-and-how-does-it-work.html

45: *Definition of Cybersecurity - Gaps and overlaps in standardisation*. [online]. [cit. 10. 12. 2017]. Dostupné z: https://www.enisa.europa.eu/publications/definition-of-cybersecurity s. 30

46: The European Union Agency for Network and Information Security

*paradigma ‚CIA' triády*[47] *pro vztahy a objekty v rámci kyberprostoru a zároveň bude toto paradigma rozšiřováno z důvodu zajištění ochrany soukromí subjektů (fyzických a právnických osob) a odolnosti [‚zotavení se' (recovery) z útoku].*"

Vzhledem ke snaze o definování pojmu kybernetické bezpečnosti je vhodné vycházet i z právních norem, které se kybernetické bezpečnosti věnují.

Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii[48] v čl. 4 odst. 2 uvádí, že „*bezpečnost sítí a informačních systémů představuje schopnost těchto sítí a informačních systémů odolávat s určitou spolehlivostí veškerým zásahům, které narušují dostupnost, autenticitu, integritu nebo důvěrnost uchovávaných, předávaných nebo zpracovávaných dat nebo souvisejících služeb, které tyto sítě a informační systémy nabízejí nebo které jsou jejich prostřednictvím přístupné.*"

Zákon o kybernetické bezpečnosti ani prováděcí vyhlášky k tomuto zákonu vlastní pojem kybernetické bezpečnosti nevymezují. To, co je v těchto právních předpisech vymezeno, však umožňuje pochopit základy a principy kybernetické bezpečnosti, jakož je i následně aplikovat.

Zákon samotný určuje povinné subjekty, které mají povinnost zavést bezpečnostní opatření. A následně těmto subjektům také definuje jejich práva a povinnosti.[49]

Výše uvedené definice se různými způsoby snaží vymezit okruh vztahů, zájmů a subjektů, vůči kterým dochází k uplatňování kybernetické bezpečnosti. Současně je v nich vymezován i kyberprostor, jakožto prostředí, ve kterém je kybernetická bezpečnost aplikována.

Díky určité nejednotnosti v názorech na to, co vše je a co není kybernetická bezpečnost, je vhodné představit vlastní definici kybernetické bezpečnosti, která vznikla jak na základě analýzy definic předchozích, tak na základě vlastních zkušeností.

**Kybernetickou bezpečnost je možné vymezit jako:**

- **souhrn právních, organizačních, technických a vzdělávacích prostředků, které směřují k zajištění ochrany počítačových systémů a dalších prvků ICT, aplikací, dat a uživatelů,**

47: Blíže viz kap. 2.2 Principy kybernetické bezpečnosti

48: Dále jen **směrnice NIS** či **NIS**. [online]. [cit. 1. 7. 2018]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32016L1148&from=EN

49: Blíže viz § 3 a násl. ZoKB

- **schopnost počítačových systémů a využívaných služeb reagovat na kybernetické hrozby či útoky a jejich následky, jakož i plánování obnovy funkčnosti počítačových systémů a služeb s nimi spojených.**

**Kybernetická bezpečnost je realizována jak v rámci kyberprostoru, tak mimo něj.** Není vhodné aplikaci výše uvedených prostředků a principů, jakkoliv geolokačně (ať již na území daného státu, Unie či kyberprostoru samotného) omezovat.

## 2.2 Principy kybernetické bezpečnosti

**Při uplatňování kybernetické bezpečnosti dochází k implementaci následujících principů, které jsou také nazývány triády kybernetické bezpečnosti.**[50]

Pro účely této monografie budou vymezeny následující tři triády:

1) **CIA** [**C** – **Confidentiality** (důvěrnost); **I** – **Integrity** (celistvost); **A** – **Availability** (dostupnost)].
2) **Prvky kybernetické bezpečnosti** (**L**idé, **T**echnologie, **P**rocesy).
3) **Životní cyklus kybernetické bezpečnosti** (**P**revence, **D**etekce, **R**eakce).

### 2.2.1 Triáda CIA

Nejznámější a nejpoužívanější triádou kybernetické bezpečnosti je triáda **CIA**, avšak prosté využívání této základní triády principů kybernetické bezpečnosti bez implementace principů dalších je v současné době k udržení adekvátní úrovně kybernetické bezpečnosti nedostačující.

V odborné literatuře se například poukazuje na uplatňování **Parkerian hexad**[51], což je de facto triáda CIA, která je doplněna o další tři prvky: **P/C - Possession/Control** (držení či kontrola), **A – Authenticity** (autentičnost) a **U – Utility** (užitečnost).

Smyslem kybernetické bezpečnosti je zajistit jak bezpečnost ICT jako takových, tak i zejména dat a informací, které jsou těmito prvky přenášeny, zpracovávány a uchovávány.

---

50: Viz např. HSU, D. Frank a D. MARINUCCI (eds.). *Advances in cyber security: technology, operations, and experiences*. New York: Fordham University Press, 2013. 272 s. ISBN 978-0-8232-4456-0. s 41.
KADLECOVÁ, Lucie. *Konceptuální a teoretické aspekty kybernetické bezpečnosti.* [online]. [cit. 21. 7. 2018]. Dostupné z: https://is.muni.cz/el/1423/podzim2015/BSS469/um/Prezentace_FSS_Konceptualni_a_teoreticke_aspekty_KB.pdf

51: Blíže viz např. *Parkerian Hexad*. [online]. [cit. 20. 8. 2016]. Dostupné z: https://vputhuseeri.wordpress.com/2009/08/16/149/

Velmi často je triáda CIA vztahována primárně právě k informacím.

Toto užší pojetí vyplývá zejména z vlastní definice **informační bezpečnosti**, která se zaměřuje na ochranu informací. V rámci této ochrany pak není podstatné, na jakém typu nosiče (papír, elektronická média aj.) či v rámci jakého systému jsou informace zpracovávány. Informační bezpečnost je pak aplikována na informace po celý jejich životní cyklus.

Informační bezpečnost je definována i řadou norem ISO 27000.[52] Mezi základní normy informační bezpečnosti patří:

- ČSN ISO/IEC 27001:2014 Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Požadavky
- ČSN ISO/IEC 27002:2014 Informační technologie - Bezpečnostní techniky - Soubor postupů pro opatření bezpečnosti informací

Otázkou je, zda je v současné době vymezení pojmu informační bezpečnost adekvátní a dostačující, respektive zda se vztahuje na všechny klíčové prvky bezpečnosti v rámci kyberprostoru.

I přes skutečnost, že v odborné literatuře i právních normách je běžněji využíván pojem informační bezpečnost, jsme přesvědčeni, že ve vztahu k aktivitám spojeným s využíváním ICT, respektive k aktivitám souvisejícím s kyberprostorem, je vhodnějším pojmem pojem kybernetická bezpečnost.

Jak již bylo uvedeno výše: „*informační bezpečnost se vztahuje na informace jako takové*". Tímto však dochází k opomenutí klíčových prvků, které se k bezpečnosti v kyberprostoru vztahují.

Za tyto významné prvky považujeme **data a** pak samotné **počítačové systémy** (resp. jednotlivé prvky ICT), které umožnují vlastní přenos dat a informací.

V odborné literatuře i v právních předpisech existuje celá řada definic pojmů data a informace. Pro účely této publikace jsou vybrány definice, které se vztahují k problematice ochrany informací, dat či ke kybernetické bezpečnosti.

Dle Úmluvy o kyberkriminalitě[53] se **počítačovými daty** rozumí „***jakékoli vyjádření faktů, informací nebo pojmů ve formě vhodné pro zpracování v počítačovém systému**, včetně programu způsobilého zapříčinit provedení funkce počítačovým systémem.*"

52: Blíže viz § 5 ZoKB a ISMS - Systém řízení bezpečnosti informací

53: Čl. 1 písm. b) Úmluvy o kyberkriminalitě. *Úmluva o kyberkriminalitě.* [online]. [cit. 20. 8. 2016]. Dostupné z: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804931c0

Data jsou tedy jakékoli prvky s informační hodnotou, které jsou zpracovávány počítačovým systémem, přičemž jsou zpracovávány tak, aby následně utvořila informaci.

**Informace** *„jsou údaje, které byly zpracovány do podoby užitečné pro příjemce. Každá informace je tedy údajem, datem, ale jakákoli uložená data se nemusejí nutně stát informací.“* [54]

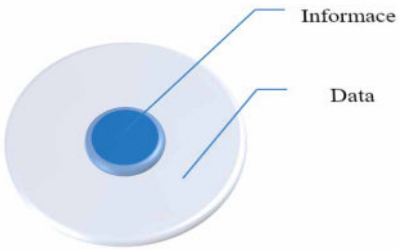
Wiener tvrdí, že *„informace je název pro obsah toho, co se vymění s vnějším světem, když se mu přizpůsobujeme a působíme na něj svým přizpůsobováním.“* Dále také uvádí, že informace není ani hmotou ani energií, ale samostatnou fyzikální kategorií.[55]

Smejkal uvádí, že za informaci je možné považovat *„každé energetické sdělení, které může mít smysl buď pro toho, kdo je činí, nebo pro toho, kdo je přijímá.“* [56]

**Informace jsou tedy vnímány jako něco „kvalifikovanějšího“, nežli data.** Data jsou fakta, která se stávají informacemi tehdy, pokud jsou vnímána či vyjádřena v kontextu a nesou význam, který je pochopitelný pro lidi.[57]

Právě ono propojení „bezvýznamných“ dat a vytvoření určitého kontextu, který z dat teprve složí „významnou“ informaci, může být klíčové z pohledu kybernetické bezpečnosti. Pokud bychom totiž respektovali výše uvedenou tezi informační bezpečnosti, v rámci které jsou chráněny pouze informace jako takové, pak by mohlo dojít k výraznému narušení bezpečnosti.

Vztah dat a informací demonstruje následující graf.[58]




54: POŽÁR, Josef. *Informační bezpečnost.* Plzeň: Aleš Čeněk, 2005, s. 25

55: Blíže viz WIENER, Norbert. *Kybernetika: neboli řízení a sdělování v živých organismech a strojích.* Praha: Státní nakladatelství technické literatury, 1960. 148 s. s. 32 a násl.

56: SMEJKAL, Vladimír. *Kybernetická kriminalita.* Plzeň: Aleš Čeněk, 2015, s. 36

57: ŠÁMAL, Pavel a kol. *Trestní zákoník II. § 140 až 421. Komentář.* 2. Vyd. Praha: C. H. Beck, 2012, s. 2308

58: POŽÁR, Josef. *Informační bezpečnost.* Plzeň: Aleš Čeněk, 2005, s. 25

Data a informace jsou v rámci kyberprostoru přenášeny pomocí počítačových systémů[59], jež jsou nedílnou součástí kybernetické či informační bezpečnosti.

Na základě výše uvedeného jsme přesvědčeni, že je třeba triádu CIA[60] uplatňovat ne jen na informace samotné, ale i na další prvky kybernetické bezpečnosti (data, počítačové systémy atp.)

**Důvěrnost (Confidentiality)**
Pojem důvěrnost definuje tu skutečnost, že k informacím, datům, či ICT mají přístup pouze subjekty, které jsou k tomu autorizované (oprávněné).

Vzhledem k velkému rozsahu zpracovávaných informací je vhodné zavést či aplikovat některou z klasifikací informací. Tyto klasifikace je pak možné aplikovat i na ostatní prvky kybernetické bezpečnosti a přístup k nim.

Bezpečnostní standardy ISO/IEC 27000 definují že:

- „*Informace by měly být klasifikovány, a to s ohledem na jejich hodnotu, právní požadavky, citlivost a kritičnost.*"
- „*Pro značení informací a zacházení s nimi by měly být vytvořeny a do praxe zavedeny postupy, které jsou v souladu s klasifikačním schématem přijatým organizací.*"
- „*Pro zabránění neautorizovanému přístupu nebo zneužití informací by měla být stanovena pravidla pro manipulaci s nimi a pro jejich ukládání.*"

Příklady některých klasifikačních schémat:

1) **Klasifikace informací dle zákona 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti[61]:**

    - **Přísně tajné (Top secret)** - neoprávněné nakládání s informacemi by mohlo způsobit mimořádně vážnou újmu zájmům České republiky.

59: Blíže viz: KOLOUCH, Jan. *CyberCrime.* Praha: CZ.NIC, 2016, s. 57 a násl.

60: Blíže viz např. EVANS, Donald, Philip, BOND a Arden BEMET. *Standards for Security Categorization of Federal Information and Information Systems.* National Institute of Standards and Technology, Computer Security Resource Center. [online]. [cit. 10. 12. 2017]. Dostupné z:
https://csrc.nist.gov/csrc/media/publications/fips/199/final/documents/fips-pub-199-final.pdf
ANDRESS, Jason. *The Basics of Information Security*. 2nd Edition. Syngress. ISBN: 9780128007440
HENDERSON, Anthony. *The CIA Triad: Confidentiality, Integrity, availability.* [online]. [cit. 13. 1. 2018].
Dostupné z: http://panmore.com/the-cia-triad-confidentiality-integrity-availability

61: Blíže viz https://www.nbu.cz/cs/pravni-predpisy/zakon-c-412-2005/1122-uplne-zneni-zakona-c-412-2005/

- **Tajné (Secret)** - neoprávněné nakládání s informacemi by mohlo způsobit vážnou újmu zájmům České republiky.
- **Důvěrné (Confidential)** - neoprávněné nakládání s informacemi by mohlo způsobit prostou újmu zájmům České republiky.
- **Vyhrazené (Restricted)** - neoprávněné nakládání s informacemi by mohlo být nevýhodné pro zájmy České republiky.

2) **Klasifikace informací využívaná v komerční sféře**:

- **Chráněné** - neoprávněné nakládání s informacemi by mohlo způsobit závažné poškození či zničení organizace (např. únik strategických informací, zdrojových kódů, schémat zabezpečení, hesel aj.).
- **Interní** - neoprávněné nakládání s informacemi by mohlo způsobit poškození organizace (např. únik osobních údajů, smluv aj.).
- **Citlivé** - neoprávněné nakládání s informacemi by mohlo mít negativní dopad na společnost (např. dosud nezveřejněné informace o projektech, plánovaných akcích aj.).
- **Veřejné** - neoprávněné nakládání s informacemi by nemělo nikoho poškodit a nemělo by mít jakýkoliv dopad na společnost (např. veřejně dostupné kontakty, prezentace projektů aj.).[62]

Vedle dvou výše uvedených klasifikací existuje celá řada dalších klasifikací, které jsou v rámci organizací či jednotlivci samotnými přijímány či akceptovány ať již na základě právního předpisu, či uvážení uživatele samotného.

Klasifikace samotné, za předpokladu, že jsou respektovány a dodržovány, mohou výrazně zmírnit dopad případného kybernetického útoku.

3) **Traffic Light Protocol**

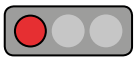
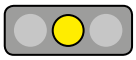
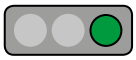
V rámci komunity kybernetické bezpečnosti vznikla v minulosti potřeba sdílet informace a data (typicky o kybernetických útocích), která mají citlivou povahu. Z tohoto důvodu byl v National Infrastructure Security Coordination Centre[63] vytvořen na počátku roku 2000 **protokol TLP** (***Traffic Light Protocol***).[64] Tento protokol si klade za cíl zrychlit výměnu informací mezi zainteresovanými subjekty a zároveň stanovuje pravidla pro nakládání s předávanými informacemi. Subjekt, který předává informace (zdroj informace), vždy označí informaci určitou barvou, která stanovuje, jak má daný příjemce s informací nakládat.

62: Srov. dále: ŠULC, Vladimír. *Kybernetická bezpečnost.* Plzeň: Aleš Čeněk, 2018. s. 20 a násl.

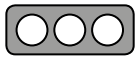
63: V současnosti Centre for Protection of National Infrastructure - CPNI

64: Blíže viz např. *Traffic Light Protocol (TLP) Definitions and Usage.* [online]. [cit. 13. 1. 2018]. Dostupné z: https://www.us-cert.gov/tlp

Protokol TLP je nejvhodněji vymezen v následující tabulce, která byla převzata z US-CERT[65]:

| Barva | Kdy má být použita | Jak lze sdílet? |
|---|---|---|
| **TLP:RED**  **Neurčeno k zveřejnění**, pouze pro účastníky. | Subjekty mohou používat TLP: RED v případech, kdy informace neumožňuje účinnou reakci dalších subjektů a mohly by vést k dopadům na soukromí, pověst nebo operace těchto subjektů, pokud by byly zneužity. | Příjemci nesmějí sdílet informace zařazené v kategorii TLP: RED s žádnými subjekty mimo konkrétní výměnu, schůzku nebo konverzaci, v rámci které byly informace TLP:RED původně zveřejněny. V rámci schůzky (setkání) se například informace TLP: RED omezuje na ty osoby, které se schůzky (setkání) přímo účastní. Ve většině případů **by informace označené TLP: RED měly být vyměňovány pouze verbálně nebo osobně**. |
| **TLP:AMBER**  **Omezené zveřejnění.** Zveřejnění je možné jen v organizaci účastníků. | Subjekty mohou používat TLP: AMBER, v případech, kdy informace vyžadují účinnou reakci dalších subjektů a přináší riziko pro soukromí, pověst nebo operace, v případě, že jsou sdíleny mimo zúčastněné organizace. | Příjemci mohou sdílet informace zařazené v kategorii TLP: AMBER s členy své vlastní organizace a s klienty nebo zákazníky, kteří potřebují tyto informace znát, aby se mohli chránit nebo zabránili dalšímu případnému poškození. **Subjekty mohou volně stanovovat další pravidla sdílení, at tato musí být dodržována.** |
| **TLP:GREEN**  **Omezené zveřejnění**, omezené na komunitu. | Subjekty mohou používat TLP: GREEN, pokud jsou informace užitečné pro zvýšení informovanosti všech zúčastněných organizací. Také je možné tyto informace sdílet s dalšímy subjekty v rámci širší komunity nebo sektoru. | Příjemci mohou sdílet informace zařazené v kategorii TLP: GREEN s partnery a partnerskými organizacemi v rámci svého sektoru nebo komunity. Informace však není možné sdílet prostřednictvím veřejně přístupných kanálů. Informace v této kategorii mohou být v rámci dané komunity komunity masivně rozšiřovány. **Informace zařazené v kategorii TLP: GREEN nesmí být uvolněna mimo komunitu.** |

65: *Traffic Light Protocol (TLP) Definitions and Usage.* [online]. [cit. 13. 1. 2018]. Dostupné z: https://www.us-cert.gov/tlp

| | | |
|---|---|---|
| **TLP:WHITE**<br>  <br>**Zveřejnění není nijak omezeno.** | Subjekty mohou používat TLP: WHITE, pokud informace obsahují minimální nebo žádné předvídatelné riziko zneužití v souladu s platnými pravidly a postupy pro zveřejnění. | V souladu s pravidly a ochranou práv autorských mohou být **informace zařazené v kategorii TLP: WHITE distribuovány bez omezení**. |

*„O nežádoucím zpřístupnění (disclosure) určitých informací se v kybernetické bezpečnosti hovoří jako o narušení jejich důvěrnosti, či úniku (leakage).“* [66]

4) **Hodnocení důvěrnosti dle vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat** (vyhláška o kybernetické bezpečnosti)[67]

Vyhláška o kybernetické bezpečnosti do značné míry přebírá výše představený Traffic Light Protocol pro stupnici hodnocení důvěrnosti (viz příloha č. 1 VoKB).

| **Úroveň** | **Popis** | **Příklady požadavků na ochranu aktiva** |
|---|---|---|
| **Nízká** | Aktiva jsou veřejně přístupná nebo byla určena ke zveřejnění. Narušení důvěrnosti aktiv neohrožuje oprávněné zájmy povinné osoby.<br>V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle tzv. traffic light protokolu (dále jen „TLP“) je využíváno označení **TLP:WHITE**. | Není vyžadována žádná ochrana. Likvidace/mazání aktiva na úrovni Nízká - viz příloha č. 4. |

66: ŠULC, Vladimír. *Kybernetická bezpečnost.* Plzeň: Aleš Čeněk, 2018. s. 19

67: Dále jen vyhláška o kybernetické bezpečnosti či **VoKB**.

| | | |
|---|---|---|
| **Střední** | Aktiva nejsou veřejně přístupná a tvoří know-how povinné osoby, ochrana aktiv není vyžadována žádným právním předpisem nebo smluvním ujednáním.<br>V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle TLP je využíváno zejména označení **TLP:GREEN** nebo **TLP:AMBER**. | Pro ochranu důvěrnosti jsou využívány prostředky pro řízení přístupu.<br>Likvidace/mazání aktiva na úrovni Střední - viz příloha č. 4. |
| **Vysoká** | Aktiva nejsou veřejně přístupná a jejich ochrana je vyžadována právními předpisy, jinými předpisy nebo smluvními ujednáními (například obchodní tajemství, osobní údaje).<br>V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle TLP je využíváno zejména označení **TLP:AMBER**. | Pro ochranu důvěrnosti jsou využívány prostředky, které zajistí řízení a zaznamenávání přístupu. Přenosy informací komunikační sítí jsou chráněny pomocí kryptografických prostředků.<br>Likvidace/mazání aktiva na úrovni Vysoká - viz příloha č. 4. |
| **Kritická** | Aktiva nejsou veřejně přístupná a vyžadují nadstandardní míru ochrany nad rámec předchozí kategorie (například strategické obchodní tajemství, zvláštní kategorie osobních údajů). V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle TLP je využíváno zejména označení **TLP:RED** nebo **TLP:AMBER**. | Pro ochranu důvěrnosti jsou využívány prostředky, které zajistí řízení a zaznamenávání přístupu. Dále metody ochrany zabraňující zneužití aktiv ze strany administrátorů. Přenosy informací jsou chráněny pomocí kryptografických prostředků.<br>Likvidace/mazání aktiva na úrovni Kritická - viz příloha č. 4. |

### Integrita (Integrity)

Dle Výkladového slovníku kybernetické bezpečnosti[68] je **integrita** definována jako *„vlastnost přesnosti a úplnosti.“* **Integrita dat** je pak ve stejném slovníku definována jako *„jistota, že data nebyla změněna. Přeneseně označuje i platnost, konzistenci a přesnost dat, např. databází nebo systémů souborů. Bývá zajišťována kontrolními součty, hašovacími funkcemi, samoopravnými kódy, redundancí, žurnálováním atd. V kryptografii a v zabezpečení informací všeobecně integrita znamená platnost dat.“* **Integrita systému** pak je *„vlastnost, že systém vykonává svou zamýšlenou funkci nenarušeným způsobem, bez záměrné nebo náhodné neautomatizované manipulace se systémem.“*

68: JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. 3. aktualiz. vyd. Praha: AFCEA, 2015, s. 58. [online]. [cit. 10. 7. 2018]. Dostupné z: http://afcea.cz/wp-content/uploads/2015/03/Slovnik_v303.pdf

**Integrita tedy představuje nemožnost zásahu do informací, dat, počítačových systémů, jejich nastavení** atp. **jinou osobou, než tou, která je k takovému úkonu oprávněna.**

Zároveň integrita představuje jakousi záruku neporušenosti systému, informací či dat.

*„O nežádoucí modifikaci (alteration) se proto v informační bezpečnosti hovoří jako o narušení integrity (integrity).“* [69]

V případě, že dojde k porušení integrity, je třeba si uvědomit, že pokud dojde k nežádoucí změně dat, nemusí být tato nežádoucí změna vůbec odhalena a může uplynout značná doba, než je porušení integrity zjištěno.

Vyhláška o kybernetické bezpečnosti v příloze č. 1 představuje také stupnici pro hodnocení integrity.

| **Úroveň** | **Popis** | **Příklady požadavků na ochranu aktiva** |
|---|---|---|
| **Nízká** | Aktivum nevyžaduje ochranu z hlediska integrity. Narušení integrity aktiva neohrožuje oprávněné zájmy povinné osoby. | Není vyžadována žádná ochrana. |
| **Střední** | Aktivum může vyžadovat ochranu z hlediska integrity. Narušení integrity aktiva může vést k poškození oprávněných zájmů povinné osoby a může se projevit méně závažnými dopady na primární aktiva. | Pro ochranu integrity jsou využívány standardní nástroje (například omezení přístupových práv pro zápis). |
| **Vysoká** | Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity aktiva vede k poškození oprávněných zájmů povinné osoby s podstatnými dopady na primární aktiva. | Pro ochranu integrity jsou využívány speciální prostředky, které dovolují sledovat historii provedených změn a zaznamenat identitu osoby provádějící změnu. Ochrana integrity informací přenášených komunikačními sítěmi je zajištěna pomocí kryptografických prostředků. |

69: ŠULC, Vladimír. *Kybernetická bezpečnost*. Plzeň: Aleš Čeněk, 2018. s. 22

| | | |
|---|---|---|
| **Kritická** | Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity vede k velmi vážnému poškození oprávněných zájmů povinné osoby s přímými a velmi vážnými dopady na primární aktiva. | Pro ochranu integrity jsou využívány speciální prostředky jednoznačné identifikace osoby provádějící změnu (například pomocí technologie digitálního podpisu). |

### Dostupnost (Availability)

Dle Výkladového slovníku kybernetické bezpečnosti[70] je **dostupnost** definována jako *„vlastnost přístupnosti a použitelnosti na žádost oprávněné entity.“*

Dostupnost je tedy možné definovat jako garanci možnosti přístupu k informaci, datům, nebo počítačovému systému v okamžiku potřeby. Sebedokonalejší systém zajišťující integritu a umožňující přístup k systému samotnému, datům či informacím je nevyužitelný, pokud nebude zajišťovat spolehlivý přístup dle potřeby.[71]

*„O zničení (destruction) určitých informací se v informační bezpečnosti hovoří jako o narušení jejich dostupnosti (availability).“* [72]

Vyhláška o kybernetické bezpečnosti v příloze č. 1 představuje i stupnici pro hodnocení dostupnosti.

| **Úroveň** | **Popis** | **Příklady požadavků na ochranu aktiva** |
|---|---|---|
| **Nízká** | Narušení dostupnosti aktiva není důležité a v případě výpadku je běžně tolerováno delší časové období pro nápravu (cca do 1 týdne). | Pro ochranu dostupnosti je postačující pravidelné zálohování. |

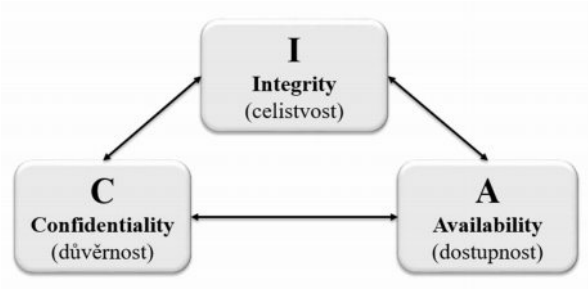
70: JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. 3. aktualiz. vyd. Praha: AFCEA, 2015, s. 43. [online]. [cit. 10. 7. 2018]. Dostupné z: http://afcea.cz/wp-content/uploads/2015/03/Slovnik_v303.pdf

71: Viz např. EVANS, Donald, Philip, BOND a Arden BEMET. *Standards for Security Categorization of Federal Information and Information Systems.* National Institute of Standards and Technology, Computer Security Resource Center. [online]. [cit. 10. 12. 2017]. Dostupné z: https://csrc.nist.gov/csrc/media/publications/fips/199/final/documents/fips-pub-199-final.pdf

72: ŠULC, Vladimír. *Kybernetická bezpečnost.* Plzeň: Aleš Čeněk, 2018. s. 24

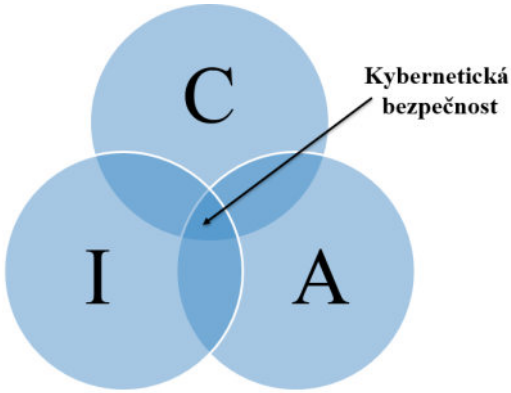
| | | |
|---|---|---|
| **Střední** | Narušení dostupnosti aktiva by nemělo překročit dobu pracovního dne, dlouhodobější výpadek vede k možnému ohrožení oprávněných zájmů povinné osoby. | Pro ochranu dostupnosti jsou využívány běžné metody zálohování a obnovy. |
| **Vysoká** | Narušení dostupnosti aktiva by nemělo překročit dobu několika hodin. Jakýkoli výpadek je nutné řešit neprodleně, protože vede k přímému ohrožení oprávněných zájmů povinné osoby. Aktiva jsou považována za velmi důležitá. | Pro ochranu dostupnosti jsou využívány záložní systémy a obnova poskytování služeb může být podmíněna zásahy obsluhy nebo výměnou technických aktiv. |
| **Kritická** | Narušení dostupnosti aktiva není přípustné a i krátkodobá nedostupnost (v řádu několika minut) vede k vážnému ohrožení oprávněných zájmů povinné osoby. Aktiva jsou považována za kritická. | Pro ochranu dostupnosti jsou využívány záložní systémy a obnova poskytování služeb je krátkodobá a automatizovaná. |

Triáda CIA bývá mnohdy pro lepší pochopení jejích jednotlivých atributů a vztahů znázorňována graficky. I z tohoto důvodu je na tomto místě prezentováno typické znázornění triády CIA. V další části této kapitoly je pak tato triáda doplněna o prvky (technologie, lidé, procesy).




Obrázek 1: Triáda CIA

Pokud bychom se snažili vymezit prostor kybernetické bezpečnosti v rámci implementace triády CIA, pak by tento prostor bylo možné zobrazit jako průnik jednotlivých principů této triády.




Obrázek 2: Triáda CIA a kybernetická bezpečnost


Obrázek 3: Zobrazení Parkenian hexad[73]

### 2.2.2 Prvky kybernetické bezpečnosti

Následující tři prvky, respektive jejich vzájemná interakce, umožňují do určité míry vytvořit či nastolit kybernetickou bezpečnost. Těmito prvky jsou:

73: *The Parkerian Hexad*. [online]. [cit. 20. 8. 2016]. Dostupné z: http://cs.lewisu.edu/mathcs/msisprojects/papers/georgiependerbey.pdf

- **lidé**,
- **technologie** a
- **procesy**.

Domníváme se, že je utopické si myslet, že je možné vytvořit absolutní kybernetickou bezpečnost či absolutně zabezpečený systém, v rámci něhož jsou využívány prvky ICT.

Teoreticky by sice bylo možné si představit zcela izolovaný počítačový systém (včetně zdroje napájení např. pomocí agregátu), uzavřený ve Faradayově kleci, se zcela jasně definovaným okruhem osob, které jsou oprávněny na tomto počítačovém systému pracovat, s tím, že není možné vnášet ani vynášet žádná média (elektronická či jiná) z tohoto unikátního prostředí.

Otázkou však je, k čemu by takto zabezpečený systém sloužil a jakým způsobem by byly využity výsledky práce na tomto systému, respektive jak by bylo možné tyto výsledky uvést v život, když není možné vynášet výsledky činnosti. Protiargumentem by pak mohlo být tvrzení, že vyneseny budou výsledky až v okamžiku ukončení projektu, do té doby bude vše chráněno a přístup bude podléhat již výše uvedenému režimu.

Nicméně je otázkou, zda takto uměle vytvořený a zcela izolovaný systém je chráněn i proti dalším hrozbám, kterými může být neexistence záloh, možnost fyzického zničení počítačového systému, vyzrazení dílčích informací lidmi, kteří s daným systémem pracují atd.

Jakýkoliv systém je tak bezpečný, jak bezpečný je jeho nejslabší článek (prvek).

### Lidé

„*People often represent the weakest link in the security chain and are chronically responsible for the failure of security systems.*“

„*Lidé často představují nejslabší článek v bezpečnostním řetězci a jsou chronicky zodpovědní za selhání bezpečnostních systémů.*“

Bruce Schneier[74]

Na lidi v interakci s kybernetickou bezpečností je možné nahlížet jako na:

- **strůjce (tvůrce) této bezpečnosti** (tj. typicky osoby, které se snaží prosadit a implementovat jednotlivé prvky kybernetické bezpečnosti, ať již ve vztahu k sobě samotnému, či ve vztahu k organizaci),

74: SCHNEIER, Bruce. [online]. [cit. 18. 7. 2018]. Dostupné z: https://www.azquotes.com/quote/570039 Překlad autora.

- **příjemce pravidel kybernetické bezpečnosti** (tj. osoby, které se rozhodly či jsou nuceny implementovat již existující pravidla kybernetické bezpečnosti),
- **subjekty, které je třeba chránit před kybernetickými útoky**,
- **subjekty, které je třeba informovat a proškolit o pravidlech a principech kybernetické bezpečnosti**,
- **riziko či hrozbu v rámci vytváření a udržování kybernetické bezpečnosti**.

Pokud se zaměříme na roli lidí v rámci budování a udržování kybernetické bezpečnosti, zejména v souvislosti se ZoKB, pak je třeba definovat a vhodným způsobem personálně zajistit následující pozice:

- výbor kybernetické bezpečnosti,
- manager kybernetické bezpečnosti,
- architekt kybernetické bezpečnosti,
- auditor kybernetické bezpečnosti,
- tým kybernetické bezpečnosti,
- garant,
  - primárních aktiv,
  - podpůrných aktiv,
- věcný správce,
- technický správce,
- provozovatel (někdy také označován jako dodavatel),
- administrátor,
- uživatel.

Lidé představují klíčový prvek jakékoliv bezpečnosti. V případě kybernetické bezpečnosti se jejich role ještě umocňuje a typicky jsou právě lidé oním nejslabším prvkem a současně nejčastějším cílem útočníků.

Důvodů, které nás vedou k tomuto tvrzení, je několik.

Tím prvním je relativně krátká doba, po kterou skutečně využíváme počítačové systémy. Většina uživatelů začala využívat některý z počítačových systémů teprve po roce 1990, k Internetu jsme se masověji začali připojovat okolo roku 1995 a „chytré“ mobilní telefony využíváme přibližně od roku 2007. Řadu sociálních sítí, které v současné době považujeme za nezbytnou součást, bez které si nedovedeme svůj život představit, však nevyužíváme více než 10 let.

Druhý důvod spočívá v obrovské dynamice vývoje jak hardwaru, tak zejména softwaru, který se s naší interakcí v digitálním světě neodmyslitelně pojí. Právě dynamika vývoje softwaru neumožňuje řadě uživatelů, aby se podrobněji zabývali otázkami bezpečnosti, které se nevyhnutelně právě k používání softwaru pojí.

Třetím a posledním důvodem je ta skutečnost, že život bez informačních a komunikačních technologií je pro naši společnost již nemyslitelný, respektive nemožný. ICT a aplikace s těmito technologiemi spojené vytváří digitální avatary nás samotných, avšak s mnohem větším množstvím informací, než jsme si jako fyzické osoby schopné zapamatovat či uchovat. Tuto skutečnost si kromě výrobců hardwaru i softwaru uvědomují i útočníci a právě z tohoto důvodu cíleně útočí na lidi v kyberprostoru.

*„Amateurs hack systems, professionals hack people."*
*„Amatéři hackují systémy, profesionálové ‚hackují' lidi."*

Bruce Schneier[75]

Dle našeho názoru je nezbytné, aby lidé, kteří užívají ICT a rozhodli se pro interakci v kyberprostoru:

- **pochopili** alespoň **základní principy a pravidla**, která se vztahují ke kybernetické **bezpečnosti**,
- **porozuměli** alespoň **základním funkcím počítačových systémů** (např. PC, notebook, mobil, smart TV aj.), **které** k této interakci **používají**,
- **zanalyzovali si aplikace, které** k této interakci **používají**, a případně, pokud jim činnost těchto aplikací či jejich smluvní podmínky nevyhovují, aplikace nevyužívali,
- **vzdělávali se** v oblasti kybernetické bezpečnosti.

Proto, abychom usnadnili alespoň poslední položku z výše uvedeného seznamu, jsme se rozhodli vytvořit tuto publikaci a shrnout v ní alespoň dílčí poznatky, které mohou využít jak laičtí uživatelé, tak IT pracovníci, kteří se rozhodli věnovat zvýšenou pozornost právě oblasti kybernetické bezpečnosti.

## Technologie

*„If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology."*

*„Pokud se domníváte, že technologie dokáže vyřešit vaše bezpečnostní problémy, nerozumíte problémům a nerozumíte technologii."*

Bruce Schneier[76]

75: SCHNEIER, Bruce. [online]. [cit. 18. 7. 2018]. Dostupné z: https://www.azquotes.com/quote/570035 Překlad autora.
76: SCHNEIER, Bruce. [online]. [cit. 18. 7. 2018]. Dostupné z: https://www.azquotes.com/quote/570040 Překlad autora.

Technologie pro uživatele zpravidla představují prostředek, který mu umožní připojit se k Internetu, sociálním sítím a dalším aplikacím. Je to nástroj, který využívá různé kancelářské balíčky při tvorbě dokumentů, zasílá e-maily, sleduje video aj. Běžný uživatel zpravidla vnímá a interaguje s koncovými technologiemi (PC, tablet, mobilní telefon aj.), které sám osobně využívá, přičemž o další technologické vrstvy, které jsou nezbytné pro jeho činnost v kyberprostoru, se zpravidla nezajímá.

Pro organizace pak technologie představují celou škálu zařízení od technologií určených pro uživatele (desktop, mobilní zařízení aj.), přes kompletní infrastrukturu sítě (LAN, aktivní prvky, Wi-Fi prvky aj.) a služeb (servery, aplikace aj.), po prvky, které slouží k zajištění zabezpečení ať již na perimetru (firewall[77], IDS/IPS[78], honeypot[79] aj.), tak v rámci infrastruktury (prvky určené k autentizaci a autorizaci, monitoringu, analýze aj.).

V rámci budování a udržování kybernetické bezpečnosti je třeba analyzovat stávající aktiva[80] a na základě této analýzy případně doplnit či modifikovat existující systémy. V rámci technologií by měly být nedílnou součástí ICT organizace, s ohledem na specifika té které organizace, následující prvky:

- detekční systémy - Intrusion Detection System (**IDS**)/Intrusion Prevention System (**IPS**),
- centrální správa uživatelů a rolí,
- centralizovaná správa klasifikace informací,
- ochrana před škodlivým kódem (aplikační firewall, antivirové, antispamové a jiné řešení),
- technologie pro zaznamenávání činností jednotlivých prvků ICT, administrátorů a uživatelů (**log system**),
- aktivní a offline zálohovací systémy; zálohy vitálních serverů, aplikací a databází (**recovery system**),
- správa síťové bezpečnosti (VLAN, DMZ, firewall aj.).[81]

Technologie jsou zpravidla tou součástí kybernetické bezpečnosti, na které, ať již jako sami uživatelé či organizace, nešetříme. Za technologie jsme ochotni zaplatit nemalou část finančních

77: Firewall je systém obsahující pravidla, dle kterých se řídí datové toky v rámci síťových technologií.

78: **IPS** (**I**ntrusion **P**revention **S**ystem), zařízení monitorující nežádoucí (škodlivé) aktivity v síti a/nebo aktivity počítačových sytémů. Dále jen **IPS**.

**IDS** (**I**ntrusion **D**etection **S**ystem) představuje systém má za úkol detekovat neobvyklé aktivity, které mohou potencionálně vést k narušení bezpěčnosti počítačové sítě, počítačových systémů, aplikací aj. Dále jen **IDS**.

79: Honeypot je systém jehož smyslem je detekovat malware či další nežádoucí aktivity, které jsou následně v tomto uměle vytvořeném prostředí analyzovány.

80: Blíže viz kap. 2.3.2 Aktivum. V tomto případě jsou aktivem míněny technologie a aplikace, které jsou v organizaci využívány.

81: Blíže viz kap. 6.1 Ochrana sítí

prostředků, buď z důvodu, že „potřebujeme nejnovější telefon", či z reálného a opodstatněného důvodu spočívajícího v zastaralosti a dalším nepodporování (aktualizaci) daného počítačového systému.

Proto, aby bylo možné zajistit kybernetickou bezpečnost, je třeba udržovat technologie v takovém stavu, aby byly schopny reagovat na změny, které se k vývoji ICT pojí. Zejména by měly být technologie (jak hardware, tak software) udržovány aktualizované a zabezpečené.

Byť jsou technologie jistě významnou součástí procesu tvorby a udržování kybernetické bezpečnosti, jsou dle našeho názoru součástí nejméně významnou. Mnohem významnějšími prvky kybernetické bezpečnosti jsou vhodně nastavené procesy a lidé, kteří umějí dané procesy v praxi aplikovat či modifikovat a předem dohodnutá pravidla dodržovat.

### Procesy

*„The mantra of any good security engineer is: ‚Security is a not a product, but a process.' It's more than designing strong cryptography into a system; it's designing the entire system such that all security measures, including cryptography, work together."*

*„Mantrou dobrého bezpečnostního inženýra je: ‚**Bezpečnost není produkt, ale proces.**' Je to víc než navrhnout silnou kryptografii do systému; je to o tom navrhnout celý systém tak, aby všechna bezpečnostní opatření, včetně kryptografie, spolupracovala."*

Bruce Schneier[82]

Procesy představují činnost, kterou je třeba vynaložit, aby bylo možné technologie a s nimi spojené služby používat lidmi.

Z hlediska plynutí času je možné sledovat procesy:

- řízení aktiv a rizik,
  - definování a kategorizace aktiv,
  - analýza a kategorizace rizik,
- implementace ICT a aplikací,
- správa uživatelů a rolí,
- autorizace a autentizace,
- údržby (aktualizace) systémů a služeb,
- testování zabezpečení jednotlivých počítačových systémů a služeb,
- analýza nápravných opatření,
- realizace nápravných opatření,

82: SCHNEIER, Bruce. [online]. [cit. 18. 7. 2018]. Dostupné z: https://www.azquotes.com/quote/570047 Překlad autora.

- audit kybernetické bezpečnosti,
- detekce anomálií či kybernetických útoků,
- reakce na kybernetické útoky či jiné incidenty,
- procesy k zajištění kontinuity,
- školení a cvičení atd.

Výše uvedený výčet jednotlivých procesů, které se pojí k vytváření a udržování kybernetické bezpečnosti, rozhodně není úplný, přičemž nastíněné procesy mohou být granularizovány. Jednotlivé procesy jsou realizovány v rámci celého životního cyklu ICT, informací, dat a ve vztahu k uživatelům.[83]

Vlastní nastavení procesů, jejich neustálá údržba či modifikace představuje nejnáročnější část budování kybernetické bezpečnosti. Zároveň tato činnost klade nejvyšší nároky na správce jednotlivých systémů.

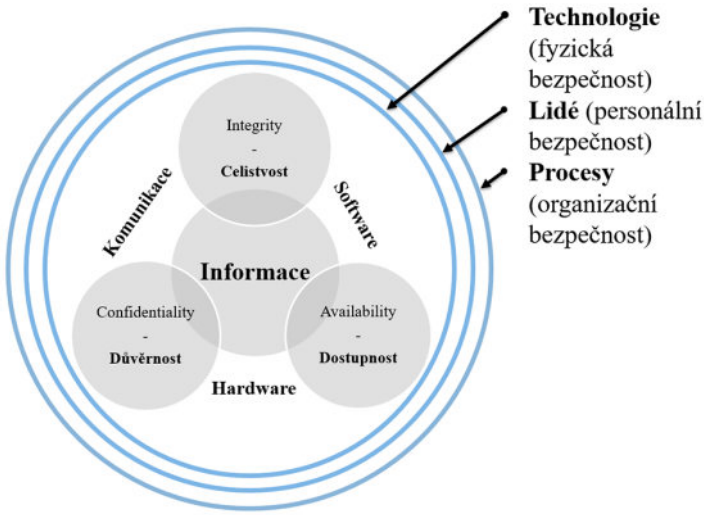
Pokud se organizace rozhodne implementovat pravidla kybernetické bezpečnosti, pak je samozřejmě vhodné udržovat hardware i software aktualizovaný, dodržovat pravidla, která jsou nastavena pro přístup k jednotlivým systémům aj.

Pokud je to možné, je vhodné v organizaci provádět i simulace typických kybernetických útoků (např. phishing, business e-mail compromise aj.) z důvodu reálné demonstrace těchto útoků a možných dopadů, pokud se osoba stane obětí takovýchto útoků.

Penetrační testování zároveň umožňuje nalézt chyby v již nastavených procesech.

Organizace by se však již při tvorbě a nastavování pravidel kybernetické bezpečnosti měla primárně zaměřit zejména na oblast lidských zdrojů a jejich edukaci.

83: Pojem uživatele je tady používán pro vyjádření fyzické osoby, která je oprávněna využívat prvky ICT, jednotlivé systémy a aplikace. Z tohoto hlediska se tedy uživatelem rozumí jak osoba s oprávněními správce, tak koncový uživatel.

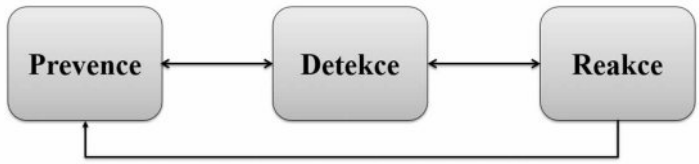



Obrázek 4: Triáda CIA doplněná o technologie, lidi a procesy[84]

### 2.2.3 Životní cyklus kybernetické bezpečnosti

Z pohledu plynutí času je při realizaci kybernetické bezpečnosti třeba uplatňovat, případně modifikovat jak triádu CIA, tak dílčí prvky kybernetické bezpečnosti v průběhu celého jejich životního cyklu. Zejména jde o prevenci, detekci a rekci na útok.[85]

Velmi často je životní cyklus kybernetické bezpečnosti zobrazován pomocí různých diagramů. Pro přehlednost uvádím některé z nich.




Obrázek 5: Zjednodušené zobrazení životní cyklu kybernetické bezpečnosti

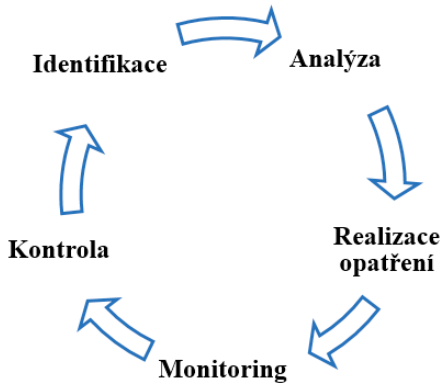
84: Předlohou grafu byl graf zveřejněný v: *CIA triad methodology*. [online]. [cit. 10. 7. 2018]. Dostupné z: https://en.wikipedia.org/wiki/Information_security#/media/File:CIAJMK1209.png

85: Blíže viz SVOBODA, Ivan. *Řešení kybernetické bezpečnosti*. Přednáška v rámci CRIF Academy. (23. 9. 2014)


Obrázek 6: Životní cyklus kybernetické bezpečnosti dle kybez.cz[86]

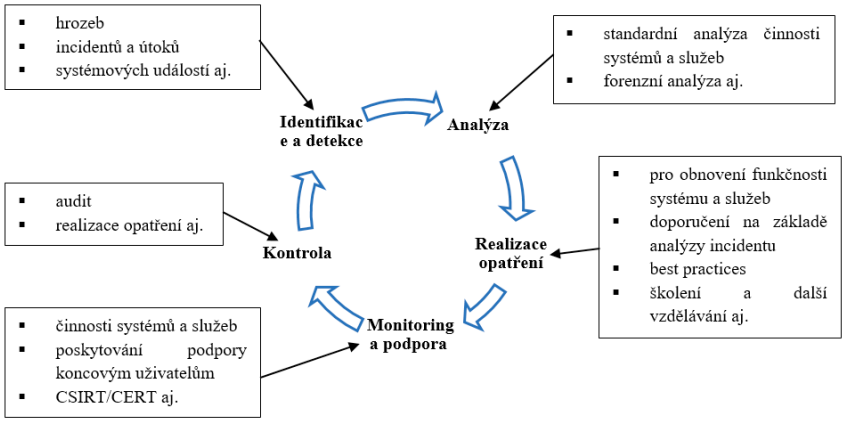
Při řešení kybernetické bezpečnosti neexistuje žádný „záchytný bod", v rámci kterého by bylo možné říci: *„Zvládli jsme to! Jsme chráněni proti kybernetickým útokům či hrozbám. Jsme kyberneticky bezpeční."*

Budování a udržování kybernetické bezpečnosti je možné přirovnat k nikdy nekončící analýze rizik, avšak s tím, že tuto běžnou analýzu je třeba doplnit o další podpůrné procesy, které mohou pomoci se zvýšením kybernetické bezpečnosti v organizaci.




Obrázek 7: Analýza rizik

86: *Základní pojmy*. [online]. [cit. 10. 7. 2018]. Dostupné z: https://www.kybez.cz/bezpecnost/pojmoslovi




Obrázek 8: Životní cyklus kybernetické bezpečnosti

Vlastní znázornění životního cyklu kybernetické bezpečnosti může být značně komplexnější.[87]


Obrázek 9: Příklad řešení kybernetické bezpečnosti

87: *The complete breadth of CGI Cyber Security services.* [online]. [cit. 10. 7. 2018]. Dostupné z: https://mss.cgi.com/service-portfolio

## Evoluce kybernetické bezpečnosti

Na závěr této subkapitoly by bylo možné si položit jednoduchou otázku: *„Proč bych se měl já (jako jedinec), nebo organizace vůbec zabývat kybernetickou bezpečností?"*

Odpověď nebude až tak komplikovaná, byť bude nutné rozbít mnohdy zakořeněný mýtus, že někdo jiný, ať již velké organizace typu Microsoft, Google, Apple či poskytovatelé cloudových služeb, konektivity atd., za mě problematiku kybernetické bezpečnosti již řeší.

Pravdou je, že tyto organizace zavedly a aplikují dílčí prvky kybernetické bezpečnosti, avšak kybernetická bezpečnost, stejně jako bezpečnost jakákoliv jiná, vždy začíná a končí u konkrétní osoby či organizace, která se chce zabezpečit, a to vždy s ohledem na specifika dané osoby či organizace.

Z Data Breach Investigations Report[88], která se zabývá narušení bezpečnosti vedoucím ke kompromitaci dat, za rok 2017 vyplývají následující fakta:

- útočníkem byla
  - **osoba mimo organizaci - 73 %**
  - osoba v rámci organizace - 28 %
  - **organizovaná zločinecká skupina - 50 %**

- k útokům bylo využito:
  - **hackingu - 48 %**
  - **malware - 30 %**
    - **49 % malware** bylo útočníkem distribuováno a následně nainstalováno **skrze e-mail**
  - **sociálního inženýrství - 43 %**
  - fyzického útoku - 8 % [89]

- oběťmi jsou organizace působící ve:
  - zdravotnictví – 24 %
  - veřejném sektoru (typicky státní správa a samospráva aj.) – 14 %

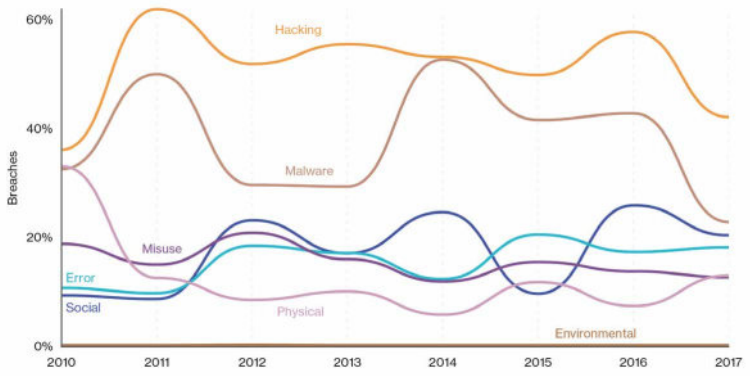
- motiv útoku:
  - **obohacení se – 76%**
  - zisk dat a informací (špionáž) – 13 %

- **68 % útoků bylo odhaleno až po několika měsících, či po delší době**

88: *2018 Data Breach Investigation Report. 11th Edition.* [online]. [cit. 28. 7. 2018]. Dostupné z: http://www.documentwereld.nl/files/2018/Verizon-DBIR_2018-Main_report.pdf

89: V rámci jednotlivých útoků zpravidla dochází ke kombinování technik a nástrojů.

Následujících graf prezentuje vývoj jednotlivých útoků od roku 2010 do konce roku 2017.




Obrázek 10: Typy útoků použitých k narušení bezpečnosti[90]

**Dle zprávy Národního úřadu pro kybernetickou a informační bezpečnost**[91] *„**lze v roce 2018 očekávat další nárůst kybernetických hrozeb,** zejména další phishingové útoky nové generace, útoky na tržiště, peněženky a směnárny kryptoměn, bezsouborové varianty ransomware, využívání umělé inteligence ke kybernetickým útokům, útoky na data v Cloudových řešeních, útoky na internet věcí, průmyslové systémy atd. **Očekává se, že se zvýší podíl státních nebo státem podporovaných aktérů kybernetických útoků, že bude i nadále docházet k masivním únikům osobních dat, hesel a přístupových údajů.** Proto je nezbytné budovat kybernetickou bezpečnost informačních a komunikačních systémů důležitých pro chod státu a jeho kritické infrastruktury.“* [92]

Oblast kybernetické bezpečnosti bude do budoucna jednou z nejvýznamnějších oblastí, neboť lze předpokládat, že k redukci využívání ICT a služeb s těmito technologiemi spojených nedojde. Kybernetická bezpečnost má pomáhat při identifikaci nedostatků v nastavení těchto systémů a služeb.

„Kybernetická bezpečnost také pomáhá identifikovat, hodnotit a řešit hrozby v kyberprostoru, snižovat kybernetická rizika a eliminovat dopady kybernetických útoků, informační kriminality,

90: *2018 Data Breach Investigation Report. 11th Edition.* [online]. [cit. 28. 7. 2018]. Dostupné z: http://www.documentwereld.nl/files/2018/Verizon-DBIR_2018-Main_report.pdf s. 7

91: Dále jen **NÚKIB**

92: *Zpráva o stavu kybernetické bezpečnosti za rok 2017.* [online]. [cit. 29. 6. 2018]. Dostupné z: https://nukib.cz/download/Zpravy-KB-vCR/Zprava-stavu-KB-2017-fin.pdf

kyberterorismu a kybernetické špionáže ve smyslu posilování důvěrnosti, integrity a dostupnosti dat, systémů a dalších prvků informační a komunikační infrastruktury.

**Hlavním smyslem kybernetické bezpečnosti je pak ochrana prostředí k realizaci informačních práv člověka**."[93]

## 2.3 Riziko, aktivum, zranitelnost

### 2.3.1 Riziko

Před vymezením pojmů hrozba, událost, incident a útok považujeme za nezbytné alespoň rámcově definovat pojem riziko, které s následně definovanými pojmy bezprostředně souvisí.

Výkladový slovník kybernetické bezpečnosti definuje riziko jako: „*(1) Nebezpečí, možnost škody, ztráty, nezdaru. (2) Účinek nejistoty na dosažení cílů. (3) Možnost, že určitá hrozba využije zranitelnosti aktiva nebo skupiny aktiv a způsobí organizaci škodu.*" [94]

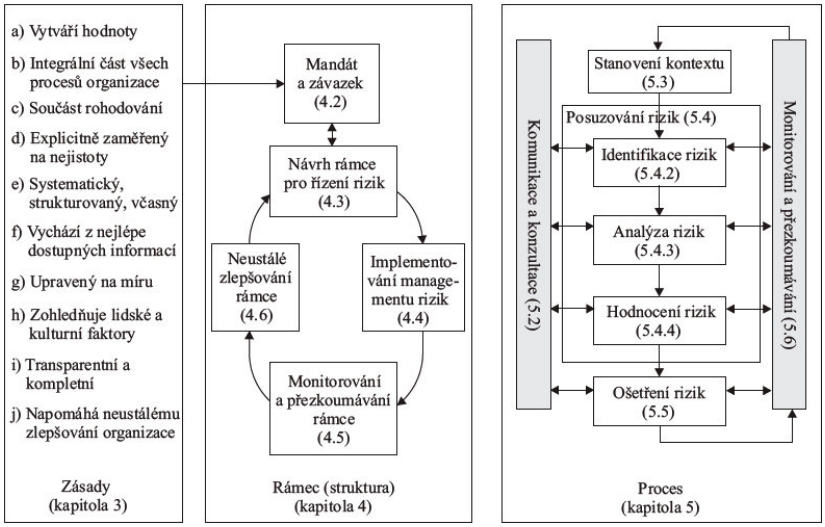
**Riziko je** také možné definovat jako **potenciál, že se hrozba stane reálnou a využije zranitelnosti aktiva**.[95] Dle čl. 4 odst. 9 NIS se **rizikem** rozumí „***jakákoli přiměřeně rozpoznatelná okolnost nebo událost, která by mohla mít negativní dopad na bezpečnost sítí a informačních systémů.***" V kyberprostoru jsou rizikům vystaveni jak uživatelé, tak počítačové systémy a aplikace, které je využívají, tak další prvky ICT.

Pojem **riziko vyjadřuje pravděpodobnost, s jakou může nastat nechtěná událost**. Míra pravděpodobnosti, s jakou tato událost nastane, se vyjadřuje pomocí analýzy rizik. Minimální normové hodnoty pro metody identifikace, analýzy, hodnocení a ošetření rizik jsou definovány v ČSN EN 31010.

93: *Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020.* [online]. [cit. 1. 7. 2018]. Dostupné z: https://www.govcert.cz/download/gov-cert/container-nodeid-998/nskb-150216-final.pdf

94: JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. 3. aktualiz. vyd. Praha: AFCEA, 2015. s. 99. Dostupné z: https://nukib.cz/download/aktuality/container-nodeid-665/slovnikkb-cz-en-1505.pdf

95: Blíže viz § 2 písm. f) VoKB
K pojmu aktiva viz kap. 2.3.2 Aktivum




Obrázek 11: Vazby mezi principy, rámcem a procesem managementu rizik[96]

Valášek a kol.[97] uvádějí, že se při stanovení rizik obvykle vychází ze tří základních otázek:

- **Co špatného (nežádoucího) se může stát? Co může selhat?**
- **Jaká je možnost / pravděpodobnost, že se to stane?**
- **Jak závažné (intenzita, velikost apod.) mohou být účinky (dopady, následky)?**

Dle Valáška však tyto otázky představují pouze základní rámec, který je schopen definovat vlastní riziko. Vedle těchto tří otázek jsou pokládány následující doplňující otázky, které se vztahují k významným faktorům ovlivňujícím charakteristiku rizika:

96: MATUROVÁ, Jana a Miroslav VALTA. *Prevence rizik – provádění kontrol technického stavu technických zařízení.* [online]. [cit. 1. 7. 2018]. Dostupné z:
https://www.bozpinfo.cz/prevence-rizik-provadeni-kontrol-technickeho-stavu-technickych-zarizeni

97: VALÁŠEK, Jarmil, František KOVÁŘÍK a kol. *Krizové řízení při nevojenských krizových situacích*. Praha: Ministerstvo vnitra - generální ředitelství Hasičského záchranného sboru ČR, 2008. [online]. [cit. 1. 7. 2018]. Dostupné z:
http://www.hzscr.cz/soubor/modul-c-krizove-rizeni-pri-nevojenskych-krizovych-situacich-pdf.aspx
ISBN 978-80-86640-93-8 s. 73

| Faktor | Otázka |
|---|---|
| Čas | „Jak dlouho budeme riziku vystaveni (ohroženi)?“ |
| Nestálost | „Jak se blíží odhady dopadů rizikové události skutečnosti?“ |
| Složitost | „Je obtížné riziku porozumět?“ |
| Vzájemné vztahy | „Jak dalece spolu souvisí různá rizika nebo rizikové faktory?“ |
| Ovlivnění | „Je možné riziko zvládat?“ |
| Životní cyklus | „Jak se riziko mění v čase?“ |
| Nákladová efektivnost | „Jak nákladná jsou opatření vůči riziku?“ |

U každého rizika se počítá stupeň významnosti rizika, který je možné vyjádřit následovně:

**Významnost** rizika = **Dopady** rizika * **Pravděpodobnost** výskytu rizika

„*Výsledkem analýzy rizik je stanovení významnosti definovaných rizik. Každé riziko, s ohledem na zadání, má různé dopady, které může způsobit. Dopady rizika neboli následky hodnotíme v pětibodové stupnici např. takto:*“

| Body | Pravděpodobnost výskytu rizika | Popis výskytu |
|---|---|---|
| 5 | JISTÉ | Riziko se téměř vždy vyskytne nebo s pravděpodobností 90 – 100 %. |
| 4 | PRAVDĚPODOBNÉ | Riziko se pravděpodobně vyskytne |
| 3 | MOŽNÉ | Riziko se někdy může vyskytnout (např. za specifických podmínek). |
| 2 | NEPRAVDĚPODOBNÉ | Riziko se někdy může vyskytnout, ale je to nepravděpodobné. |
| 1 | VYLOUČENÉ | Riziko se vyskytne pouze ve výjimečných případech a za specifických podmínek. |

*Kromě dopadu jednotlivá rizika mohou nastat anebo také nemusí. Proto se stanovuje pravděpodobnost vzniku rizika. Výskyt opět hodnotíme na pětibodové stupnici takto:*[98]

| Body | Dopad rizika | Popis dopadu |
|---|---|---|
| 5 | KRIZOVÉ | Situace zásadně omezí nebo ukončí provoz firmy (např. bankrot, ztráty na životech apod.). |
| 4 | VÝZNAMNÉ | Situace velmi nebezpečně ovlivňuje vnitřní i vnější chod firmy (např. vznik významných ztrát finančních - 100% nad rozpočet, časových, vznik soudních sporů, vzniknou zranění apod.). |
| 3 | STŘEDNÍ | Situace nebezpečně ovlivní vnitřní i vnější chod firmy (např. ztráty vzniknou, ale firma je schopna dále fungovat, vzniknou finanční ztráty do výše 30 % rozpočtu apod.). |
| 2 | NEVÝZNAMNÉ | Situace omezuje vnitřní chod firmy (např. dojde k časovým zpožděním do max. výše 30 dní). |
| 1 | ZANEDBATELNÉ | Situace sice negativně omezuje chod firmy, ale nezpůsobuje ztráty větší než 5 %. |

Při hodnocení rizika je krom výše uvedeného třeba přihlédnout i k dalším okolnostem, kterými jsou:

- vlastní povaha (druh) rizika či hrozby,
- zranitelnost aktiva,
- pravděpodobnosti, že se riziko promění v bezpečnostní událost či incident.[99]

Analýza rizik je značně obtížná a vyžaduje znalost aktiv, hrozeb a zejména je třeba mít v této oblasti již nějaké zkušenosti. Na základě analýzy rizik je možné stanovit opatření za účelem minimalizace nebo úplného odstranění rizik.

98: *Analýza rizik*. [online]. [cit. 1. 7. 2018]. Dostupné z: https://www.vlastnicesta.cz/metody/analyza-rizik-risk/

99: Viz kap. 2.4.2 Kybernetická bezpečnostní událost a 2.4.3 Kybernetický (bezpečnostní) incident

### 2.3.2 Aktivum

**Aktivem se rozumí cokoliv, co má určitou hodnotu pro osobu, organizaci či stát.**

Aktivum může být věcí **hmotnou** (budova, počítačový systém, sítě, energie, zboží aj.) **či nehmotnou** (informace, znalosti, data, programy aj.) z pohledu občanského práva.

Aktivem však může být i **vlastnost** (např. dostupnost a funkčnost systému a dat aj.) či **dobré jméno**, reputace atd. **Lidé** (uživatelé, administrátoři aj.) a jejich znalosti a zkušenosti jsou také z pohledu kybernetické bezpečnosti aktivem.

Dle § 2 písm. f) a g) VoKB se **aktiva** dělí na **podpůrná** a **primární.**

**Podpůrným aktivem** je technické aktivum, zaměstnanci a dodavatelé podílející se na provozu, rozvoji, správě nebo bezpečnosti informačního a komunikačního systému.

**Primárním aktivem** je informace nebo služba, kterou zpracovává nebo poskytuje informační a komunikační systém.

### 2.3.3 Zranitelnost

Zranitelnost (vulnerability) označuje slabé místo aktiva, softwaru, zabezpečení, které je využito jednou nebo více hrozbami.

Zranitelnost, stejně jako hrozba, může být způsobena celou řadou faktorů spočívajících jak v jednání člověka, technické závadě, tak případně zásahu vyšší moci (blíže viz kap. 2.4.1 - konkrétně klasifikace hrozeb).

V oblasti kybernetické bezpečnosti se zranitelnosti dělí na:

- **zranitelnosti známé** (publikované)
  - **opravené** (ošetřené) – typickým případem jsou zranitelnosti softwaru, na který již výrobce vydal aktualizaci
  - **neopravené** (neošetřené) – dotčený subjekt (výrobce, správce aj.) o zranitelnosti ví, ale nezajistil její opravu

- **zranitelnosti neznámé**
  - skryté
  - neobjevené

V případě neznámých zranitelností je významné, zda jsou objeveny útočníkem, výrobcem, bezpečnostním analytikem, osobou zabývající se penetračním testováním či uživatelem. Stejně tak je významná motivace osoby, která danou zranitelnost objeví.

Bezpečnostní zranitelnosti jsou potenciálními bezpečnostními hrozbami. Bezpečnostní zranitelnosti lze do určité míry eliminovat důsledným aktualizováním a záplatováním veškerého softwaru.[100]

Vyhláška o kybernetické bezpečnosti v příloze č. 3 uvádí příkladmo některé ze zranitelností. **Dle** této **vyhlášky je zranitelností:**

1) nedostatečná údržba informačního a komunikačního systému,
2) zastaralost informačního a komunikačního systému,
3) nedostatečná ochrana vnějšího perimetru,
4) nedostatečné bezpečnostní povědomí uživatelů a administrátorů,
5) nevhodné nastavení přístupových oprávnění,
6) nedostatečné postupy při identifikování a odhalení negativních bezpečnostních jevů, kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů,
7) nedostatečné monitorování činnosti uživatelů a administrátorů a neschopnost odhalit jejich nevhodné nebo závadné způsoby chování,
8) nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí,
9) nedostatečná ochrana aktiv,
10) nevhodná bezpečnostní architektura,
11) nedostatečná míra nezávislé kontroly,
12) neschopnost včasného odhalení pochybení ze strany zaměstnanců.

## 2.4 Kybernetické hrozby, události, incidenty a útoky

Vypořádat se s problematikou „negativních kybernetických jevů" může být poněkud problematické, neboť různá odborná literatura, jakož i právní normy mnohdy používají pro definování určitého negativního jevu různá synonyma, která mají vyjádřit totéž.

Důvodem pro neustálenost terminologie je jednak opět relativně krátká doba, po kterou se vypořádáváme s kybernetickými hrozbami, útoky a incidenty, a jednak i ne vždy shodný překlad z angličtiny, která je v oblasti IT využívána primárně.

100: Srov. JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. 3. aktualiz. vyd. Praha: AFCEA, 2015. s. 29. Dostupné z: https://nukib.cz/download/aktuality/container-nodeid-665/slovnikkb-cz-en-1505.pdf

### 2.4.1 Kybernetická hrozba

Hrozbu můžeme nejjednodušeji definovat jako něco, co je schopno narušit běžný či řádný stav věcí a zasáhnout do práv jiných subjektů. Jde o negativní působení, které může, ale nemusí být dokončeno. Pro vlastní definici je dostačující, že možnost negativního stavu hrozí a je reálná.

Dle dikce Ministerstva vnitra ČR se za hrozbu považuje „*jakýkoli fenomén, který má potenciální schopnost poškodit zájmy a hodnoty chráněné státem. Míra hrozby je dána velikostí možné škody a časovou vzdáleností (vyjádřenou obvykle pravděpodobností čili rizikem) možného uplatnění této hrozby.*“ [101]

Výkladový slovník kybernetické bezpečnosti definuje několik pojmů, které se bezprostředně vztahují ke kybernetickým hrozbám.

Vlastní pojem **hrozba** (threat) je definován jako „*potenciální příčina nechtěného incidentu, jehož výsledkem může být poškození systému nebo organizace.*“ [102]

S tímto základním pojmem pak bezprostředně souvisí i pojem **bezpečnostní hrozba** (Information security threat)[103], který je definován jako „*potenciální příčina nežádoucí události, která může mít za následek poškození systému a jeho aktiv, např. zničení, nežádoucí zpřístupnění (kompromitaci), modifikaci dat nebo nedostupnost služeb.*“ [104]

Vedle dvou výše uvedených pojmů definují autoři ve výkladovém slovníku i pojmy **aktivní hrozba, pasivní hrozba a pokročilá a trvalá hrozba.**[105]

101: *Hrozba.* [online]. [cit. 28. 7. 2018]. Dostupné z: http://www.mvcr.cz/clanek/hrozba.aspx

102: JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. 3. aktualiz. vyd. Praha: AFCEA, 2015. s. 52. Dostupné z:
https://nukib.cz/download/aktuality/container-nodeid-665/slovnikkb-cz-en-1505.pdf

103: V tomto případě je vidět problém s překladem některých pojmů z angličtiny a naopak. Pokud bychom chtěli důsledně přeložit pojem Information security threat, pak správným českým ekvivalentem je např. hrozba pro bezpečnost informací; hrozba zabezpečení informací aj.

104: JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. Výkladový slovník kybernetické bezpečnosti. [online]. 3. aktualiz. vyd. Praha: AFCEA, 2015. s. 52. Dostupné z:
https://nukib.cz/download/aktuality/container-nodeid-665/slovnikkb-cz-en-1505.pdf

105: Tamtéž s. 16, 81 a 87

Oxford dictionary uvádí, že **kybernetickou hrozbou je možnost škodlivého pokusu o poškození nebo narušení počítačové sítě nebo systému.**[106] Přičemž za systém je v tomto kontextu považován počítačový systém.

**Kybernetickou hrozbu** lze také definovat jako akt směřující ke změně[107] informace, aplikací či systému samotného.

Jirovský vymezuje čtyři skupiny základních hrozeb a zároveň charakterizuje jejich vztah:[108]

1) **Únik informace** je stav, kdy dojde k vyzrazení chráněné informace neautorizovanému subjektu.
2) **Narušení integrity** představuje poškození, změnu, či vymazání dat.
3) **Potlačení služby** znamená úmyslné bránění v přístupu k informacím, aplikacím, či systému.[109]
4) **Nelegitimní použití** je užití informací neautorizovaným subjektem či neoprávněným způsobem.[110]

Uvedený vztah je nejlépe znázorněn na následujícím obrázku.

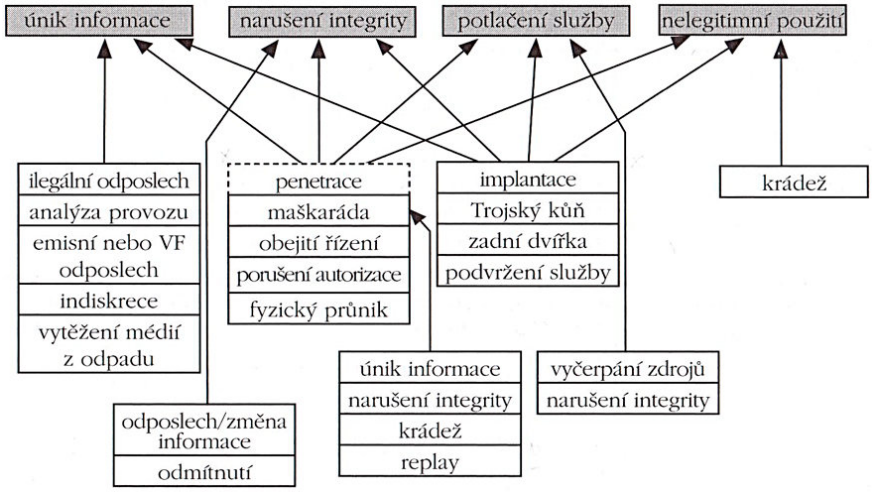
106: *Cyberthreat.* [online]. [cit. 6. 7. 2018]. Dostupné z:
https://en.oxforddictionaries.com/definition/cyberthreat Překlad autora.

107: Změnou je míněna i krádež informace, její zničení, či zmaření jejího užití.

108: Srov. JIROVSKÝ, Václav. *Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada Publishing, a. s., 2007. s. 21 a násl.

109: Jde například o útoky typu **DoS - Denial of Service**, **DDoS – Distributed Denial of Service** aj. Blíže viz KOLOUCH, Jan. *CyberCrime.* Praha: CZ.NIC, 2016, s. 295 a násl.

110: Například dojde k napadení zpoplatněného systému a využívání jeho služeb bez platby za služby.




Obrázek 12: Vzájemný vztah jednotlivých kybernetických hrozeb dle Jirovského

## Klasifikace kybernetických hrozeb

Vlastních klasifikací kybernetických hrozeb existuje celá řada, přičemž nejčastěji jsou tyto hrozby členěny dle:

1) **Zdroje hrozby**

- **Hrozby způsobené člověkem.** V případě, že je hrozba způsobena člověkem, je vhodné se zaměřit i na formu zavinění, jež vedlo k iniciaci dané hrozby. Z tohoto pohledu je možné rozlišovat hrozby způsobené:

  - **úmyslně,**
    Mezi úmyslně způsobené kybernetické hrozby je možné zařadit například:
    - úmyslné smazání dat, konfigurace systému aj.,
    - fyzické poškození počítačového systému či jiného prvku ICT,
    - zcizení dat a informací,
    - kybernetické útoky (malware, DoS, DDoS, phishing, neoprávněný odposlech aj.).[111]

  - **z nedbalosti.**
    Mezi kybernetické hrozby způsobené z nedbalosti je možné zařadit například:
    - omylem smazaná data,

111: Jednotlivé kybernetické útoky viz např.: KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, 2016, s. 181 a násl.

    - fyzické poškození počítačového systému či jiného prvku ICT (např. pádem, překopnutím strukturované kabeláže aj.),
    - poškození dat, systémů či jiných prvků na základě neseznámení se s interními akty (právními či technickými),
    - jiná chyba uživatele.

- **Technické chyby** (např. chyba softwaru či hardwaru).

- **Vis maior (vyšší moc)**.
  Mezi kybernetické hrozby způsobené vyšší mocí je možné zařadit například:
    - neplánovaný výpadek napájení (pokud se nejedná o hrozbu způsobenou člověkem z nedbalosti),
    - přírodní události (zásah blesku, vichřice aj.) či katastrofy (povodně, zemětřesení aj.),
    - požár (pokud se nejedná o hrozbu způsobenou člověkem).

2) **Zdroje působení**

- **hrozby vnitřní** (zdroj hrozby se nachází uvnitř organizace)
- **hrozby vnější** (zdroj hrozby se nachází mimo organizaci)[112]

3) **Cíle hrozby**

- **Útok na triádu CIA.**
    - **Confidentiality** (důvěrnost) – např. krádeže dat, přístupových údajů a klíčů, hardware aj.
    - **Integrity** (celistvost) – chyby v databázích, v nastavení oprávnění aj.
    - **Availability** (dostupnost) – např. DoS a DDoS útoky; fyzické útoky na servery a strukturovanou kabeláž; výpadky proudu aj.

- **Útok na některý z prvků kybernetické bezpečnosti.**
    - **Lidé –** útoky sociálním inženýrstvím (ve světě reálném, ale i kyberprostoru), phishing, malware, krádeže aj.
    - **Technologie –** veškeré hrozby uvedené v bodě 1 této klasifikace. Typicky mohou hrozby působit na:
        - hardware (koncové počítačové systémy, servery, řídící prvky sítě, IoT aj.),
        - databáze,
        - síť a síťovou infrastrukturu,
        - software (operační systém či jiné aplikace),
        - informace a data uložená v počítačových systémech.

112: Blíže viz např. POŽÁR, Josef. *Vybrané hrozby informační bezpečnosti organizace.* [online]. [cit. 6. 7. 2018]. Dostupné z: https://www.cybersecurity.cz/data/pozar2.pdf

◦ **Procesy –** neoprávněné testování zabezpečení či funkčnosti procesů nastavených v organizaci aj.

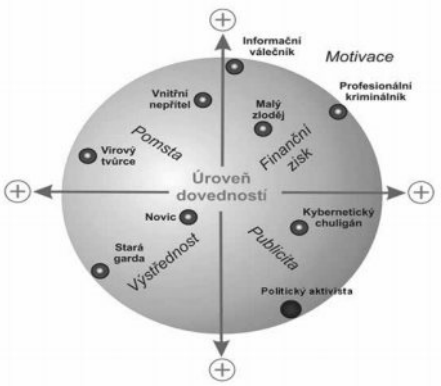
4) **Motivace**

Pokud je hrozba způsobena úmyslným jednáním člověka, je vhodné se při řešení hrozby zabývat i její motivací. Na základě analýzy motivace takovéhoto jednání je v rámci procesu reakce na hrozbu možné vytvořit nápravná opatření, aby nedocházelo ke stimulu této motivace i v budoucnu.

Dle motivace lze sledovat:

- hrozby za účelem získání finančního prospěchu,
- hrozby za účelem získání konkurenční převahy,
- hrozby za účelem dokázání svých schopností,
- hrozby za účelem odplaty,
- hrozby z důvodu neplnění povinností.[113]

Další členění útočníků dle motivace představuje i Rak[114], který znázorňuje nejobecnější typizaci útočníků dle jejich motivace, přičemž mnohé z uvedených typů motivací se mohou následně dělit či vzájemně splývat.




Obrázek 13: Možné členění útočníků v kyberprostoru dle motivace

113: *Před čím chránit? – Bezpečnostní hrozby, události, incidenty.* [online]. [cit. 6. 7. 2018]. Dostupné z: https://www.kybez.cz/bezpecnost/pred-cim-chranit

114: Zdroj: RAK, Roman. Homo sapiens versus security. ICT fórum/PERSONALIS 2006. [předneseno 27. 9. 2006]. Praha (prezentace na konferenci).

5) **Typ hrozby**

- sociální inženýrství,
- botnet,
- malware,
- ransomware,
- spam/scam,
- podvodné nabídky,
- phishing, pharming, spear phishing, vishing, smishing,
- hacking,
- sniffing,
- DoS, DDoS, DRDoS útoky,
- šíření závadového obsahu,
- identity theft,
- APT (Advanced Persistent Threat),
- kyberterorismus,
- kybernetické výpalné či vydírání (cyber extortion).

Vyhláška o kybernetické bezpečnosti v příloze č. 3 uvádí příkladmo některé z hrozeb. **Dle** této **vyhlášky je hrozbou:**

1) porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů a administrátorů,
2) poškození nebo selhání technického anebo programového vybavení,
3) zneužití identity,
4) užívání programového vybavení v rozporu s licenčními podmínkami,
5) škodlivý kód (například viry, spyware, trojské koně),
6) narušení fyzické bezpečnosti,
7) přerušení poskytování služeb elektronických komunikací nebo dodávek elektrické energie,
8) zneužití nebo neoprávněná modifikace údajů,
9) ztráta, odcizení nebo poškození aktiva,
10) nedodržení smluvního závazku ze strany dodavatele,
11) pochybení ze strany zaměstnanců,
12) zneužití vnitřních prostředků, sabotáž,
13) dlouhodobé přerušení poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých služeb,
14) nedostatek zaměstnanců s potřebnou odbornou úrovní,
15) cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik,
16) zneužití vyměnitelných technických nosičů dat,
17) napadení elektronické komunikace (odposlech, modifikace).

### 2.4.2 Kybernetická bezpečnostní událost

Prosise a Mandiva charakterizují tzv. **„počítačovou bezpečnostní událost"** (kterou lze chápat jako počítačový útok či počítačový trestný čin), jako nezákonnou, nepovolenou, neautorizovanou, nepřijatelnou akci, která zahrnuje počítačový systém či počítačovou síť. Tato akce může být zaměřena například na krádež osobních údajů, spam či jiné obtěžování, zpronevěru, šíření či držení dětské pornografie aj.[115]

Jirásek a kol. definují bezpečnostní událost (Security event), jako: *„**událost, která může způsobit nebo vést k narušení** informačních systémů a technologií a pravidel definovaných k jeho ochraně (bezpečnostní politika).*"[116]

Definici pojmu bezpečnostní událost je možné nalézt i v čl. 3.5 ISO/IEC 27001, kde je uvedeno, že takovouto událostí je: *„**identifikovatelný stav** systému, služby, nebo sítě**, ukazující na možné porušení bezpečnostní politiky nebo selhání bezpečnostních opatření**. Může se také jednat o jinou předtím nenastalou situaci, která může být důležitá z pohledu bezpečnosti informací.*"

Obdobnou definici je možné nalézt i v příručce NIST, 800-61 Computer Security Incident Handling Guide, kde je uvedeno, že bezpečnostní událostí je: *„nepříznivá událost s negativním důsledkem, jako jsou havárie (pády) systému, packet flooding, neautorizované použití systémových oprávnění, neautorizovaný přístup k citlivým datům nebo spuštění škodlivého kódu, který ničí data.*"[117]

**Kybernetickou bezpečnostní událost** definuje i zákon o kybernetické bezpečnosti v § 7 odst. 1 jako *„**událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací**.*"

De facto **jde o událost bez zatím reálného negativního následku** pro daný komunikační nebo informační systém, ve své podstatě se jedná pouze o hrozbu, která však musí být reálná.

Autoři se zároveň dopouštějí tautologie, neboť vysvětlují událost, jako událost.

---

115: PROSISE, Chris a Kevin MANDIVA. *Incident response & computer forensic, second edition.* Emeryville: McGraw -Hill, 2003, s. 13

Srov. dále CASEY, Eoghan. *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, Second Edition.* London: Academic Press, 2004, s. 9 a násl.

116: JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. 3. aktualiz. vyd. Praha: AFCEA, 2015. s. 28. Dostupné z:
https://nukib.cz/download/aktuality/container-nodeid-665/slovnikkb-cz-en-1505.pdf

117: *Computer Security Incident Handling Guide* [online]. [cit. 13. 8. 2018], s. 6. Dostupné z:
https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf Překlad autora.

Domníváme se, že pojem kybernetická bezpečnostní událost by bylo vhodnější a zřejmě i srozumitelnější označovat a vykládat jako **kybernetickou hrozbu**, neboť zde skutečně pouze existuje potencionální příčina, která může způsobit nežádoucí událost.

**Příklad:** *Uživateli je do interní firemní pošty doručena e-mailová zpráva obsahující v příloze škodlivý kód (malware). Tento malware je však zkomprimován (např. pomocí WinZip) a bez další činnosti uživatele nemůže být nainstalován. Takováto událost ještě sama o sobě nemusí znamenat narušení bezpečnosti, ale je za jistých okolností způsobilá ji narušit.*

### 2.4.3 Kybernetický (bezpečnostní) incident

Jirásek a kol. definují bezpečnostní incident (Security Incident), jako *„porušení nebo bezprostřední hrozbu porušení bezpečnostních politik, bezpečnostních zásad nebo standardních bezpečnostních pravidel provozu Informační a komunikační technologie.“* [118]

Vlastní definici **informačního bezpečnostního incidentu**, pak přináší norma ISO/IEC 27001. V čl. 3.6 této normy je informační bezpečnostní incident definován jako: *„jedna nebo více nechtěných nebo neočekávaných bezpečnostních událostí, u kterých existuje vysoká pravděpodobnost kompromitace činnosti organizace a ohrožení bezpečnosti informací.“*

Velmi podobnou definici **počítačového bezpečnostního incidentu** je také možné nalézt i v příručce NIST, 800-61 Computer Security Incident Handling Guide, která uvádí, že jde o *„porušení nebo bezprostřední hrozbu porušení bezpečnostních politik, politiky akceptovatelného použití (systému, služby) nebo standardní bezpečnostní praxe.“* [119]

**Kybernetický bezpečnostní incident** definuje i zákon o kybernetické bezpečnosti v § 7 odst. 2 jako *„**narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události.**“*

Z dikce zákona tedy vyplývá, že incident může být způsoben jak úmyslným, tak nedbalostním jednáním člověka, ale i vyšší mocí. Podstatné je, že **dojde k narušení bezpečnosti informací, nebo služeb a informačních a komunikačních systémů s nimi spojených.**

---

118: JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. 3. aktualiz. vyd. Praha: AFCEA, 2015. s. 25. Dostupné z: https://nukib.cz/download/aktuality/container-nodeid-665/slovnikkb-cz-en-1505.pdf

119: *Computer Security Incident Handling Guide* [online]. [cit. 17. 2. 2018], s. 6. Dostupné z: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

Kybernetický bezpečnostní incident tak představuje skutečné narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací, tj. narušení informačního nebo komunikačního systému s negativním dopadem.

Za určitou část kybernetických bezpečnostních incidentů jsou zodpovědné i náhodné jevy, chyby hardwaru, softwaru, chyby učiněné při konfiguraci administrátory, chyby uživatelů systémů aj.

**Příklad:** *Navážeme-li na předchozí příklad, pak v okamžiku, kdy uživatel spustí na počítači škodlivý kód, mluvíme již o vzniku bezpečnostního incidentu.*

### 2.4.4 Kybernetický útok (Cyber Attack)

Jirásek a kol. definují kybernetický útok, jako: *„Útok na IT infrastrukturu za účelem způsobit poškození a získat citlivé či strategicky důležité informace. Používá se nejčastěji v kontextu politicky či vojensky motivovaných útoků.“* [120]

Takovéto vymezení kybernetického útoku by bylo značně zužující a nepostihující všechny negativní aktivity uživatelů kyberprostoru[121], zejména z toho důvodu, že kumulativně slučuje podmínky poškození IT a získání informací. Kybernetickým útokem přitom může být i jednání v podobě sociálního inženýrství, kde je jediným cílem získat informace, či naopak útok DoS, či DDoS, kde může být jediným cílem potlačení (tedy nikoliv poškození) funkčnosti jednoho či více počítačových systémů, případně poskytovaných služeb.

Rozdíl mezi kybernetickým bezpečnostním incidentem a kybernetickým útokem primárně spočívá v otázce zavinění. Jak již bylo uvedeno dříve, kybernetický bezpečnostní incident může být způsoben jak úmyslným, tak nedbalostním jednáním člověka, případně vyšší mocí. U kybernetického útoku však jde o úmyslné jednání člověka.

Na základě výše uvedeného je tedy možné **kybernetický útok**[122] definovat jako **jakékoli úmyslné jednání útočníka v kyberprostoru, které směřuje proti zájmům jiné osoby**.

120: JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. 3. aktualiz. vyd. Praha: AFCEA, 2015. s. 71. Dostupné z:
https://nukib.cz/download/aktuality/container-nodeid-665/slovnikkb-cz-en-1505.pdf

121: V uvedené definici chybí zejména vymezení jakékoliv jiné motivace útočníka, než té, která spočívá ve *…způsobení poškození či zisku strategicky důležitých informací.* Jako příklad, který tato definice nepostihuje, lze uvést ekonomicky motivované útoky, jejichž počet v současnosti dramaticky roste.

122: Od pojmu kybernetický útok je třeba odlišit pojem bezpečnostní incident, který představuje narušení bezpečnosti IS/IT a pravidel definovaných k jeho ochraně (bezpečnostní politika).

Kybernetický útok lze také definovat jako jednání útočníka či skupiny útočníků, které využívá informační a komunikační technologie k útoku na jinou informační a komunikační infrastrukturu, ať už s cílem narušit dostupnost, důvěrnost nebo integritu dat.

### 2.4.5 Kyberkriminalita (Cybercrime)

Na závěr pojednání o kybernetických incidentech a útocích považujeme za nutné alespoň rámcově vymezit vztah mezi těmito útoky či incidenty a kyberkriminalitou.

Při vymezení obsahu pojmu **kyberkriminalita** je třeba si uvědomit, že spolu s růstem možností využívání informačních a komunikačních prostředků roste i možnost jejich užívání (zneužívání) k páchání trestné činnosti. Proto v podstatě neexistuje jakási univerzální, obecně přijímaná definice, která by rozsah a hloubku tohoto pojmu plně postihla.

Nejobecněji je možné kyberkriminalitu definovat **jako jednání namířené proti počítačovému systému, počítačové síti, datům či uživatelům nebo jako jednání, při němž je počítačový systém použit jako nástroj pro spáchání trestného činu.** Neopomenutelnou skutečností pro to, aby bylo možné uplatnit definici kyberkriminality, je fakt, že počítačová síť, respektive kyberprostor je pak prostředím, v němž se tato činnost odehrává.

Kyberkriminalita, resp. kybernetická trestná činnost, představuje jakousi nejširší množinu pro veškerou trestnou činnost, ke které dochází v prostředí informačních a komunikačních technologií. Velmi často je přenášena „klasická trestná činnost" do kyberprostoru, neboť je zde tuto trestnou činnost možné páchat rychleji a efektivněji (např. podvody, šíření materiálů zobrazujících zneužívání dětí aj.). Vedle této transpozice známé kriminality pak dochází ke vzniku nových, mnohdy dosud právem neřešených útoků.

Je třeba si uvědomit, že ne každý kybernetický útok musí být trestným činem, ale každý kybernetický trestný čin musí být zároveň kybernetickým útokem. Řadu kybernetických útoků je, i díky absenci trestněprávní normy, možné subsumovat pod jednání, které bude mít povahu správněprávního, či občanskoprávního deliktu, případně se nemusí jednat o jednání, které je postižitelné jakoukoli právní normou (může jít např. pouze o nemorální či netolerované jednání).

*„Proč nám skvělá technika, která šetří práci a usnadňuje život, dosud přinesla tak málo štěstí? Odpověď je prostá: protože jsme se jí nenaučili rozumně užívat."*

Albert Einstein

# 2 Legislativa

# II Legislativa

## 3 Legislativní základ kybernetické bezpečnosti

*„Ten, kdo se ve jménu bezpečnosti vzdává svobody, nezaslouží si ani svobodu, ani bezpečnost."*
Benjamin Franklin

Důvodů pro zavádění a implementaci kybernetické bezpečnosti existuje celá řada. Mezi ty nejběžnější je možné zařadit například negativní ekonomický dopad v případě úspěšného kybernetického útoku, při kterém jsou zcizena citlivá data. Úspěšný kybernetický útok také může ohrozit vlastní chod a fungování organizace, neboť může dojít například k omezení přístupu k počítačovým systémům nebo datům pomocí ransomware. Dalším z důvodů pro zavedení kybernetické bezpečnosti také může být i ztráta kredibility dané napadené organizace aj.

Posledním, avšak o nic méně významným důvodem pro implementaci kybernetické bezpečnosti je respektování právních předpisů a práv a povinností z těchto předpisů vyplývajících. Tento **legislativní důvod** pro mnoho subjektů vyplývá ze zákona o kybernetické bezpečnosti, je však mylné se domnívat, že se jedná o jedinou právní normu, která souvisí s problematikou kybernetické bezpečnosti.

Zejména v posledních letech dochází k masivnímu nárůstu primárně mezinárodní právní úpravy, která se specificky zaměřuje na činnost subjektů (fyzických, právnických osob či států a dalších organizací) v kyberprostoru.

Tato kapitola se bude věnovat legislativnímu vývoji kybernetické bezpečnosti v ČR a základním právním předpisům, které problematiku kybernetické bezpečnosti upravují nebo s ní souvisí.

### 3.1 Legislativní vývoj kybernetické bezpečnosti v ČR

Problematika kybernetické bezpečnosti začala být poprvé systémově státem řešena v roce **2000**. V tomto roce vznikla na Ministerstvu vnitra ČR[123] **Koncepce boje proti trestné činnosti v oblasti informačních technologií včetně Harmonogramu opatření.**[124] Byť se tato koncepce primárně zaměřila na problematiku potírání trestné činnosti v oblasti informačních technologií, je zde možné sledovat snahu státu spočívající ve vytvoření podmínek pro systémový přístup státu k této trestné činnosti.

123: Dále jen **MVČR**

124: *Koncepce boje proti trestné činnosti v oblasti informačních technologií včetně Harmonogramu opatření.* [online]. Dostupné z: http://www.mvcr.cz/soubor/koncepce-pdf.aspx

Vedle potírání kybernetické trestné činnosti se tento dokument vyjadřuje i k otázkám kybernetické bezpečnosti, neboť uvádí, že *„**je zapotřebí vytvořit prostředí pro vzájemnou osvětu** a informační výměnu mezi subjekty, získávajícími poznatky o jednotlivých bezpečnostních aspektech, spojených s používáním nových technologií. **Je úlohou státních orgánů vytvářet stabilní a bezpečné prostředí, které dává občanům oprávněně pocit právní jistoty při využívání moderních informačních a komunikačních prostředků.***

***K získaným poznatkům o jednotlivých obecných i konkrétních bezpečnostních rizicích by měla mít bezprostřední přístup i veřejnost.** K tomuto úkolu je třeba přistoupit aktivně, tedy průběžně provádět preventivně cílenou informační kampaň ve spolupráci všech odpovědných resortů a za účinné participace dalších zainteresovaných subjektů.“* [125]

Uvedená koncepce mimo jiné stanovila požadavek, aby byl vypracován projekt hlásného systému pro trestnou činnost v oblasti informačních technologií; iniciován a podporován vznik a činnost skupin typu CERT (Central Emergency Response Team).[126] Gestorem této problematiky byl primárně odbor bezpečnostní politiky MVČR, který spolupracoval s dalšími odbory MVČR, Policejním prezidiem, Úřadem vyšetřování, Kriminalistickým ústavem, Policejní akademií ČR a dalšími subjekty.

V roce **2004** byl představen dokument **Státní informační a komunikační politika e-Česko 2006.**[127] Tento dokument byl schválen usnesením vlády ČR č. 265 ze dne 24. března 2004 a definoval následující prioritní oblasti z pohledu státu:

- **dostupné a bezpečné komunikační služby,**
- **informační vzdělanost,**
- **moderní veřejné služby on-line (např. e-government; e-zdravotnictví aj.),**
- **dynamické prostředí pro elektronické podnikání.**

Z uvedených priorit byla významnou oblastí oblast bezpečnosti elektronických komunikací, kde si stát kladl za cíl zejména:

- *do konce roku 2004:* ustanovit pracovní skupinu pro boj s počítačovou kriminalitou,
- *do konce roku 2004:* zpracovat Národní strategii informační bezpečnosti,
- *průběžně:* vybavit postupně čipovými kartami vedoucí a odborné pracovníky veřejné správy,

125: *Koncepce boje proti trestné činnosti v oblasti informačních technologií včetně Harmonogramu opatření.* [online]. [cit. 13. 8. 2018], s. 3. Dostupné z: http://www.mvcr.cz/soubor/koncepce-pdf.aspx

126: Blíže viz *Koncepce boje proti trestné činnosti v oblasti informačních technologií včetně Harmonogramu opatření.* [online]. [cit. 13. 8. 2018], s. 6. Dostupné z: http://www.mvcr.cz/soubor/koncepce-pdf.aspx

127: *Státní informační a komunikační politika e-Česko 2006.* [online]. Dostupné z: http://www.culturenet.cz/res/data/002/000269.pdf

- *do konce roku 2005:* umožnit spolehlivé a bezpečné propojení orgánů veřejné správy,
- *do konce roku 2006:* definovat, legislativně ošetřit a následně zavést do praxe jednotný bezvýznamový národní identifikátor.

V roce **2005** došlo v návaznosti na novelu „Státní informační a komunikační politiky: e-Česko 2006" a na dokument „Bezpečnostní strategie ČR"(schválena usnesením vlády ČR č. 1254 ze dne 10. prosince 2003) ke vzniku **Národní strategie informační bezpečnosti ČR.**[128] Gestorem této problematiky bylo nejprve Ministerstvo informatiky a po jeho zániku převzaly jeho úkoly MVČR, Ministerstvo průmyslu a obchodu a Ministerstvo pro místní rozvoj.

Tato národní strategie si stanovila následujících šest cílů:

1) zlepšení řízení informační bezpečnosti a řízení rizik,
2) rozvoj znalostí o informační bezpečnosti,
3) podpora národní a mezinárodní spolupráce v oblasti informační bezpečnosti,
4) podpora používání nejlepší praxe v oblasti informační bezpečnosti,
5) podpora ochrany lidských práv a svobod,
6) podpora konkurenceschopnosti české ekonomiky.

V rámci prvního cíle, který bezprostředně souvisel s problematikou kybernetické bezpečnosti, byla definována následující opatření, v rámci kterých bylo třeba:

- zavést nejlepší praxe do systémů řízení informační bezpečnosti,
- soustavně monitorovat hrozby,
- **realizovat systém včasného varování a reakce** (v rámci tohoto opatření mělo dojít i k ustanovení centra pro řízení, monitoring a analýzu bezpečnostního prostředí informačních a komunikačních systémů ČR),
- monitorovat účinnost navržených protiopatření,
- zlepšit informační bezpečnost orgánů veřejné správy,
- ochránit kritickou informační infrastrukturu státu.[129]

V roce **2005** byl také usnesením vlády č. 1466 schválen **Národní akční plán boje proti terorismu (Aktualizované znění pro léta 2005–2007)**. V rámci tohoto akčního plánu byla řešena i problematika *Koncepce boje proti trestné činnosti v oblasti informačních technologií* a byl vypracován

128: *Národní strategie informační bezpečnosti ČR. NSIB. Verze: 0.8. 4. 10. 2005.* [online]. Dostupné z: http://www.micr.cz/scripts/detail.php?id=2470 či https://moodle.unob.cz/pluginfile.php/20182/mod_resource/content/1/N%C3%A1rodn%C3%AD%20strategie%20informa%C4%8Dn%C3%AD%20bezpe%C4%8Dnosti%20%C4%8CR.pdf

129: Blíže viz *Národní strategie informační bezpečnosti ČR. NSIB. Verze: 0.8. 4. 10. 2005.* [online]. [cit. 13. 8. 2018], s. 6. Dostupné z: http://www.micr.cz/scripts/detail.php?id=2470

materiál *Aktuální úroveň zajištění kybernetické bezpečnosti České republiky.* Tento dokument vztahující se ke kybernetické bezpečnosti byl v roce 2007 předložen Bezpečnostní radě státu, která jej opakovaně vrátila ministru vnitra k dopracování, přičemž upravený text dokumentu byl opětovně předložen Bezpečnostní radě státu v letech 2008, 2009 a 2010. Jako nejvhodnější završení řešení stávajícího stavu bylo navrhováno vytvoření specializovaného *Centra pro studium kybernetických hrozeb.*[130]

Dokument **Koncepce boje proti trestné činnosti v oblasti informačních technologií včetně Harmonogramu opatření** byl v roce 2008 nahrazen **Koncepcí boje proti organizovanému zločinu (2000).**[131] Aktualizovaná koncepce boje proti organizovanému zločinu již více reflektovala nárůst kybernetické trestné činnosti a kybernetických hrozeb.

V roce 2010 bylo přijato usnesení vlády č. 205, které se věnuje Řešení problematiky kybernetické bezpečnosti České republiky.[132] Toto usnesení ustanovilo MVČR gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast. Ministru vnitra bylo dále uloženo:

1) koordinovat činnost ostatních státních institucí v oblasti zajišťování kybernetické bezpečnosti,
2) koordinovat zastupování České republiky v otázkách kybernetické bezpečnosti na mezinárodních fórech, včetně účasti státních orgánů na činnosti příslušných mezinárodních organizací,
3) do 30. dubna 2010 předložit vládě ke schválení statut meziresortní koordinační rady pro kybernetickou bezpečnost,
4) do 15. prosince 2010 předložit vládě strategii pro oblast kybernetické bezpečnosti,
5) nejpozději k 31. prosinci 2010 zahájit zajišťování provozu vládního pracoviště CSIRT (Computer Security Incident Response Team).

Dne **19. října 2011** přijala vláda České republiky usnesení č. 781 o ustavení Národního bezpečnostního úřadu gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast.[133] Současně tímto usnesením Vláda ČR zřídila **Radu pro kybernetickou**

130: Blíže viz *Koncepce boje proti organizovanému zločinu (2000).* [online]. s. 22 a násl. Dostupné z: https://www.databaze-strategie.cz/cz/mv/strategie/koncepce-boje-proti-organizovanemu-zlocinu?typ=download

131: *Koncepce boje proti organizovanému zločinu (2000).* [online]. Dostupné z: https://www.databaze-strategie.cz/cz/mv/strategie/koncepce-boje-proti-organizovanemu-zlocinu?typ=download

132: *USNESENÍ VLÁDY ČESKÉ REPUBLIKY ze dne 15. března 2010 č. 205 o řešení problematiky kybernetické bezpečnosti České republiky.* [online]. Dostupné z: https://apps.odok.cz/attachment/-/down/KORN97BQ9ASZ

133: *USNESENÍ VLÁDY ČESKÉ REPUBLIKY ze dne 19. října 2011 č. 781 o ustanovení Národního bezpečnostního úřadu gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast.* [online]. Dostupné z: https://apps.odok.cz/attachment/-/down/KORN97BUKZ3E

**bezpečnost** [134] a schválila vznik **Národního centra kybernetické bezpečnosti** (jakožto součásti NBÚ). Vedle toho Vláda ČR uložila řadu úkolů jak jednotlivým ministerstvům, tak NBÚ. Mezi nejvýznamnější úkoly, kterými byl NBÚ pověřen, patřilo:

1) předložit do 31. března 2012
   - aktualizovanou *Strategii pro oblast kybernetické bezpečnosti České republiky na období let 2011 až 2015,*
   - aktualizovaný *Akční plán opatření ke Strategii pro oblast kybernetické bezpečnosti České republiky na období let 2011 až 2015,*
   - návrh věcného záměru zákona o kybernetické bezpečnosti. Vlastní návrh zákona měl být předložen do 31. července 2013.

2) **vybudovat do 31. prosince 2015 plně funkční Národní centrum kybernetické bezpečnosti a** jako jeho součást vládní koordinační místo pro okamžitou reakci na počítačové incidenty (**vládní CERT** - Computer Emergency Response Team)

V roce **2011** byla přijata **Strategie pro oblast kybernetické bezpečnosti České republiky na období let 2011 až 2015**[135] a **akční plán k této strategii.** Nicméně díky převodu gesce z MVČR na NBÚ je tato strategie častěji označována jako: **Strategie pro oblast kybernetické bezpečnosti České republiky na období let 2012 až 2015.**[136]

V předložené strategii byly vytýčeny následující strategické cíle a opatření:

- vytvoření legislativního rámce,
- vybudování Národního centra kybernetické bezpečnosti a vládního pracoviště CERT,
- ochrana kritických informačních infrastruktur,
- posilování kybernetické bezpečnosti informačních a komunikačních systémů veřejné správy,
- zefektivnění potírání kriminality v kybernetickém prostoru,
- koordinace aktivit k zajištění kybernetické bezpečnosti v Evropě,
- používání spolehlivých a důvěryhodných informačních technologií,
- zvyšování povědomí o kybernetické bezpečnosti,
- odezva na kybernetické útoky.

134: Tato rada je poradním orgánem předsedy vlády pro oblast kybernetické bezpečnosti.

135: *Strategie pro oblast kybernetické bezpečnosti České republiky na období let 2011 až 2015.* [online]. Dostupné z: https://www.databaze-strategie.cz/cz/cr/strategie/strategie-pro-oblast-kyberneticke-bezpecnosti-cr-2011-2015?typ=struktura

136: *Strategie pro oblast kybernetické bezpečnosti České republiky na období 2012–2015.* [online]. Dostupné z: https://www.govcert.cz/download/legislativa/container-nodeid-719/20120209strategieprooblastkbnbu.pdf

Vedle přípravy strategie a akčního plánu kybernetické bezpečnosti ČR se Národní bezpečnostní úřad od října 2011 plně pustil do přípravy věcného záměru zákona o kybernetické bezpečnosti.[137] Tento věcný záměr zákona byl vládou schválen usnesením č. 382 ze dne 30. května 2012. Dne 15. dubna 2013 rozeslal NBÚ do meziresortního připomínkového řízení návrh zákona o kybernetické bezpečnosti.

Na přípravě návrhu pracovala odborná komise vedená NBÚ a složená ze zástupců Ministerstva vnitra, Ministerstva obrany, ČTÚ a dalších příslušných institucí. Začátkem roku 2013 úřad konzultoval návrh po dobu dvou měsíců s odbornou veřejností.

Je třeba dodat, že takto otevřený přístup není v podmínkách ČR zcela běžný, o to víc je však ceněn.

Dne 28. června 2013 předložil NBÚ návrh zákona o kybernetické bezpečnosti Vládě České republiky. Následný legislativní proces proběhl bez významnějších připomínek a **zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů** (zákon o kybernetické bezpečnosti) vstoupil v platnost dne 29. srpna 2014 s účinností od **1. ledna 2015.**

Současně se zákonem byly vypracovávány i prováděcí právní předpisy, konkrétně:

- vyhláška č. 316/2014, o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (**vyhláška o kybernetické bezpečnosti**);
- **vyhláška** č. 317/2014, **kterou se stanoví významné informační systémy a jejich určující kritéria**;
- **vyhláška** č. 315/2014, novela nařízení vlády č. 432/2010 Sb., **o kritériích pro určení prvku kritické infrastruktury**.

Veškeré prováděcí předpisy nabyly účinnosti současně se zákonem o kybernetické bezpečnosti.

V srpnu 2015 byl na základě požadavků stanovených v ZoKB vybrán provozovatel Národního CERT týmu. Tímto provozovatelem se stalo sdružení CZ.NIC.[138] Dne 18. prosince 2015 pak došlo k podpisu Veřejnoprávní smlouvy o zajištění činnosti Národního CERT a o spolupráci v oblasti kybernetické bezpečnosti.[139] Tato smlouva byla uzavřena na dobu neurčitou.

137: Viz *Věcný záměr zákona o kybernetické bezpečnosti*. [online]. Dostupné z: https://www.govcert.cz/download/legislativa/container-nodeid-926/vecny-zamer-final-vlada.pdf

138: Viz https://www.nic.cz/page/351/

139: Blíže viz [online]. Dostupné z: https://www.nic.cz/files/nic/doc/NBU-Smlouva-narodni-cert-201512.pdf

Zákon o kybernetické bezpečnosti od roku 2015, kdy nabyl účinnosti, prošel dvěma obsahově významnými novelizacemi.

První novelizace byla provedena zákonem č. 104/2017 Sb.,[140] s účinností od 1. července 2017. Tato novela rozšířila okruh povinných osob spadajících pod ZoKB o provozovatele informačních systémů a dále upravila některé sankce.

Druhá obsahově významnější novelizace byla provedena zákonem č. 205/2017 Sb.,[141] s účinností od 1. srpna 2017. Touto novelou byla do ZoKB implementována **Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (NIS)** a zároveň byl zřízen **Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB)**, který po NBÚ převzal práva a povinnosti v oblasti kybernetické bezpečnosti včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany. NÚKIB je ve výše uvedených oblastech ústředním správním orgánem. Vedle těchto oblastí má NÚKIB na starosti také problematiku neveřejné služby v rámci družicového systému Galileo.

Aktuální znění zákona o kybernetické bezpečnosti je účinné od 7. března 2018.

V souvislosti s těmito novelami došlo i k novelizaci prováděcích právních předpisů a vytvoření předpisu nového. Konkrétně se jedná o:

- vyhlášku č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (**vyhláška o kybernetické bezpečnosti**);
- vyhlášku č. 437/2017 Sb., **o kritériích pro určení provozovatele základní služby**.

140: Zákon č. 104/2017 Sb., kterým se mění zákon č. 365/2000 Sb., **o informačních systémech veřejné správy** a o změně některých dalších zákonů, ve znění pozdějších předpisů, zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), a některé další zákony. [online]. Dostupné z: https://www.zakonyprolidi.cz/cs/2017-104

141: Zákon č. 205/2017 Sb., **kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti** a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění zákona č. 104/2017 Sb., a některé další zákony. [online]. Dostupné z: https://www.zakonyprolidi.cz/cs/2017-205

Současně s novelizací právních předpisů byla také přijata **Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020**[142] a její **Akční plán.**[143] Mezi hlavní cíle Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020 patří:

- zajištění efektivity a posilování všech struktur, procesů a spolupráce při zajišťování kybernetické bezpečnosti,
- aktivní mezinárodní spolupráce,
- ochrana národní KII a VIS,
- spolupráce se soukromým sektorem,
- výzkum a vývoj / spotřebitelská důvěra,
- podpora vzdělávání, osvěta a rozvoj informační společnosti,
- podpora rozvoje schopností Policie České republiky vyšetřovat a postihovat informační kriminalitu,
- právní úprava pro kybernetickou bezpečnost (vytváření právního rámce), účast na tvorbě a implementaci evropských a mezinárodních pravidel.

Z výše popsaných změn je zřejmá snaha státu jednak o zajištění kybernetické bezpečnosti klíčových prvků a služeb, na nichž jsou stát, organizace či uživatelé přímo závislí. Zároveň lze také pozorovat výraznou snahu o zvyšování obecného povědomí o kybernetických útocích, kybernetické bezpečnosti, právech a povinnostech jednotlivých dotčených subjektů i běžných uživatelů.

## 3.2 Právní normy vztahující se ke kybernetické bezpečnosti

Snahy o řešení problematiky kybernetické bezpečnosti je možné vypozorovat de facto již od počátku využívání informačních a komunikačních technologií. Postupně v této oblasti docházelo k přijímání doporučení, standardů, či technických norem, které zpravidla definovaly minimální požadavky zaručující určitou úroveň bezpečnosti.

Oblast kybernetické bezpečnosti se značně liší od jiných oblastí, na které jsou aplikovány standardní principy bezpečnosti ve světě reálném. Ona odlišnost spočívá především v možnosti dynamického vývoje a okamžité změny kybernetických útoků a hrozeb (většina hrozeb ve světě reálném zůstává relativně neměnná), což ve vztahu k legislativě může přinášet určité problémy.

142: Blíže viz: [online]. Dostupné z:
https://www.govcert.cz/download/gov-cert/container-nodeid-998/nskb-150216-final.pdf

143: Blíže viz: *Akční plán k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020.* [online]. Dostupné z:
https://www.govcert.cz/download/gov-cert/container-nodeid-967/akc48dnc3adplc3a1n-rkb-final-150408.pdf

Právní regulace této oblasti musí být na jednu stranu dostatečně obecná, aby umožňovala efektivně reagovat na dílčí negativní kybernetické jevy bez nutnosti jejich detailní specifikace, na druhou stranu však nesmí být příliš vágní, aby nezasáhla do práv a oprávněných zájmů osob ve větší míře, než je nezbytně nutné.

Před vlastní analýzou stávající platné a účinné legislativy v oblasti kybernetické bezpečnosti je třeba podotknout, že nejen v rámci Evropské unie je zřetelná snaha po implementaci účinnějších právních nástrojů, které by zvyšovaly kvalitu kybernetické bezpečnosti a umožnily adekvátně reagovat na kybernetické hrozby a útoky. V současnosti dochází k postupnému odstraňování rozporů a nedostatků v právních normách členských států EU a dalších států, které se rozhodly aktivně zapojit do vytváření kybernetické bezpečnosti.

*„**Způsoby ochrany dat a informačních systémů jsou dnes předmětem nejednoho vědního výzkumu, ovšem toliko technická ochrana těchto systémů a dat bez právního podkladu může být neefektivní v důsledku nejasného vymezení, kam až je možno při takové ochraně zajít.** V tomto kontextu se naplno projevuje nesoulad právních úprav jednotlivých států s právními úpravami států ostatních. Díky rozvoji počítačových a informačních technologií, které udávají mezinárodní charakter kybernetických trestných činů, je efektivní ochrana počítačových systémů a dat nemyslitelná bez existence mezinárodního resp. nadnárodního právního rámce, a to nejen mezi členskými státy EU, ale v celosvětovém měřítku.“*[144]

### 3.2.1 Dokumenty EU/ES sloužící k harmonizaci právních úprav při řešení problematiky kybernetické bezpečnosti

Zejména díky specifičnosti spočívající v neohraničenosti kyberprostoru a potřebě účinné mezinárodní spolupráce se EU snaží sblížit právní úpravu jednotlivých členských států tak, aby bylo možné efektivně řešit problematiku kybernetické bezpečnosti.

Prostředkem pro sbližování práva jednotlivých zemí EU jsou především nařízení, směrnice, rámcová rozhodnutí a další dokumenty EU/ES. Z pohledu kybernetické bezpečnosti jsou nejvýznamnějšími následující dokumenty:

***Primární právo EU***

- Listina základních práv Evropské unie

144: KOLOUCH, Jan a Petr VOLEVECKÝ. *Trestněprávní ochrana před kybernetickou kriminalitou.* Praha: Policejní akademie České republiky v Praze, 2013, s. 65

***Směrnice Evropského parlamentu a Rady***

- 91/250/EHS o právní ochraně počítačových programů
- 98/34/ES o postupu při poskytování informací v oblasti norem a technických předpisů, ve znění směrnice 98/48/ES
- 1999/5/ES o rádiových zařízeních a telekomunikačních koncových zařízeních a vzájemném uznávání jejich shody
- 2000/31/ES o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu (směrnice o elektronickém obchodu)
- 2002/19/EC o přístupu k sítím elektronických komunikací a přidruženým zařízením a o jejich propojení (přístupová směrnice)
- 2002/20/ES o oprávnění pro sítě a služby elektronických komunikací (autorizační směrnice), ve znění směrnice 2009/140/ES
- 2002/21/ES o společném předpisovém rámci pro sítě a služby elektronických komunikací (rámcová směrnice), ve znění směrnice 2009/140/ES
- 2002/22/EC o universální službě a uživatelských právech týkajících se sítí a služeb elektronických komunikací (směrnice o universální službě)
- 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací
- 2006/24/ES o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí
- 2008/114/ES o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu
- 2011/93/EU o boji proti pohlavnímu zneužívání a pohlavnímu vykořisťování dětí a proti dětské pornografii, kterou se nahrazuje rámcové rozhodnutí Rady 2004/68/SVV
- 2013/11/EU o alternativním řešení spotřebitelských sporů a o změně nařízení (ES) č. 2006/2004 a směrnice 2009/22/ES (směrnice o alternativním řešení spotřebitelských sporů)
- 2013/40/EU o útocích na informační systémy a nahrazení rámcového rozhodnutí Rady 2005/222/SVV
- 2015/1535 o postupu při poskytování informací v oblasti technických předpisů a předpisů pro služby informační společnosti
- 2015/2366 o platebních službách na vnitřním trhu, kterou se mění směrnice 2002/65/ES, 2009/110/ES a 2013/36/EU a nařízení (EU) č. 1093/2010 a zrušuje směrnice 2007/64/ES („revidovaná směrnice o platebních službách“)
- 2016/680 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV
- 2016/1148 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (**NIS**)

*Nařízení Evropského parlamentu a Rady*

- 460/2004/ES o zřízení Evropské agentury pro bezpečnost sítí a informací ve znění nařízení č. 1007/2008
- 1077/2011/ES kterým se zřizuje Evropská agentura pro provozní řízení rozsáhlých informačních systémů v prostoru svobody, bezpečnosti a práva
- 526/2013 o Agentuře Evropské unie pro bezpečnost sítí a informací (**ENISA**) a o zrušení nařízení (ES) č. 460/2004 Text s významem pro EHP
- 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (**eIDAS**[145])
- 679/2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů - **GDPR**)
- **Návrh nařízení** o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích a o zrušení směrnice 2002/58/ES (nařízení o soukromí a elektronických komunikacích – **ePrivacy**)[146]

*Rozhodnutí Rady*

- 92/242/EHS o bezpečnosti informačních systémů
- 2005/222/SVV o útocích proti informačním systémům
- 2011/292/EU o bezpečnostních pravidlech na ochranu utajovaných informací EU

*Další dokumenty*

- Úmluva Rady Evropy č. 185 o kybernetické kriminalitě
- Dodatkový protokol Rady Evropy č. 189 k Úmluvě o kyberkriminalitě
- Úmluva Rady Evropy č. 196 o prevenci terorismu
- Prováděcí nařízení Komise (EU) 2018/151, kterým se stanoví pravidla pro uplatňování směrnice Evropského parlamentu a Rady (EU) 2016/1148, pokud jde o bližší upřesnění prvků, které musí poskytovatelé digitálních služeb zohledňovat při řízení bezpečnostních rizik, jimž jsou vystaveny sítě a informační systémy, a parametrů pro posuzování toho, zda je dopad incidentu významný

*Mezinárodní normy*

- ISMS řady ISO/IEC 27000
- v ČR ČSN ISO/IEC 27001:2014

145: Dále jen **eIDAS**

146: [online]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52017PC0010

### 3.2.2 Právní normy ČR

V současné době je problematika kybernetické bezpečnosti specificky řešena zákonem o kybernetické bezpečnosti, nicméně dílčí aspekty ochrany České republiky před kybernetickými útoky je možné nalézt i v jiných právních předpisech. Z pohledu kybernetické bezpečnosti jsou nejvýznamnějšími následující dokumenty:

***Ústavní zákony***

- Ústavní zákon č. 1/1993 Sb., Ústava České republiky, ve znění pozdějších předpisů
- Ústavní zákon č. 2/1993 Sb., Listina základních práv a svobod, ve znění pozdějších předpisů[147]
- Ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky

***Zákony***

- zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů
- zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů[148]
- zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů
- zákon č. 240/2000 Sb., o krizovém řízení a změně některých zákonů (krizový zákon), ve znění pozdějších předpisů
- zákon č. 365/2000 Sb., o informačních systémech veřejné správy, ve znění pozdějších předpisů
- zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti), ve znění pozdějších předpisů[149]
- zákon č. 127/2005 Sb., o elektronických komunikacích, ve znění pozdějších předpisů[150]
- zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů[151]
- zákon č. 69/2006 Sb., o provádění mezinárodních sankcí, ve znění pozdějších předpisů
- zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů

147: Dále jen Listina základních práv a svobod či **Listina**.

148: Dále jen zákon o ochraně osobních údajů či **ZoOU**. V souvislosti s účinností GDPR dojde k rekodifikaci tohoto zákona a předpokládá se, že bude nahrazen zákonem o zpracování osobních údajů. Blíže viz např. [online]. Dostupné z: https://apps.odok.cz/veklep-detail?pid=KORNAQCDZPW5

149: Dále jen zákon o některých službách informační společnosti či **ZSIS**.

150: Dále jen **ZoEK**

151: Dále jen **ZoOUI**

- zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů[152]
- zákon č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů
- zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim
- zákon č. 89/2012 Sb., občanský zákoník
- **zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)**
- zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce

***Prováděcí předpisy***

- nařízení vlády č. 522/2005 Sb., kterým se stanoví seznamy utajovaných informací, ve znění pozdějších předpisů
- vyhláška č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor, ve znění pozdějších předpisů
- vyhláška č. 529/2006 Sb., o požadavcích na strukturu a obsah informační koncepce a provozní dokumentace a o požadavcích na řízení bezpečnosti a kvality informačních systémů veřejné správy (vyhláška o dlouhodobém řízení informačních systémů veřejné správy)
- **nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury**
- vyhláška 357/2012 Sb., o uchovávání, předávání a likvidaci provozních a lokalizačních údajů
- **vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích**
- **vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby**
- **vyhláška č. 82/2018 Sb.**, o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (**vyhláška o kybernetické bezpečnosti**)

## 3.3 Exkurze do práv a povinností vyplývajících z některých právních norem

Před vlastním výkladem a rozborem jednotlivých ustanovení zákona o kybernetické bezpečnosti považujeme za nezbytné alespoň rámcově vymezit vztah některých významných právních dokumentů EU/ES a ČR právě k problematice kybernetické bezpečnosti. Pozornost bude konkrétně věnována GDPR, ePrivacy, občanskému a trestnímu zákoníku.

Jsme bytostně přesvědčeni o tom, že **není vhodné odděleně řešit problematiku kybernetické bezpečnosti a dalších oblastí** (např. ochrany osobních údajů, dat souvisejících s elektronickými komunikacemi a jiných obdobných dat).

152: Dále jen trestní zákoník, či **TZK**.

Důvod pro toto přesvědčení spočívá ve stále větší integraci a vzájemné provázanosti různých kategorií dat s počítačovými systémy a aplikacemi v nich provozovanými. Tato provázanost a digitalizace analogových dat do budoucna jen poroste.

Z tohoto důvodu se jako vhodné východisko jeví řešit problematiku bezpečnosti komplexně, a ne jen v souvislosti s právy a povinnostmi vyplývajícími ze zákona o kybernetické bezpečnosti, či z jiného právního předpisu.

Cílem organizace či jednotlivce by mělo být zavedení takových pravidel, procesů, postupů a bezpečnostních opatření, která budou splňovat jak požadavky vyplývající ze ZoKB, tak i například z GDRP, ePrivacy, eIDAS, ZoEK aj. Takovýto postup umožní vytvořit **integrovanou bezpečnost**.[153]


Obrázek 14: Ukázka řešení integrované bezpečnosti[154]

153: Blíže viz např. GREENFIELD, David. *Integrovaná bezpečnost: Už nastal její čas?* [online]. [cit. 1. 3. 2018]. Dostupné z: http://www.controlengcesko.com/hlavni-menu/artykuly/artykul/article/integrovana-bezpecnost-uz-nastal-jeji-cas/

154: *Integrovaná multidisciplinární bezpečnost.* [online]. [cit. 17. 2. 2018]. Dostupné z: https://www2.deloitte.com/cz/cs/pages/risk/solutions/integrovana-multidisciplinarni-bezpecnost.html

### 3.3.1 GDPR

Obecné nařízení o ochraně osobních údajů (EU) 2016/679 (anglicky: General Data Protection Regulation neboli GDPR)[155] je jedním z významných mezinárodních právních dokumentů, který s problematikou kybernetické bezpečnosti bezprostředně souvisí, byť není primárně cílen do oblasti ICT.

„***GDPR ≠ IT + software.***
*Nové nařízení o ochraně osobních údajů má 778 řádků a z toho jen 26 se přímo týká IT bezpečnosti. Máte představu, co obsahují ty ostatní?*"

Mgr. Eva Škorničková[156]

Právě na GDPR a implementaci povinností z tohoto nařízení vyplývajících je možné demonstrovat tu skutečnost, že je vhodné řešit komplexně problematiku bezpečnosti, a ne uměle izolovat povinnosti vyplývající z různých právních norem (v tomto případě ze zákona o kybernetické bezpečnosti a GDPR).

Cílem této publikace není provést samostatný a komplexní rozbor problematiky GDPR. Na tomto místě budou definovány pouze dílčí pojmy a práva a povinnosti, které z GDPR vyplývají a zároveň mají přesah do oblasti kybernetické bezpečnosti.

Nařízení GDPR představuje **obecný právní rámec ochrany osobních údajů** platný a účinný na celém území EU a v určitých případech i mimo toto teritorium.[157] Hlavním cílem GDPR je zajistit komplexní ochranu práv subjektů údajů proti neoprávněnému zacházení s jejich daty a osobními údaji, nastolit rovnováhu mezi oprávněnými zájmy správců, zpracovatelů a subjektů údajů, vytvořit systém jednotné vymahatelnosti práva a jednotného sankčního mechanismu v této oblasti atd.

„***Ač ochrana osobních údajů u nás platí od roku 1992****, ač úřad zřízený zákonem o ochraně osobních údajů kontroluje povinnosti tímto zákonem uložené už téměř dvě desetiletí,* ***pro mnohé, kteří si se zákonem starosti nedělali, jako by šlo o novou věc.***"[158]

155: [online]. Dostupné z:
http://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32016R0679&qid=1488972453767&from=CS

156: ŠKORNIČKOVÁ, Eva. *Jednoduchý test: Jak jste na tom s přípravou na GDPR?* [online]. [cit. 10. 11. 2017]. Dostupné z: *https://www.gdpr.cz/blog/jednoduchy-test-jak-jste-na-tom-s-pripravou-na-gdpr/*

157: Blíže viz kap. 3.3.1.1 Místní působnost GDPR

158: *GDPR stručně.* [online]. [cit. 7. 8. 2018]. Dostupné z:
https://www.uoou.cz/gdpr%2Dstrucne/ds-4843/archiv=0&p1=3938

Listina základních práv a svobod v čl. 10 odst. 2 a 3 uvádí:

„*Každý má* ***právo na ochranu před neoprávněným zasahováním do soukromého a rodinného života.***"

„*Každý má* ***právo na ochranu před NEOPRÁVNĚNÝM shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě.***"

Další ochranu osobních údajů zajišťuje zákon č. 101/2000 Sb., o ochraně osobních údajů či například zákon č. 89/2012 Sb., občanský zákoník[159], zákon č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách), zákon č. 85/1996 Sb., o advokacii, zákon č. 127/2005 Sb., o elektronických komunikacích, ve znění pozdějších předpisů, aj.

Bylo by tedy teoreticky možné konstatovat, že ochrana osobních údajů, jakož i osob, kterých se tyto údaje týkají, zde existovala a existuje. Nicméně rychlý technologický rozvoj a globalizace (zejména dat a služeb v oblasti ICT) s sebou nutně přinesly nové výzvy i pro oblast ochrany osobních údajů.

Rozsah shromažďování a sdílení osobních údajů právě díky informačním a komunikačním technologiím a službám, které jsou na ně navázány, významně vzrostl. Informační a komunikační technologie umožňují jak soukromým společnostem, tak orgánům veřejné moci využívat při provádění jejich činností osobní údaje v nebývalém rozsahu. Na druhou stranu je také možné pozorovat masivní dobrovolné zveřejňování osobních údajů samotnými fyzickými osobami, jichž se tyto údaje týkají.

Informační a komunikační technologie výrazně změnily ekonomiku i společenský život a měly by usnadňovat volný pohyb osobních údajů v rámci Evropské unie a předávání těchto údajů do třetích zemí a mezinárodním organizacím. Současně by však tyto technologie a procesy s nimi spojené měly zajistit vysokou úroveň ochrany osobních údajů.[160]

159: Viz kap. 3.3.3 Občanský zákoník

160: Srov. recitál 6 GDPR

Díky výše uvedenému však **vzniká zajímavý paradox**, který spočívá v následujících bodech:

- **fyzické osoby samy a dobrovolně o sobě zveřejňují stále větší množství dat** (fotografie, videa aj.), přičemž k distribuci těchto dat typicky využívají služby informační společnosti, které jsou založeny na EULA[161] či SLA[162] mezi uživatelem a poskytovatelem služby,

- **nejvíce jsou osobní údaje zveřejňovány v rámci sociálních sítí**, které z podstaty své funkce takovéto zveřejňování předpokládají a zakotvují ve smluvních podmínkách pravidla, na základě kterých je s takovýmito daty zacházeno,

- **fyzické osoby při využívání řady služeb informační společnosti předpokládají, a mnohdy i očekávají interakci mezi těmito technologiemi a jejich kyberosobností,**[163]

- mezinárodní společenství, stát, ale i **fyzické osoby** samy **vyžadují vyšší zabezpečení osobních údajů a znemožnění přístupu k těmto údajům jiným** (zpravidla neoprávněným) **subjektům, a to vše za podmínky zachování existence prvních tří bodů tohoto paradoxu.**

Důsledek tohoto paradoxu je zřejmý. Poskytovatelé služeb informační společnosti[164] tak musí věnovat vyšší úsilí zabezpečení jednotlivých služeb, které koncovému uživateli poskytují, vyšší úrovni zabezpečení dat vztahujících se k uživateli, modifikaci stávajících smluvních podmínek a zavedení dalších požadavků vyplývajících z GDPR.

---

161: **EULA** (**E**nd **U**sers **L**icence **A**greement) je označení pro smluvní podmínky, umožňující využití služby daného poskytovatele služby. EULA představuje smlouvu, která je zpravidla jednostranně vymezena poskytovatelem služby. Uživatel však není nikterak omezován na svých právech, neboť má možnost volby v podobě nevyužití takto jednostranně stanovených smluvních podmínek. V případě souhlasu s využíváním takovýchto služeb je možné obecně konstatovat, že dojde primárně k aplikaci soukromoprávních norem.

Otázkou je, zda si uživatel skutečně uvědomuje, jaké smluvní podmínky odsouhlasil, kdy se pro něj stávají závaznými a jaký možný (legální) zásah do jeho základních lidských práv a svobod takto vyslovený souhlas představuje. Další neopomenutelnou skutečností pak je, že takto poskytovaná služba může ovlivnit práva a oprávněné zájmy (např. bezpečnost IT, důvěryhodnost dat aj.) třetích osob (např. zaměstnavatele aj.), které k využívání předmětné služby explicitně souhlas nevyjádřily. Smutným faktem zůstává ta skutečnost, že velmi malé procento uživatelů je ochotno číst smluvní podmínky, vztahující se k té které poskytované službě.

162: **SLA** (**S**ervice-**L**evel **A**greement) označuje smlouvu sjednanou mezi poskytovatelem služby a jejím uživatelem.

163: Viz kap. 1 Kyberprostor (Cyberspace). **Tuto interakci je možné sledovat při využívání polohových a geolokačních služeb** (např. Google Maps, Waze, Seznam mapy aj.), neboť fyzická osoba předpokládá, že ji bude počítačový systém schopen lokalizovat a zobrazit jí nejvýhodnější cestu. Stejně tak je ona interakce očekávána např. **u služeb umožňujících prodej a nákup zboží** (např. Letgo – viz doporučené inzeráty dle geolokace či již nakoupeného zboží), **restauračních a ubytovacích službách** (např. Tripadvisor, Booking.com, Airbnb aj.) aj.

164: Blíže viz KOLOUCH, Jan. *CyberCrime.* Praha: CZ.NIC, 2016, s. 78 a násl. a s. 109 a násl.

### 3.3.1.1 Místní působnost GDPR

Někoho by mohlo napadnout, že způsobem, jak se vyhnout GDPR, by bylo přesunout se mimo jeho dosah, tedy mimo teritorium EU. Nařízení GDPR se však uplatní v případech, kdy:

- **provozovna správce nebo zpracovatele je v EU**, bez ohledu na to, zda zpracování probíhá v EU,
- **správci nebo zpracovatelé nejsou usazení v EU**, **ale**
  - zboží nebo služby jsou nabízeny subjektům údajů v EU (bez ohledu na úplatu),
  - je monitorováno chování subjektů údajů v rámci EU.[165]

Díky takto vymezené místní působnosti má GDPR exteritoriální dosah a de facto se bude vztahovat na všechny služby informační společnosti, ke kterým lze získat přístup z geografického teritoria EU, nebo které monitorují chování subjektů údajů v rámci EU.

### 3.3.1.2 Osobní údaj

Osobním údajem dle čl. 4 odst. 1 GDPR jsou *„**veškeré informace o identifikované nebo identifikovatelné fyzické osobě**. Identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat zejména odkaz na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.“*

Z vlastního znění výše uvedeného článku, ve srovnání s § 4 ZoOU vyplývá, že došlo de facto jen ke stylistickým, nikoliv však obsahovým změnám. Nicméně to, co **GDPR** zásadně **změnilo,** je **rozšíření okruhu dat a informací, které je možné považovat za osobní údaje**.

Osobním údajem je dle GDRP **jakákoliv informace** (např. obrazová, písemná, slovní, digitální, genetická, zdravotnická aj.), která **má vztah** (obsahem – např. jméno, adresa, pracovní zařazení, e-mail aj.), **k subjektu údajů.**[166] Z tohoto pohledu a v souladu s výkladem uvedeným v recitálech 30, 34, 35, 38 GDPR[167] je třeba za osobní údaj považovat:

---

165: Viz Čl. 3 GDPR – Místní působnost

166: **Subjektem údajů je** dle čl. 4 odst. 1 GDPR identifikovaná nebo identifikovatelná **fyzická osoba**.

**Subjekt může být identifikován:**

- **přímo,**
- **nepřímo (např. výběr vyčleněním aj.).**

167: Recitály jsou ustanovení předcházející vlastnímu textu nařízení GDPR a jsou v některých případech výkladem či do jisté míry důvodovou zprávou k vlastnímu textu nařízení.

- jméno a příjmení,
- **identifikační číslo**,
- rodné číslo,
- **lokační údaje (geo-)**,
- věk a datum narození,
- pohlaví,
- osobní stav,
- občanství,
- **síťové identifikátory**,
  - **IP adresa**,
  - **identifikátory cookies**,
  - radio frequency identification tags aj.,
- **fotografie**,
- **prvky** fyzické, fyziologické, genetické, psychické, ekonomické, **kulturní nebo společenské identity**,
- osobní či pracovní adresa,
- osobní či pracovní telefonní číslo,
- **osobní či pracovní e-mail**,
- **ověřovací identifikační údaje**,
- identifikační čísla vydaná státem.

Tučně vyznačené osobní údaje mají typicky vztah k informačním a komunikačním technologiím a aplikacím, které tyto technologie využívají. Rozšíření okruhu dat, jež je možné považovat za osobní údaje, výrazným způsobem zasahuje do problematiky kybernetické bezpečnosti a zajištění ochrany dat, která jsou spravována v dané organizaci.

Pokud se zaměříme na **položku síťových identifikátorů a ověřovacích identifikačních údajů, zjistíme, že za osobní údaj může a zřejmě i bude považována řada dat umožňujících základní fungování počítačového systému v síti.**

Velmi často byla v praxi diskutována otázka - je IP adresa osobním údajem?

V této věci je vhodné krom GDPR přihlédnout i k judikatuře Soudního dvora EU, který mimo jiné rozhodoval v kauze: **Patrick Breyer** proti **Bundesrepublik Deutschland.**[168]

Patrick Breyer se u německých soudů domáhal, aby Německo přestalo uchovávat jeho IP adresy, které získalo při jeho „návštěvách" několika internetových stránek německých spolkových

168: Blíže viz: [online]. Dostupné z: http://curia.europa.eu/juris/document/document.jsf?text=&docid=184668&pageIndex=0&doclang=cs&mode=lst&dir=&occ=first&part=1&cid=1403270

orgánů, které byly veřejně přístupné. Z pohledu činnosti provozovatelů dotčených webových stránek se jednalo o klasické logování služeb tímto ISP[169] nabízených.

Německé soudy přerušily řízení a položily předběžnou otázku soudnímu dvoru EU, protože v dané věci neexistuje jednotný výklad práva EU.

Jde zejména o to, jestli k tomu, aby nějaký údaj byl osobním údajem, a tedy identifikoval konkrétní osobu, je třeba vycházet z *„objektivního"*, či *„relativního"* kritéria.

**„Objektivní" kritérium** znamená, že údaje, jako jsou **IP adresy**, **by mohly být považovány za osobní údaje** zpracovávané ISP jiných služeb než připojení (např. provozovatelem internetové stránky), **a to i tehdy, pokud by byla schopna identifikovat konkrétního uživatele jen třetí osoba** (typicky ISP připojení).

**„Relativní" kritérium** znamená, **že IP adresy by mohly být považovány za osobní údaj u ISP připojení**, neboť mu umožňují přesně určit totožnost uživatele, **ale už ne u ISP služeb, který disponuje skutečně pouze údajem o IP adrese a nezná jméno návštěvníka.**

Soudní dvůr EU konstatoval, že **je nesporné, že dynamická IP adresa nepředstavuje informaci o „identifikované osobě"**, neboť **adresa přímo neodhaluje totožnost fyzické osoby**, která je majitelem počítače, ze kterého byla navštívena internetová stránka, **ani totožnost jiné osoby, která mohla tento počítač používat**.

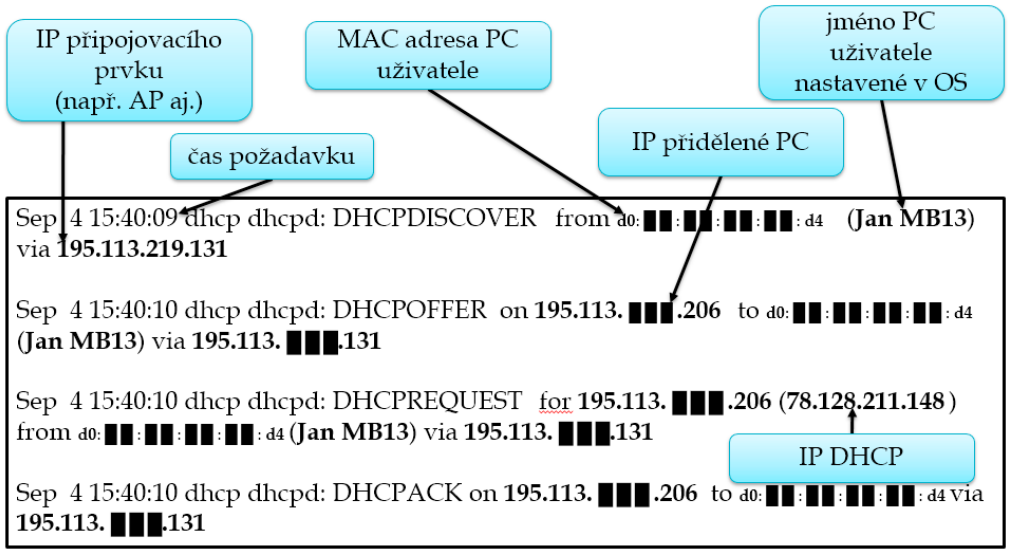
Na druhou stranu však Soudní dvůr (druhý senát) také uvedl (následně i rozhodl), že **dynamická adresa** internetového protokolu, **kterou poskytovatel on-line mediálních služeb uchovává v souvislosti s přístupem osoby na internetovou stránku,** kterou tento poskytovatel zpřístupnil veřejnosti, pro uvedeného poskytovatele **představuje osobní údaj ve smyslu** článku 2 písm. a) směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, **pokud má poskytovatel k dispozici právní prostředky, které mu umožňují nechat identifikovat subjekt údajů díky dalším informacím, kterými disponuje poskytovatel internetového připojení tohoto subjektu.**

Dynamická IP adresa může být dle tohoto rozsudku, z 19. října 2016, za určitých okolností osobním údajem.

Dopad té skutečnosti, že **IP adresa, jakožto i další síťové identifikátory mohou být osobním údajem,** demonstrujeme na dvou příkladech.

169: K vlastnímu pojmu ISP, právům a povinnostem jednotlivých ISP viz blíže např. KOLOUCH, Jan. *CyberCrime.* Praha: CZ.NIC, 2016, s. 78 a násl. a s. 109 a násl.

Na následujícím obrázku je možné vidět komunikaci PC a jednotlivých prvků sítě (AP, DHCP server) a následné připojení PC do sítě.



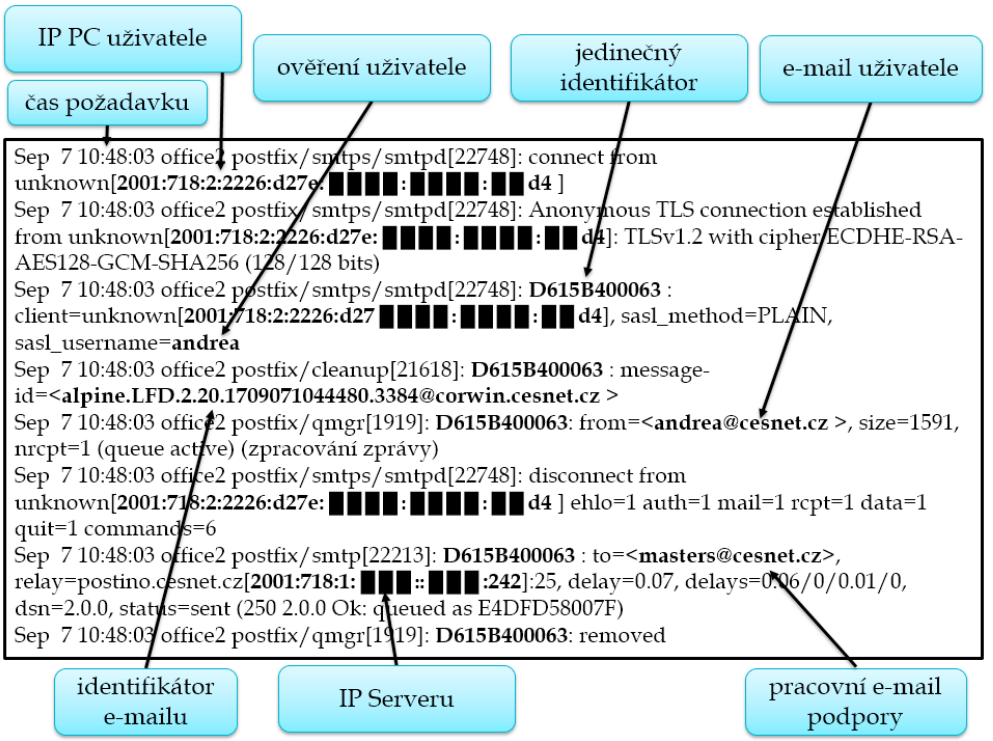

Obrázek 15: DHCP

Pokud se důsledně zaměříme na **data** (informace)**, která mají vztah k subjektu údajů a jsou jej schopny identifikovat**, pak osobním údajem v tomto případě nebude pouze IP adresa připojovacího prvku a IP adresa DHCP serveru.

Osobním údajem je teoreticky i čas daného požadavku, neboť se jedná o stopu, která může být zejména v kombinaci s jedinečnými identifikátory a dalšími informacemi, které servery získávají, použita k identifikaci fyzické osoby.[170] Zároveň se jedná o velmi podstatnou informaci, neboť bez přesného času není možné identifikovat, komu (jakému počítačovému systému) byla přidělena konkrétní IP adresa.

Dalším příkladem zobrazujícím rozsah zpracovávání dat, která je možné považovat za osobní údaje, je zpracování osobních údajů při odeslání e-mailu prostřednictvím SMTP.

170: Blíže viz recitál 30 GDPR




Obrázek 16: SMTP

Pokud se opět důsledně zaměříme na **data** (informace)**, která mají vztah k subjektu údajů a jsou schopna jej identifikovat**, pak osobním údajem v tomto případě nebude pouze IP adresa serveru.

Pracovní e-mail podpory by mohl být opět osobním údajem, pokud k němu budou přiřazeny další identifikátory, které jsou schopné identifikovat fyzickou osobu.

**Klíčovou otázkou je, zda jsme** v rámci veškerých procesů, které se odehrávají v počítačových systémech (prvcích ICT), které jsou daným subjektem (fyzická či právnická osoba) spravovány, **schopni rozlišit situaci, kdy dochází k přenosu dat čistě mezi počítačovými systémy, bez vztahu k jakékoliv fyzické osobě, a kdy už se do těchto procesů zapojí fyzická osoba jakožto subjekt údajů dle GDPR**.

Domníváme se, že až na specifické výjimky nebudeme schopni vyčlenit procesy, které se odehrávají bez lidské interakce. Na základě tohoto tvrzení je následně třeba aplikovat požadavky vyplývající z GDPR na veškeré procesy, při nichž dochází k manipulaci s informacemi, které mají vztah k subjektu údajů a jsou jej schopny identifikovat. Zároveň bude třeba přijmout dostatečná bezpečnostní opatření, aby byla dostatečně chráněna jak přenosová soustava, počítačové systémy a aplikace, které s takovýmito informacemi pracují, tak informace (resp. data) samotná.

Vedle shora uvedených osobních údajů definuje GDPR zvláštní kategorie osobních údajů, mezi které patří údaje o:

- rasovém či etnickém původu,
- vyznání,
- politických názorech,
- členství v odborech či jiných organizacích,
- sexuální orientaci,
- spáchání deliktů (trestný čin/přestupek aj.) a potrestání za ně,
- genetické údaje (DNA & RNA),
- biometrické údaje,
- údaje o zdravotním stavu.

### 3.3.1.3 Zpracování osobních údajů

Zpracováním osobních údajů se dle čl. 4 odst. 2 GDRP rozumí **jakákoliv operace** nebo soubor operací **s osobními údaji** nebo soubory osobních údajů, **který je prováděn pomocí či bez pomoci automatizovaných postupů**, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení.

Ochrana subjektu údajů se vztahuje na zpracování osobních údajů, pokud jsou tyto údaje uloženy v evidenci nebo do ní mají být vloženy.[171]

Pojem **zpracování** dle GDPR však **nelze chápat jako jakékoli nakládání s osobním údajem. Zpracování osobních údajů je nutné považovat již za sofistikovanější činnost, kterou správce s osobními údaji provádí za určitým účelem a z určitého pohledu tak činí systematicky.**[172]

171: Viz recitál 15 GDPR

172: Blíže viz *Základní příručka k GDPR.* [online]. [cit. 7. 8. 2018]. Dostupné z: https://www.uoou.cz/zakladni%2Dprirucka%2Dk%2Dgdpr/ds-4744/archiv=0&p1=3938

Ze zpracování osobních údajů dle GDPR je mimo jiné **vyňata činnost prováděná fyzickou osobou v rámci čistě osobní povahy nebo činnosti prováděné výhradně v domácnosti, a tedy bez jakékoliv souvislosti s profesní nebo obchodní činností.**[173]

V čl. 5 odst. 1 písm. a) GDPR jsou stanoveny zásady zpracování osobních údajů. Mezi tyto zásady dle GDPR patří:

- **zákonnost, korektnost, transparentnost** [čl. 5 odst. 1 písm. a) GDPR] – správce osobních údajů je povinen:
  - informovat subjekt údajů o probíhající operaci zpracování a jejích účelech,
  - informovat subjekt údajů o profilování a o jeho důsledcích,
  - informovat subjekt údajů, pokud jsou osobní údaje získávány od něj, zda je povinen tyto údaje poskytnout, a o důsledcích jejich případného neposkytnutí,
  - **prokázat existenci nejméně jednoho právního důvodů pro zpracování osobních údajů**,
  - **dokumentovat:**
    - co, jak, proč zpracovává,
    - souhlas a zákonný důvod,
    - čas, po který zpracovává,
    - **přijaté záruky a bezpečnostní opatření**.

- **omezení účelu** [čl. 5 odst. 1 písm. b) GDPR] – osobní údaje musí být shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný,

- **minimalizace údajů** [čl. 5 odst. 1 písm. c) GDPR] – osobní údaje musí být přiměřené a relevantní ve vztahu k účelu, pro který jsou zpracovávány,

- **přesnost** [čl. 5 odst. 1 písm. d) GDPR] – osobní údaje musí být přesné a v případě potřeby aktualizované; musí být přijata veškerá rozumná opatření, aby osobní údaje, které jsou nepřesné s přihlédnutím k účelům, pro které se zpracovávají, byly bezodkladně vymazány nebo opraveny,

- **omezení uložení** [čl. 5 odst. 1 písm. e) GDPR] – osobní údaje by měly být uloženy ve formě umožňující identifikaci subjektu údajů jen po nezbytnou dobu pro dané účely, pro které jsou zpracovávány,

- **integrita a důvěrnost** [čl. 5 odst. 1 písm. f) GDPR] – osobní údaje musí být **zpracovávány způsobem, který zajistí náležité zabezpečení, včetně jejich ochrany pomocí vhodných**

173: Viz recitál 15 GDPR

**technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením.**

### 3.3.1.4 Zabezpečení osobních údajů

Jednou z oblastí, které se GDPR explicitně věnuje, je i **problematika zabezpečení zpracování osobních údajů**.

V čl. 32 GDPR je uvedeno, že **správce** (případně zpracovatel) **musí** s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, **přijmout vhodná technická a organizační opatření, aby zajistil úroveň zabezpečení odpovídající danému riziku**, případně včetně:

- **pseudonymizace a šifrování osobních údajů,**
- **schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování,**
- **schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů,**
- **procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.**

„***Při posuzování vhodné úrovně bezpečnosti se zohlední zejména rizika**, která představuje zpracování, zejména náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim.*“ [174]

Při určování rizika je třeba vycházet zejména z kategorie osobních údajů, které by mohly být porušením zabezpečení dotčeny, charakteru porušení zabezpečení a počtem dotčených subjektů údajů. Vyšší riziko představují „citlivější“ osobní údaje (viz např. zvláštní kategorie osobních údajů), rozsáhlejší soubor osobních údajů, případně údaje, jimiž lze způsobit subjektu údajů újmu či zásah do jeho práv.

Dle čl. 32 odst. 4 GDPR přijmou správce a zpracovatel opatření pro zajištění toho, aby jakákoliv fyzická osoba, která jedná z pověření správce nebo zpracovatele a má přístup k osobním údajům, zpracovávala tyto osobní údaje pouze na pokyn správce, pokud jí jejich zpracování již neukládá právo Unie nebo členského státu.

174: Čl. 32 odst. 2 GDPR

### 3.3.1.5 Posouzení vlivu na ochranu osobních údajů (DPIA)

Posouzení vlivu na ochranu osobních údajů (**D**ata **P**rotection **I**mpact **A**ssessment **– DPIA)** je nástrojem, který se využije v případě, kdy **je pravděpodobné, že** určitý druh **zpracování, zejména při využití nových technologií, bude** s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování **mít za následek vysoké riziko pro práva a svobody fyzických osob.** Jde o nástroj, který může správcům pomoci identifikovat případná rizika zpracování osobních údajů a zavedení vhodných opatření.

Posouzení vlivu na ochranu osobních údajů je třeba provést v případech:

- **systematického a rozsáhlého vyhodnocování osobních aspektů týkajících se fyzických osob, které je založeno na automatizovaném zpracování, včetně profilování**, a na němž se zakládají rozhodnutí, která vyvolávají ve vztahu k fyzickým osobám právní účinky nebo mají na fyzické osoby podobně závažný dopad,
- **zpracování zvláštních kategorií osobních údajů** (biometrických údajů, nebo údajů o odsouzení v trestních věcech a o trestných činech či souvisejících bezpečnostních opatřeních),
- rozsáhlého systematického monitorování veřejně přístupných prostor,
- **jakýchkoliv jiných operací, kdy má příslušný dozorový úřad za to, že je pravděpodobné, že zpracování bude představovat vysoké riziko pro práva a svobody subjektů údajů.**

Obsahem posouzení vlivu na ochranu osobních údajů by měl být:

- popis zamýšlených operací zpracování,
- posouzení nezbytnosti a přiměřenosti operací z hlediska účelu (**test proporcionality)**,
- **posouzení rizik pro práva a svobody subjektů**,
- **plánovaná opatření k řešení těchto rizik, včetně záruk, bezpečnostních opatření aj.**

Vlastní nařízení GDPR obsahuje i další instituty (např. pseudonymizace, požadavky na výmaz či přenositelnost osobních údajů aj.), které se mohou vztahovat k činnosti, jež jsou prováděny v rámci informačních a komunikačních systémů, a které vyžadují náležitou úroveň zabezpečení a ochrany.

Podstatné je identifikovat vliv (dopad) GDPR na organizaci, na její jednotlivé části a procesy. De facto jde o provedení auditu, kde všude v organizaci, případně u jednotlivce se pracuje s osobními údaji ve vztahu ke GDPR. Následně postup spočívá v modifikaci či tvorbě pravidel a procesů (pokud je to třeba) jak uvnitř organizace, tak ve vztahu k subjektu údajů. Veškerá tato činnost by současně měla respektovat základní principy bezpečnosti.

Stejně jako při zavádění bezpečnostních pravidel obecně, tak při implementaci GDPR či jiných dokumentů a doporučení je třeba si uvědomit, že neexistuje jedno pravidlo, vzor, nástroj, řešení či postup aplikovatelný pro každou organizaci a každou situaci či každou organizaci.

Je třeba přijmout a implementovat vlastní řešení v souladu s GDPR.

Je třeba individualizovat…

### 3.3.2 ePrivacy

Druhým právním dokumentem EU, kterému se chceme stručně věnovat, je **Návrh nařízení** o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích a o zrušení směrnice 2002/58/ES (nařízení o soukromí a elektronických komunikacích – **ePrivacy**).[175]

Byť se zatím jedná o právní normu v podobě návrhu, její případný dopad na oblast kybernetické bezpečnosti je významný. Zároveň tento návrh bezprostředně souvisí s GDPR, neboť ještě více rozšiřuje okruh subjektů a služeb, na které se vztahuje ochrana osobních údajů.

Důvodem vzniku nařízení ePrivacy je **přezkum směrnice 2002/58/ES („směrnice o soukromí a elektronických komunikacích")**, která byla do právního řádu ČR implementována zákonem č. 127/2005 Sb., o elektronických komunikacích. Nařízení ePrivacy by tedy mělo dopad i na tento zákon.

Nařízení ePrivacy stanoví pravidla **ochrany základních práv a svobod fyzických a právnických osob při poskytování a využívání služeb elektronických komunikací,** a zejména práv na respektování soukromého života a komunikace a ochranu fyzických osob v souvislosti se zpracováním osobních údajů.[176]

V recitálu 1 ePrivacy je uvedeno, že **článek 7 Listiny základních práv Evropské unie chrání** základní **právo každého jedince na respektování jeho soukromého a rodinného života, obydlí a komunikace a že respektování soukromí komunikace je základním rozměrem tohoto práva.** Důvěrný charakter elektronických komunikací zajišťuje, že informace, které si strany mezi sebou vymění, a vnější prvky této komunikace, včetně údajů o tom, kdy byla informace zaslána, odkud a komu, nesmí být vyzrazeny nikomu jinému než stranám, které se komunikace účastní.

175: [online]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52017PC0010

176: Čl. 1 odst. 1 ePrivacy

***Zásada důvěrnosti by se měla vztahovat na stávající a budoucí komunikační prostředky, včetně volání, přístupu k Internetu, aplikací pro výměnu rychlých zpráv, elektronické pošty, internetových telefonních volání a zasílání osobních zpráv prostřednictvím sociálních médií.***

Z výše uvedeného znění recitálu 1 ePrivacy je tedy zřejmé, že se zákonodárce rozhodl zavést regulaci do oblasti, která prozatím v podmínkách České republiky nespadala pod zákon o elektronických komunikacích (viz e-mailové služby aj.), ale spíše do působnosti zákona o některých službách informační společnosti.

Příčinou zavádění regulace do této oblasti je dle důvodové zprávy k ePrivacy ta skutečnost, že se *„**spotřebitelé a podniky namísto tradičních komunikačních služeb stále více spoléhají na nové internetové služby umožňující interpersonální komunikaci**, jako například VoIP, výměnu rychlých zpráv (instant messaging) **a webové e-mailové služby**. **Tyto komunikační služby ‚Over-the-Top (OTT)'** obecně **nepodléhají stávajícímu unijnímu rámci pro elektronické komunikace**, včetně směrnice o soukromí a elektronických komunikacích."*

Pro to, aby bylo možné účinně zajistit **právo na respektování soukromí a komunikace, je** dle tvůrců tohoto nařízení **nezbytné rozšířit oblast působnosti tak, aby zahrnovala poskytovatele služeb OTT**. Zároveň je těmito subjekty konstatováno, že *„…ochranu základních práv nelze ponechat na samoregulaci odvětví…"*

### 3.3.2.1 Působnost ePrivacy

Článek 3 ePrivacy definuje místní působnost této právní normy, přičemž ta je stanovena tak, že se nařízení vztahuje na:

- **poskytování služeb elektronických komunikací koncovým uživatelům v Unii** bez ohledu na to, zda je od koncového uživatele vyžadována platba,
- **využívání těchto služeb**,
- **ochranu informací souvisejících s koncovými zařízeními koncových uživatelů** nacházejících se v Unii.

Pokud jde o vymezení poskytovatelů služeb informační společnosti, na něž se ePrivacy vztahuje, je třeba využít recitálu 8 tohoto nařízení, kde je uvedeno, že půjde o:

- poskytovatele služeb elektronických komunikací,[177]
- **poskytovatele softwaru umožňujícího elektronické komunikace včetně získávání a prezentování informací na Internetu**,

177: De facto ISP připojení. Blíže viz ZoEK a ZSIS

- poskytovatele veřejně dostupných seznamů,
- **fyzické a právnické osoby, které služby elektronických komunikací používají** k zasílání přímých marketingových obchodních sdělení nebo **ke shromažďování informací souvisejících s koncovými zařízeními koncových uživatelů nebo uložených v těchto zařízeních.**

Nařízení ePrivacy se dle čl. 2 odst. 2 nevztahuje na:

a) činnosti, které nespadají do oblasti působnosti práva Unie;
b) činnosti členských států, které spadají do oblasti působnosti hlavy V kapitoly 2 Smlouvy o Evropské unii (tj. zvl. Ustanovení o společné zahraniční a bezpečnostní politice);
c) **služby elektronických komunikací, které nejsou veřejně dostupné**;
d) **činnosti příslušných orgánů za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení**.

Z výše uvedeného znění je dle našeho názoru nejvýznamnější právě pasáž, rozšiřující dopad nařízení na **poskytovatele softwaru umožňujícího elektronické komunikace včetně získávání a prezentování informací na Internetu.** Do této skupiny subjektů tak do budoucna budou spadat mimo jiné i poskytovatelé nabízející v rámci svých služeb i *interpersonální komunikační služby.*[178]

### 3.3.2.2 Základní terminologie ePrivacy

Nařízení ePrivacy modifikuje stávající či zavádí nové pojmosloví. Z tohoto důvodu považujeme za nezbytné vymezit některé pojmy. Konkrétně se jedná o:

- **Síť elektronických komunikací**
  Sítí elektronických komunikací se rozumí přenosové systémy, ať jsou založeny na trvalé infrastruktuře nebo centralizované správní kapacitě, či nikoli.
- **Služba elektronických komunikací**
  Jde o službu obvykle poskytovanou za úplatu, prostřednictvím sítí elektronických komunikací, která **zahrnuje:**
  - **„službu přístupu k Internetu" a/nebo**
  - **interpersonální komunikační službu** a/nebo
  - službu či služby spočívající zcela nebo převážně v přenosu signálů.

178: Viz kap. 3.3.2.2 Základní terminologie ePrivacy

*„Propojená zařízení a stroje mezi sebou navzájem stále více komunikují prostřednictvím sítí elektronických komunikací* (**IoT**). **Přenos komunikace mezi stroji** zahrnuje přenos signálů po síti, **a** obvykle tedy **představuje službu elektronických komunikací.**"[179] **Toto nařízení by se tedy mělo vztahovat i na přenos komunikace mezi stroji.**

- **Interpersonální komunikační služba**
  Má být dle Návrhu Směrnice Evropského parlamantu a Rady, kterou se stanoví evropský kodex pro elektronické komunikace, na které ePrivacy odkazuje, službou obvykle poskytovanou za úplatu, **která prostřednictvím sítí elektronických komunikací umožňuje přímou interpersonální a interaktivní výměnu informací mezi konečným počtem osob**, kdy osoby, které komunikaci zahajují nebo se jí účastní, určují jejího/její příjemce. **Tato služba nezahrnuje služby, které interpersonální a interaktivní komunikaci umožňují pouze jako nepodstatnou pomocnou funkci, která je ze své podstaty spjata s jinou službou**.[180]

  **Dle čl. 4 odst. 2 ePrivacy:** *„interpersonální komunikační služba"* **zahrnuje služby, které umožňují interpersonální a interaktivní komunikaci pouze jako nepodstatnou pomocnou funkci, která je ze své podstaty spjata s jinou službou.**

  Toto zdánlivě nepatrné rozšíření definice pojmu **interpersonální služby** však představuje monstrózní rozšíření okruhu působnosti vlastního nařízení ePrivacy. Jde o to, že v současné digitální společnosti umožňuje drtivá většina aplikací přímou interpersonální a interaktivní výměnu informací mezi konečným počtem osob, přičemž tato vlastnost je pouze nepodstatnou pomocnou funkcí, která je ze své podstaty spjata s jinou službou.

  Mezi ***„klasické interpersonální komunikační služby"***, které umožňují přímou interpersonální a interaktivní výměnu informací mezi konečným počtem osob **a nezahrnují služby**, **které interpersonální** a interaktivní **komunikaci umožňují pouze jako nepodstatnou pomocnou funkci**, která je ze své podstaty spjata s jinou službou, je možné zařadit služby, jež jsou primárně určeny k telekomunikaci (např. Skype, WhatsApp, Viber, Messenger a jiné VoIP služby, e-mailové služby aj.).

  Dle definice ePrivacy by však za ***„interpersonální komunikační služby"*** bylo možné považovat i služby, **které umožňují interpersonální a interaktivní komunikaci pouze jako nepodstatnou pomocnou funkci spjatou s jinou službou.** Díky tomuto rozšíření by definici interpersonální komunikační služby splnily i např.:

179: Recitál 12 ePrivacy

180: Blíže viz *Návrh SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY, kterou se stanoví evropský kodex pro elektronické komunikace (přepracované znění).* [online]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:52016PC0590

- veškeré sociální sítě (byť neumožňují VoIP komunikaci či odesílání e-mailů, ale umožňují chat),
- veškeré hry umožňující chat či přímou komunikaci mezi hráči v rámci hry,
- aplikace a programy, jež za určitých okolností umožňují chat či jiný způsob komunikace mezi uživateli (např. TeamViewer aj.),
- prvky IoT, které interagují s osobou (např. Google Glass, Amazon Alexa, Siri aj.).


Obrázek 17: Služba elektronických komunikací dle ePrivacy

- **Data elektronických komunikací**
  Data elektronických komunikací jsou definována dostatečně širokým a technologicky neutrálním způsobem a dělí se na:
  - **Obsah elektronických komunikací** (obsah vyměňovaný prostřednictvím služeb elektronických komunikací, jako například text, hlas, video, obrazy a zvuk).
  - **Metadata elektronických komunikací**, kterými jsou:
    - údaje zpracovávané v síti elektronických komunikací pro účely přenášení, šíření nebo výměny obsahu elektronických komunikací, **a to včetně údajů sloužících k vysledování a identifikaci zdroje a cíle komunikace**, údajů o poloze zařízení generovaných v kontextu poskytování služeb elektronických komunikací a data, času, době trvání a typu komunikace;
    - **data, která umožňují vyvozovat přesné závěry týkající se osobního života osob** účastnících se elektronické komunikace, například jejich sociální vztahy, zvyky a každodenní činnosti, zájmy, vkus atd.

Data elektronických komunikací **jsou považována za důvěrná.** Mělo by být **zakázáno jakkoli zasahovat do přenosu dat elektronických komunikací**, ať už přímo lidským zásahem, nebo zprostředkovaně automatizovaným strojovým zpracováním, **bez souhlasu všech komunikujících stran**.

**K zachycování těchto dat může dojít:**

- při odposlechu hovorů, čtení, skenování či ukládání obsahu elektronických komunikací nebo metadat pro jiné účely, než je výměna komunikace;
- v případě, že **třetí strana monitoruje navštívené internetové stránky, načasování návštěv, interakci s ostatními atd. bez souhlasu dotčeného koncového uživatele**.

- **Elektronická pošta**
  Elektronickou poštou je dle návrhu ePrivacy **jakákoli elektronická zpráva obsahující informace** jako **text, hlas, video, zvuk nebo obraz zaslaná prostřednictvím sítě elektronických komunikací**, kterou lze uchovávat v síti nebo v souvisejících výpočetních zařízeních, nebo v koncovém zařízení jejího příjemce.

Návrh nařízení ePrivacy propojuje řadu oblastí, a tak se velmi reálně může stát, že poskytovatel služby např. elektronické pošty dle ePrivacy bude současně např. poskytovatelem elektronických komunikací, softwaru umožňujícího elektronické komunikace, a zároveň osobou shromažďující informace související s koncovými zařízeními koncových uživatelů nebo uložených v těchto zařízeních.

### 3.3.2.3 Zpracování dat

Návrh nařízení ePrivacy definuje povolené zpracovávání, uchovávání a výmaz dat. Nastavení těchto pravidel ovlivní dobu a způsob uchovávání dat v rámci jednotlivých počítačových systémů a bezesporu bude třeba revidovat stávající procesy vztahující se k nakládání s daty souvisejícími s přenosem komunikace.

Dle čl. 6 ePrivacy **mohou poskytovatelé** služeb a sítí elektronických komunikací **zpracovávat data** elektronických komunikací, **pokud:**

a) **je to nezbytné pro přenos komunikace, po dobu nutnou pro tento účel, nebo**
b) **je to nezbytné pro zachování nebo obnovení bezpečnosti služeb a sítí** elektronických komunikací nebo **pro odhalení technických závad** a/nebo **chyb v přenosu elektronických komunikací**, po dobu nutnou pro tento účel.

**Poskytovatelé mohou zpracovávat metadata, pokud:**

a) je to nezbytné pro **splnění povinných požadavků na kvalitu služby** podle směrnice, kterou se stanoví evropský kodex pro elektronické komunikace, nebo nařízení (EU) 2015/2120, **po dobu nutnou pro tento účel, nebo**
b) **je to nezbytné pro vyúčtování, výpočet plateb za propojení, odhalení podvodného užívání nebo zneužívání služeb elektronických komunikací, zamezení takovému podvodnému užívání nebo zneužívání nebo pro přihlášení se k užívání těchto služeb, nebo**
c) dotčený **koncový uživatel udělil svůj souhlas se zpracováním metadat** svých komunikací pro jeden nebo více konkrétních účelů, včetně poskytování konkrétních služeb těmto koncovým uživatelům, **za předpokladu, že tento účel nebo účely nelze splnit zpracováním anonymizovaných informací.**

**Poskytovatelé mohou zpracovávat obsah:**

a) za účelem poskytování konkrétní služby koncovému uživateli, **pokud dotčený koncový uživatel** nebo koncoví uživatelé[181] **udělili svůj souhlas** se zpracováním svého obsahu elektronických komunikací **a danou službu nelze bez zpracování tohoto obsahu poskytnout, nebo**
b) **pokud všichni dotčení koncoví uživatelé udělili svůj souhlas** se zpracováním svého obsahu elektronických komunikací pro jeden nebo více konkrétních účelů, které nelze splnit zpracováním anonymizovaných informací, **a poskytovatel konzultoval dozorový úřad.** Pro konzultaci dozorového úřadu se použije čl. 36 odst. 2 a 3 nařízení (EU) 2016/679.

Povoleným zpracováním je také **zpracování dat** elektronických komunikací **za účelem zajištění bezpečnosti a kontinuity služeb elektronických komunikací, včetně kontroly z hlediska bezpečnostních hrozeb, jako je například přítomnost malwaru, nebo zpracování metadat za účelem zajištění nezbytných požadavků na kvalitu služby, jako je například latence, kolísání atd.**[182]

Návrh nařízení ePrivacy také stanoví v čl. 7 podmínky pro uchování a výmaz dat. Pokud jde o **obsah elektronických komunikací, poskytovatel po obdržení obsahu zamýšleným příjemcem** nebo příjemci jej **vymaže nebo tato data anonymizuje.** Tento postup nemusí dodržet, pokud:

181: Otázkou je, co je myšleno pojmem koncový uživatel. Je to ten, kdo odesílá (zahajuje komunikaci), i ten, kdo je příjemcem? Co když nebude příjemce souhlasit s tím, že jsem mu např. odeslal zprávu?

182: Blíže viz recitál 16 ePrivacy

- je to **nezbytné pro zachování nebo obnovení bezpečnosti služeb a sítí** elektronických komunikací nebo **pro odhalení technických závad** a/nebo **chyb v přenosu elektronických komunikací**, po dobu nutnou pro tento účel,
- dotčený koncový **uživatel udělil svůj souhlas** a danou službu nelze bez zpracování tohoto obsahu poskytnout.

**Pokud jde o metadata, poskytovatel je vymaže, nejsou-li již potřebná pro účely přenosu komunikace.** Metadata nemusí být vymazána, pokud:

- je to **nezbytné pro zachování nebo obnovení bezpečnosti služeb a sítí** elektronických komunikací nebo **pro odhalení technických závad** a/nebo **chyb v přenosu elektronických komunikací**, po dobu nutnou pro tento účel,
- dotčený koncový **uživatel udělil svůj souhlas** a danou službu nelze bez zpracování tohoto obsahu poskytnout,
- je to nezbytné pro **splnění povinných požadavků na kvalitu služby**,
- ke **zpracování metadat dochází za účelem vyúčtování**, **mohou být příslušná metadata uchovávána do konce období, v němž lze v souladu s vnitrostátními právními předpisy vyúčtování právně napadnout nebo uplatňovat nárok na platbu.**

Jak již bylo uvedeno v závěru subkapitoly o GDPR, jsme i zde přesvědčeni, že i při případné implementaci ePrivacy je třeba si uvědomit, že neexistuje jedno pravidlo, vzor, nástroj, řešení či postup aplikovatelný pro každou organizaci a každou situaci.

Je třeba zachovat zdravý rozum, přijmout a implementovat vlastní řešení v souladu s ePrivacy a dalšími právními předpisy.

Současně je třeba proaktivně reagovat na připravovanou legislativu a již při tvorbě či modifikaci pravidel a procesů souvisejících s bezpečností, resp. kybernetickou bezpečností, myslet i na možnost doplnění stávajících pravidel a procesů o nová pravidla a procesy.

### 3.3.3 Občanský zákoník

Vůči subjektům (fyzickým či právnickým osobám), které se pohybují v kyberprostoru a svojí činností zasáhnou do práv jiných subjektů, je vedle norem veřejného práva[183] možné uplatnit i normy soukromoprávní, zejména pak občanský zákoník. Pro účely této monografie jsme vybrali pouze některá ustanovení, která mohou mít vztah ke kybernetické bezpečnosti, ochraně osobních údajů aj.

183: Např. ZoKB, trestní zákoník aj.

### 3.3.3.1 Ochrana soukromí

Soukromí je jedním ze základních lidských práv, zakotvených ve Všeobecné deklaraci lidských práv z roku 1948[184]. Do českého právního řádu byla tato ustanovení transponována zejména v rámci článků 7, 10, 13 Listiny.[185]

Ustanovení § 84 OZ stanoví, že „***zachytit** jakýmkoli způsobem **podobu člověka tak, aby podle zobrazení bylo možné určit jeho totožnost, je možné jen s jeho svolením.***" Občanský zákoník dále zakazuje zasahovat do soukromí jiného, bez zákonného důvodu. Demonstrativně pak v § 86 vyjmenovává jednání, která jsou zakázána. Jedná se například o sledování soukromého života jiného, a to včetně pořizování zvukového nebo obrazového záznamu této osoby. Dále je zakázáno využívat takové či jiné záznamy pořízené o soukromém životě člověka třetí osobou, nebo takové záznamy o jeho soukromém životě šířit. Ve stejném rozsahu chrání občanský zákoník i **soukromé písemnosti osobní povahy.**

Svolení k zásahu do výše uvedených práv pak není třeba, jestliže se podobizna nebo zvukový či obrazový záznam pořídí nebo použijí k výkonu nebo ochraně jiných práv nebo právem chráněných zájmů jiných osob, nebo se pořídí nebo použijí na základě zákona k úřednímu účelu nebo v případě, že někdo veřejně vystoupí v záležitosti veřejného zájmu.[186] **Svolení také není třeba, pokud je podobizna nebo zvukový či obrazový záznam pořízen k vědeckému nebo uměleckému účelu a pro tiskové, rozhlasové, televizní nebo obdobné zpravodajství.**[187]

---

184: Dostupné online: http://www.osn.cz/wp-content/uploads/2015/03/vseobecna-deklarace-lidskych-prav.pdf
Ve všeobecné deklaraci lidských práv jsou tato práva primárně zakotvena v článcích 12 a 18.
Čl. 12: „***Nikdo nesmí být vystaven svévolnému zasahování do soukromého života**, do rodiny, domova **nebo korespondence**, ani útokům na svou čest a pověst. **Každý má právo na zákonnou ochranu proti takovým zásahům nebo útokům.***"
Čl. 18: „*Každý má právo na svobodu myšlení, svědomí a náboženství; toto právo zahrnuje v sobě i volnost změnit své náboženství nebo víru, jakož i svobodu projevovat své náboženství nebo víru, sám nebo společně s jinými, ať veřejně nebo soukromě, vyučováním, prováděním náboženských úkonů, bohoslužbou a zachovávaním obřadů.*"
185: Čl. 7 odst. 1 Listiny: „***Nedotknutelnost osoby a jejího soukromí je zaručena. Omezena může být jen v případech stanovených zákonem.***"
Čl. 10 odst. 2 a 3 Listiny:
„***Každý má právo na ochranu před neoprávněným zasahováním do soukromého a rodinného života.***"
„*Každý má právo na **ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě.***"
ČL. 13 Listiny: „*Nikdo nesmí porušit listovní tajemství ani tajemství jiných písemností a záznamů, ať již uchovávaných v soukromí, nebo zasílaných poštou anebo jiným způsobem, s výjimkou případů a způsobem, které stanoví zákon. Stejně se zaručuje tajemství zpráv podávaných telefonem, telegrafem nebo jiným podobným zařízením.*"
186: Viz § 88 OZ
187: Viz § 89 OZ

## Věci a virtuální majetek

Občanský zákoník v § 489 OZ stanoví, že **věcí je vše, co je rozdílné od osoby** (fyzické či právnické) **a co slouží potřebě lidí**. Věcí dle tohoto ustanovení je tedy jak hardware (v podobě počítačových systémů, sítí aj.), tak software. Zároveň **je věcí** i například **ovladatelná přírodní síla** (§ 497 OZ, např. elektrická energie aj.), či **cokoliv, co může sloužit k uspokojování potřeb člověka**. **Z okruhu věcí jsou pak vyloučena zvířata** (§ 494 OZ), **lidské tělo a jeho části** (§ 494 OZ) **a skutečnosti mimo dosah lidské moci** (např. sluneční světlo, vítr, déšť aj.), byť se jedná o elementy, které mohou sloužit k uspokojování potřeb člověka, avšak člověk není schopen je ovládat, tedy učinit předmětem svého vlastnictví. Posledním kritériem definujícím věc je **existence této věci ve vnějším světě**.

Toto kritérium od sebe odlišuje věci samostatné (např. postel, vrtačka aj.) a součásti věci. Součástí věci se dle § 505 OZ rozumí vše, *„co k ní podle její povahy náleží a co nemůže být od věci odděleno, aniž se tím věc znehodnotí."* Lavický vysvětluje, že *„součást věci nemá samostatnou funkci, a nemůže být proto samostatným předmětem práv. Začleněním do celku součást ztrácí svou individualitu (volant, kolo osobního automobilu, harddisk počítače, rypadlo jeřábu) a získává individualitu celku (věci složité)."* [188]

Občanský zákoník (§ 496 OZ) dále dělí věci na **věci hmotné** (*res corporales*) a věci nehmotné (*res incorporales*), přičemž hmotnou věcí je ovladatelná část vnějšího světa, jež má povahu samostatného předmětu, a **věcí nehmotnou** jsou práva, jejichž povaha to připouští, a jiné věci bez hmotné podstaty. *„Za nehmotné věci se považují statky, které existují jen právně (in iure consistunt), např. majetková práva z obligací, typicky pohledávky nebo služebnosti."*[189] Z definice obsažené v občanském zákoníku vyplývá, že věcí jsou práva a povinnosti, jejichž povaha to připouští. Typicky se bude jednat o práva majetková (všechna majetková práva, s nimiž lze nakládat, pohledávky, služebnosti, případně i vlastnické právo), předměty majetkových práv k duševnímu vlastnictví (know-how, označení tvořící ochrannou známku, obchodní firma, doména či doménové jméno aj.), nehmotné statky (patenty, ochranné známky aj.), spoluvlastnický podíl, osobní námaha, práce, pohledávky aj.

*„Dříve jsme si mysleli, když to zjednoduším, že s předmětem se dá obchodovat, jen když ho nacpeme do krabice a pošleme. To už dnes není pravda. Stále větší počet věcí a služeb můžeme poslat přes hranice států. Jsou to elektrony, co se pohybuje, ne krabice."* [190]

188: LAVICKÝ, Petr a kol. *Občanský zákoník I. Obecná část (§ 1–654). Komentář.* Praha: C. H. Beck, 2014. s. 1790

189: ELIÁŠ, Karel. *Věc, jako pojem soukromého práva.* [online]. [cit. 6. 6. 2016]. Dostupné z: http://www.pavelpetr.cz/soubory/29/87/Karel_Elias_Vec_jako_pojem_soukromeho_prava.pdf

190: GUZMAN, Andrew, Joost H. B. PAUWELYN. *International Trade Law*. Aspen Publishers, 2012, s. 37.

**Ve vztahu k ICT tedy nehmotnou věcí může být například právo užívat autorské dílo** [např. píseň, či film, program (za stanovených podmínek), aniž bych si jej musel kupovat ve fyzické podobě. Doručen je uživateli čistě obsah.], **herní či jiné virtuální účty aj.**

Za **virtuální majetek je** možné označit **majetek v digitální podobě**. **Může se jednat o data či informace, které si uživatel sám vytvořil, uložil** (soubory, databáze, poznámky, e-maily aj.), získal (programy, aplikace aj.) **apod., nebo může jít i o věc pocházející z virtuální hry, či jiného programu, aplikace.**

Virtuální majetek není možné považovat pouze za součást věci, neboť byť je a vždy bude vázán na nějakou fyzickou materii (např. harddisk či jiné paměťové medium), tak na této materii nemusí být zcela závislý, neboť může být přesunut na jiné médium, nebo je například duplikovaně ukládán v rámci poskytované služby či hry na datových nosičích ISP (nejčastěji cloudových úložištích).

### 3.3.3.2 Právní jednání

Občanský zákoník stanoví, co se rozumí právním jednáním v § 545: „*Právní jednání vyvolává právní následky, které jsou v něm vyjádřeny, jakož i právní následky plynoucí ze zákona, dobrých mravů, zvyklostí a zavedené praxe stran.*“ Význam právního jednání spočívá v tom, že u ICT, respektive u řady služeb poskytovaných v prostředí kyberprostoru, se vyžaduje aktivní činnost uživatele, spočívající v jeho odsouhlasení smluvních podmínek. Toto jednání sice bude právním jednáním (i s odkazem na § 546 OZ), ale nebude se však zpravidla jednat o případ uvedený v § 561 OZ, kde je uvedeno, že „*K platnosti právního jednání učiněného v písemné formě se vyžaduje podpis jednajícího. Podpis může být nahrazen mechanickými prostředky tam, kde je to obvyklé.*“ Případy, kdy je právně jednáno v elektronické formě[191], totiž z povahy věci vyžadují, aby tomu odpovídal i podpis jednajícího. Jedná se tedy o elektronický podpis, který je v ČR legislativně zakotven v zákoně č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce.

### 3.3.3.3 Náhrada škody

V případě kybernetických útoků se velmi často může stát, že je počítač či počítačový systém zneužit třetí osobou (například z důvodu zcela chybějícího zabezpečení, či ponechání počítače přístupného třetím osobám aj.). V takovém případě je možné využít právě institutu občanského

191: Srov dále § 562 OZ

práva, který se vztahuje k náhradě škody. Dále je případně možné využít institutů trestního práva při respektování principu subsidiarity trestní represe.[192]

Ustanovení § 2900 OZ uvádí, že pokud to vyžadují okolnosti případu nebo zvyklosti soukromého života, **musí si každý počínat při svém konání tak, aby nedošlo k nedůvodné újmě na svobodě, životě, zdraví nebo na vlastnictví jiného**. Toto ustanovení definuje generální prevenční povinnost každé osoby.

**V případě, že škůdce způsobí újmu úmyslným porušením dobrých mravů, je povinen ji nahradit.**[193] Pokud škůdce způsobí škodu porušením zákonné povinnosti (tedy i povinnosti vyplývající z § 2900 OZ), má se za to, že škodu zavinil z nedbalosti.[194] Občanský zákoník dále v § 2912 odst. 1 stanoví, že: „*Nejedná-li škůdce, jak lze od osoby průměrných vlastností v soukromém styku důvodně očekávat, má se za to, že jedná nedbale.*"

V souvislosti s náhradou škody je třeba se věnovat i § 2913 OZ (Porušení smluvní povinnosti), kde je stanoveno, že „***poruší-li strana povinnost ze smlouvy, nahradí škodu z toho vzniklou*** *druhé straně nebo i osobě, jejímuž zájmu mělo splnění ujednané povinnosti zjevně sloužit.*" **Povinnosti k náhradě škody je možné se zprostit, pokud škůdce prokáže,** „***že mu ve splnění povinnosti ze smlouvy*** *dočasně nebo trvale* ***zabránila mimořádná nepředvídatelná a nepřekonatelná překážka vzniklá nezávisle na jeho vůli****. Překážka vzniklá ze škůdcových osobních poměrů nebo vzniklá až v době, kdy byl škůdce s plněním smluvené povinnosti v prodlení, ani překážka, kterou byl škůdce podle smlouvy povinen překonat, ho však povinnosti k náhradě nezprostí.*"

Na závěr je třeba se zabývat i možností, že **škodu způsobí věc sama od sebe**. **V takovém případě je povinen škodu nahradit ten, kdo měl mít nad věcí dohled.** Nelze-li takovou osobu určit, platí, že je jí vlastník věci. Pokud dotyčná osoba prokáže, že náležitý dohled nezanedbala, zprostí se povinnosti k náhradě škody.

### 3.3.4 Trestní zákoník

Z pohledu trestního práva se pro účely této monografie zaměříme pouze na oblast trestního práva hmotného, které chrání zájmy společnosti, ústavní zřízení ČR, práva a oprávněné zájmy fyzických a právnických osob zejména tím, že stanoví podmínky trestní odpovědnosti, výčet trestných činů a sankce, které lze za trestné činy uložit (viz čl. 39 Listiny).[195]

192: Viz § 12 odst. 2 TZK: „*Trestní odpovědnost pachatele a trestněprávní důsledky s ní spojené lze uplatňovat jen v případech společensky škodlivých,* ***ve kterých nepostačuje uplatnění odpovědnosti podle jiného právního předpisu.***"

193: § 2909 a násl. OZ

194: § 2911 OZ

195: NOVOTNÝ, František, Josef SOUČEK a kol. *Trestní právo hmotné*. 3. rozš. vyd. Plzeň: Aleš Čeněk, 2010, s. 15

V České republice je možné trestněprávně postihnout pouze takové jednání, které naplňuje znaky trestného činu uvedeného v trestním zákoně.

**Trestným činem je protiprávní čin, který trestní zákon označuje za trestný a který vykazuje znaky uvedené v takovém zákoně**.[196] K trestní odpovědnosti za trestný čin je třeba úmyslného zavinění, nestanoví-li trestní zákon výslovně, že postačí zavinění z nedbalosti.[197]

**Trestněprávní postih útočníka, spáchajícího kybernetický útok, který nebude možné podřadit pod žádné ustanovení trestního zákona, nebude možný.** To však nevylučuje postih útočníka prostředky občanského či správního práva.

Pokud jde o vymahatelnost práva v oblasti veřejného práva (trestní, správní aj. právo), vystupuje zpravidla aktivně při vymáhání práva sám stát (respektive jeho orgány). Pokud jde o právo soukromé, je zpravidla třeba, aby se na vymožení svého práva aktivně podílela osoba, která byla incidentem (protiprávním jednáním) dotčena.

### Vymezení působnosti českého trestního práva hmotného

Působností práva se rozumí okruh společenských vztahů, na které se právo vztahuje, respektive uplatňuje. Obecně jsou teorií rozeznávány čtyři druhy působnosti trestních zákonů:

- **působnost časová** (trestnost činu se posuzuje dle zákona účinného v době spáchání trestného činu),
- **působnost osobní** (okruh pachatelů, na něž se trestní zákon vztahuje – viz exempce hmotně a procesněprávní),
- **působnost místní** (užití trestního zákona ve vztahu k místu, kde byl trestný čin spáchán),
- **působnost věcná** (definuje okruh společenských vztahů, na které se zákon vztahuje).

Pokud jde o problematiku kybernetických útoků (či trestných činů), **nejproblematičtější je určení místa, kde k útoku či trestnému činu došlo**.

Pokud chceme řešit otázku: „*Kde byl trestný čin spáchán?*“, je třeba využít institutů uvedených v trestním zákoníku, neboť Česká republika se zavazuje stíhat trestné činy i tehdy, pokud se pachatel nacházel mimo území ČR. U kyberkriminality dojde především k využití **zásad teritoriality** (§ 4 TZK), **registrace** (§ 5 TZK), **personality** (§ 6 TZK), **ochrany a univerzality** (§ 7 TZK) a **subsidiární zásady univerzality** (§ 8 TZK).

196: Kybernetické útoky a jejich případná trestně právnií kvalifikace je popsána např v: KOLOUCH, Jan. *CyberCrime.* Praha: CZ.NIC, 2016, s. 181 a násl.

197: § 13 TZK

Velmi zjednodušeně je možné pomocí následující tabulky vymezit okruh trestných činů, kterými se budou zabývat české orgány činné v trestním řízení.

| | **Místo činu** | **Pachatelé** | **Trestné činy** | **Další podmínky** |
|---|---|---|---|---|
| **Zásada teritoriality** (§ 4 odst. 1 TZK) | Trestný čin byl zcela spáchán v ČR.<br><br>Trestný čin byl z části spáchán v ČR.* | Všechny osoby bez omezení. | Veškeré trestné činy uvedené v TZK | - |
| **Zásada registrace** (§ 5 TZK) | Čin byl spáchán mimo území České republiky na palubě lodi nebo jiného plavidla, anebo letadla nebo jiného vzdušného dopravního prostředku, které jsou registrovány v České republice. | Všechny osoby bez omezení. | Veškeré trestné činy uvedené v TZK | - |
| **Zásada personality – aktivní princip** (§ 6 TZK) | V cizině | Občan ČR** | Veškeré trestné činy uvedené v TZK | - |
| **Zásada ochrany a zásada universality** (§ 7 odst. 1 TZK) | V cizině | Cizinec*** | Trestné činy vyjmenované v § 7 odst. 1 TZK | |

* Dle § 4 TZK je trestný čin spáchán na území ČR i tehdy, pokud se pachatel dopustil na území ČR části jednání, i když porušení nebo ohrožení zájmu chráněného trestním zákonem nastalo nebo mělo nastat zcela nebo zčásti v cizině, nebo na tomto území nastala část následku, i když se jednání dopustil v cizině. Stejně tak je spáchán čin na území ČR, pokud zde zčásti jednal účastník činu spáchaného v cizině.

| | | | | |
|---|---|---|---|---|
| **Zásada personality – psivní princip** (§ 7 odst. 2 TZK) | V cizině | Cizinec | Trestné činy, u nichž platí oboustranná trestnost, nebo místo spáchání činu nepodléhá žádné trestní pravomoci. | Proti občanu ČR nebo proti osobě bez státní příslušnosti, která má na území České republiky povolen trvalý pobyt. |
| **Subsidiární zásada univerzality** (§ 8 TZK) | V cizině | Cizinec | - | a) čin je trestný i podle zákona účinného na území, kde byl spáchán,<br><br>b) pachatel byl dopaden na území České republiky, proběhlo vydávací nebo předávací řízení a pachatel nebyl vydán nebo předán k trestnímu stíhání nebo výkonu trestu cizímu státu nebo jinému oprávněnému subjektu a<br><br>c) cizí stát nebo jiný oprávněný subjekt, který žádal o vydání nebo předání pachatele k trestnímu stíhání nebo výkonu trestu, požádal o provedení trestního stíhání pachatele v České republice. |

** Vedle občana ČR se zásada personality vztahuje i na osobu bez státní příslušnosti, která má na jejím území povolen trvalý pobyt.

*** Pojmem cizinec se dle trestního zákoníku rozumí: „Cizí státní příslušník nebo osoba bez státní příslušnosti, která nemá na území České republiky povolen trvalý pobyt."

U trestné činnosti páchané v kyberprostoru pak bude pro posouzení otázky, zda stíhat či nestíhat trestný čin, zpravidla rozhodujícím místem to **místo, kde buď nastal následek trestného činu, nebo kde došlo k jednání** (ať již zcela, nebo z části).

## 4 Zákon o kybernetické bezpečnosti

*„Nevěř tomu, čemu nerozumíš, ale nezavrhuj, cos neprozkoumal."*

Karel Čapek

Citát Karla Čapka v úvodu této kapitoly jednak vhodně demonstruje to, jak by měla být problematika kybernetické bezpečnosti vnímána, a jednak má pro jednoho z autorů této publikace i osobní přesah spočívající mimo jiné i v evoluci, kterou v oblasti kybernetické bezpečnosti sám prodělal.

V roce 2008 jsem začal spolupracovat s Andreou Kropáčovou a jejími kolegy ve sdružení CESNET, z. s. p. o. Andrea v roce 2004 v tomto sdružení založila vůbec první tým typu CERT[198] v České republice. Když jsem s Andreou začal spolupracovat, měl jsem mnohdy představu, že oblast kybernetické bezpečnosti, řešení bezpečnostních incidentů aj. nutně potřebuje legislativní úpravu, která by jasně stanovovala práva a povinnosti jednotlivým subjektům. Úpravu, která by právě díky právní normě umožnila rychlejší a efektivnější výměnu dat a de facto by vynutila spolupráci.

Důvod tohoto „zúženého vnímání" spočíval především v oblasti, které jsem se v té době primárně věnoval, tj. trestněprávní odpovědnosti. V oblasti veřejného práva[199] totiž **mohou státní orgány činit pouze to, co jim zákon** (případně jiný právní předpis) **výslovně umožňuje**. Naopak **občané** (resp. i jiné subjekty, které nejsou státními orgány) **mohou činit vše, co není zákonem zakázáno.**[200]

S postupem času a zejména díky hlubšímu pochopení principů a mnohdy ne zcela formálních pravidel využívaných v oblasti kybernetické bezpečnosti jsem sám toto zúžené vnímání zavrhl a v mnoha případech se stal zastáncem řešení, při kterém není třeba aplikovat právo (resp. rigidně stanovené postupy), ale pouze zdravý selský rozum. Děkuji těm, kdo mi pomohli a pomáhají vnímat svět ICT jinak.

Domnívám se, že tento poněkud anarchistický pohled na věc ve mně přetrvává a byl i příčinou, proč jsem nebyl zastáncem nutnosti přijetí zákona o kybernetické bezpečnosti v takovém rozsahu, v jakém byl v roce 2012 navržen.

198: Blíže viz kap. 7 CERT/CSIRT týmy, či: **CESNET-CERTS**. Dostupné online: https://csirt.cesnet.cz/cs/index

199: Právo veřejné představuje souhrn právních norem, které v sobě obsahují prvky nerovného (vrchnostenského postavení). Jedním z účastníků vztahu v právu veřejném je stát (resp. orgány veřejné moci). Právo veřejné je protipólem práva soukromého, jež je postaveno na principu rovnosti stran (účastníků).

Do práva veřejného je možné zařadit např.: ústavní, správní, trestní, finanční právo aj. **Součástí práva veřejného je i zákon o kybernetické bezpečnosti.**

200: Viz čl. 2 odst. 3 a 4 Ústavy

Díky možnosti vznášet připomínky a podněty k vlastnímu znění ZoKB jsem však nucen souhlasit i s druhou částí Čapkova citátu: *„nezavrhuj, cos neprozkoumal."* Právě ony konzultace k zákonu, jakož i možnost bližšího pochopení záměru tehdejšího gestora kybernetické bezpečnosti (NBÚ) a jasnější vymezení smyslu a cíle této právní normy mě přesvědčily o nezbytnosti určité právní regulace kybernetické bezpečnosti (minimálně v oblasti státní správy a samosprávy). Tato nezbytnost spočívá mimo jiné i v jasném definování práv a povinností orgánu veřejné moci, který se problematice kybernetické bezpečnosti bude systematicky věnovat, neboť jak již bylo uvedeno: **státní moc lze uplatňovat jen v případech, v mezích a způsoby, které stanoví zákon.**

S odstupem času a genezí legislativy v oblasti kybernetické bezpečnosti (jak v ČR, tak v právních dokumentech EU), ochrany osobních údajů aj. je třeba konstatovat, že postup, který k tvorbě zákona o kybernetické bezpečnosti přijalo NBÚ, byl značně progresivní.

Následující kapitoly se věnují zákonu o kybernetické bezpečnosti a prováděcím vyhláškám k tomuto zákonu a jsou pojaty jako komentář k těmto právním předpisům. Z tohoto důvodu bylo v následujících kapitolách využito zejména vlastního znění **zákona č. 181/2014 Sb., o kybernetické bezpečnosti** a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), prováděcích vyhlášek, důvodové zprávy k ZoKB a dalších dokumentů publikovaných NBÚ či NÚKIB.[201]

Problémem v oblasti legislativy, která se týká kybernetické bezpečnosti, je mimo jiné i nedostatek judikatury, kterou by bylo možné na danou oblast aplikovat.

## 4.1 Příčiny vzniku ZoKB

**V obecné části důvodové zprávy k ZoKB z roku 2013 je uvedeno**, že výrazný nárůst používání informačních technologií v současném světě vede na jedné straně k vytvoření informační společnosti, urychlení komunikace a velkému rozvoji služeb, a tím celé společnosti. Závislost společnosti a jejího fungování na informačních technologiích rapidně narůstá, a to ve všech oblastech (nejedná se pouze o služby informační společnosti jako je internetový obchod, ale i o fungování informačních systémů, na jejichž správné funkci je závislá celá řada základních služeb jako například řízení dopravy, přenos energií, výkon veřejné moci apod.). **Se vzrůstající závislostí společnosti na informačních technologiích pak ale na straně druhé vzrůstá i riziko zneužívání těchto technologií nebo útoků na tyto technologie, které mají rozsáhlé dopady do činnosti subjektů, které s nimi pracují, a potencionálně mohou vést ke značným škodám.**

201: Text v následujících kapitolách byl mnohdy zcela převzat ze znění zákona, vyhlášky, důvodové zprávy či dokumentu vydaného NBÚ či NÚKIB. K tomuto znění je zpravidla přidán komentář či dílčí vysvětlení.

**Obecným trendem v celém světě je kvalitní ochrana těchto informačních technologií před zásahy, které mohou ohrozit jejich chod.** Cílené útoky proti informačním technologiím jsou celosvětovým fenoménem a jejich dopad způsobuje rozsáhlé ekonomické škody ve veřejném i v soukromém sektoru a současně jsou schopny vyvolat negativní politické důsledky, a to jak v národním měřítku, tak v měřítku globálním. **V případech, kdy je útok veden proti prvkům kritické infrastruktury, může být v konečném důsledku ohrožena bezpečnost nebo samotná existence státu.**

Útoky proti informačním technologiím jsou stále sofistikovanější a komplexnější. Ze sféry přímého ekonomického prospěchu individuálních útočníků se útoky přesouvají do oblasti organizované kybernetické průmyslové špionáže a kybernetického terorismu. Útočníci se stále více zaměřují na prvky kritické infrastruktury, jako jsou energetické systémy, produktovody, zdravotnické informační systémy a informační systémy veřejné správy.

**S ohledem na fakt, že kybernetický prostor nezná hranic a není tedy otázkou teritoriální, je nutné útoky na informační technologie řešit z pohledu mezinárodního společenství a s ohledem na závazky České republiky vůči státům Organizace Severoatlantické smlouvy** (dále jen „NATO“) **a Evropské unie** (dále jen „EU“). V rámci mezinárodní regulace tohoto fenoménu je vyvíjen na Českou republiku tlak, aby problematiku ochrany kybernetického prostoru řešila formou závazné právní regulace.

Bezhraničnost a všudypřítomnost kybernetických hrozeb vyžaduje intenzivní mezinárodní spolupráci a také intenzivní úsilí při zajišťování kybernetické bezpečnosti jednotlivých států.

**Oblast kybernetické bezpečnosti je a bude jedním z určujících aspektů bezpečnostního prostředí České republiky.** Všechny vyspělé země, mezi něž Česká republika bezesporu patří, jsou již zcela závislé na správném fungování informačních a komunikačních systémů. Tyto systémy podmiňují vznik a rozvoj konkurenceschopné společnosti založené na využívání vyspělých technologií a správnou funkci informační společnosti. Služby informační společnosti a související zařízení a činnosti jsou jedním z nejdynamičtěji se rozvíjejících sektorů každé moderní ekonomiky, na jejichž fungování závisí ekonomický úspěch řady podnikatelských subjektů a do jisté míry i kvalita života všech občanů. Bezpečnost kybernetického prostoru každé země se stává hodnotícím kritériem pro investory a významně ovlivňuje konkurenceschopnost dané země.

V době, v níž se stále větší část ekonomické aktivity přesouvá do prostředí Internetu a roste procento hrubého domácího produktu, které je závislé na správném fungování technologií, lze konstatovat, že investice do kybernetické bezpečnosti je adekvátním a odůvodněným nákladem pro prevenci, resp. snížení rizika častých a rozsáhlých útoků a incidentů výrazně oslabujících či negujících ekonomické, politické, kulturní a další přínosy rozvoje elektronické sféry.

Je zřejmé, že nejen ekonomické aktivity se přesouvají do kybernetického prostoru. Vznikem sociálních sítí, herních sítí a zájmových sítí se z nejznámější části kybernetického prostoru, z Internetu, stává významný celospolečenský jev, jehož prostřednictvím lze společnost výrazně pozitivně nebo i negativně ovlivňovat.

**V České republice se ochrana kybernetického prostoru řeší především prostřednictvím osob soukromého práva bez regulace, prostřednictvím partikulárních pracovišť.**

**V oblasti veřejné správy neexistuje jednotný způsob stanovení bezpečnostních standardů, které by minimalizovaly potencionální škody vzniklé z kybernetických útoků. Rovněž chybí systém prevence a včasného varování před těmito útoky.** V souvislosti s probíhající elektronizací veřejné správy je hrozba kybernetických útoků stále aktuálnější a je zcela nezbytné přijmout opatření, která by státu umožňovala reagovat na tuto celospolečenskou hrozbu z centrální pozice, tak jak to odpovídá zahraničním zkušenostem se závažnými útoky. Osoby soukromého práva, které provozují systémy nebo technologie, které jsou důležité pro kritickou infrastrukturu, mají sice v převážné většině zavedeny bezpečnostní standardy, které vychází ze standardů ISO/IEC 20000 a ISO/IEC 27000, avšak ve vztahu k těmto subjektům stát v současné době nedisponuje žádnou pravomocí, v rámci níž by mohl přijmout opatření k odvracení kybernetických útoků.

Vzhledem k tomu, že **státní moc lze uplatňovat výlučně na základě a v mezích zákona a soukromoprávním subjektům lze ukládat povinnosti jen zákonem, je třeba regulaci oblasti kybernetické bezpečnosti provést zákonem, s podrobným rozdělením povinností subjektů, které jsou primárně důležité pro chod státu, a subjektů ostatních, vymezením rolí subjektů dotčených veřejnoprávní regulací a sjednocením pojmů užívaných v oblasti kybernetické bezpečnosti.**

Nezbytnost právní úpravy je nutno řešit jednak vzhledem k materii společenské otázky, která je předmětem právní regulace, a dále pak vzhledem k nezbytnosti pokrytí této společenské otázky specifickou právní regulací. Je tedy třeba k odůvodnění navrhované právní úpravy odpovědět kladně na otázku, zda předmětný fenomén představuje aktuální společenský problém, a rovněž je nutno odpovědět i na otázku, zda nestačí tento fenomén pokrýt stávajícími společenskými nástroji (tj. zda se společnost s tímto fenoménem nedokáže vypořádat bez regulatorního působení státu).

Ze shora uvedených vnějších a vnitřních důvodů pro regulaci fenoménu kybernetické bezpečnosti formou navrhované právní úpravy vyplývají tři základní problémové okruhy, jejichž řešení je na národní úrovni nezbytné, a to:

1) ochrana existence a funkčnosti prostředí tvořeného informačními systémy a službami a sítěmi elektronických komunikací tak, aby v něm mohly subjekty pod jurisdikcí České republiky realizovat své **právo na informační sebeurčení**,

2) ochrana existence a funkčnosti prostředí tvořeného informačními systémy a službami a sítěmi elektronických komunikací tak, aby kybernetické bezpečnostní incidenty nemohly ohrozit fungování základních společenských funkcionalit chráněných **nedistributivními právy České republiky,**

3) ochrana existence a funkčnosti prostředí tvořeného informačními systémy a službami a sítěmi elektronických komunikací tak, **aby nebyla národní kybernetická infrastruktura zneužitelná k útokům mimo Českou republiku**.

Vzhledem k tomu, že jednotlivé informační a komunikační systémy včetně systémů kritického významu mají různé správce a fungují v různých právních režimech, nelze docílit jejich koordinovaného zabezpečení na národní úrovni jinak než prostřednictvím činnosti státu – žádný jednotlivý orgán veřejné moci, soukromé ani akademické sdružení nebo jiný spolek totiž nepokrývá tyto součásti v jejich souhrnu a není zde tak subjekt, který by mohl zajistit jejich koordinovanou ochranu před kybernetickými bezpečnostními incidenty. **Úloha státu je tedy v tomto případě podobně jako v ostatních oblastech bezpečnostní politiky unikátní a nenahraditelná.**

Při zajišťování kriticky důležitých společenských informačních funkcionalit nebo při zajišťování významných činností veřejné správy nelze spoléhat či pasivně čekat na to, že se všechny subjekty, jejichž činnost je pro fungování těchto systémů kriticky důležitá, vzájemně dohodnou na koordinovaném postupu nebo na jednotných pravidlech vzájemné spolupráce. Samoorganizační řešení spoléhající jen na aktivní prozíravost všech zúčastněných by totiž nikdy nebylo úplné a ve svém důsledku by tak mělo charakter provizoria do momentu, než fakticky nastane bezpečnostní problém natolik závažný, aby všechny zúčastněné donutil aktivně spolupracovat (přičemž lze dokonce pochybovat o tom, že i pak by iniciativní řešení zahrnulo všechny rizikové faktory).

## 4.2 Základní cíle a principy ZoKB

Cíl, jehož se ZoKB snaží dosáhnout, je **zajištění bezpečného fungování české informační společnosti,** tj. **zajištění bezpečné realizace základního práva na informační sebeurčení a ochrana nedistributivních práv státu**.

Zákon o kybernetické bezpečnosti **nezakládá civilní ani trestní odpovědnost pachatelů kybernetických útoků**, ale **vytváří systém bezpečnostních opatření, která mají výskytu kybernetických bezpečnostních incidentů předcházet**, resp. která mají **zajistit, že** případný kybernetický bezpečností **incident neohrozí celkové fungování informačních a komunikačních systémů** nebo fungování kriticky důležitých společenských informačních funkcionalit.

Cílový stav kybernetické bezpečnosti v sobě zahrnuje:

- definování základní úrovně bezpečnostních opatření,
- zavedení detekce kybernetických bezpečnostních událostí,
- zavedení hlášení kybernetických bezpečnostních incidentů,
- vytvoření systému protiopatření k reakci na kybernetické bezpečnostní incidenty,
- definování činnosti dohledových pracovišť (národní CERT a vládní CERT).

**Zákon** o kybernetické bezpečnosti **je postaven na následujících principech**:

1) princip **technologické neutrality**,
2) princip **ochrany informačního sebeurčení člověka**,
3) princip **ochrany nedistributivních práv**,
4) princip **minimalizace státního donucení**,
5) princip **autonomie vůle regulovaných subjektů**,
6) princip **bdělosti ve vztahu k ostatním státům a k mezinárodnímu společenství**.

**Ad. 1. Princip technologické neutrality**
Tento princip se v ZoKB projevuje:

- **Striktním zaměřením zákonných povinností k technologickým aspektům fungování služeb informační společnosti** (tj. informačních systémů a služeb a sítí elektronických komunikací).[202] Zákon o kybernetické bezpečnosti důsledně odděluje bezpečnost fungování služeb informační společnosti od informačního obsahu a **předmětem regulace zde není obsah přenášených informací**.

  Předmětem ZoKB nejsou například projevy obsahové kyberkriminality, jako např. šíření dětské pornografie, stalking nebo porušování práv duševního vlastnictví.

  **Práva a povinnosti vyplývající ze ZoKB postihují pouze kybernetické bezpečnostní incidenty** – žádná ze součástí navrhované právní úpravy tak neumožňuje státu nebo jeho orgánům provádět obsahovou cenzuru Internetu nebo jiných informačních sítí či služeb.

- **Užitím výhradně obecných kritérií pro standardní zabezpečení informačních systémů a služeb a sítí elektronických komunikací.** Bezpečnostní opatření, k jejichž dodržování zavazuje ZoKB vybrané subjekty (např. správce systémů kritické informační infrastruktury) jsou definována tak, aby mohlo být jejich splnění řešeno za užití různých technologií a postupů.

202: Jedná se o aplikaci základních principů kybernetické bezpečnosti vůči jejím jednotlivým prvkům.

**Subjekty mohou dle vlastního uvážení volit konkrétní způsob zabezpečení svých informačních struktur, a to včetně volby dodavatelů příslušných bezpečnostních řešení.** Nedochází tak k upřednostňování či zvýhodňování konkrétního dodavatele (technologií, aplikací aj.) a ani k narušení standardních tržních mechanismů v oboru bezpečnostních ICT.

**Ad. 2. Princip ochrany informačního sebeurčení člověka**
Bezpečnost nelze vnímat jako samostatně existující legitimní hodnotu. Legitimní jsou totiž jen ta bezpečnostní opatření, jejichž prostřednictvím je chráněn (zabezpečen) legitimní společenský zájem.[203] Zákon o kybernetické bezpečnosti je primárně založen na principu zabezpečení informačního sebeurčení člověka.

Pojem **informačního sebeurčení člověka** zavedl do právní praxe Spolkový ústavní soud[204] jako souhrnné označení pro katalog absolutních informačních práv člověka. **Původní chápání** pojmu informačního sebeurčení **zahrnovalo především jeho pasivní složku, tj. ochranu diskrétní informační sféry, a projevovalo se především ochranou soukromí a ochranou osobních údajů**.

Dalším rozvojem ústavní judikatury a judikatury Evropského soudu pro lidská práva **dospěla právní doktrína k aktuálnímu chápání informačního sebeurčení, které** kromě pasivní složky (tj. ochrany diskrétních informací) **zahrnuje též aktivní složku, tj. právo aktivně přijímat, zpracovávat a komunikovat informace.** Aktivní aspekt informačního sebeurčení přitom vychází z předpokladu, že člověk nemůže žít plnohodnotný soukromý život bez toho, aby měl možnost komunikovat s okolním světem.[205]

Právo na informační sebeurčení označuje následující distributivní práva primárně informační povahy:

- svobodu projevu a vědeckého bádání,
- ochranu soukromí, osobnosti a práva na aktivní soukromý život,
- právo na vzdělání,
- ochranu osobních údajů,
- přístup k informacím a další informační práva člověka aj.[206]

203: Srov. POLČÁK, Radim, Jakub HARAŠTA a Vaclav STUPKA. *Právní problémy kybernetické bezpečnosti*. Brno: Masarykova univerzita, 2016. ISBN 978-80-210-8426-1. str. 21.

204: Viz BVerfG, 15. prosince 1983, 1 BvR 209/83 u. a. – Volkszählung – BVerfGE 65, 1.

205: srov. např. I. ÚS 22/10 ze dne 07. 4. 2010, N 77/57 SbNU.

206: Blíže viz POLČÁK, Radim. *Internet a proměny práva*. Praha: AUDITORIUM, 2012. s. 66
ISBN 978-80-87284-22-3

Zaměření ZoKB k ochraně práva na informační sebeurčení se odráží též v konkrétní **struktuře informací zpracovávaných dohledovými pracovišti**, přičemž tvorba, zpracování ani archivace záznamů o výskytu a řešení kybernetických bezpečnostních incidentů nesměřují k identifikaci osob nebo k jiným zásahům do práva na soukromí nebo do práva na ochranu osobních údajů. Zákon o kybernetické bezpečnosti je konstruován tak, aby detekčních nebo obranných mechanismů, s jejichž zavedením u vybraných služeb a sítí počítá, nebylo možno zneužít ke sledování uživatelů služeb informační společnosti.

**Ad. 3. Princip ochrany nedistributivních práv**
Zákon o kybernetické bezpečnosti je vedle ochrany informačního sebeurčení člověka postaven též na principu **ochrany nedistributivních (veřejných) práv**. Konkrétně se jedná o právo státu na zajištění vnitřní bezpečnosti, na ochranu základních funkcionalit státu a na ochranu před škodlivými následky výjimečných stavů. V oblasti kybernetické bezpečnosti jde především o zajištění veřejného zájmu na bezpečnosti kritické informační infrastruktury a významných informačních systémů a v otázce úpravy stavu kybernetického nebezpečí.

Kybernetický útok může v krajním případě ohrozit například energetický sektor, zásobování obyvatelstva základními službami a komoditami, sociální služby nebo dopravní obsluhu.

**Ad. 4. Princip minimalizace státního donucení**
Zákon o kybernetické bezpečnosti nedopadá na veškeré informační systémy, respektive služby a sítě elektronických komunikací, ale zaměřuje se pouze na ty informační a komunikační systémy, které mají aktuálně vzhledem ke stanovenému účelu zákona zásadní význam. Zabezpečení těchto systémů před běžnými formami kybernetických útoků tak je řešeno pouze ve vztahu k systémům a sítím tvořícím kritickou informační infrastrukturu a dále pak ve vztahu k významným informačním systémům a některým digitálním službám.

Povinnost aplikace standardního zabezpečení včetně povinnosti hlásit výskyt kybernetických bezpečnostních incidentů a odpovídajícím způsobem na ně reagovat je tedy obecně definována pouze pro správce systémů značného společenského významu (tj. systémů, jejichž ochrana má ve shora uvedeném smyslu zásadní význam pro ochranu práv na informační sebeurčení a nedistributivních informačních práv státu).

Stát se snaží zasahovat pouze do práv těch subjektů, u kterých je respektování principů kybernetické bezpečnosti (viz triáda CIA aj.) zcela nezbytné. Lze tedy konstatovat, že věcný a osobní rozsah ZoKB je relativně minimalistický a sleduje dosažení stanoveného účelu za užití nejnižší možné míry právní regulace.

Rozšíření rozsahu povinností poskytovatelů služeb elektronických komunikací a subjektů zajišťujících sítě elektronických komunikací mimo kritickou informační infrastrukturu je zákonem předpokládáno pouze při vyhlášení stavu kybernetického nebezpečí.

Vedle standardního povinného zapojení shora uvedených subjektů do systému ochrany před kybernetickými bezpečnostními incidenty počítá ZoKB s tím, že řada subjektů provozujících informační systémy, sítě a služby projeví zájem o dobrovolné zapojení do národního systému kybernetické bezpečnosti.

Zkušenosti ze zahraničí ukazují, že spolupráce s CSIRT/CERT týmy přináší podnikatelským subjektům i akademickému nebo neziskovému sektoru vysoce pozitivní efekty a že zájem o tuto spolupráci bývá velký - správci soukromých nebo akademických informačních systémů, sítí nebo služeb mají v takových případech možnost vzájemně sdílet poznatky o hrozbách v oblasti kybernetické bezpečnosti a díky metodickému působení národního CSIRT/CERT týmu mohou vlastní infrastrukturu daleko účinněji bránit před kybernetickými bezpečnostními incidenty. Zákon tedy v tomto směru počítá s možností dobrovolného zapojení do systému národní kybernetické bezpečnosti i pro subjekty mimo okruh povinných osob.

**Ad. 5. Princip autonomie vůle regulovaných subjektů**
Princip autonomie vůle regulovaných subjektů se projevuje tak, že ZoKB stanovuje základní povinnosti a standardní bezpečnostní parametry, přičemž je adresátům právních povinností ponechána volnost ve způsobech, jakými dosáhnou jejich naplnění.

Zákon o kybernetické bezpečnosti počítá s tím, že lze standardní zabezpečení informačních systémů a sítí řešit za užití různých zabezpečovacích technologií. Konkrétní organizační a technické postupy včetně např. řízení dodavatelů, školení zaměstnanců, interních kontrol apod. ponechává ZoKB plně v diskreci povinných osob. Tím je zajištěno, že výsledné zabezpečení informačních a komunikačních systémů bude ve svém souhrnu spolehlivě funkční, přičemž individualita jednotlivých partikulárních bezpečnostních řešení umožní efektivní využití příslušných zdrojů.

Zjednodušeně řečeno se tedy princip autonomie vůle regulovaných subjektů v důsledku projeví tak, že prostředky vynaložené na zabezpečení příslušných informačních systémů, služeb a sítí elektronických komunikací budou použity v přímém vztahu ke konkrétním potřebám povinných osob, tj. zpravidla účelně a hospodárně.

Významným projevem principu autonomie vůle je možnost dobrovolného zapojení subjektů mimo okruh povinných osob do systému kybernetické bezpečnosti.

**Ad. 6. Princip bdělosti ve vztahu k ostatním státům a k mezinárodnímu společenství**
Primárním cílem ZoKB je zajištění bezpečnosti informačních a komunikačních systémů, avšak v zákoně je pamatováno i na respektování mezinárodněprávního principu due dilligence[207], tj. principu, na jehož základě je suverénní stát povinen v rámci své jurisdikce aktivně bránit škodám, které by mohly vzniknout ostatním státům nebo mezinárodnímu společenství.

Účinný národní systém detekce a řešení kybernetických bezpečnostních incidentů tak dle důvodové zprávy k ZoKB bude chránit české národní zájmy nejen bezprostředně, ale též formou ochrany před budoucí možnou mezinárodní odpovědností České republiky ostatním státům nebo mezivládním organizacím z titulu nedostatečného zabezpečení kybernetického prostoru před možností zneužití zdejších informačních systémů, sítí a služeb elektronických komunikací k útokům na zahraniční nebo mezinárodní infrastrukturu.

## 4.3 Komentář k ZoKB

HLAVA I
ZÁKLADNÍ USTANOVENÍ

**§ 1**
**Předmět úpravy**

**(1) Tento zákon upravuje práva a povinnosti osob a působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti.**
**(2) Tento zákon zapracovává příslušné předpisy Evropské unie a upravuje zajišťování bezpečnosti sítí elektronických komunikací a informačních systémů.**
**(3) Tento zákon se nevztahuje na informační nebo komunikační systémy, které nakládají s utajovanými informacemi.**

207: viz např. SHACKELFORD, Scott J., Scott RUSSEL a Andreas KUEHN. *Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors*. Chicago Journal of International Law. 2016, 17(1). ISSN 1529-0816.

Z důvodové zprávy:[208]

*Věcná působnost zákona je vymezena obecně pro oblast kybernetické bezpečnosti s výjimkou informačních a komunikačních systémů nakládajících s utajovanými informacemi. Pojmu kybernetické bezpečnosti je užito k odlišení od pojmu informační bezpečnosti resp. počítačové bezpečnosti a ke zdůraznění specifického zaměření zákona na ochranu funkčnosti síťového prostředí umožňujícího vznik, zpracování, uchovávání a komunikaci informací, které je tvořeno informačními systémy a službami a sítěmi elektronických komunikací.*

*Specifické omezení působnosti zákona vztahující se k informačním a komunikačním systémům nakládajícím s utajovanými informacemi je důsledkem toho, že úprava povinných bezpečnostních parametrů těchto systémů včetně navazujících právních povinností, kompetencí orgánů veřejné moci, kontroly, sankcí apod., je komplexně provedena zákonem č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů. Do této právní úpravy není v současné době důvod zasahovat, neboť tyto systémy podléhají certifikaci, tj. vyšší formě regulace.*

Z důvodové zprávy k novele ZoKB:

*V souladu s čl. 48 odst. 3 Legislativních pravidel vlády se do zákona zavádí odkaz na směrnici. Tato úprava je transpoziční k čl. 25 odst. 1 směrnice NIS. Je zapotřebí konstatovat, že termín „zajišťování bezpečnosti sítí a informačních systémů" je věcně zahrnut v terminu „zajišťování kybernetické bezpečnosti". Kybernetickou bezpečností se přitom v souladu s Národní strategií kybernetické bezpečnosti na období let 2015 až 2020 rozumí souhrn organizačních, politických, právních, technických a vzdělávacích opatření a nástrojů směřujících k zajištění zabezpečeného, chráněného a odolného kyberprostoru v České republice, a to jak pro subjekty veřejného a soukromého sektoru, tak pro širokou českou veřejnost. Kybernetická bezpečnost pomáhá identifikovat, hodnotit a řešit hrozby v kyberprostoru, snižovat kybernetická rizika a eliminovat dopady kybernetických útoků, informační kriminality, kyberterorismu a kybernetické špionáže ve smyslu posilování důvěrnosti, integrity a dostupnosti dat, systémů a dalších prvků informační a komunikační infrastruktury.*

**K odst. 1**
Toto ustanovení vymezuje **věcnou působnost ZoKB**. Zákon o kybernetické bezpečnosti upravuje práva a povinnosti osob a působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti.

208: V další části textu bude využito důvodových zpráv k textu ZoKB. Tyto důvodové zprávy by měly objasnit smysl daného ustanovení. Využívány budou dvě důvodové zprávy, které budou v textu odlišeny následovně:

- **Z důvodové zprávy**. Zdroj: *Důvodová zpráva.* [online]. [cit. 21. 8. 2018]. Dostupné z: https://www.govcert.cz/download/legislativa/container-nodeid-708/nbu-zkb-navrh-130415-duvodzprava.pdf
- **Z důvodové zprávy k novele ZoKB**. Zdroj: *Důvodová zpráva k návrhu zákona č. 205/2014 Sb.* [online]. [cit. 21. 8. 2018]. Dostupné z: https://apps.odok.cz/veklep-detail?pid=ALBSABVH86O2

**Orgánem veřejné moci** se rozumí orgány, které reprezentují veřejnou moc a jsou oprávněny vrchnostensky (viz orgány moci výkonné nebo soudní) či zprostředkovaně (viz orgány moci zákonodárné) rozhodovat o právech a povinnostech osob (fyzických či právnických). Orgány veřejné moci se dělí na:

- orgány státu (státní orgány) – např. soudy, ministerstva, správní úřady aj.,
- orgány samosprávy – např. územní (obce, kraje), zájmová (komory – např. advokátní, lékařská aj.) a věcná samospráva (např. svazky obcí aj.).

**Vrchnostenským orgánem veřejné moci vykonávajícím státní správu v oblasti kybernetické bezpečnosti je Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB[209]).** Vedle NÚKIB svěřuje ZoKB významné úkoly i národnímu[210] a vládnímu[211] CERT týmu.

K pojmu **kybernetická bezpečnost** viz kap. 2.1 Kybernetická bezpečnost.

**K odst. 2**
Zákon o kybernetické bezpečnosti zapracoval do svého aktuálního znění zejména Směrnici Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (**směrnice NIS**).

**Sítí elektronických komunikací** se dle čl. 4 odst. 1 písm. a) NIS[212] rozumí *„přenosové systémy, a popřípadě i spojovací nebo směrovací zařízení a jiné prostředky, včetně aktivních síťových prvků, které umožňují přenos signálů po vedení, rádiovými, optickými nebo jinými elektromagnetickými prostředky, včetně družicových sítí, pevných (**okruhově nebo paketově komutovaných, včetně Internetu**) a mobilních pozemních sítí, sítí pro rozvod elektrické energie v rozsahu, v jakém jsou používány pro přenos signálů, sítí pro rozhlasové a televizní vysílání a sítí kabelové televize, bez ohledu na typ přenášené informace.“*

Pokud tuto definici srovnáme s platnou českou právní úpravou, zjistíme, že je až na drobné odchylky téměř totožná (rozdíly jsou v jednotlivých definicích vyznačeny tučně).

V českém právu je pojem **síť elektronických komunikací** upraven v § 2 písm. h) ZoEK následovně: *„sítí elektronických komunikací se rozumí přenosové systémy, popřípadě spojovací nebo směrovací zařízení a jiné prostředky, **včetně prvků sítě, které nejsou aktivní**, které umožňují přenos signálů po vedení, rádiovými, optickými nebo jinými elektromagnetickými prostředky, včetně*

209: Blíže viz: https://nukib.cz/

210: **CSIRT.cz** Blíže viz: https://www.csirt.cz/

211: **GovCERT.cz** Blíže viz: https://nukib.cz/cs/vladni-cert/govcert-cz/

212: S odkazem na směrnici 2002/21/ES [online]. Dostupné z:
https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2002L0021:20091219:CS:PDF

*družicových sítí, pevných sítí s komutací okruhů nebo paketů a mobilních zemských sítí, sítí pro rozvod elektrické energie v rozsahu, v jakém jsou používány pro přenos signálů, sítí pro rozhlasové a televizní vysílání a sítí kabelové televize, bez ohledu na druh přenášené informace.*"

**Informačním systémem** se dle čl. 4 odst. 1 písm. b) NIS rozumí zařízení nebo skupina vzájemně propojených nebo souvisejících zařízení, z nichž jedno nebo více provádí na základě programu automatické zpracování digitálních dat.

Dle této definice by bylo možné za informační systém považovat počítačový systém tak, jak jej definuje např. české trestní právo.[213] **Počítačovým systémem se rozumí funkční jednotka, která je složena z jednoho nebo více počítačů a přidruženého softwaru**, využívající paměťové médium pro všechny, nebo část programů a dat nezbytných pro vykonání programů. **Počítačový systém může být samostatnou funkční jednotkou** (pracující samostatně - např. osobní počítač, notebook, smartphone aj.), **nebo může jít o soubor několika vzájemně propojených počítačových systémů** (např. počítačová síť).

Avšak dle čl. 4 odst. 1 písm. c) NIS **se za informační systém dále považují i digitální data**, jež jsou prvky sítě elektronických komunikací a informačním systémem (viz výše – míněno počítačovým systémem) uchovávána, zpracovávána, opětovně vyhledávána nebo předávána za účelem jejich provozu, použití, ochrany a údržby.

**Pojem bezpečnost sítí a informačních systémů** je v čl. 4 odst. 2 NIS definován jako schopnost sítí a informačních systémů odolávat s určitou spolehlivostí veškerým zásahům, které narušují dostupnost, autenticitu, integritu nebo důvěrnost[214] uchovávaných, předávaných nebo zpracovávaných dat nebo souvisejících služeb, které tyto sítě a informační systémy nabízejí nebo které jsou jejich prostřednictvím přístupné.

**K odst. 3**
**Věcná působnost ZoKB** je také uvedena v § 1 odst. 3, s tím, že je zde **vymezen okruh vztahů a zájmů, na něž se tento zákon neuplatní**. Toto omezení vyplývá především z úpravy uvedené v zákoně č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů. Tento zákon komplexně definuje zacházení s daty, jakož i s informačními a komunikačními technologiemi, které pracují s utajovanými informacemi.

**Utajovanou informací** se dle § 2 písm. a) ZoOUI rozumí informace zaznamenaná v jakékoliv podobě na jakémkoliv nosiči označená v souladu se ZoOUI. Současně musí být splněna podmínka, že vyzrazení nebo zneužití takové informace může způsobit újmu zájmu České republiky nebo může být pro tento zájem nevýhodné. Poslední podmínkou je, že se jedná

213: Viz § 230 a násl. TZK

214: Blíže viz kap. 2.2 Principy kybernetické bezpečnosti

o informaci uvedenou v seznamu utajovaných informací. Dle § 4 ZoOUI se utajovaná informace klasifikuje stupněm utajení: přísně tajné, tajné, důvěrné, vyhrazené.[215]

Informační systém nakládající s utajovanými informacemi je definován v § 34 ZoOUI a podléhá certifikaci Národním bezpečnostním úřadem. Komunikační systém nakládající s utajovanými informacemi je definován v § 35 ZoOUI. Tento komunikační systém je možné provozovat pouze na základě projektu bezpečnosti komunikačního systému schváleného Národním úřadem pro kybernetickou a informační bezpečnost.[216]

**§ 2**
**Vymezení pojmů**

**V tomto zákoně se rozumí**

**a) kybernetickým prostorem digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací[217],**
**b) kritickou informační infrastrukturou prvek nebo systém prvků kritické infrastruktury v odvětví komunikační a informační systémy [218] v oblasti kybernetické bezpečnosti,**
**c) bezpečností informací zajištění důvěrnosti, integrity a dostupnosti informací a dat,**
**d) významným informačním systémem informační systém spravovaný orgánem veřejné moci, který není kritickou informační infrastrukturou ani informačním systémem základní služby a u kterého narušení bezpečnosti informací může omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci,**
**e) správcem informačního systému orgán nebo osoba, které určují účel zpracování informací a podmínky provozování informačního systému,**
**f) správcem komunikačního systému orgán nebo osoba, které určují účel komunikačního systému a podmínky jeho provozování,**
**g) provozovatelem informačního nebo komunikačního systému orgán nebo osoba zajišťující funkčnost technických a programových prostředků tvořících informační nebo komunikační systém**
**h) významnou sítí síť elektronických komunikací zajišťující přímé zahraniční propojení do veřejných komunikačních sítí nebo zajišťující přímé připojení ke kritické informační infrastruktuře,**

215: Blíže viz kap. 2.2.1 Triáda CIA

216: Viz § 35 odst. 2 ZoOUI

217: Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů.

218: § 2 zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů. Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury.

**i) základní službou služba, jejíž poskytování je závislé na sítích elektronických komunikací[219] nebo informačních systémech a jejíž narušení by mohlo mít významný dopad na zabezpečení společenských nebo ekonomických činností v některém z těchto odvětví**

**1. energetika,**
**2. doprava,**
**3. bankovnictví,**
**4. infrastruktura finančních trhů,**
**5. zdravotnictví,**
**6. vodní hospodářství,**
**7. digitální infrastruktura,**
**8. chemický průmysl,**

**j) informačním systémem základní služby informační systém, na jehož fungování je závislé poskytování základní služby,**

**k) provozovatelem základní služby orgán nebo osoba, která poskytuje základní službu a která je určena Národním úřadem pro kybernetickou a informační bezpečnost (dále jen „Úřad") podle § 22a; pro účely plnění informační povinnosti podle příslušného předpisu Evropské unie[220] se za provozovatele základní služby považují též orgány a osoby uvedené v § 3 písm. c) a d),**

**l) digitální službou služba informační společnosti podle zákona upravujícího některé služby informační společnosti[221], která spočívá v provozování**

**1. on-line tržiště, které spotřebiteli nebo prodávajícímu umožňuje on-line uzavírat s prodávajícím podnikatelem[222] kupní smlouvu nebo smlouvu o poskytnutí služeb, a to prostřednictvím internetové stránky on-line tržiště nebo prostřednictvím internetové stránky prodávajícího, který využívá službu poskytovanou on-line tržištěm,**
**2. internetového vyhledávače, který umožňuje provádět vyhledávání v zásadě na všech internetových stránkách, a to na základě dotazu uživatele na jakékoliv téma v podobě klíčového slova, sousloví nebo jiného zadání, přičemž služba poskytuje odkazy, na nichž lze nalézt informace související s požadovaným obsahem, nebo**
**3. cloud computingu, který umožňuje přístup k rozšiřitelnému a přizpůsobitelnému úložišti nebo výpočetním zdrojům, které je možné sdílet, a**

**m) příslušným orgánem orgán vykonávající působnost v oblasti kybernetické bezpečnosti.**

---

219: § 2 písm. h) zákona č. 127/2005 Sb., ve znění pozdějších předpisů.

220: Čl. 5 odst. 7 směrnice Evropského parlamentu a Rady (EU) 2016/1148

221: § 2 písm. a) zákona č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti).

222: § 2 odst. 1 písm. a) a b) zákona č. 634/1992 Sb., o ochraně spotřebitele, ve znění pozdějších předpisů. § 419 a 420 zákona č. 89/2012 Sb., občanský zákoník.

Z důvodové zprávy:

*Pojem **kybernetického prostoru** je definován jako informační prostředí k realizaci informačních transakcí, které je vytvořeno technologiemi, jejichž definice a podmínky užívání upravují zvláštní zákony, tj. informačními systémy, službami a sítěmi elektronických komunikací. Jedná se přitom i o takové informační systémy, služby a sítě elektronických komunikací, které nejsou připojeny k veřejné síti, tj. k internetu.*

*Pojem **kybernetické bezpečnosti** není definován obecně ale jako souhrn základních zákonných institutů. Účelem definice tohoto pojmu prostřednictvím odkazu ke konkrétním zákonným institutům je dostát principu minimalizace zásahu do práv povinných osob a stanovit působnost zákona a pravomoc příslušných orgánů veřejné moci jen v nezbytně nutném rozsahu. Zákon definuje legislativní význam tohoto pojmu, přičemž jeho materiální rozsah je omezen v souladu s věcnou působností zákona, tj. na právní, organizační, technické a vzdělávací prostředky k dosažení účelu zákona. Mezi právní prostředky patří vedle samotného zákona též prováděcí právní předpisy a individuální právní akty vydávané na základě tohoto zákona, tj. protiopatření. Organizačními a technickými prostředky jsou myšlena především zákonná organizační a technická bezpečnostní opatření. Jako vzdělávací prostředky jsou označeny nejrůznější informační a osvětové nástroje, jejichž tvorbu a užití zákon předpokládá za účelem prevence kybernetických bezpečnostních incidentů.*

*Definice pojmu **kritická informační infrastruktura** vychází z právních předpisů upravujících oblast krizového řízení. Vychází se přitom z předpokladu, že kritická informační infrastruktura bude součástí kritické infrastruktury, která je vymezena zákonem č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon) ve znění pozdějších předpisů („dále jen krizový zákon"). Aby mohl být určitý informační systém nebo služba a síť elektronických komunikací zařazena do kritické informační infrastruktury, bude muset splnit definiční kritéria kritické infrastruktury, jakož i prvku kritické infrastruktury, vymezené krizovým zákonem a dále pak i průřezová a odvětvová kritéria stanovená nařízením vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury. V odvětvových kritériích pro určení prvku kritické infrastruktury se předpokládá doplnění bodu VI. „Komunikační a informační systémy" o oblast kybernetické bezpečnosti, v níž budou stanovena odvětvová kritéria pro určení daného informačního systému, služby nebo sítě elektronických komunikací kritickou informační infrastrukturou. Těmito kritérii bude především skutečnost, že daný informační systém, služba nebo síť elektronických komunikací bude zajišťovat provoz již určeného prvku kritické infrastruktury a bude pro tento prvek nenahraditelný anebo, že daný informační systém, služba nebo síť elektronických komunikací bude zajišťovat jinou významnou činnost nebo službu sám o sobě, aniž by byl spojen s již určeným prvkem. Pokud jednotlivé informační systémy, služby a sítě elektronických komunikací splní všechny shora uvedené podmínky, budou určeny prvkem kritické infrastruktury standardním postupem podle krizového zákona. Pokud bude provozovatelem daného prvku organizační složka státu, bude prvek určen usnesením vlády, v ostatních případech pak opatřením obecné povahy vydaným NBÚ a tímto postupem se tyto systémy, služby nebo sítě stanou kritickou informační infrastrukturou podle zákona o kybernetické bezpečnosti.*

*Pojem **bezpečnosti informací** vychází ve své definici z významu tohoto pojmu v odvětví informačních věd a týká se důvěrnosti (tj. diskrece), jednoty (tj. integrity) a dostupnosti informace. Pojem se netýká obsahu informace, ale pouze funkčnosti prostředí, v němž je informace tvořena, zpracovávána, uchovávána a komunikována. To odpovídá principu technologické neutrality, na němž zákon spočívá a má za následek důsledné vyčlenění kritéria obsahu informací z věcné působnosti zákona.*

*Pojem **významného informačního systému** odkazuje k systémům, jejichž správcem je orgán veřejné moci a které mají zásadní význam pro fungování veřejné správy. V tomto případě není použito rozdělení na informační a komunikační systém, neboť z definice plyne, že do pojmu informačního systému spadá vždy i jeho vnitřní komunikační složka.*

*Významným informačním systémem podle zákonné definice může být i systém, který neodpovídá definici obsažené v § 2 zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů, jehož správcem je orgán veřejné moci a jehož důležitost odůvodnila jeho zařazení mezi významné informační systémy.*

*Pojem **správce informačního, respektive komunikačního systému** je definován obdobně jako v zákoně č. 365/2000 Sb., přičemž definice je založena na faktickém stanovení účelu příslušného systému a podmínek jeho provozování. Pro účely tohoto zákona je třeba vymezit pojem správce, neboť ten bude především povinnou osobou, na níž bude dopadat právní regulace. Pokud by tento pojem vymezen nebyl, mohly by vznikat interpretační obtíže s tím, kdo ponese odpovědnost za neplnění povinností stanovených tímto zákonem. Povinnou osobu by tak podle navrhované definice měl být ten, kdo určuje účel daného systému, respektive podmínky jeho provozování (typicky jeho vlastník), nikoliv ten, kdo se smluvně zavázal k provozu daného systému.*

*Pojem **významné sítě** je definován tak, aby zahrnoval jednak páteřní sítě, jejichž prostřednictvím je kybernetický prostor na území České republiky propojen do zahraničí. Vzhledem k důležitosti kritické informační infrastruktury je jako významná síť označena touto legální definicí též síť, která sama o sobě není prvkem kritické informační infrastruktury, ale která zajišťuje připojení kritické informační infrastruktury ke kybernetickému prostoru. Relativně menší bezpečnostní expozice významné sítě v porovnání s kritickou informační infrastrukturou se projevuje v dalších ustanoveních zákona omezeným katalogem povinností ukládaných zákonem jejich správcům.*

Z důvodové zprávy k novele ZoKB:

*Ustanovení doplňuje a zpřesňuje již existující definici **bezpečnosti informací**, která s ohledem na probíhající novelu zákona o kybernetické bezpečnosti zahrnuté ve sněmovním tisku č. 852 zahrnuje i bezpečnost dat. Termín autenticita, který nad rámec uvedených požadavků uvádí směrnice, lze obsahově zahrnout pod integritu, z tohoto důvodu nebyl tento termín do návrhu zákona zapracován.*

*Navrhovaná úprava ustanovení písmene d) výslovně stanoví, že* ***významný informační systém není totožný s informačním systémem základní služby****, jak je dále definován zákonem. Tato úprava odpovídá systematice zákona o kybernetické bezpečnosti, který rozlišuje mezi informačním systémem a komunikačním systémem kritické informační infrastruktury, významným informačním systémem a informačním systémem základní služby (dále také „informační systém ZS") a spolu s nimi mezi adresáty zákonných povinností, tedy správci a provozovateli informačního systému základní služby a provozovateli základních služeb.*

*Ustanovení transponuje do českého právního řádu čl. 4 směrnice NIS, který definuje pojmy dále ve směrnici používané. Návrh zákona neobsahuje všechny definice ze směrnice, neboť některé z nich bude zapotřebí definovat až v prováděcím právním předpise. Předložený návrh zákona v případě, že některý z definičních termínů je již v českém právním řádu upraven, nevytváří novou definici, ale prostřednictvím poznámky pod čarou odkazuje na již existující pojem.*

*Jeden z nových významných termínů pro budoucí aplikaci zákona „****základní služba****" je v tomto ustanovení definována za použití základních definičních znaků uvedených v čl. 5 odst. 2 směrnice, které tato služba musí splňovat, a vymezení odvětví tak, aby NBÚ mohl následně za použití podrobných kritérií stanovených prováděcím právním předpisem určit provozovatele základní služby. Taxativně stanovená odvětví vychází jak z Přílohy II směrnice, tak i z praktických zkušeností NBÚ. Význam základních služeb je pak vnímán obdobně významu služeb, jež jsou závislé na komunikačních nebo informačních systémech kritické komunikační infrastruktury. Provozovatelé základních služeb budou určováni členským státem, ve kterém poskytují základní službu, přičemž se předpokládá, že v tom samém státě budou zpravidla i usazeni. V případě možného přeshraničního dopadu bude mít takový členský stát povinnost před určením konzultovat ostatní dotčené členské státy EU.*

*Odvětvími, která vymezuje příloha II směrnice, jsou: energetika, doprava, bankovnictví, infrastruktura finančních trhů, zdravotnictví, dodávky a rozvody pitné vody a digitální infrastruktura. Směrnice však ukládá členským státům regulovat provozovatele základní služby podle zásady minimální harmonizace, je tudíž možné, aby členské státy tuto úpravu rozšířily i na další, směrnicí neuváděná odvětví. NBÚ již dříve identifikoval oblasti, které nejsou současnou regulací pokryty (viz dokument Bílá místa kybernetické bezpečnosti v České republice schválený usnesením vlády ze dne 24. srpna 2016 č. 725), přičemž v rámci výše zmíněného principu se rozhodl začlenit mezi nově regulované oblasti i chemický průmysl, který může dle názoru NBÚ představovat z pohledu kybernetického ohrožení možný cíl.*[223] *Nebezpečné jsou v tomto ohledu zejména malwary napadající průmyslové řídicí systémy (např. Duqu). Příkladem mohou být tzv. Nitro útoky z roku 2011, jejichž cílem byla průmyslová* špionáž, která postihla nejméně 48 firem, z nichž 29 spadalo do oblasti chemického průmyslu.[224]

223: Více k důležitosti ochrany kybernetické bezpečnosti chemického průmyslu např. zde: http://www.idsa.in/cbwmagazine/chemicals-controls-and-cyber_msharma

224: Viz zpráva společnosti Symantec: https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_nitro_attacks.pdf

*Do odvětví digitální infrastruktury bude prováděcí vyhláška v souladu se směrnicí zahrnovat: výměnné uzly internetu, poskytovatele služeb systému doménových jmen a registry internetových domén nejvyšší úrovně.*

*Podle recitálu 18 je funkcí výměnného uzlu internetu propojovat sítě. Výměnný uzel internetu neposkytuje přístup k internetu ani nefunguje jako poskytovatel tranzitního připojení nebo tranzitní infrastruktury. Výměnný uzel internetu rovněž neposkytuje další služby, které nesouvisejí s propojením, což ovšem nebrání provozovateli uzlu, aby takové služby poskytoval. Výměnný uzel internetu existuje za účelem propojení sítí, které jsou z technického a organizačního hlediska oddělené. Pojem „autonomní systém" se používá k označení technicky soběstačné sítě.*

*U poskytovatelů služeb systému doménových jmen by mělo jít především o registrátory domén. Co se týče registrů internetových domén nejvyšší úrovně, jsou jimi myšleny zejména registry národních domén, v případě České republiky tedy registr národní domény.CZ.*

*Směrnice NIS výslovně vyjímá ze své působnosti podnikatele zajišťující veřejné sítě elektronických komunikací a poskytující veřejně dostupnou službu elektronických komunikací a poskytovatele služeb vytvářejících důvěru pro elektronické transakce na vnitřním trhu.*

*Na rozdíl od oblasti základních služeb, která vychází z principu minimální harmonizace, v oblasti digitálních služeb směrnice zavádí maximální harmonizaci. Okruh digitálních služeb je tedy jasně taxativně stanoven na služby vyhledávače, online tržiště a cloud computingu.*

***Definice vyhledávače** samozřejmě zahrnuje klasické provozovatele této služby, jako je například www.seznam.cz nebo www.google.com. Předkladatel však pokládá za podstatné zdůraznit, že v souladu se směrnicí a jejím recitálem 16 se za vyhledávač nepovažuje vyhledávání v rámci jedné konkrétní internetové stránky, obvykle nabízené pod ikonkou lupy, či textového odkazu na vyhledávání.*

***Definice on-line tržiště** je ve směrnici odlišná (širší), než jak je tento pojem vymezen v nařízení o řešení spotřebitelských sporů on-line a o změně nařízení (ES) č. 2006/2004 a směrnice 2009/22/ES (nařízení o řešení spotřebitelských sporů on-line), které v čl. 4 písm. f) definuje internetové tržiště („online marketplace") jako službu „umožňující spotřebitelům a obchodníkům uzavírat kupní smlouvy nebo smlouvy o poskytování služeb uzavírané on-line, na obchodníkových stránkách", ačkoliv další definiční znaky pojmu on-line tržiště (obchodník a spotřebitel) jsou totožné, neboť obě směrnice u těchto pojmů odkazují na směrnici 2013/11/EU o alternativním řešení spotřebitelských sporů a o změně nařízení (ES) č. 2006/2004 a směrnice 2009/22/ES (směrnice o alternativním řešení spotřebitelských sporů).*

*Podrobnější vymezení on-line tržiště je v recitálu 15, který stanoví, že prostřednictvím on-line tržiště mohou spotřebitelé a obchodníci s konečnou platností uzavírat s obchodníky on-line smlouvy o prodeji nebo o poskytnutí služeb. Neměly by na něm být nabízeny on-line služby, jež fungují pouze jako služby*

*zprostředkovatelské, směřující ke službám třetích stran, s nimiž lze teprve uzavřít smlouvu. Neměly by na něm být tudíž nabízeny on-line služby, jež poskytují srovnání cen konkrétních produktů či služeb různých obchodníků, aby následně uživatele přesměrovaly k nákupu u zvoleného obchodníka. Výpočetní služby poskytované on-line tržištěm mohou zahrnovat zpracování transakcí, shromažďování údajů nebo sestavování uživatelských profilů. Za druh on-line tržiště se mají považovat obchody s aplikacemi, jež jsou provozovány jako on-line obchody umožňující digitální distribuci aplikací nebo softwarových programů třetích stran.*

*Za službu on-line tržiště tedy nelze pokládat on-line služby, jako jsou například stránky www.heureka.cz.*

***Definice cloud computingu** uvedená v návrhu zákona odpovídá smyslu definice upravené směrnicí, přičemž by předkladatel rád zdůraznil, že tato definice zahrnuje různé typy cloud computingu, jako například IaaS (Infrastructure as a Service), PaaS (Platform as a Service), SaaS (Software as a Service).*

*Směrnice ve svém čl. 1 odst. 2 písm. e) stanoví povinnost členských států určit vnitrostátní příslušné orgány pro zajištění řádné implementace směrnice, kterým je v České republice NBÚ. Předkladatel považoval za důležité vymezit věcnou působnost těchto příslušných orgánů jak s ohledem na působnost NBÚ, tak i vzhledem k přeshraniční spolupráci mezi příslušnými orgány, kterou směrnice taktéž upravuje.*

Ustanovení § 2 ZoKB se věnuje vymezení základních pojmů, které jsou dále v zákoně využívány. Některé z těchto pojmů byly již v této monografii definovány, proto na ně bude pouze odkázáno.

**K písm. a)**
**Kybernetický prostor**
K pojmu **kybernetický prostor** viz kap. 1 Kyberprostor (Cyberspace).
K pojmu **informační systém** viz § 1 ZoKB
K pojmu **síť elektronických komunikací** viz § 1 ZoKB, § 2 písm. h) ZoEK či čl. 4 odst. 1 písm. a) NIS.

**Službou elektronických komunikací** se dle § 2 písm. n) ZoEK rozumí služba obvykle poskytovaná za úplatu, která spočívá zcela nebo převážně v přenosu signálů po sítích elektronických komunikací, včetně telekomunikačních služeb a přenosových služeb v sítích používaných pro rozhlasové a televizní vysílání a v sítích kabelové televize, s výjimkou služeb, které nabízejí obsah prostřednictvím sítí a služeb elektronických komunikací nebo vykonávají redakční dohled nad obsahem přenášeným sítěmi a poskytovaným službami elektronických komunikací; nezahrnuje služby informační společnosti, které nespočívají zcela nebo převážně v přenosu signálů po sítích elektronických komunikací.

Z výše uvedené dikce zákona jednoznačně vyplývá, že do služby elektronických komunikací není možné zařadit služby informační společnosti, které jsou poskytované na základě zákona č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti).

Definice kybernetického prostoru dle § 2 písm. a) ZoKB tak může působit nedostatečně, neboť by se muselo jednat o prostředí, které je tvořeno informačními systémy a službami a sítěmi elektronických komunikací.

Zákonodárce v definici opomenul služby, které jsou službami informační společnosti (viz NIS a ZSIS), a které představují podstatnou část služeb poskytovaných jednotlivými ISP v kyberprostoru. Byť je možné konstatovat, že v souladu s čl. 4 odst. 1 písm. c) NIS nebylo třeba novelizovat či měnit pojem informační systém, neboť se za tento systém považují i digitální data, jsme přesvědčeni o tom, že by bylo vhodné vlastní pojem kybernetický prostor lépe definovat. De lege ferenda by bylo například možné využít následující definici:

„*Kybernetickým prostorem se rozumí digitální prostředí umožňující vznik, zpracování a výměnu* ***digitálních dat*** *a informací, tvořené informačními systémy* ***a službami informační společnosti***.“ [225]

Pojem služba informační společnosti je pojmem nadřazeným pojmům služba a sítě elektronických komunikací dle ZoEK.

Vlastní **pojem služba** je třeba vykládat i v kontextu Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000 o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu („směrnice o elektronickém obchodu“) a Směrnice Evropského Parlamentu a Rady (EU) 2015/1535 ze dne 9. září 2015 o postupu při poskytování informací v oblasti technických předpisů a předpisů pro služby informační společnosti[226], která v čl. 1 písm. b) uvádí, že službou se rozumí: *„jakákoli služba informační společnosti, tj. každá služba poskytovaná zpravidla za úplatu, na dálku, elektronicky a na individuální žádost příjemce služeb.“*

Dle čl. 2 písm. b) směrnice 2000/31/ES je **poskytovatelem** každá fyzická nebo právnická osoba, která poskytuje určitou službu informační společnosti.

Služba informační společnosti dle výše uvedených právních norem i dle ZSIS v sobě totiž zahrnuje služby, které jsou poskytované jak poskytovateli připojení, tak poskytovateli dalších služeb (např. cashing, hosting).

225: Navržené změny jsou vyznačeny tučně.

226: Dále jen **směrnice 2015/1535**

**K písm. b)**

## Kritická informační infrastruktura

**Kritickou infrastrukturou** se dle § 2 písm. g) zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon)[227] rozumí prvek kritické infrastruktury nebo systém prvků kritické infrastruktury narušení, jehož funkce by mělo závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu.

**Prvkem kritické infrastruktury** se dle § 2 písm. i) KZ rozumí zejména stavba, zařízení, prostředek nebo veřejná infrastruktura[228], určené podle průřezových a odvětvových kritérií.

**Průřezová a odvětvová kritéria** jsou stanovena nařízením vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury.

**Průřezovým kritériem** dle § 1 nařízením vlády č. 432/2010 Sb., ve znění novely č. 315/2014 Sb. pro určení prvku kritické infrastruktury **je hledisko:**

a) **obětí** s mezní hodnotou více než 250 mrtvých nebo více než 2500 osob s následnou hospitalizací po dobu delší než 24 hodin,
b) **ekonomického dopadu** s mezní hodnotou hospodářské ztráty státu vyšší než 0,5 % hrubého domácího produktu, nebo
c) **dopadu na veřejnost** s mezní hodnotou rozsáhlého omezení poskytování nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího více než 125000 osob.

V případě, že může mít narušení bezpečnosti informací (viz triáda CIA) konkrétního informačního nebo komunikačního systému za následek **alespoň jedno z výše uvedených průřezových kritérií, je třeba dále zkoumat, zda jsou naplněna i odvětvová kritéria**. V případě, že budou naplněna i odvětvová kritéria je daný prvek nebo systém prvků možné označit za **kritickou informační infrastrukturu.**

**Odvětvová kritéria** pro určení prvku kritické infrastruktury **v oblasti kybernetické bezpečnosti** jsou uvedena v příloze nařízení vlády č. 432/2010 Sb., ve znění novely č. 315/2014 Sb. **odvětví VI., část G.** Konkrétně se jedná o:

a) **informační systém**, který **významně** nebo **zcela ovlivňuje činnost** určeného **prvku kritické infrastruktury**, a který je **nahraditelný** jen **při vynaložení nepřiměřených nákladů nebo** v časovém období přesahujícím **8 hodin**,

227: Dále jen krizový zákon či **KZ**

228: Zákon č. 183/2006 Sb., o územním plánování a stavebním řádu (stavební zákon), ve znění pozdějších předpisů

b) **komunikační systém**, který **významně** nebo **zcela ovlivňuje činnost** určeného **prvku kritické infrastruktury**, a který je **nahraditelný** jen **při vynaložení nepřiměřených nákladů nebo** v časovém období přesahujícím **8 hodin**,
c) **informační systém spravovaný orgánem veřejné moci obsahující osobní údaje o více než 300000 osobách**,
d) **komunikační systém, zajišťující připojení nebo propojení prvku kritické infrastruktury**, s kapacitou garantovaného datového přenosu nejméně **1 Gbit/s**.

Dále je možné pro určení prvku kritické infrastruktury v oblasti kybernetické bezpečnosti využít i odvětvová kritéria uvedená v písmenech A. až F., za podmínky, že je ochrana prvku naplňujícího tato kritéria nezbytná pro zajištění kybernetické bezpečnosti. Konkrétně se jedná o:

VI. KOMUNIKAČNÍ A INFORMAČNÍ SYSTÉMY

**A. Technologické prvky pevné sítě elektronických komunikací:**
a) centrum řízení a podpory sítě,
b) řídící ústředna,
c) mezinárodní ústředna,
d) transitní ústředna,
e) datové centrum,
f) telekomunikační vedení.

**B. Technologické prvky mobilní sítě elektronických komunikací:**
a) centrum řízení a podpory sítě,
b) ústředna mobilní sítě,
c) základnová řídící jednotka sítě pokrývající strategickou lokalitu,
d) základnová stanice sítě pokrývající strategickou lokalitu,
e) datové centrum.

**C. Technologické prvky sítí pro rozhlasové a televizní vysílání:**
a) vysílací zařízení pro šíření televizního nebo rozhlasového signálu určených pro informaci obyvatelstva za krizových situací s vysílacím výkonem nejméně 1 kW k zajištění provozu rozhlasového a televizního vysílání veřejnoprávního provozovatele,
b) řídící pracoviště provozu,
c) datové centrum,
d) síť pro rozhlasové a televizní vysílání k zajištění provozu rozhlasového a televizního vysílání veřejnoprávního provozovatele.

**D. Technologické prvky pro satelitní komunikaci:**
a) hlavní pozemní satelitní přijímací a vysílací stanice,
b) Evropský globální navigační družicový systém,

c) pozemní řídící a komunikační středisko,
d) pozemní propojovací síť.

**E. Technologické prvky pro poštovní služby:**
a) centrální a regionální výpočetní středisko, středisko centrálního snímání a úložiště dat,
b) sběrný přepravní uzel,
c) řídící a mezinárodní pošta,
d) poštovní dopravní infrastruktura.

**F. Technologické prvky informačních systémů:**
a) řídicí centrum,
b) datové centrum,
c) síť elektronických komunikací,
d) technologický prvek zajišťující provoz registru doménových jmen „CZ" a zabezpečení provozu domény nejvyšší úrovně „CZ".

Proces určování prvku kritické informační infrastruktury je vhodně znázorněn v následujícím diagramu vydaném NÚKIB.[229]

229: *Proces určování kritické informační infrastruktury.* [online]. [cit. 7. 8. 2018]. Dostupné z: https://nukib.cz/download/kii-vis/Schema_KII.pdf

Obrázek 18: Kritická informační infrastruktura

# Kritická informační infrastruktura

## Proces určování podle zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon) a nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury ve znění novely č. 315/2014 Sb.

Národní úřad pro kybernetickou a informační bezpečnost

NÚKIB

**Jsou dána tato průřezová kritéria:**

*(Průřezová kritéria podle § 1 nařízení vlády č. 432/2010 Sb., ve znění novely č. 315/2014 Sb.)*

a) Více než 250 mrtvých nebo více než 2 500 osob s následnou hospitalizací delší než 24 hodin.

b) Mezní hodnota hospodářské ztráty je větší než 0,5 % HDP (např. v r. 2013 = 19,4 mld. Kč).

c) Omezení poskytování nezbytných služeb nebo jiný závažný zásah do každodenního života postihující více než 125 000 osob.

Může mít narušení bezpečnosti informací (důvěrnosti, dostupnosti, integrity) Vašeho IS nebo KS za následek **ALESPOŇ** jedno z výše uvedených průřezových kritérií?

ANO

NE

Váš IS nebo KS v tuto chvíli není kritickou informační infrastrukturou. Může však být významným informačním systémem (jste-li orgánem veřejné moci), viz. schéma o významných informačních systémech, dostupné na webu www.GovCERT.cz.

**Jsou dána tato odvětvová kritéria v oblasti kybernetické bezpečnosti:**

*(Odvětvová kritéria podle nařízení vlády č. 432/2010 Sb. ve znění novely č. 315/2014 Sb., příloha - odvětví VI., část G.)*

a), b) Ovlivňuje Váš IS nebo KS významně nebo zcela činnost určeného prvku KI a zároveň je nahraditelný jen při vynaložení nepřiměřených nákladů nebo v časovém období delším jak 8 hodin?

c) Je Váš IS spravovaný orgánem veřejné moci obsahující osobní údaje o více než 300 tis. osobách?

d) Je Váš systém komunikačním systémem, který zajišťuje připojení nebo propojení prvku KI s kapacitou garantovaného datového přenosu min. 1 Gbit/s?

e) Odvětvová kritéria pro určení prvku KI uvedená v písm. A. – F., odvětví VI. přílohy nařízení vlády č. 432/2010 Sb., ve znění novely č. 315/2014 Sb., se použijí přiměřeně pro oblast KB, pokud je ochrana prvku naplňujícího tato kritéria nezbytná pro zajištění kybernetické bezpečnosti.

Splňuje Váš IS nebo KS **ALESPOŇ** jedno z výše uvedených odvětvových kritérií?

ANO

NE

**Jsou dána tato odvětvová kritéria (odvětví VI. Komunikační a informační systémy)**

**A. Technologické prvky pevné sítě elektronických komunikací**:
a) centrum řízení a podpory sítě,
b) řídící ústředna,
c) mezinárodní ústředna,
d) transitní ústředna,
e) datové centrum,
f) telekomunikační vedení.

**B. Technologické prvky mobilní sítě elektronických komunikací**:
a) centrum řízení a podpory sítě,
b) ústředna mobilní sítě,
c) základnová řídící jednotka sítě pokrývající strategickou lokalitu,
d) základnová stanice sítě pokrývající strategickou lokalitu,
e) datové centrum.

**C. Technologické prvky sítí pro rozhlasové a televizní vysílání**:
a) vysílací zařízení pro šíření televizního nebo rozhlasového signálu určených pro informaci obyvatelstva za krizových situací vysílacím výkonem nad 1 kW k zajištění rozhlasového a televizního vysílání veřejnoprávního provozovatele
b) řídící pracoviště provozu,
c) datové centrum,
d) síť pro rozhlasové a televizní vysílání k zajištění provozu rozhlasového a televizního vysílání veřejnoprávního provozovatele.

**D. Technologické prvky pro satelitní komunikaci**:
a) hlavní pozemní satelitní přijímací a vysílací stanice,
b) Evropský globální navigační družicový systém,
c) pozemní řídící a komunikační středisko,
d) pozemní propojovací síť.

**E. Technologické prvky pro poštovní služby**:
a) centrální a regionální výpočetní středisko, středisko centrálního snímání a úložiště dat,
b) sběrný přepravní uzel,
c) řídící a mezinárodní pošta,
d) poštovní dopravní infrastruktura.

**F. Technologické prvky informačních systémů**:
a) řídící centrum,
b) datové centrum,
c) síť elektronických komunikací,
d) technologický prvek zajišťující provoz registru doménových jmen „CZ" a zabezpečení provozu domény nejvyšší úrovně „CZ".

**G. Oblast kybernetické bezpečnosti**:
viz. předchozí blok vlevo

Váš IS nebo KS splňuje podmínky pro zařazení do kritické informační infrastruktury.

Jste organizační složkou státu?

ANO

NE

Váš IS nebo KS určí jako KII vydáním opatření obecné povahy NÚKIB. Podle § 2, písm. b) zákona č. 181/2014 Sb. se Váš KS nebo IS stává prvkem kritické informační infrastruktury.

NÚKIB navrhne Ministerstvu vnitra zařadit Váš IS nebo KS do seznamu, který bude následně předložen vládě ČR. Vláda ČR rozhodne usnesením a navrhovaný IS nebo KS určí v příloze k tomuto usnesení prvkem KI. Podle § 2, písm. b) zákona č. 181/2014 Sb. se Váš KS nebo IS stává prvkem kritické informační infrastruktury.

Více informací o procesech určování a posuzování, včetně povinností orgánů a osob, naleznete na www.GovCERT.cz

Použité zkratky: IS - informační systém, KB - kybernetická bezpečnost, KI - kritická infrastruktura, KII - kritická informační infrastruktura, KS - komunikační systém, NÚKIB - Národní úřad pro kybernetickou a informační bezpečnost, OOP - opatření obecné povahy

verze 2.0, platná ke dni 20. 3. 2018

**Poznámka:**

V rámci procesu určování kritické informační infrastruktury (KII) bude NÚKIB s dotčenými subjekty jednat a to již před samotným určením. Samotné určení pak proběhne, po oboustranném jednání. U organizačních složek státu probíhá určení prvků KII vydáním usnesení vlády ČR. U orgánů nebo osob, které nejsou organizační složkou státu, probíhá určení vydáním opatření obecné povahy (OOP), které vydá NÚKIB. NÚKIB je k dispozici k případnému jednání a k poskytnutí metodické pomoci v rámci posouzení naplnění určujících kritérií.

**Upozornění:**

**Dokument slouží pouze jako podpůrné vodítko, nenahrazuje žádný ze zákonů a souvisejících prováděcích předpisů. Právo změny tohoto dokumentu vyhrazeno.**

**K písm. c)**

### Bezpečnost informací

Pojem **bezpečnost informací** je v kontextu ZoKB chápán jako zajištění **důvěrnosti, integrity a dostupnosti informací a dat. K** těmto **základním principům kybernetické bezpečnosti a k pojmu data** viz kap. 2.2 Principy kybernetické bezpečnosti.

Regulace bezpečnosti informací, tak jak je vymezena v ZoKB, se **nevztahuje na obsah informace, ale pouze funkčnosti prostředí, v němž je informace tvořena, zpracovávána, uchovávána a komunikována.** Toto negativní vymezení působnosti ZoKB odpovídá principu technologické neutrality.[230]

**K písm. d)**

### Významný informační systém

**Významným informačním systémem** je **informační systém spravovaný orgánem veřejné moci a u kterého narušení bezpečnosti informací může omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci.**

**Významným informačním systémem není systém**, který je kritickou informační infrastrukturou či informačním systémem základní služby.

Dle § 2 písm. b) zákona č. 365/2000 Sb., o informačních systémech veřejné správy se **informačním systémem veřejné správy** rozumí funkční celek nebo jeho část zabezpečující cílevědomou a systematickou informační činnost pro účely výkonu veřejné správy. Každý informační systém veřejné správy zahrnuje data, která jsou uspořádána tak, aby bylo možné jejich zpracování a zpřístupnění, provozní údaje a dále nástroje umožňující výkon informačních činností.

Vlastní stanovení významných informačních systémů je uvedeno ve **vyhlášce č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích.**[231] Pro to, aby mohl být informační systém označen za významný, musí splnit určující kritéria, kterými jsou:

a) **dopadová určující kritéria** a
b) **oblastní určující kritéria**.

**Zároveň vyhláška** č. 317/2014 Sb. **negativně vymezuje informační systémy, které nejsou významným informačním systémem**. Konkrétně se jedná o informační systém, jehož správcem je obec[232] a při výkonu působnosti obce hlavní město Praha.

230: Viz kap. 4.2 Základní cíle a principy ZoKB

231: [online]. Dostupné z: https://nukib.cz/download/kii-vis/VVIS_UZ.pdf

232: Zákon č. 128/2000 Sb., o obcích (obecní zřízení), ve znění pozdějších předpisů.

**Dopadovým určujícím kritériem** dle § 4 písm. a) vyhlášky č. 317/2014 Sb. je skutečnost, že **úplná nebo částečná nefunkčnost informačního systému** způsobená narušením bezpečnosti informací **by mohla mít negativní vliv na**:

1) **fungování orgánu veřejné moci**,
2) **poskytování služeb** nebo informací orgánem veřejné moci veřejnosti,
3) **hospodaření** orgánu veřejné moci nebo hospodaření orgánu veřejné moci, který je správcem významného informačního systému, anebo hospodaření orgánu nebo osoby, která je správcem informačního nebo komunikačního systému kritické informační infrastruktury, nebo
4) **provoz jiného významného informačního systému** využívajícího služeb hodnoceného informačního systému, který je nefunkční.

Zároveň musí být naplněna podmínka, že **omezení činnosti takového systému by mohlo mít za následek omezení výkonu působnosti orgánu** veřejné moci **po dobu delší než 3 pracovní dny**, nebo **výrazné ohrožení výkonu působnosti orgánu** veřejné moci, **které lze odvrátit za vynaložení nepřiměřených nákladů**[233] na provoz nebo obnovu informačního systému.

Vedle výše uvedeného je **dopadovým určujícím kritériem** dle § 4 písm. b) vyhlášky č. 317/2014 Sb. také ta skutečnost, že úplná nebo částečná nefunkčnost informačního systému způsobená narušením bezpečnosti informací by mohla způsobit:

1) **ohrožení nebo narušení prvku kritické infrastruktury**,
2) **oběti na životech** s mezní hodnotou více než **10 mrtvých nebo 100 zraněných osob** vyžadujících lékařské ošetření, s případnou hospitalizací s dobou delší než 24 hodin,
3) **finanční nebo materiální ztráty** s mezní hodnotou **více než 5 % stanoveného rozpočtu orgánu veřejné moci**,
4) **zásah do** osobního **života** nebo do práv fyzických nebo právnických osob postihující nejméně **50000 osob**, nebo
5) **výrazné ohrožení nebo narušení veřejného zájmu,**

přičemž následky podle bodů 1 až 4 nedosáhnou hodnot pro určení prvku kritické infrastruktury podle průřezových kritérií stanovených krizovým zákonem.

**Oblastní určující kritéria** vyplývají z přílohy č. 2 vyhlášky č. 317/2014 Sb. a spočívají ve vedení některé z níže uvedených agend či činností.

233: K pojmu **nepřiměřené náklady** blíže viz:
https://nukib.cz/download/kii-vis/container-nodeid-738/neprimerenenaklady.pdf

V případě **orgánů veřejné moci** se jedná o:

1) vedení správního řízení,
2) databáze obsahující osobní údaje,
3) hospodaření orgánu veřejné moci,
4) výkon spisové služby,
5) státní dozor,
6) kontrolní a inspekční činnost,
7) příprava na krizové situace a jejich řešení,
8) tvorba právních předpisů,
9) elektronická pošta,
10) vedení internetových stránek,
11) mezirezortní spolupráce,
12) mezinárodní spolupráce,
13) zadávání veřejných zakázek,
14) státní statistická služba.

V případě **orgánů veřejné moci – kraje v rámci přenesené působnosti** se jedná o:

1) databáze obsahující osobní údaje,
2) vedení správního řízení,
3) hospodaření orgánu veřejné moci,
4) elektronická pošta,
5) vedení internetových stránek,
6) příprava na krizové situace a jejich řešení,
7) mezinárodní spolupráce,
8) státní dozor,
9) kontrolní a inspekční činnost,
10) zadávání veřejných zakázek.

Dle přílohy č. 1 k vyhlášce č. 317/2014 Sb. mezi významné informační systémy patří:

| PČ | SPRÁVCE | NÁZEV |
|---|---|---|
| 1 | Agentura ochrany přírody a krajiny České republiky | Ekonomický informační systém JASU CS |
| 2 | Agentura ochrany přírody a krajiny České republiky | Elektronický systém spisové služby - státní správa |

| | | |
|---|---|---|
| 3 | Česká inspekce životního prostředí | Centrální informační systém (CIS) |
| 4 | Česká národní banka | JERRS - Jednotná evidence regulovaných a registrovaných subjektů |
| 5 | Česká národní banka | KRZR - Komunikační rozhraní pro Základní registry |
| 6 | Český statistický úřad | Integrovaný agendový informační systém - registr osob (IAIS-ROS) |
| 7 | Český telekomunikační úřad | ASMKS |
| 8 | Český telekomunikační úřad | MOSS |
| 9 | Český telekomunikační úřad | Spectra |
| 10 | Český úřad zeměměřický a katastrální | IS územní identifikace (ISÚI) |
| 11 | Český úřad zeměměřický a katastrální | Informační systém katastru nemovitostí (ISKN) |
| 12 | Energetický regulační úřad | Jednotný informační systém Energetického regulačního úřadu |
| 13 | Generální ředitelství cel | Centrální registr subjektů (CRS) |
| 14 | Hlavní město Praha | Ekonomický systém |
| 15 | Hlavní město Praha | Spisová služba |
| 16 | Hlavní město Praha | Webový portál (Praha.eu) |
| 17 | Hlavní město Praha | Elektronický poštovní systém |
| 18 | Jihočeský kraj | Elektronický systém |
| 19 | Jihočeský kraj | Spisová služba |
| 20 | Jihočeský kraj | Firemní e-mailová komunikace (elektronický poštovní systém) |
| 21 | Jihočeský kraj | Webový portál (webové stránky kraje) |
| 11 | Jihomoravský kraj | Poštovní server - Exchange |
| 23 | Jihomoravský kraj | Geoportál |
| 24 | Jihomoravský kraj | Ginis |

| | | |
|---|---|---|
| 25 | Jihomoravský kraj | Kevis - Krajský evidenční informační systém |
| 26 | Jihomoravský kraj | Redakční systém JMK |
| 27 | Kancelář veřejného ochránce práv | Personální informační systém VEMA |
| 28 | Kancelář veřejného ochránce práv | Informační systém spisové služby a ekonomických informací GINIS |
| 29 | Kancelář veřejného ochránce práv | Systém elektronické pošty MS Exchange |
| 30 | Karlovarský kraj | Ekonomický systém (ERP) |
| 31 | Karlovarský kraj | Spisová služba |
| 32 | Karlovarský kraj | Integrační směrnice |
| 33 | Karlovarský kraj | Webový portál (Webové stránky kraje) |
| 34 | Kraj Vysočina | Webový portál WISMO |
| 35 | Kraj Vysočina | Elektronický poštovní systém |
| 36 | Kraj Vysočina | GINIS - spisová služba |
| 37 | Kraj Vysočina | GINIS - ekonomické moduly |
| 38 | Královéhradecký kraj | Spisová služba EZOP |
| 39 | Královéhradecký kraj | Ekonomický informační systém |
| 40 | Liberecký kraj | Informační systém ekonomické agendy |
| 41 | Liberecký kraj | Informační systém elektronické spisové služby |
| 42 | Liberecký kraj | Webový portál Libereckého kraje |
| 42 | Liberecký kraj | Elektronický poštovní systém |
| 43 | Ministerstvo dopravy | Přeprava nebezpečných věcí (ADR) |
| 44 | Ministerstvo dopravy | Centralizovaný informační systém STK (CIS STK) |
| 45 | Ministerstvo dopravy | Rejstřík podnikatelů v silniční dopravě (RPSD) |
| 46 | Ministerstvo dopravy | Databáze vozidel (DAVOZ) |
| 47 | Ministerstvo dopravy | Aplikace pro testování nových řidičů a dopravců v rámci autoškol (eTesty) |
| 48 | Ministerstvo dopravy | IS Digitální tachograf (ISDT) |
| 49 | Ministerstvo dopravy | Informační systém pro podporu při schvalování technické způsobilosti vozidel (ZTP) |

| | | |
|---|---|---|
| 50 | Ministerstvo dopravy | Evidence údajů o mýtném (MÝTO) |
| 51 | Ministerstvo dopravy | Informační systém o silniční a dálniční síti ČR (ISSDS) |
| 52 | Ministerstvo financí | ISPROFIN - IS programového financování |
| 53 | Ministerstvo obrany | Biologický a monitorovací informační systém (BMIS) |
| 54 | Ministerstvo obrany | Informační systém Vojenské policie (ISVP) |
| 55 | Ministerstvo obrany | LETVIS |
| 56 | Ministerstvo obrany | Síť včasného zjištění armádní radiační monitorovací sítě (SVZ ARMS) |
| 57 | Ministerstvo obrany | Štábní informační systém AČR (ŠIS) |
| 58 | Ministerstvo obrany | Zdravotnický IS (ZDRAVIS) |
| 59 | Ministerstvo práce a sociálních věcí | Informační systém registr poskytovatelů sociálních služeb |
| 60 | Ministerstvo práce a sociálních věcí | Jednotný informační systém práce a sociálních věcí |
| 61 | Ministerstvo práce a sociálních věcí | Informační systém sociálně-právní ochrany dětí |
| 62 | Ministerstvo průmyslu a obchodu | Registr živnostenského podnikání |
| 63 | Ministerstvo průmyslu a obchodu | Ekonomický informační systém |
| 64 | Ministerstvo spravedlnosti | Evidence znalců a tlumočníků - prezenční část |
| 65 | Ministerstvo spravedlnosti | Seznam ústavů kvalifikovaných pro znaleckou činnost |
| 66 | Ministerstvo školství, mládeže a tělovýchovy | Informační systém pro kvalifikace a autorizace ISKA |
| 67 | Ministerstvo školství, mládeže a tělovýchovy | EIS (Ekonomický IS) |
| 68 | Ministerstvo školství, mládeže a tělovýchovy | EPD |

| | | |
|---|---|---|
| 69 | Ministerstvo školství, mládeže a tělovýchovy | Informační systém Akreditační komise (ISACC) |
| 70 | Ministerstvo vnitra | AIS PČR - Agendový informační systém Policie ČR |
| 71 | Ministerstvo vnitra | AZYL II - Informační systém pro evidenci udělení azylu |
| 72 | Ministerstvo vnitra | DP-2 - Informační systém orgánu sociálního zabezpečení, výpočet a výplata dávek sociálního zabezpečení |
| 73 | Ministerstvo vnitra | EKIS MV - Ekonomický informační systém Ministerstva vnitra |
| 74 | Ministerstvo vnitra | GINIS - Informační systém elektronické spisové služby |
| 75 | Ministerstvo vnitra | IS ISVS - Informační systém o informačních systémech veřejné správy |
| 76 | Ministerstvo vnitra | PVS - Portál veřejné správy |
| 77 | Ministerstvo vnitra | Systém SO - Informační systém - registr státního občanství |
| 78 | Ministerstvo vnitra | Informační systém Ústřední evidence fyzických osob, které nabyly nebo pozbyly státní občanství České republiky |
| 79 | Ministerstvo vnitra | ISoSS - Informační systém o státní službě |
| 80 | Ministerstvo zahraničních věcí | ePasy |
| 81 | Ministerstvo zahraničních věcí | Víza ČR (EVC2) |
| 82 | Ministerstvo zdravotnictví | Národní zdravotnický informační systém (NZIS) |
| 83 | Ministerstvo zdravotnictví | Ochrana veřejného zdraví |
| 84 | Ministerstvo zemědělství | Informační systém VODA |
| 85 | Ministerstvo zemědělství | Informační systém vodovodů a kanalizací (IS VaK) |
| 86 | Ministerstvo zemědělství | Integrovaný zemědělský registr (IZR) |
| 8/ | Ministerstvo zemědělství | Evidence využití půdy podle uživatelských vztahů (LPIS) |

| | | |
|---|---|---|
| 88 | Ministerstvo zemědělství | Společný zemědělský registr (SZR) |
| 89 | Ministerstvo životního prostředí | IRZ - Integrovaný registr znečišťování životního prostředí |
| 90 | Ministerstvo životního prostředí | ISPOP - Integrovaný systém plnění ohlašovacích povinností |
| 91 | Ministerstvo životního prostředí | Informační systém SEA |
| 92 | Ministerstvo životního prostředí | Informační systém EIA |
| 93 | Ministerstvo životního prostředí | MA ISOH - modul autovraky IS odpadového hospodářství |
| 94 | Ministerstvo životního prostředí | Registr CITES |
| 95 | Ministerstvo životního prostředí | IPPC - IS integrované prevence |
| 96 | Moravskoslezský kraj | Integrační sběrnice |
| 97 | Moravskoslezský kraj | Firemní e-mailová komunikace (Elektronický poštovní systém) |
| 98 | Moravskoslezský kraj | Webový portál (Webové stránky kraje www.msk.cz) |
| 99 | Moravskoslezský kraj | Systém GINIS |
| 100 | Nejvyšší kontrolní úřad | Kontrolní informační systém (KIS) |
| 101 | Nejvyšší státní zastupitelství | Centrální evidence stíhaných osob |
| 102 | Olomoucký kraj | ERP - Ekonomický systém |
| 103 | Olomoucký kraj | Spisová služba (SSL) |
| 104 | Olomoucký kraj | Integrační směrnice (ISb) |
| 105 | Olomoucký kraj | Webový portál (WP) |
| 106 | Olomoucký kraj | Elektronický poštovní systém (EPS) |
| 107 | Pardubický kraj | Integrovaný informační systém GINIS |
| 108 | Plzeňský kraj | Mailový server |
| 109 | Plzeňský kraj | Integrační sběrnice |
| 110 | Plzeňský kraj | Spisová služba |
| 111 | Plzeňský kraj | Webový portál kraje |
| 112 | Plzeňský kraj | ERP |

| | | |
|---|---|---|
| 113 | Probační a mediační služba | Agendový informační systém AIS PMS |
| 114 | Rada pro rozhlasové a televizní vysílání | Intranet RRTV |
| 115 | Správa státních hmotných rezerv | IS Argis - IS pro plánování civilních zdrojů (provozní i cvičné prostředí) |
| 116 | Správa státních hmotných rezerv | IS Krizkom - IS krizové komunikace |
| 117 | Správa základních registrů | Systém řízení přístupů do základních registrů (RACS) |
| 118 | Státní fond životního prostředí | EIS-JASU |
| 119 | Státní fond životního prostředí | SFZP-CENTRAL |
| 120 | Státní fond životního prostředí | E-SPIS |
| 121 | Státní pozemkový úřad | Agendový systém pro pozemkové úpravy (ASPU - DMS) |
| 122 | Státní pozemkový úřad | Centrální informační systém (CIS) |
| 123 | Státní úřad inspekce práce | Registr elektronizace úkonů inspekce práce (REÚIP) |
| 124 | Státní úřad pro jadernou bezpečnost | Registr externích adres (REA) |
| 125 | Státní ústav pro kontrolu léčiv | Centrální úložiště elektronických receptů |
| 126 | Státní ústav pro kontrolu léčiv | Registr léčivých přípravků s omezením |
| 127 | Státní zemědělská a potravinářská inspekce | Kontrolní a laboratorní činnost (KLČ) |
| 128 | Státní zemědělská a potravinářská inspekce | Spisová služba SZPI |
| 129 | Státní zemědělský intervenční fond | Informační systém platební agentury (ISPA) |
| 130 | Středočeský kraj | IS Ginis - ekonomický systém |
| 131 | Středočeský kraj | E-spis - spisová služba |
| 132 | Středočeský kraj | Firemní e-mailová komunikace (elektronický poštovní systém) |
| 133 | Středočeský kraj | Webový portál (webové stránky kraje) |

| | | |
|---|---|---|
| 134 | Úřad pro civilní letectví | IS Úřadu pro civilní letectví |
| 135 | Úřad pro ochranu hospodářské soutěže | GINIS - gordic integrovaný informační systém |
| 136 | Úřad pro ochranu hospodářské soutěže | elektronická pošta |
| 137 | Úřad pro ochranu hospodářské soutěže | internetové stránky |
| 138 | Úřad pro ochranu osobních údajů | IS UOOU |
| 139 | Úřad pro zastupování státu ve věcech majetkových | Informační systém majetku státu (ISMS) |
| 140 | Úřad průmyslového vlastnictví | Informační systém duševního vlastnictví (ISDV) |
| 141 | Úřad průmyslového vlastnictví | Systém průmyslových práv (SyPP) |
| 142 | Úřad vlády České republiky | Elektronická knihovna legislativního procesu (eKLEP) |
| 143 | Úřad vlády České republiky | IS výzkumu, experimentálního vývoje a inovací (IS VaVal) |
| 144 | Ústecký kraj | Ekonomický systém Navision |
| 145 | Ústecký kraj | Spisová a archivní služba EZOP |
| 146 | Ústecký kraj | Internetový portál Ústeckého kraje VISMO |
| 147 | Ústecký kraj | Poštovní server Microsoft Exchange |
| 148 | Vězeňská služba České republiky | Vězeňský informační systém (VIS) |
| 149 | Všeobecná zdravotní pojišťovna České republiky | Centrální registr pojištěnců |
| 150 | Zeměměřický úřad | IS zeměměřictví |
| 151 | Zlínský kraj | Ekonomický systém a spisová služba |
| 152 | Zlínský kraj | Webové stránky kraje |
| 153 | Zlínský kraj | Elektronický poštovní systém |

Proces určování významného informačního systému je vhodně znázorněn v diagramu vydaném NÚKIB.[234]

**K písm. e)**

**Správce informačního systému**

**Správcem informačního systému** se rozumí **orgán nebo osoba, které určují účel zpracování informací a podmínky provozování informačního systému.** Definice správce tak, jak je uvedena v ZoKB, koresponduje s vymezením správce informačního systému veřejné správy dle § 2 písm. b) zák. č. 365/2000 Sb.

Správce je osobou, na kterou bude dopadat právní regulace, zejména jí budou dle ZoKB ukládány povinnosti k zajištění kybernetické bezpečnosti (zejména dodržování bezpečnostních opatření). Správcem je ta osoba, která určuje účel daného systému, respektive podmínky jeho provozování (typicky jeho vlastník), nikoliv ten, kdo se smluvně zavázal k provozu daného systému.

**K písm. f)**

**Správce komunikačního systému**

**Správcem komunikačního systému** se rozumí **orgán nebo osoba, které určují účel komunikačního systému a podmínky jeho provozování**.

K výkladu správce viz výklad uvedený u písm. e).

**K písm. g)**

**Provozovatel informačního nebo komunikačního systému**

**Provozovatelem informačního nebo komunikačního systému** se rozumí **orgán nebo osoba zajišťující funkčnost technických a programových prostředků tvořících informační nebo komunikační systém.**

Pojem **technických a programových prostředků** je dle *„Informace o institutu provozovatele informačního nebo komunikačního systému"* vydaného NÚKIB[235] třeba vykládat tak, že postačuje, aby provozovatel zajišťoval jak pouze technické prostředky, tak pouze programové prostředky, nebo případně jejich kombinaci.

*„Jinými slovy, provozovatelem informačního či komunikačního systému je orgán nebo osoba (či také orgány či osoby), která pro správce zajišťuje funkčnost systému v určité požadované kvalitě, úrovni*

234: *Proces určování významných informačních systémů.* [online]. [cit. 7. 8. 2018]. Dostupné z: https://nukib.cz/download/kii-vis/Schema_VIS.pdf

235: [online]. Dostupné z: https://nukib.cz/download/kii-vis/provozovatel_IS-KS_v1.0-final.pdf

*bezpečnosti a rozsahu (tj. odpovídá za funkčnost hardware **nebo** software informační systém tvořící, například prostřednictvím smlouvy o zajištění určité úrovně podpory).*“ [236]

Na základě výše uvedeného výkladu jsme přesvědčeni o tom, že znění § 2 písm. g) ZoKB by mělo být následující:

„*Provozovatelem informačního nebo komunikačního systému se rozumí orgán nebo osoba zajišťující funkčnost technických **a/nebo** programových prostředků tvořících informační nebo komunikační systém.*“

Dle stanoviska NÚKIB není provozovatelem pouze subjekt, který zajišťuje pro správce funkčnost systému jako celku, ale i o osoby, které zajišťují funkčnost části systému. **NÚKIB za provozování** ve výše uvedeném smyslu také **nepovažuje jednorázové dodávky** technických a programových prostředků, bez dalších navazujících činností (typicky se jedná o servis, support aj.).

NÚKIB nepovažuje za provozovatele **subdodavatele** (dodavatele provozovatelů), neboť dle § 6a odst. 1 ZoKB může orgán nebo osobu pověřit provozováním dotčených systémů pouze jejich správce.

Ve vztahu k provozovateli je významný zejména **notifikační proces**, kterým správce informuje provozovatele o tom, že provozuje informační či komunikační systém, který spadá pod ZoKB.

**V případě, že správce neprovozuje svůj informační či komunikační systém**, tedy nezajišťuje funkčnost programových a/nebo technických prostředků, **musí provozovatele informovat** o tom, že je povinnou osobou dle konkrétního písmena § 3 ZoKB. V tomto případě je **notifikační proces stanoven přímo zákonem** (viz § 4a odst. 1 ZoKB).

NÚKIB výše popsaný vztah schematicky demonstruje na příkladu z praxe zobrazeném na Obrázku 19.

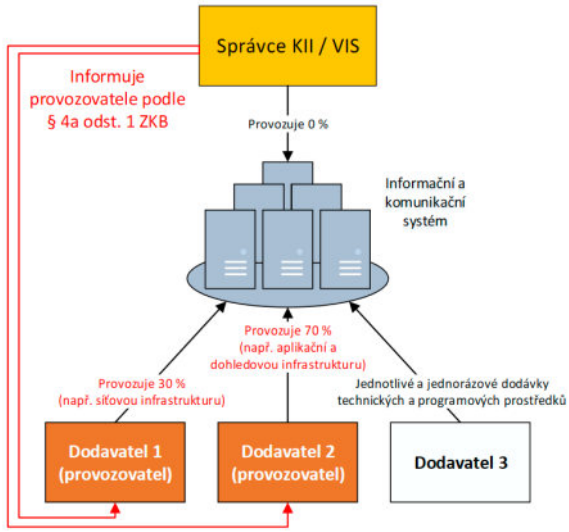
**V případě, že správce částečně provozuje svůj informační či komunikační systém a částečně využívá služeb provozovatelů** (dodavatelů), **může provozovatele pověřit provozováním** (viz § 6a odst. 1 ZoKB).

NÚKIB výše popsaný vztah schematicky demonstruje na příkladu z praxe zobrazeném na Obrázku 20.

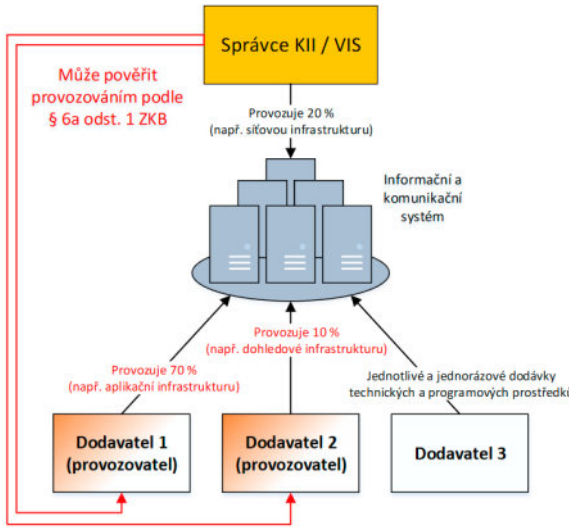
**V případě, že správce zcela provozuje svůj informační či komunikační systém, není notifikace třeba, neboť takovýto subjekt je současně správcem i provozovatelem.**

---

236: *Informace o institutu provozovatele informačního nebo komunikačního systému.* [online]. [cit. 7. 8. 2018]. Dostupné z: https://nukib.cz/download/kii-vis/provozovatel_IS-KS_v1.0-final.pdf s. 4




Obrázek 19: Schéma identifikace provozovatele dle § 4a odst. 1 ZoKB




Obrázek 20: Schéma identifikace provozovatele dle § 6a odst. 1 ZoKB

**K písm. h)**
**Významná síť elektronických komunikací**
K pojmu **síť elektronických komunikací** viz § 1 ZoKB.

**Významnou sítí** se rozumí sítě, které **zajišťují přímé zahraniční propojení do veřejných komunikačních sítí** nebo **zajišťující přímé připojení ke kritické informační infrastruktuře**.

Tento pojem zahrnuje jak páteřní sítě, jejichž prostřednictvím je kybernetický prostor na území České republiky propojen do zahraničí, tak síť, která sama o sobě není prvkem kritické informační infrastruktury, ale která zajišťuje připojení kritické informační infrastruktury ke kybernetickému prostoru.

**K písm. i), j), k)**
**Základní služba. Informační systém základní služby. Provozovatel základní služby.**
***Základní služba je služba, která je závislá na informačních systémech nebo sítích elektronických komunikací v odvětvích***:

1) **energetika,**
2) **doprava,**
3) **bankovnictví,**
4) **infrastruktura finančních trhů,**
5) **zdravotnictví,**
6) **vodní hospodářství,**
7) **digitální infrastruktura nebo**
8) **chemický průmysl.**

Vymezení jednotlivých základních služeb, jakož i stanovení kritérií pro určení provozovatele základní služby a informačního systému základní služby je uvedeno ve **vyhlášce č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby.**[237] Tato vyhláška vstoupila v účinnost 1. února 2018.

Při určení toho, zda je daná služba **základní službou**, se užijí **odvětvová a dopadová kritéria** [viz § 28 odst. 2 písm. e) ZoKB].

237: [online]. Dostupné z: https://www.zakonyprolidi.cz/cs/2017-437

**Odvětvová kritéria** jsou určena:

- druhem služby,
- druhem subjektu a
- speciálním kritériem druhu subjektu.

Speciální kritérium druhu subjektu dle § 2 odst. 2 vyhlášky č. 437/2017 Sb. zohledňuje **významnost subjektu v jednotlivém odvětví**.

**Příklad:** *Odvětvová kritéria jsou ve vyhlášce stanovena následovně (v závorce uveden zjednodušený příklad odpovídající prvnímu odvětví dle přílohy k vyhlášce):*

- *1. Odvětví (Energetika)*
- *1.1. Pododvětví (Elektřina) – pododvětví jsou stanovena*
- *pouze u odvětví Energetika a Doprava, v textu vyhlášky jsou označována souslovím „část odvětví“*
- *1.1.1. Druh služby (Výroba elektřiny)*
- *Druh subjektu (Výrobce elektřiny podle energetického zákona)*
- *a) Speciální kritérium druhu subjektu – jedná se o kritérium významnosti poskytované služby v rámci daného odvětví (Výrobna s celkovým instalovaným elektrickým výkonem nejméně 500 MW)*

*Odvětvová kritéria na sebe navazují a postupuje se od obecného ke speciálnímu.*

*Tedy v každé kategorii podle vzoru: 1. – 1.1. – 1.1.1. – Druh subjektu – a) Speciální kritérium druhu subjektu.*

*Pokud jsou odvětvová kritéria subjektem naplněna, je možné přistoupit ke kritériím dopadovým.*[238]

**Dopadová kritéria stanovují hranice možných škod** způsobených kybernetickým bezpečnostním incidentem v informačních systémech a sítích elektronických komunikací, kterých musí být pro určení dosaženo. Dopadová kritéria jsou ve vyhlášce č. 347/2017 Sb. stanovena následovně:

> Kybernetický bezpečnostní incident v informačním systému či síti elektronických komunikací by mohl způsobit:

238: *Informace o institutu základní služby.* [online]. [cit. 7. 8. 2018]. Dostupné z: https://nukib.cz/download/kii-vis/Informace_o_institutu_z%C3%A1kladn%C3%AD_slu%C5%BEby_v1.2.pdf s. 4

I. závažné omezení či narušení (či nedostupnost) druhu služby postihující více než 25000, 50000 nebo 500000 osob[239],

II. závažné omezení či narušení jiné základní služby, nebo omezení či narušení provozu prvku kritické infrastruktury,

III. hospodářskou ztrátu vyšší než 0,25 % HDP,

IV. nedostupnost druhu služby pro více než 1600 osob, která není nahraditelná jiným způsobem bez vynaložení nepřiměřených nákladů,

V. oběti na životech s mezní hodnotou více než 100 nebo 200[240] mrtvých nebo 1000 zraněných osob vyžadujících lékařské ošetření

VI. narušení veřejné bezpečnosti na významné části správního obvodu obce s rozšířenou působností, které by mohlo vyžadovat provedení záchranných a likvidačních prací složkami integrovaného záchranného systému nebo

VII. kompromitaci citlivých osobních údajů o 200000 osobách.

**Pokud subjekt naplní odvětvová kritéria a kybernetický bezpečnostní incident v jeho systému či systémech naplní dopadová kritéria, bude určen jako provozovatel základní služby a předmětný systém jako informační systém základní služby.**

Proces určení provozovatele základní služby a informačního systému základní služby je vhodně znázorněn v diagramu vydaném NÚKIB.[241]

V příloze č. 1 vyhlášky č. 437/2017 jsou definována jednotlivá odvětvová a dopadová kritéria pro určení provozovatele základní služby. Tato kritéria jsou definována následovně:

239: Hodnoty se liší v rámci jednotlivých odvětví nebo pododvětví.

240: Hodnoty se liší v rámci jednotlivých odvětví nebo pododvětví.

241: *Proces určování provozovatelů základních služeb a informačních systémů základních služeb.* [online]. [cit. 7. 8. 2018]. Dostupné z: https://nukib.cz/download/kii-vis/Schema_rozhodovani_PZS_v2.1.pdf

## 1. Energetika

### *1.1* Elektřina

| **Odvětvová kritéria** | | | **Dopadová kritéria** |
|---|---|---|---|
| **Druh služby** | **Druh subjektu** | **Speciální kritéria druhu subjektu** | |
| 1.1.1. Výroba elektřiny | Výrobce elektřiny podle energetického zákona | a) Výrobna s celkovým instalovaným elektrickým výkonem nejméně 500 MW,<br><br>b) výrobna poskytující podpůrné služby s celkovým instalovaným elektrickým výkonem nejméně 100 MW nebo<br><br>c) technický dispečink využívaný k výrobě elektřiny. | Dopad kybernetického bezpečnostního incidentu v informačním systému nebo síti elektronických komunikací, na jejichž fungování je závislé poskytování služby, může způsobit<br><br>I. závažné omezení, narušení či nedostupnost druhu služby postihující více než 50000 osob,<br><br>II. závažné omezení či narušení jiné základní služby nebo omezení či narušení provozu prvku kritické infrastruktury,<br><br>III. hospodářskou ztrátu vyšší než 0,25 % HDP,<br><br>IV. oběti na životech s mezní hodnotou více než 100 mrtvých nebo 1000 zraněných osob vyžadujících lékařské ošetření nebo<br><br>V. narušení veřejné bezpečnosti na významné |
| 1.1.2. Prodej elektřiny | Obchodník s elektřinou podle energetického zákona | a) Systémy využívané k prodeji elektřiny, mající přímý vliv na dodávku elektřiny koncovým zákazníkům. | |
| 1.1.3. Provoz přenosové soustavy | Provozovatel přenosové soustavy podle energetického zákona | a) Vedení přenosové soustavy,<br><br>b) elektrická stanice přenosové soustavy nebo<br><br>c) technický dispečink využívaný k provozu přenosové soustavy. | |
| 1.1.4. Provoz distribuční soustavy | Provozovatel distribuční soustavy podle energetického zákona | a) Vedení distribuční soustavy,<br><br>b) elektrická stanice distribuční soustavy nebo<br><br>c) technický dispečink využívaný k provozu distribuční soustavy. | |

| | | | |
|---|---|---|---|
| | | | části správního obvodu obce s rozšířenou působností, které by mohlo vyžadovat provedení záchranných a likvidačních prací složkami integrovaného záchranného systému. |

### *1.2* Ropa

| **Odvětvová kritéria** | | | **Dopadová kritéria** |
|---|---|---|---|
| **Druh služby** | **Druh subjektu** | **Speciální kritéria druhu subjektu** | |
| 1.2.1. Provoz rafinérie, skladu nebo přenosového zařízení na ropu nebo těžba, zpracování nebo úprava ropy | Provozovatel zařízení na těžbu, zpracování, rafinaci nebo úpravu ropy, skladovacího nebo přenosového zařízení na ropu | a) Zařízení na těžbu, zpracování, rafinaci nebo úpravu ropy s instalovanou roční výrobní kapacitou minimálně 3000000 tun,<br><br>b) zásobník nebo komplex zásobníků s kapacitou nejméně 20000 $m^3$,<br><br>c) skladovací zařízení na LPG o kapacitě nejméně 20000 $m^3$,<br><br>d) produktovod s kapacitou přepravy produktů více než 3000000 tun ročně,<br><br>e) přenosové zařízení na ropu nebo<br><br>f) technický dispečink využívaný k provozu rafinérie, skladu, přenosového zařízení na ropu nebo k těžbě, zpracování nebo úpravě ropy. | Dopad kybernetického bezpečnostního incidentu v informačním systému nebo síti elektronických komunikací, na jejichž fungování je závislé poskytování služby, může způsobit<br><br>I. závažné omezení či narušení druhu služby postihující více než 50000 osob,<br><br>II. závažné omezení či narušení jiné základní služby nebo omezení či narušení provozu prvku kritické infrastruktury,<br><br>III. hospodářskou ztrátu vyšší než 0,25 % HDP, |

| | | | |
|---|---|---|---|
| 1.2.2. Provoz ropovodu | Provozovatel ropovodu | a) Vnitrostátní ropovod s kapacitou přepravy ropy více než 500000 tun ročně,<br><br>b) koncové zařízení pro předání ropy nebo<br><br>c) technický dispečink využívaný k provozu ropovodu. | IV. nedostupnost druhu služby pro více než 1600 osob, která není nahraditelná jiným způsobem bez vynaložení nepřiměřených nákladů,<br><br>V. oběti na životech s mezní hodnotou více než 100 mrtvých nebo 1000 zraněných osob vyžadujících lékařské ošetření nebo<br><br>VI. narušení veřejné bezpečnosti na významné části správního obvodu obce s rozšířenou působností, které by mohlo vyžadovat provedení záchranných a likvidačních prací složkami integrovaného záchranného systému. |

### *1.3* Zemní plyn

| **Odvětvová kritéria** | | | **Dopadová kritéria** |
|---|---|---|---|
| **Druh služby** | **Druh subjektu** | **Speciální kritéria druhu subjektu** | |
| 1.3.1. Provoz plynárenského podniku | Plynárenský podnik podle příslušného předpisu Evropské unie* | a) Výroba nebo těžba plynu v ročním objemu alespoň ve výši 15 % roční spotřeby České republiky. | Dopad kybernetického bezpečnostního incidentu v informačním systému nebo síti elektronických komunikací, na jejichž fungování je závislé poskytování služby, může způsobit<br><br>I. závažné omezení, narušení či nedostupnost druhu služby postihující více než 50000 osob,<br><br>II. závažné omezení či narušení jiné základní služby nebo omezení či narušení provozu prvku kritické infrastruktury,<br><br>III. hospodářskou ztrátu vyšší než 0,25 % HDP,<br><br>IV. oběti na životech s mezní hodnotou více než 100 mrtvých nebo 1000 zraněných osob vyžadujících lékařské ošetření nebo vyžadovat provedení záchranných a likvidačních prací složkami integrovaného záchranného systému. |
| 1.3.2. Provoz zařízení na rafinaci nebo úpravu plynu | Provozovatel zařízení na rafinaci nebo úpravu plynu | - | |
| 1.3.3. Prodej plynu | Obchodník s plynem podle energetického zákona | a) Systémy využívané k prodeji plynu, mající přímý vliv na dodávku plynu koncovým zákazníkům. | |
| 1.3.4. Provoz přepravní soustavy | Provozovatel přepravní soustavy podle energetického zákona | a) Provoz přepravní soustavy plynu nebo<br><br>b) technický dispečink využívaný k provozu přepravní soustavy plynu. | |
| 1.3.5. Provoz distribuční soustavy | Provozovatel distribuční soustavy podle energetického zákona | a) Provoz distribuční soustavy plynu nebo<br><br>b) technický dispečink využívaný k provozu distribuční soustavy plynu. | |
| 1.3.6. Provoz skladovacího zařízení | Provozovatel skladovacího zařízení podle příslušného předpisu Evropské unie** | a) Provoz skladovacího zařízení nebo<br><br>b) technický dispečink využívaný k provozu skladovacího zařízení. | |

| | | | |
|---|---|---|---|
| 1.3.7. Provoz zařízení LNG | Provozovatel zařízení LNG podle příslušného předpisu Evropské unie*** | a) Provoz zařízení provádějícího zkapalnění plynu nebo<br><br>b) provoz zařízení provádějícího dovoz, vykládání nebo znovuzplynování LNG. | V. narušení veřejné bezpečnosti na významné části správního obvodu obce s rozšířenou působností, které by mohlo |

* Čl. 2 bod 1 směrnice Evropského parlamentu a Rady 2009/73/ES ze dne 13. července 2009 o společných pravidlech pro vnitřní trh se zemním plynem a o zrušení směrnice 2003/55/ES.
** Čl. 2 bod 10 směrnice Evropského parlamentu a Rady 2009/73/ES ze dne 13. července 2009 o společných pravidlech pro vnitřní trh se zemním plynem a o zrušení směrnice 2003/55/ES
*** Čl. 2 bod 12 směrnice Evropského parlamentu a Rady 2009/73/ES ze dne 13. července 2009 o společných pravidlech pro vnitřní trh se zemním plynem a o zrušení směrnice 2003/55/ES

### *1.4* Teplárenství

| **Odvětvová kritéria** | | | **Dopadová kritéria** |
|---|---|---|---|
| **Druh služby** | **Druh subjektu** | **Speciální kritéria druhu subjektu** | |
| 1.4.1. Výroba tepelné energie | Držitel licence na výrobu tepelné energie podle energetického zákona | a) Zdroj tepelné energie,<br><br>b) vyvedení tepelného výkonu ze zdroje tepelné energie nebo<br><br>c) technický dispečink využívaný k výrobě tepelné energie. | Dopad kybernetického bezpečnostního incidentu v informačním systému nebo síti elektronických komunikací, na jejichž fungování je závislé poskytování služby, může způsobit<br><br>I. závažné omezení, narušení či nedostupnost druhu služby postihující více než 25000 osob,<br><br>II. závažné omezení či narušení jiné základní služby nebo omezení či narušení provozu prvku kritické infrastruktury, |

| | | | |
|---|---|---|---|
| 1.4.2. Provoz soustavy zásobování tepelnou energií | Držitel licence na rozvod tepelné energie podle energetického zákona | a) Rozvodné tepelné zařízení nebo<br><br>b) technický dispečink využívaný k provozu soustavy zásobování tepelnou energií. | III. hospodářskou ztrátu vyšší než 0,25 % HDP,<br><br>IV. oběti na životech s mezní hodnotou více než 100 mrtvých nebo 1000 zraněných osob vyžadujících lékařské ošetření nebo<br><br>V. narušení veřejné bezpečnosti na významné části správního obvodu obce s rozšířenou působností, které by mohlo vyžadovat provedení záchranných a likvidačních prací složkami integrovaného záchranného systému. |

**2. Doprava**

***2.1*** **Letecká doprava**

| **Odvětvová kritéria** | | | **Dopadová kritéria** |
|---|---|---|---|
| **Druh služby** | **Druh subjektu** | **Speciální kritéria druhu subjektu** | |
| 2.1.1. Provoz letecké dopravy | Letecký dopravce podle zákona o civilním letectví | a) Letecká přeprava alespoň 500000 osob za rok nebo<br><br>b) nabídka letecké přepravy pro alespoň 500000 osob za rok. | Dopad kybernetického bezpečnostního incidentu v informačním systému nebo síti elektronických komunikací, na jejichž fungování je závislé poskytování služby, může způsobit<br><br>I. závažné omezení či narušení druhu služby |

| | | | |
|---|---|---|---|
| 2.1.2. Provoz letiště nebo pomocných zařízení v rámci letiště | Provozovatel letiště podle zákona o civilním letectví nebo subjekt provozující pomocná zařízení v rámci letiště | a) V rámci globálního nebo hlavního letiště.* | postihující více než 50000 osob,<br><br>II. závažné omezení či narušení jiné základní služby nebo omezení či narušení provozu prvku kritické infrastruktury,<br><br>III. hospodářskou ztrátu vyšší než 0,25 % HDP,<br><br>IV. nedostupnost druhu služby pro více než 1600 osob, která není nahraditelná jiným způsobem bez vynaložení nepřiměřených nákladů,<br><br>V. oběti na životech s mezní hodnotou více než 200 mrtvých nebo 1000 zraněných osob vyžadujících lékařské ošetření nebo<br><br>VI. narušení veřejné bezpečnosti na významné části správního obvodu obce s rozšířenou působností, které by mohlo vyžadovat provedení záchranných a likvidačních prací složkami integrovaného záchranného systému. |
| 2.1.3. Služba řízení letového provozu | Poskytovatel letových navigačních služeb podle přímo použitelného předpisu Evropské unie** | a) Přibližovací služba řízení globálního nebo hlavního letiště nebo letiště určeného jako prvek kritické infrastruktury,<br><br>b) služba řízení letového provozu pro řízené lety přilétajících a odlétajících letadel,<br><br>c) letištní služba řízení globálního nebo hlavního letiště nebo letiště určeného jako prvek kritické infrastruktury,<br><br>d) oblastní služba řízení nebo<br><br>e) služba řízení letového provozu pro řízené lety v řízených oblastech. | |

* Nařízení Evropského parlamentu a Rady (EU) č. 1315/2013 ze dne 11. prosince 2013 o hlavních směrech Unie pro rozvoj transevropské dopravní sítě a o zrušení rozhodnutí č. 661/2010/EU, v platném znění

** Čl. 2 bod 5 nařízení Evropského parlamentu a Rady (ES) č. 549/2004 ze dne 10. března 2004, kterým se stanoví rámec pro vytvoření jednotného evropského nebe (rámcové nařízení), v platném znění

### *2.2* Železniční doprava

| **Odvětvová kritéria** | | | **Dopadová kritéria** |
|---|---|---|---|
| **Druh služby** | **Druh subjektu** | **Speciální kritéria druhu subjektu** | |
| 2.2.1. Provoz dráhy | Provozovatel dráhy podle zákona o drahách | a) Pověření k zřízení, správě a udržování železniční infrastruktury, včetně řízení dopravy, zabezpečení nebo signalizace,<br><br>b) centrální dispečerské stanoviště,<br><br>c) kontrolně analytické centrum,<br><br>d) automatické stavění vlakových cest,<br><br>e) automatické vedení vlaku nebo<br><br>f) evropský systém řízení železniční dopravy. | Dopad kybernetického bezpečnostního incidentu v informačním systému nebo síti elektronických komunikací, na jejichž fungování je závislé poskytování služby, může způsobit<br><br>I. závažné omezení či narušení druhu služby postihující více než 50000 osob,<br><br>II. závažné omezení či narušení jiné základní služby nebo omezení či narušení provozu prvku kritické infrastruktury,<br><br>III. hospodářskou ztrátu vyšší než 0,25 % HDP,<br><br>IV. nedostupnost druhu služby pro více než 1600 osob, která není nahraditelná jiným způsobem bez vynaložení nepřiměřených nákladů,<br><br>V. oběti na životech s mezní hodnotou více než 100 mrtvých nebo 1000 zraněných osob |

| | | | |
|---|---|---|---|
| 2.2.2. Provoz drážní dopravy nebo zařízení služeb | Provozovatel drážní dopravy nebo zařízení služeb podle zákona o drahách | a) Poskytování hnacích vozidel zařazených na tratě transevropské dopravní sítě (TEN-T), systému mezinárodních železničních magistrál (AGC), systému nejdůležitějších tras mezinárodní kombinované dopravy a souvisejících objektů (AGTC) nebo železničního koridoru pro mezinárodní nákladní dopravu (RFC),<br><br>b) provozovatel železniční dopravy, jehož hlavní činností je přeprava zboží nebo cestujících na tratích transevropské dopravní sítě (TEN-T), systému mezinárodních železničních magistrál (AGC), systému nejdůležitějších tras mezinárodní kombinované dopravy a souvisejících objektů (AGTC) nebo železničního koridoru pro mezinárodní nákladní dopravu (RFC) nebo<br><br>c) podnik odpovědný za řízení alespoň jednoho zařízení služeb nebo za poskytování alespoň jedné doplňkové nebo pomocné služby podle zákona o drahách. | vyžadujících lékařské ošetření nebo<br><br>VI. narušení veřejné bezpečnosti na významné části správního obvodu obce s rozšířenou působností, které by mohlo vyžadovat provedení záchranných a likvidačních prací složkami integrovaného záchranného systému. |

### *2.3* Vodní doprava

| **Odvětvová kritéria** | | | **Dopadová kritéria** |
|---|---|---|---|
| **Druh služby** | **Druh subjektu** | **Speciální kritéria druhu subjektu** | |
| 2.3.1. Provoz vnitrozemské, námořní nebo pobřežní osobní nebo nákladní vodní dopravy | Subjekty provozující vnitrozemskou, námořní nebo pobřežní osobní nebo nákladní vodní dopravu | a) Provoz vodní dopravy nebo nabídka provozu vodní dopravy, která není nahraditelná nebo by byla nahraditelná pouze s vynaložením nepřiměřených nákladů. | Dopad kybernetického bezpečnostního incidentu v informačním systému nebo síti elektronických komunikací, na jejichž fungování je závislé poskytování služby, může způsobit<br><br>I. závažné omezení či narušení jiné základní služby nebo omezení či narušení provozu prvku kritické infrastruktury,<br><br>II. hospodářskou ztrátu vyšší než 0,25 % HDP,<br><br>III. nedostupnost druhu služby pro více než 1600 osob, která není nahraditelná jiným způsobem bez vynaložení nepřiměřených nákladů,<br><br>IV. oběti na životech s mezní hodnotou více než 100 mrtvých nebo 1000 zraněných osob vyžadujících lékařské ošetření nebo<br><br>V. narušení veřejné bezpečnosti na významné |
| 2.3.2. Provoz řídícího orgánu přístavu nebo provoz díla nebo zařízení v rámci přístavu | Řídící orgán přístavu, včetně jeho přístavních zařízení podle přímo použitelného předpisu Evropské unie* nebo subjekt provozující dílo nebo zařízení v rámci přístavu | - | |
| 2.3.3. Provoz služby lodní dopravě | Provozovatel služby lodní dopravě podle příslušného předpisu Evropské unie** | - | |

| | | | |
|---|---|---|---|
| | | | části správního obvodu obce s rozšířenou působností, které by mohlo vyžadovat provedení záchranných a likvidačních prací složkami integrovaného záchranného systému. |

* Čl. 2 bod 11 nařízení Evropského parlamentu a Rady (ES) č. 725/2004 ze dne 31. března 2004, o zvýšení bezpečnosti lodí a přístavních zařízení, v platném znění

** Čl. 3 písm. o) směrnice Evropského parlamentu a Rady 2002/59/ES ze dne 27. června 2002, kterou se stanoví kontrolní a informační systém Společenství pro provoz plavidel a kterou se zrušuje směrnice Rady 93/75/EHS

### *2.4* Silniční doprava

| **Odvětvová kritéria** | | | **Dopadová kritéria** |
|---|---|---|---|
| **Druh služby** | **Druh subjektu** | **Speciální kritéria druhu subjektu** | |
| 2.4.1. Činnost subjektu odpovědného za kontrolu řízení provozu | Subjekt odpovědný za plánování, kontrolu nebo správu pozemních komunikací spadajících do jeho územní působnosti | a) Kontrola řízení provozu na pozemních komunikacích. | Dopad kybernetického bezpečnostního incidentu v informačním systému nebo síti elektronických komunikací, na jejichž fungování je závislé poskytování služby, může způsobit<br><br>I. závažné omezení či narušení druhu služby postihující více než 50000 osob,<br><br>II. závažné omezení či narušení jiné základní služby nebo omezení či narušení provozu prvku kritické infrastruktury, |

| | | | |
|---|---|---|---|
| 2.4.2. Provoz inteligentní-ho dopravní-ho systému | Poskytovatel služby inteligentního dopravního systému podle zákona o pozemních komunikacích | a) Provoz inteligentního dopravního systému v oblasti silniční dopravy, v oblasti řízení provozu nebo mobility nebo v oblasti rozhraní s jinými druhy dopravy. | III. hospodářskou ztrátu vyšší než 0,25 % HDP,<br><br>IV. nedostupnost druhu služby pro více než 1600 osob, která není nahraditelná jiným způsobem bez vynaložení nepřiměřených nákladů,<br><br>V. oběti na životech s mezní hodnotou více než 100 mrtvých nebo 1000 zraněných osob vyžadujících lékařské ošetření nebo<br><br>VI. narušení veřejné bezpečnosti na významné části správního obvodu obce s rozšířenou působností, které by mohlo vyžadovat provedení záchranných a likvidačních prací složkami integrovaného záchranného systému. |

### 3. Bankovnictví

| Odvětvová kritéria | | | Dopadová kritéria |
|---|---|---|---|
| **Druh služby** | **Druh subjektu** | **Speciální kritéria druhu subjektu** | |
| 3.1. Výkon činnosti úvěrové instituce | Úvěrová instituce podle přímo použitelného předpisu Evropské unie* | a) Počet klientů nad 500000 nebo<br><br>b) tržní podíl přesahující 1 % z bilanční sumy bankovního sektoru. | Dopad kybernetického bezpečnostního incidentu v informačním systému nebo síti elektronických komunikací, na jejichž fungování je závislé poskytování služby, může způsobit<br><br>I. závažné omezení druhu služby postihující více než 500000 osob,<br><br>II. závažné omezení či narušení jiné základní služby nebo omezení či narušení provozu prvku kritické infrastruktury,<br><br>III. hospodářskou ztrátu vyšší než 0,25 % HDP nebo<br><br>IV. narušení veřejné bezpečnosti na významné části správního obvodu obce s rozšířenou působností, které by mohlo vyžadovat provedení záchranných a likvidačních prací složkami integrovaného záchranného systému. |

* Čl. 4 odst. 1 bod 1 nařízení Evropského parlamentu a Rady (EU) č. 575/2013 ze dne 26. června 2013 o obezřetnostních požadavcích na úvěrové instituce a investiční podniky a o změně nařízení (EU) č. 648/2012, v platném znění

**4. Infrastruktura finančních trhů**

| **Odvětvová kritéria** | | | **Dopadová kritéria** |
|---|---|---|---|
| **Druh služby** | **Druh subjektu** | **Speciální kritéria druhu subjektu** | |
| 4.1. Provoz obchodního systému | Provozovatel obchodního systému podle zákona o podnikání na kapitálovém trhu | - | Dopad kybernetického bezpečnostního incidentu v informačním systému nebo síti elektronických komunikací, na jejichž fungování je závislé poskytování služby, může způsobit<br><br>I. závažné omezení či narušení druhu služby postihující více než 50000 osob, |
| 4.2. Výkon činnosti ústřední protistrany | Ústřední protistrana podle přímo použitelného předpisu Evropské unie* | - | II. závažné omezení či narušení jiné základní služby nebo omezení či narušení provozu prvku kritické infrastruktury,<br><br>III. hospodářskou ztrátu vyšší než 0,25 % HDP,<br><br>IV. nedostupnost druhu služby pro více než 1600 osob, která není nahraditelná jiným způsobem bez vynaložení nepřiměřených nákladů nebo<br><br>V. narušení veřejné bezpečnosti na významné části správního obvodu obce s rozšířenou působností, které by mohlo |

| | | | |
|---|---|---|---|
| | | | vyžadovat provedení záchranných a likvidačních prací složkami integrovaného záchranného systému. |

* Čl. 2 bod 1 nařízení Evropského parlamentu a Rady (EU) č. 648/2012 ze dne 4. července 2012 o OTC derivátech, ústředních protistranách a registrech obchodních údajů, v platném znění

## 5. Zdravotnictví

| **Odvětvová kritéria** | | | **Dopadová kritéria** |
|---|---|---|---|
| **Druh služby** | **Druh subjektu** | **Speciální kritéria druhu subjektu** | |
| 5.1. Poskytování zdravotních služeb | Poskytovatel zdravotních služeb podle zákona o zdravotních službách | a) Celkový počet akutních lůžek v posledních třech kalendářních letech nejméně 800 nebo<br><br>b) statut centra vysoce specializované traumatologické péče podle zákona o zdravotních službách. | Dopad kybernetického bezpečnostního incidentu v informačním systému nebo síti elektronických komunikací, na jejichž fungování je závislé poskytování služby, může způsobit<br><br>I. závažné omezení druhu služby postihující více než 50000 osob,<br><br>II. závažné omezení či narušení jiné základní služby nebo omezení či narušení provozu prvku kritické infrastruktury,<br><br>III. nedostupnost druhu služby pro více než 1600 osob, která není nahraditelná jiným způsobem bez vynaložení nepřiměřených nákladů, |

| | | | |
|---|---|---|---|
| | | | IV. oběti na životech s mezní hodnotou více než 100 mrtvých nebo 1000 zraněných osob vyžadujících lékařské ošetření,<br><br>V. narušení veřejné bezpečnosti na významné části správního obvodu obce s rozšířenou působností, které by mohlo vyžadovat provedení záchranných a likvidačních prací složkami integrovaného záchranného systému, nebo<br><br>VI. kompromitaci citlivých osobních údajů o více než 200000 osobách. |

**6. Vodní hospodářství**

| **Odvětvová kritéria** | | | **Dopadová kritéria** |
|---|---|---|---|
| **Druh služby** | **Druh subjektu** | **Speciální kritéria druhu subjektu** | |
| 6.1. Výroba, dodávání nebo distribuce pitné vody nebo odvádění nebo čištění odpadních vod | Výrobce, dodavatel nebo distributor pitné vody nebo subjekt zajišťující odvod nebo čištění odpadních vod, s výjimkou distributora, pro něhož je distribuce pitné vody pouze částí jeho | a) Výroba, dodávky nebo distribuce pitné vody,<br><br>b) čistírna odpadních vod,<br><br>c) úpravna vody nebo<br><br>d) provoz vodovodu nebo kanalizace. | Dopad kybernetického bezpečnostního incidentu v informačním systému nebo síti elektronických komunikací, na jejichž fungování je závislé poskytování služby, může způsobit<br><br>I. závažné omezení druhu služby postihující více než 50000 osob, |

| | | | |
|---|---|---|---|
| | obecné činnosti spočívající v distribuci jiného zboží | | II. závažné omezení či narušení jiné základní služby nebo omezení či narušení provozu prvku kritické infrastruktury,<br><br>III. hospodářskou ztrátu vyšší než 0,25 % HDP,<br><br>IV. nedostupnost druhu služby pro více než 1600 osob, která není nahraditelná jiným způsobem bez vynaložení nepřiměřených nákladů,<br><br>V. oběti na životech s mezní hodnotou více než 100 mrtvých nebo 1000 zraněných osob vyžadujících lékařské ošetření nebo<br><br>VI. narušení veřejné bezpečnosti na významné části správního obvodu obce s rozšířenou působností, které by mohlo vyžadovat provedení záchranných a likvidačních prací složkami integrovaného záchranného systému. |

**7. Digitální infrastruktura**

| **Odvětvová kritéria** | | | **Dopadová kritéria** |
|---|---|---|---|
| **Druh služby** | **Druh subjektu** | **Speciální kritéria druhu subjektu** | |
| 7.1. Propojování technicky soběstačných sítí | Poskytovatel služby výměnného uzlu internetu (IXP) existujícího za účelem propojení sítí, které jsou z technického a organizačního hlediska oddělené | a) Propojení více než 50 autonomních sítí a průměrný datový tok naměřený v pětiminutovém intervalu za 24 hodin přesahující 50 Gb/s. | Dopad kybernetického bezpečnostního incidentu v informačním systému nebo síti elektronických komunikací, na jejichž fungování je závislé poskytování služby, může způsobit<br><br>I. závažné omezení či narušení druhu služby postihující více než 50000 osob,<br><br>II. závažné omezení či narušení jiné základní služby nebo omezení či narušení provozu prvku kritické infrastruktury,<br><br>III. hospodářskou ztrátu vyšší než 0,25 % HDP,<br><br>IV. nedostupnost druhu služby pro více než 1600 osob, která není nahraditelná jiným způsobem bez vynaložení nepřiměřených nákladů, nebo<br><br>V. narušení veřejné bezpečnosti na významné části správního obvodu obce s rozšířenou působností, které by mohlo |
| 7.2. Poskytování služeb systému doménových jmen (DNS) na internetu | Poskytovatel služeb DNS | a) Poskytování služby autoritativního DNS a správa nebo hosting více než 10000 domén druhého řádu. | |
| 7.3. Správa nebo provoz registru internetových domén nejvyšší úrovně | Subjekt spravující nebo provozující registr internetových domén nejvyšší úrovně | a) Správa registru internetových domén nejvyšší úrovně s počtem registrovaných domén přesahujícím 100000. | |

| | | | |
|---|---|---|---|
| | | | vyžadovat provedení záchranných a likvidačních prací složkami integrovaného záchranného systému. |

**8. Chemický průmysl**

| **Odvětvová kritéria** | | | **Dopadová kritéria** |
|---|---|---|---|
| **Druh služby** | **Druh subjektu** | **Speciální kritéria druhu subjektu** | |
| 8.1. Výroba technických plynů | Výrobce technických plynů | - | Dopad kybernetického bezpečnostního incidentu v informačním systému nebo síti elektronických komunikací, na jejichž fungování je závislé poskytování služby, může způsobit<br><br>I. závažné omezení či narušení druhu služby postihující více než 50000 osob,<br><br>II. závažné omezení či narušení jiné základní služby nebo omezení či narušení provozu prvku kritické infrastruktury,<br><br>III. hospodářskou ztrátu vyšší než 0,25 % HDP,<br><br>IV. nedostupnost druhu služby pro více než 1600 osob, která není nahraditelná jiným způsobem bez vynalo- |
| 8.2. Výroba hnojiv nebo dusíkatých sloučenin | Výrobce hnojiv nebo dusíkatých sloučenin | - | |
| 8.3. Výroba pesticidů nebo jiných agrochemických přípravků | Výrobce pesticidů nebo jiných agrochemických přípravků | - | |
| 8.4. Výroba výbušnin | Výrobce výbušnin | - | |
| 8.5. Zpracování jaderného paliva | Subjekt zpracovávající jaderné palivo | - | |

| | | | |
|---|---|---|---|
| 8.6. Výroba základních farmaceutických výrobků | Výrobce základních farmaceutických výrobků | - | žení nepřiměřených nákladů,<br><br>V. oběti na životech s mezní hodnotou více než 100 mrtvých nebo 1000 zraněných osob vyžadujících lékařské ošetření nebo<br><br>VI. narušení veřejné bezpečnosti na významné části správního obvodu obce s rozšířenou působností, které by mohlo vyžadovat provedení záchranných a likvidačních prací složkami integrovaného záchranného systému. |
| 8.7. Výroba farmaceutických přípravků | Výrobce farmaceutických přípravků | - | |
| 8.8. Výroba jiných základních anorganických látek | Výrobce jiných základních anorganických látek | - | |
| 8.9. Výroba jiných základních organických chemických látek | Výrobce jiných základních organických chemických látek | - | |

**K písm. l)**

## Digitální služba

**Digitální službou** se rozumí **služba informační společnosti**, která **spočívá v provozování jedné ze tří níže uvedených služeb** (on-line tržiště, internetový vyhledávač, či cloud computing).

Pojem digitální služba byl do ZoKB transponován ze směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (NIS). V této směrnici je digitální služba definována v čl. 4 odst. 5, kde je uvedeno, že *„digitální službou je služba ve smyslu čl. 1 odst. 1 písm. b) směrnice Evropského parlamentu a Rady (EU) 2015/1535, jejíž druh je uveden v příloze III.“*

Dle čl. 1 odst. 1 písm. b) směrnice 2015/1535 se **službou rozumí jakákoli služba informační společnosti**, tj. každá služba poskytovaná zpravidla za úplatu, na dálku, elektronicky a na individuální žádost příjemce služeb.

Velmi obdobně je služba informační společnosti definována i v zákoně o některých službách informační společnosti. V § 2 písm. a) ZSIS je uvedeno, že **službou informační společnosti** se rozumí *„jakákoliv služba poskytovaná elektronickými prostředky na individuální žádost uživatele podanou elektronickými prostředky, poskytovaná zpravidla za úplatu. Služba je poskytnuta elektronickými prostředky, pokud je odeslána prostřednictvím sítě elektronických komunikací a vyzvednuta uživatelem z elektronického zařízení pro ukládání dat.*"

Z obou dvou definic (dle směrnice 2015/1535 i ZSIS) vyplývají čtyři základní znaky služby informační společnosti:

- **je poskytována elektronicky**,
- **je poskytována na individuální žádost uživatele**,
- **je zpravidla poskytována za odměnu**,
- **je poskytována distančně** (na dálku).

Pojem poskytování služby **elektronicky** je uveden ve směrnici 2015/1535 v čl. 1 písm. b) ii), kde je definováno, že se jedná o službu, která je odeslána z výchozího místa a je přijata v místě jejího určení prostřednictvím elektronického zařízení pro zpracování (včetně digitální komprese) a uchovávání dat. Tato služba je jako celek odeslána, přenesena nebo přijata drátově, rádiově, opticky nebo jinými elektromagnetickými prostředky. Česká úprava využívá demonstrativního výčtu, kde je uvedeno, že se jedná zejména o síť elektronických komunikací, elektronická komunikační zařízení, automatické volací a komunikační systémy, telekomunikační koncová zařízení a elektronickou poštu.[242]

**Individuální žádost uživatele** znamená, že se musí jednat o aktivní činnost ze strany uživatele. Husovec uvádí, že jde o případy, kdy například uživatel sám vepíše adresu do políčka prohlížeče (Edge, Firefox, Chrome, Opera, Safari aj.), čímž formuluje žádost na otevření příslušné stránky, nebo napíše SMS zprávu. Typickým příkladem služby, která je poskytována bez individuální žádosti, pak podle Husovce je např. televizní vysílání.[243]

Nejproblematičtějším kritériem definice služby informační společnosti je, že tato **služba je poskytována za odměnu**. Česká úprava kopíruje i v tomto bodě úpravu mezinárodní a obsahuje ustanovení *„zpravidla za úplatu*". V prostředí Internetu či jiných počítačových sítí existuje celá řada služeb, které jsou poskytovány „zdarma". Husovec zcela správně argumentuje tím, že pod pojmem odměna si je možné představit celou řadu skutečností odlišných od ryze peněžitého plnění.[244] Může se jednat o plnění, které bude mít podobu nepeněžitého charakteru, kdy ISP získá o uživatelích informace v podobě osobních, technických a jiných údajů, času stráveného

242: Viz § 2 písm. c) ZSIS

243: Blíže viz HUSOVEC, Martin. *Zodpovednosť na Internete podľa českého a slovenského práva*. Praha: CZ.NIC, 2014, s. 100

244: Tamtéž s. 98

užíváním dané služby, nabídne uživateli reklamu na jiné produkty atd. Nicméně i tato podmínka by měla dle Husovce být interpretována extenzivněji, a to tak, že je vyvíjena činnost *potenciálně ekonomická*.[245]

Díky tomu, že si pod pojmem úplata lze představit skutečně rozlišné možnosti (např. poděkování, návštěva stránky či odkazu, finanční či jiné plnění), a díky znění zákona o některých službách informační společnosti (viz „*zpravidla za úplatu*") lze vyvodit závěr, že činnost poskytovatele služeb informační společnosti může být poskytována i zdarma.

Pojem **na dálku** definuje směrnice 2015/1535 jako službu, která je poskytována bez současné přítomnosti stran.[246]

Husovec ve své monografii dále uvádí příklady, které demonstrují, co vše lze považovat za službu informační společnosti. Pod tento pojem je třeba dle směrnice 2000/31/ES Evropského parlamentu a Rady zařadit celou řadu činností, ke kterým dochází v on-line světě. Může se jednat o on-line prodej zboží, služby, které poskytují on-line informace, komerční komunikaci, či služby poskytující nástroje pro vyhledávání, přístup a získávání údajů, služby poskytující přenos informací prostřednictvím komunikační sítě aj.

„*Judikatura Soudního dvora EU již přímo či nepřímo uznala za službu informační společnosti například službu AdWords (inzertní služba ve vyhledávači Google)*[247]*, službu pojištění motorových vozidel přes Internet*[248]*, on-line prodej kontaktních čoček*[249]*, připojení se k Internetu*[250]*, rezervaci hotelu skrze e-mail* [251]*, rezervaci služeb cestovní kanceláře skrze e-mail* [252]*, aukční server eBay*[253] *a klasické vyhledávání od společnosti Google*" [254]

Pro to, aby byla služba službou informační společnosti, **není nezbytně nutné naplnit kritérium úplaty za tuto službu, avšak ostatní tři podmínky** (tj. jde o službu poskytovanou na dálku, elektronicky a na individuální žádost příjemce služeb), resp. jejich naplnění, **jsou obligatorní.**

245: Blíže viz HUSOVEC, Martin. *Zodpovednosť na Internete podľa českého a slovenského práva*. Praha: CZ.NIC, 2014, s. 99

246: Viz čl. čl. 1 písm. b) i) směrnice 2015/1535.

247: Rozhodnutie *Google France* C-236/08 až C-238/08.

248: Rozhodnutie *Bundesverband* C-298/07.

249: Rozhodnutie *Ker-Optika* C-108/09.

250: Rozhodnutie *Promusicae* C-275/06 a *Tele 2*. C-557/07

251: Rozhodnutie *Alpenhof* C-144/09.

252: Rozhodnutie *Pammer* C-585/08.

253: Rozhodnutie *L'Oreal v. Ebay* 324/09.

254: HUSOVEC, Martin. *Zodpovednosť na Internete podľa českého a slovenského práva*. Praha: CZ.NIC, 2014.
ISBN: 978-80-904248-8-3, s. 101–102.

V příloze III. NIS jsou jako digitální služby určeny **on-line tržiště**, **internetový vyhledávač** a **služba cloud computingu**. Byť služeb informační společnosti existuje mnohem více (viz výše), než tyto tři uvedené služby, **je dopad směrnice NIS i ZoKB omezen pouze na tyto tři služby informační společnosti**.

**Digitální službou** dle ZoKB **je jedna z následujících tří služeb informační společnosti:**

1) **on-line tržiště**, které spotřebiteli nebo prodávajícímu umožňuje on-line uzavírat s prodávajícím podnikatelem[255] kupní smlouvu nebo smlouvu o poskytnutí služeb, a to prostřednictvím internetové stránky on-line tržiště nebo prostřednictvím internetové stránky prodávajícího, který využívá službu poskytovanou on-line tržištěm,

2) **internetového vyhledávače**, který umožňuje provádět vyhledávání v zásadě na všech internetových stránkách, a to na základě dotazu uživatele na jakékoliv téma v podobě klíčového slova, sousloví nebo jiného zadání, přičemž služba poskytuje odkazy, na nichž lze nalézt informace související s požadovaným obsahem, nebo

3) **cloud computingu**, který umožňuje přístup k rozšiřitelnému a přizpůsobitelnému úložišti nebo výpočetním zdrojům, které je možné sdílet.

**On-line tržištěm** se dle čl. 4 odst. 17 NIS **rozumí digitální služba, která spotřebitelům** a **obchodníkům** umožňuje uzavírat s obchodníky on-line smlouvy o prodeji a o poskytnutí služeb, a to prostřednictvím internetových stránek on-line tržiště nebo prostřednictvím internetových stránek obchodníka, jež využívají výpočetních služeb poskytovaných on-line tržištěm.

Definice pojmů **spotřebitel** a **obchodník** vyplývá ze směrnice Evropského parlamentu a Rady 2013/11/EU o alternativním řešení spotřebitelských sporů a o změně nařízení (ES) č. 2006/2004 a směrnice 2009/22/ES (směrnice o alternativním řešení spotřebitelských sporů).[256]

Dle čl. 4 odst. 1 písm. a) směrnice 2013/11/EU se za **spotřebitele** považuje **fyzická osoba**, která jedná za účelem, který nelze považovat za provozování jejího obchodu, živnosti nebo řemesla anebo výkonu jejího povolání.

Dle čl. 4 odst. 1 písm. b) směrnice 2013/11/EU se za **obchodníka** považuje **fyzická nebo právnická osoba**, bez ohledu na to, zda je v soukromém nebo veřejném vlastnictví, jež jedná,

255: § 2 odst. 1 písm. a) a b) zákona č. 634/1992 Sb., o ochraně spotřebitele, ve znění pozdějších předpisů. § 419 a 420 OZ

256: [online]. Dostupné z:
https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32013L0011&from=CS

včetně jednání jakékoli osoby jednající jejím jménem nebo z jejího pověření, za účelem souvisejícím s jejím obchodem, živností nebo řemeslem anebo výkonem jejího svobodného povolání.

**Kupní smlouvou** je dle čl. 4 odst. 1 písm. c) směrnice 2013/11/EU **smlouva, na jejímž základě obchodník převádí vlastnictví zboží spotřebiteli nebo se zavazuje k převedení tohoto vlastnictví** a spotřebitel hradí cenu tohoto zboží nebo se zavazuje k její úhradě, včetně smluv majících za předmět zboží i služby.

**Smlouvu o poskytování služeb** je dle čl. 4 odst. 1 písm. d) směrnice 2013/11/EU **jakákoli smlouva jiná než kupní smlouva**, **na jejímž základě obchodník poskytuje službu** spotřebiteli **nebo se zavazuje k jejímu poskytnutí** a spotřebitel hradí cenu této služby nebo se zavazuje k její úhradě.

**Prostřednictvím on-line tržiště mohou spotřebitelé a obchodníci s konečnou platností uzavírat s obchodníky on-line smlouvy o prodeji nebo o poskytnutí služeb.** V rámci on-line tržiště by neměly být nabízeny on-line služby:

- fungující pouze jako služby zprostředkovatelské, směřující ke službám třetích stran, s nimiž lze teprve uzavřít smlouvu,
- on-line služby poskytující srovnání cen konkrétních produktů či služeb různých obchodníků, za účelem následného přesměrování uživatele (spotřebitele) k nákupu u zvoleného obchodníka.

Výpočetní služby poskytované on-line tržištěm mohou zahrnovat zpracování transakcí, shromažďování údajů nebo sestavování uživatelských profilů.

Za druh on-line tržiště se mají považovat obchody s aplikacemi, jež jsou provozovány jako on-line obchody umožňující digitální distribuci aplikací nebo softwarových programů třetích stran.[257]

Z porovnání § 2 písm. l) bod 1. ZoKB a čl. 4 dost. 17 NIS lze pozorovat rozdílnost těchto definic, ta je však dána pouze transpozicí a její obsah zůstává nezměněn.[258]

To, co je v české právní úpravě změněno, jsou některé použité pojmy. Při jejich definování je třeba primárně vycházet z občanského zákoníku a zákona č. 634/1992 Sb., o ochraně spotřebitele.[259]

257: Recitál 15 NIS

258: Viz *Podpůrný materiál k identifikaci poskytovatelů digitálních služeb.* [online]. [cit. 7. 8. 2018]. Dostupné z: https://nukib.cz/download/kii-vis/Definice_DSP_v1.pdf s. 8–9

259: Dále jen **ZoS**

**Spotřebitelem** je dle § 419 OZ každý člověk (tedy fyzická osoba), který mimo rámec své podnikatelské činnosti nebo mimo rámec samostatného výkonu svého povolání uzavírá smlouvu s podnikatelem nebo s ním jinak jedná.

Dle § 2 odst. 1 písm. a) ZoS je spotřebitelem *„fyzická osoba, která nejedná v rámci své podnikatelské činnosti nebo v rámci samostatného výkonu svého povolání.*"

Dle § 2 písm. d) ZoEK je spotřebitelem *„každá fyzická osoba, která využívá nebo žádá veřejně dostupnou službu elektronických komunikací pro účely mimo rámec její podnikatelské činnosti.*"

**Prodávajícím podnikatelem** se dle § 2 odst. 1 písm. b) ZoS rozumí *„**podnikatel, který spotřebiteli prodává výrobky nebo poskytuje služby**.*" Uvedené ustanovení dále odkazuje na § 420 OZ, kde je stanoveno, že *„kdo samostatně vykonává na vlastní účet a odpovědnost výdělečnou činnost živnostenským nebo obdobným způsobem se záměrem činit tak soustavně za účelem dosažení zisku, je považován se zřetelem k této činnosti za podnikatele.*"

Za on-line tržiště se nepovažují internetové stránky, které

- přesměrovávají uživatele na další internetové stránky, aby až tam uzavřeli s konečnou platností smlouvu (*např. srovnávače cen*);
- slouží pouze k propojení prodávajících podnikatelů (prodávajících) se spotřebiteli a prodávajícími (kupující) (*např. inzertní webové stránky*);
- slouží prodávajícímu podnikateli (prodávající) přímo k prodeji zboží spotřebitelům a prodávajícím (kupující) (*např. on-line maloobchod*).[260]

**Internetovým vyhledávačem** se dle čl. 4 odst. 18 NIS **rozumí** digitální **služba, která uživatelům umožňuje provádět vyhledávání v zásadě na všech internetových stránkách** nebo na internetových stránkách v určitém jazyce, a to **na základě dotazu** na jakékoli téma v podobě klíčového slova, sousloví nebo jiného zadání, **přičemž služba poskytuje odkazy**, na nichž lze nalézt informace související s požadovaným obsahem.

Definice internetového vyhledávače uvedená v NIS by se neměla vztahovat na:

- vyhledávací funkce, jež jsou omezeny na obsah konkrétních internetových stránek, a to bez ohledu na to, zda vyhledávací funkci poskytuje externí internetový vyhledávač,
- na on-line služby, jež poskytují srovnání cen konkrétních produktů či služeb různých obchodníků, aby poté uživatele přesměrovaly k nákupu u zvoleného obchodníka.[261]

260: *Podpůrný materiál k identifikaci poskytovatelů digitálních služeb.* [online]. [cit. 7. 8. 2018]. Dostupné z: https://nukib.cz/download/kii-vis/Definice_DSP_v1.pdf s. 10

261: Recitál 16 NIS

Souslovím „**v zásadě na všech internetových stránkách**“, který je uveden v § 2 písm. l) bod 2. ZoKB, se dle NÚKIB *„rozumí všechny běžně prostřednictvím sítě dostupné internetové stránky. Tato podmínka je splněna, i pokud je vyhledávač zaměřen na vyhledávání stránek v určitém jazyce. Naopak vyloučeny jsou vyhledávací funkce dostupné na jednotlivých internetových stránkách, které prohledávají toliko tuto konkrétní internetovou stránku, či vyhledávací funkce v rámci omezených rejstříků či knihoven. Stejně tak jsou vyloučeny služby, které pouze srovnávají výrobky a jejich ceny s odkazem na web konkrétních prodejců.“* [262]

**Službou cloud computingu** se dle čl. 4 odst. 19 NIS **rozumí digitální služba umožňující přístup k rozšiřitelnému a přizpůsobitelnému úložišti výpočetních zdrojů**, které je možno sdílet. Definice dle NIS je shodná s definicí dle ZoKB.

**Cloud computing** umožňuje užívání (sdílené) informačních technologií technologií (jak počítačových systémů, tak i softwaru) více uživateli (prostřednictvím sítě) formou poskytované služby.[263] Smyslem cloud computingu je efektivnější utilizace výpočetního výkonu a aplikací. Další možnou definicí cloud computingu je, že jde o *„poskytování výpočetních služeb uživatelům, skrze síťovou architekturu, která umožňují vzdálený přístup k těmto službám. Tyto služby jsou zpravidla poskytovány třetí stranou.“* [264]

Cloud computing lze dělit z několika hledisek, přičemž nejběžněji je dělen podle služby kterou poskytuje a podle způsobu, jakým je poskytován. **Podle služby jakou cloud computing poskytuje** je možné definovat tři hlavní typy služeb (distribuční modely).[265] Jedná se o:

- **Infrastructure-as-a-Service (IaaS). Infrastruktura jako služba** zavazuje poskytovatele poskytnout infrastrukturu (hardware) jiným uživatelům (typickým příkladem IaaS je

262: *Podpůrný materiál k identifikaci poskytovatelů digitálních služeb.* [online]. [cit. 7. 8. 2018]. Dostupné z: https://nukib.cz/download/kii-vis/Definice_DSP_v1.pdf s. 11

263: *Cloud Computing Begins to Gain Traction on Wall Street.* [online]. [cit. 15. 4. 2012]. Dostupné z: http://www.wallstreetandtech.com/it-infrastructure/212700913

264: *Security authorization. An Approach for Community Cloud Computing Environments* [online]. [cit. 15. 4. 2012]. Dostupné z: www.federalnewsradio.com/pdfs/SecurityAuthorizationandAssessmentSECURITYNov2009.pdf

265: Mimo uvedené dělení je v cloud computingu možné rozeznávat například služby:

- ***Infrastrukturní***, jejichž účelem je zajistit splnění požadavků, které jsou zakotveny v dohodě, která stanovuje úroveň poskytovaných služeb [např. velikost úložného prostoru (kapacita), doba uchovávání dat, dostupnost služby, úroveň zabezpečení, aj.].
- Služby, které umožňují ***funkčnost prostředí pro cloud computing*** (např. speciální účtovací software, který zajišťuje, aby v cloudových výpočetních prostředích různé velikosti a s různou úrovní poskytovaných služeb bylo možné vyúčtovat poskytnuté služby).
- ***Konzultační***, které jsou nejčastěji poskytovány v souvislosti s přechodem na cloud computing, případně při odstraňování potíží s cloud computingem.

vizualizace). V případech IaaS uživatel běžně platí za to, co využívá. Tento systém je také nazýván „*utility computing*“[266]. Typickými příklady IaaS jsou Amazon WS, Rackspace aj.[267]

- **Platform-as-a-Service (PaaS). Platforma jako služba** je také nazývána „**cloudware**“[268] a poskytuje uživateli „computing platform“ (v podobě jak hardwarové architektury, tak softwaru – v rámci této služby je možné kombinovat, modifikovat a vyvíjet software, respektive aplikace) a „*solution stack*“.[269] Jako příklady PaaS je možné uvést Google App Engine.[270]

- **Software-as-a-Service (SaaS)**. **Software jako služba** je vlastně způsobem poskytování aplikace uživateli. Aplikace je zpravidla licencována a uživatelé si tak „kupují“ přístup k aplikaci, nikoli aplikaci jako dílo. Příkladem jsou např. Google Apps.[271] Nejčastějšími příklady SaaS aplikací jsou: desktop as a service, business process as a service, communication as a service aj.

**Podle způsobu, jakým je cloud computing poskytován**, je možné rozeznat následující cloudy:

- **Veřejný cloud.** Tento typ cloudu je mnohdy označován jako klasický model cloud computingu. Jedná se o veřejně a volně přístupné služby[272], které jsou poskytovány neomezenému okruhu uživatelů. Tyto služby bývají volně dostupné z Internetu a typickými příklady jsou služby Free Mail, Messenger, Office nebo Storage.

- **Privátní (soukromý) cloud** je typem cloudu, který je zpravidla vytvořen a provozován v rámci jedné firmy, či společnosti. Jde zpravidla o jednoúčelový, privátní cloud s externím poskytovatelem služeb. Takovýto cloud je zaměřen na plnění specifických požadavků firmy a poskytuje ICT služby dynamicky dle potřeb.

---

266: Definice pojmu viz např. *Utility computing.* [online]. [cit. 10. 4. 2012]. Dostupné z: http://searchdatacenter.techtarget.com/definition/utility-computing.

267: http://aws.amazon.com/ (v případě využívání této služby jsou například uživatelům poskytovány unikátní IP adresy a datový prostor – on demand); http://www.rackspace.com/

268: Blíže viz např. *Cloudware.* [online]. [cit. 10.4.2012]. Dostupné z: http://www.cloudwareinc.com/

269: Součásti software, nebo komponenty, nezbytné pro chod zcela funkčních řešení (průduktů, nebo služeb). Blíže viz např. *PaaS Solution Stacks: WINS And LAMP.* [online]. [cit. 10. 4. 2012]. Dostupné z: http://thecloudguytim.wordpress.com/2010/09/08/paas-solution-stacks-wins-lamp/

270: https://developers.google.com/appengine/?hl=cs;

271: http://www.google.com/apps/intl/cs/business/index.html#utm_campaign=cs&utm_source=cs-ha-emea-cs-bk&utm_medium=ha&utm_term=%2Bgoogle%20%2Bapps

272: Byť jsou ve většině případů upraveny a podmíněny souhlasem s licenčním ujednáním.

- **Hybridní cloud** je příkladem cloudu, kdy je infrastruktura cloudu sdílena několika firmami, společnostmi, skupinami jedinců aj. V současnosti se jedná o nejběžnější formu cloud computingu.

Pojmem **rozšiřitelný** se rozumí ta skutečnost, že v zájmu pokrytí nerovnoměrné poptávky jsou výpočetní zdroje přidělovány poskytovatelem cloudových služeb flexibilně, bez ohledu na zeměpisnou polohu zdrojů.

**Přizpůsobitelné úložiště** označuje tu skutečnost, že výpočetní zdroje jsou poskytovány a uvolňovány na základě poptávky. Cílem je urychleně zvyšovat i snižovat dostupné zdroje se zřetelem na zatížení.

Pojmem „**které je možno sdílet**" se rozumí, že výpočetní zdroje jsou poskytovány vícero uživatelům, kteří k dané službě sdílejí společný přístup, avšak zpracování probíhá pro každého uživatele odděleně, byť je služba poskytována z téhož elektronického zařízení.[273]

„***Pokud služeb*** *nabízených ze strany poskytovatelů digitálních služeb* ***využívají orgány veřejné správy*** *členských států,* ***zejména pokud jde o služby cloud computingu, mohou se tyto orgány rozhodnout, že budou od poskytovatelů dotyčných služeb vyžadovat dodatečná bezpečnostní opatření*** *nad rámec obvyklé nabídky poskytovatelů digitálních služeb, která je v souladu s požadavky této směrnice. Měly by mít možnost tak učinit formou smluvních závazků.*"[274]

**K písm. m)**

## Příslušný orgán

**Příslušným orgánem** se rozumí orgán vykonávající působnost v oblasti kybernetické bezpečnosti.

„*Vzhledem k odlišnostem jednotlivých vnitrostátních správních struktur a s cílem podpořit již existující odvětvová opatření nebo kontrolní a regulační orgány Unie a zamezit zdvojování činností by členské státy měly mít* ***možnost určit více než jeden vnitrostátní příslušný orgán odpovědný za plnění úkolů spojených s bezpečností sítí a informačních systémů provozovatelů základních služeb a poskytovatelů digitálních služeb podle této směrnice.***"[275]

Příslušné orgány by dle recitálu 61 NIS měly mít k dispozici potřebné prostředky k plnění svých povinností, včetně pravomoci mít přístup k informacím nezbytným pro posouzení míry bezpečnosti sítí a informačních systémů.

273: Recitál 17 NIS

274: Recitál 54 NIS

275: Recitál 30 NIS

Zároveň by však tyto orgány měly věnovat náležitou pozornost zachování neformálních a důvěryhodných informačních kanálů pro sdílení informací. Zveřejňování incidentů ohlášených příslušným orgánům by mělo zachovávat patřičnou rovnováhu mezi zájmem veřejnosti být informovanou o hrozbách a možným poškozením pověsti či obchodních zájmů provozovatelů základních služeb a poskytovatelů digitálních služeb, kteří incidenty ohlašují.[276]

**§ 3**

**Orgány a osobami, kterým se ukládají povinnosti v oblasti kybernetické bezpečnosti, jsou**

**a) poskytovatel služby elektronických komunikací a subjekt zajišťující síť elektronických komunikací[277], pokud není orgánem nebo osobou podle písmene b),**
**b) orgán nebo osoba zajišťující významnou síť, pokud nejsou správcem nebo provozovatelem komunikačního systému podle písmene d),**
**c) správce a provozovatel informačního systému kritické informační infrastruktury,**
**d) správce a provozovatel komunikačního systému kritické informační infrastruktury,**
**e) správce a provozovatel významného informačního systému,**
**f) správce a provozovatel informačního systému základní služby, pokud nejsou správcem nebo provozovatelem podle písmene c) nebo d),**
**g) provozovatel základní služby, pokud není správcem nebo provozovatelem podle písmene f), a**
**h) poskytovatel digitální služby.**

Z důvodové zprávy:

*Vymezení okruhu povinných osob je částečně založeno na užití stávajících pojmů zákona o elektronických komunikacích.*

*Povinné osoby lze v zásadě rozdělit do dvou skupin. První z nich tvoří poskytovatelé služeb elektronických komunikací a subjekty zajišťující sítě elektronických komunikací vymezení v zákoně o elektronických komunikacích, a subjekty zajišťující tzv. významné sítě, na něž bude regulace tohoto zákona dopadat pouze minimálně, a to v rozsahu povinnosti oznámit kontaktní údaje a jejich změny národnímu CERT, respektive v povinnosti provádět protiopatření za stavu kybernetického nebezpečí. Subjekty zajišťující významné sítě budou nadto povinny detekovat kybernetické bezpečnostní události a hlásit kybernetické bezpečnostní incidenty. Druhou skupinu pak budou tvořit správci informačních systémů kritické informační infrastruktury, správci komunikačních systémů kritické informační infrastruktury, a správci významných informačních systémů, na něž bude dopadat regulace tohoto*

276: Recitál 59 NIS

277: Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů.

*zákona v plném rozsahu. Tato skupina povinných osob tak bude povinna oznámit kontaktní údaje a jejich změnu vládnímu CERT, zavést bezpečnostní opatření, detekovat kybernetické bezpečnostní události, hlásit kybernetické bezpečnostní incidenty a provádět protiopatření.*

*Toto rozdělení povinných osob s následným omezením rozsahu zákonných povinností na nezbytné minimum v závislosti na významnosti informačních a komunikačních systémů, které povinné osoby spravují, odpovídá principu minimalizace státních zásahů, na němž je tento zákon založen. Shora uvedená klasifikace povinných osob má kaskádovitý charakter. Typicky tedy např. subjekt zajišťující významnou síť, která bude zařazena do kritické informační infrastruktury, bude mít ve vztahu k této síti na úseku kybernetické bezpečnosti povinnosti odpovídající správci komunikačního systému zařazeného do kritické informační infrastruktury.*

Z důvodové zprávy k novele ZoKB:

*Do ustanovení § 3, který určuje subjekty (orgány a osoby), jimž zákon o kybernetické bezpečnosti ukládá povinnosti v oblasti kybernetické bezpečnosti, se na základě směrnice doplňují nové subjekty provozovatelé základních služeb, správci a provozovatelé informačního systému základní služby a poskytovatelé digitálních služeb. V případě, že provozovatelé základních služeb nejsou identičtí se správci nebo provozovateli informačních systémů základních služeb, vztahuje se plnění zákonných povinností především na správce a provozovatele informačních systémů základních služeb, a to zejména proto, že právě oni mohou reálně zajišťovat bezpečnost informačních systémů základní služby, na nichž poskytování základní služby závisí.*

*Základní povinnosti podle zákona o kybernetické bezpečnosti, tj. implementace bezpečnostních opatření, hlášení incidentů aj. musí být uloženy vlastníkovi aktiv, tj. subjektu, který určuje účel zpracování informací a podmínky provozování informačního systému. Tím je správce informačního systému. Ve většině případů předpokládáme, že provozovatel základní služby bude zároveň správcem informačního systému základní služby, a výše uvedené povinnosti se na něj budou vztahovat. Nelze však vyloučit, že provozovatel základní služby nebude mít vůči systému rozhodovací pravomoci. V takovém případě po něm nelze chtít, aby plnil povinnosti úzce související s provozováním informačního systému. Z tohoto důvodu je provozovateli základní služby uloženo pouze minimum povinností, přičemž se předpokládá, že hlavní povinnosti uložené zákonem o kybernetické bezpečnosti bude tento subjekt plnit jako správce informačního systému základní služby.*

Ustanovení § 3 ZoKB charakterizuje **osm subjektů** (orgány a osoby), kterým se ukládají povinnosti v oblasti kybernetické bezpečnosti. Mimo subjekty uvedené v § 3 ZoKB jsou zákonem specificky upravena práva a povinnosti provozovatele národního CERT (viz § 18 a násl. ZoKB), vládního CERT (viz § 20 a násl. ZoKB) a Úřadu (viz § 21a a násl. ZoKB).

Krom těchto subjektů se mohou dobrovolně zapojit do systému kybernetické bezpečnosti i další fyzické či právnické osoby, na něž se ZoKB nevztahuje. V tomto případě jde o respektování jednoho ze základních principů ZoKB[278], konkrétně principu autonomie vůle.

Byť není z hlediska komentáře k ZoKB zcela správné vymezovat u těchto subjektů i jejich práva a povinnosti (neboť ty jsou uvedeny v dalších ustanoveních ZoKB), z důvodu přehlednosti zde tato práva a povinnosti uvedeme.

Některé z pojmů již byly definovány, proto na ně bude pouze odkázáno.

**K písm. a)**
**Poskytovatel služby elektronických komunikací a subjekt zajišťující síť elektronických komunikací**

Zákon o kybernetické bezpečnosti při definování prvního z povinných subjektů využil **terminologie uvedené v zákoně o elektronických komunikacích**, který zároveň stanoví podmínky pro podnikání v elektronických komunikacích.

K pojmu **síť elektronických komunikací** viz § 1 ZoKB, § 2 písm. h) ZoEK či čl. 4 odst. 1 písm. a) NIS.

K pojmu **služba elektronických komunikací** viz § 2 písm. a) ZoKB - Kybernetický prostor, § 2 písm. n) ZoEK.

Zákon o elektronických komunikacích v § 2 písm. a) definuje pojem **účastník** jako každého, *„**kdo uzavřel s podnikatelem** poskytujícím veřejně dostupné služby elektronických komunikací **smlouvu na poskytování těchto služeb.**“* Logickým výkladem tohoto ustanovení je možné definovat i pojem **poskytovatele** veřejně dostupné **služby elektronických komunikací**, jako **podnikatele** poskytujícího tyto služby.

Dle § 2 písm. e) ZoEK je operátorem *„podnikatel, který zajišťuje nebo je oprávněn zajišťovat **veřejnou komunikační síť** nebo přiřazené prostředky.“*

V obou dvou výše uvedených ustanoveních je poskytovatel služby či subjekt zajišťující síť elektronických komunikací definován jako **podnikatel** (fyzická či právnická osoba). **Předmětem podnikání v elektronických komunikacích je** dle § 8 odst. 1 ZoEK:

a) zajišťování veřejných komunikačních sítí,
b) poskytování služeb elektronických komunikací.

278: Viz kap. 4.2 Základní cíle a principy ZoKB

Ve vztahu k předmětu podnikání je třeba se věnovat i pojmům **veřejná komunikační síť** a **veřejně dostupná služba elektronických komunikací.**

**Veřejnou komunikační sítí** elektronických komunikací se ve smyslu § 2 písm. j) ZoEK rozumí „***síť** elektronických komunikací, **která slouží zcela nebo převážně k poskytování veřejně dostupných služeb elektronických komunikací**, a která podporuje přenos informací mezi koncovými body sítě, nebo síť elektronických komunikací, jejímž prostřednictvím je poskytovaná služba šíření rozhlasového a televizního vysílání.*"

**Veřejně dostupnou službou elektronických komunikací** se ve smyslu § 2 písm. j) ZoEK rozumí **služba** elektronických komunikací, **z jejíhož využívání není nikdo předem vyloučen.**

**Obecné podmínky pro podnikání** v oblasti elektronických komunikací jsou upraveny v § 8 odst. 2 ZoEK následovně:

a) **u fyzických osob dosažení věku nejméně 18 let,**
b) **u fyzických osob plná způsobilost k právním úkonům,**
c) **bezúhonnost fyzické nebo právnické osoby.**

Za bezúhonného se pro účely tohoto zákona považuje osoba, která nebyla pravomocně odsouzena pro úmyslný trestný čin související s vykonáváním komunikačních činností podle § 7 ZoEK nebo se na ni hledí, jako by nebyla odsouzena. U právnické osoby musí tuto podmínku splňovat osoba oprávněná jednat jménem právnické osoby.

Oprávnění k podnikání vzniká těmto osobám dnem doručení oznámení podnikání[279], které splňuje náležitosti podle § 13 ZoEK, není-li stanoveno jinak.

Jak již bylo uvedeno výše, **zákon o kybernetické bezpečnosti** při definování prvního z povinných subjektů využil terminologie uvedené v zákoně o elektronických komunikacích, **tím však současně omezil okruh osob, na které se § 3 písm. a) ZoKB vztahuje**.

Konkrétně se jedná o podnikatele v elektronických komunikacích podle všeobecného oprávnění[280], za předpokladu, že nejsou orgánem nebo osobou podle § 3 písm. b) ZoKB.

279: § 13 odst. 1 ZoEK: Fyzická a právnická osoba, která hodlá vykonávat komunikační činnost, která je podnikáním v elektronických komunikacích, je povinna předem tuto skutečnost písemně oznámit (dále jen „oznámení") **Úřadu (Českému telekomunikačnímu úřadu).** Oznámení je učiněno dnem jeho doručení Úřadu.

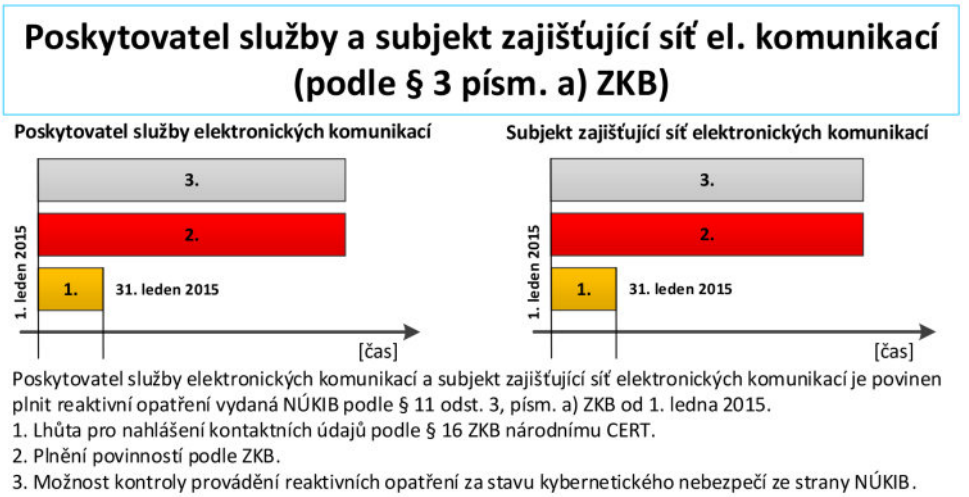
280: Viz *Evidence podnikatelů v elektronických komunikacích podle všeobecného oprávnění*. [online]. [cit. 21. 8. 2018]. Dostupné z:
https://www.ctu.cz/vyhledavaci-databaze/evidence-podnikatelu-v-elektronickych-komunikacich-podle-vseobecneho-opravneni

**Shrnutí aktiv, práv a povinností** dle **ZoKB**:

| | **Poskytovatel služby elektronických komunikací a subjekt zajišťující sítě elektronických komunikací** [§ 3 písm. a) ZoKB], pokud není orgánem nebo osobou podle písmene b) |
|---|---|
| **Soubor aktiv** | • **síť elektronických komunikací** [§ 2 písm. h) ZoEK]<br>• **služba elektronických komunikací** [§ 2 písm. n) ZoEK] |
| **Povinnosti, které je třeba vykonávat mandatorně za všech okolností** | • **hlásit kontaktní údaje národnímu CERT**<br>◦ CSIRT.CZ - https://csirt.cz/<br>◦ formulář je dostupný na: https://www.csirt.cz/contactreport/<br>◦ kontaktní údaje podle § 16 je třeba nahlásit nejpozději do 30 dnů ode dne nabytí účinnosti tohoto zákona (tj. do 31. 1. 2015)<br>◦ v případě, že se subjekt stane orgánem nebo osobou uvedenou v § 3 písm. a) ZoKB po výše uvedeném datu, provede nahlášení těchto údajů bezodkladně |
| **Povinnosti, které je třeba vykonávat jen za stavu kybernetického nebezpečí a za nouzového stavu** | • **provádět reaktivní opatření** podle § 11 odst. 3 písm. a) ZoKB pouze za stavu kybernetického nebezpečí nebo nouzového stavu (Ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky, ve znění ústavního zákona č. 300/2000 Sb.), vyhlášeného na základě § 21 odst. 6 ZoKB.<br>• **oznámit vládnímu CERT provedení reaktivního opatření a jeho výsledek**<br>◦ oznámení o provedení reaktivních opatření se uskutečňuje jen za stavu kybernetického nebezpečí nebo za nouzového stavu<br>◦ o provedení reaktivního opatření jsou orgány nebo osoby nuceny informovat, formou hlášení, NÚKIB |
| | ◦ forma a náležitosti hlášení o provedení reaktivního opatření je součástí jedné z příloh vyhlášky o kybernetické bezpečnosti<br>• **strpět kontroly v oblasti kybernetické bezpečnosti ze strany NÚKIB** |

| | |
|---|---|
| **Práva a spolupráce** | **Provozovatel národního CERT**<br>• přijímá oznámení kontaktních údajů a tyto údaje eviduje a uchovává [§ 17 odst. 2) písm. a) ZoKB]<br>• poskytuje orgánům a osobám metodickou podporu, pomoc a součinnost při výskytu kybernetického bezpečnostního incidentu [§ 17 odst. 2) písm. d) ZoKB]<br>• působí jako kontaktní místo pro orgány a osoby [§ 17 odst. 2) písm. e) ZoKB]<br>• provádí hodnocení zranitelností v oblasti kybernetické bezpečnosti [§ 17 odst. 2) písm. f) ZoKB]<br>• předává Úřadu údaje o kybernetických bezpečnostních incidentech ohlášených podle § 8 odst. 3, bez uvedení ohlašovatele [§ 17 odst. 2) písm. g) ZoKB]<br>• předává na vyžádání Úřadu za stavu kybernetického nebezpečí kontaktní údaje orgánů a osob [§ 17 odst. 2) písm. h) ZoKB]<br><br>**Vládní CERT**<br>• přijímá podněty a údaje od orgánů a osob uvedených v § 3 a od jiných orgánů a osob a tyto podněty a údaje vyhodnocuje [§ 20 písm. f) ZoKB]<br>• provádí hodnocení zranitelností v oblasti kybernetické bezpečnosti [§ 20 písm. j) ZoKB]<br><br>**Úřad (NÚKIB)**<br>• vydá varování, dozví-li se o hrozbě v oblasti kybernetické bezpečnosti [§ 12 odst. 1) ZoKB]<br>• varování Úřad zveřejní na svých internetových stránkách<br>• oznámí je orgánům a osobám uvedeným v § 3 ZoKB<br><br>**Další subjekty**<br>• subjekt zajišťující síť elektronických komunikací má právo být neprodleně a prokazatelně informován orgánem a osobou, které se staly správci nebo provozovateli informačních nebo komunikačních systémů kritické informační infrastruktury, |

| | |
|---|---|
| | že je jejich předmětný informační nebo komunikační systém kritické informační infrastruktury připojen právě sítí elektronických komunikací tohoto subjektu [§ 4a odst. 2) ZoKB]<br>• současně se tento subjekt informuje o tom, že se stal orgánem nebo osobou podle § 3 písm. b) ZoKB |
| **Přestupky** | **§ 25 odst. 1 písm. a) a b) ZoKB**<br>a) nesplní za stavu kybernetického nebezpečí povinnost uloženou Úřadem v rozhodnutí nebo v opatření obecné povahy podle § 13, nebo<br>b) nesplní některou z povinností uloženou nápravným opatřením podle § 24<br>*Za přestupek lze uložit pokutu do 1 000 000 Kč, jde-li o přestupek podle § 25 odst. 1 písm. a) nebo b) ZoKB.* |




Obrázek 21: Lhůty pro plnění povinností podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti[281]

281: *Lhůty pro plnění povinností podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti.* [online]. [cit. 21. 8. 2018]. Dostupné z: https://nukib.cz/download/kii-vis/Schema_lhuty.pdf
V rámci převzatých obrázků je uváděna zkratka **ZKB**, která koresponduje se zkratkou **ZoKB** používanou v této publikaci.

**K písm. b)**
## Orgán nebo osoba zajišťující významnou síť
K pojmu **Významná síť** elektronických komunikací viz § 2 písm. h) ZoKB

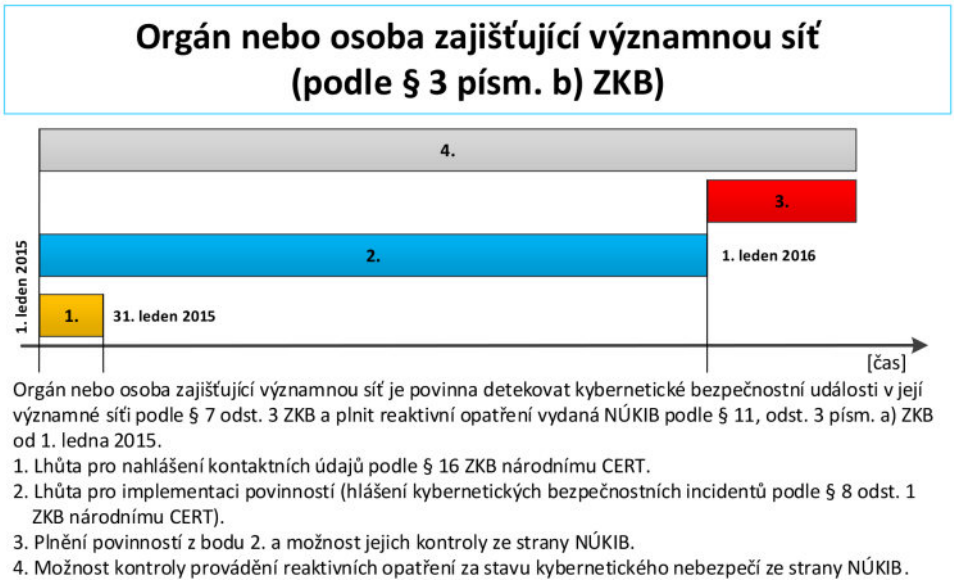
Pojem významná síť v sobě zahrnuje i pojem síť elektronických komunikací (dle ZoEK), z tohoto pohledu se tedy i na orgán nebo osobu zajišťující významnou síť přiměřeně užijí ustanovení ZoEK popsaná v § 3 písm. a) ZoKB.

**Shrnutí aktiv, práv a povinností** dle **ZoKB**:

| | **Orgán nebo osoba zajišťující významnou síť** [§ 3 písm. b) ZoKB], pokud nejsou správcem nebo provozovatelem komunikačního systému podle písmene d) |
|---|---|
| **Soubor aktiv** | • **významná síť** [§ 2 písm. h) ZoKB]<br>• **síť zajišťující přímé připojení ke kritické informační infrastruktuře** [§ 2 písm. h) ZoKB]<br>◦ **síť elektronických komunikací** [§ 2 písm. h) ZoEK] |
| **Povinnosti, které je třeba vykonávat mandatorně za všech okolností** | • **hlásit kontaktní údaje národnímu CERT**<br>◦ CSIRT.CZ - https://csirt.cz/<br>◦ formulář je dostupný na: https://www.csirt.cz/contactreport/<br>◦ kontaktní údaje podle § 16 je třeba nahlásit nejpozději do 30 dnů ode dne nabytí účinnosti tohoto zákona (tj. do 31. 1. 2015)<br>◦ v případě, že se subjekt stane orgánem nebo osobou uvedenou v § 3 písm. a) ZoKB po výše uvedeném datu, provede nahlášení těchto údajů bezodkladně<br>• **hlásit národnímu CERT (CSIRT.CZ) kybernetické bezpečnostní incidenty**<br>◦ formulář je dostupný na: https://www.csirt.cz/stateincidentreport/<br>◦ e-mailová adresa pro hlášení bezpečnostních incidentů je abuse@csirt.cz<br>◦ je možné využít i telefonický kontakt: +420 910 101 010 (každý pracovní den od 09:00–17:00)<br>◦ v urgentních případech je mimo pracovní dobu možné využít telefonní číslo +420 222 745 111 |

| | |
|---|---|
| | ◦ lhůta pro implementaci povinností (hlášení kybernetických bezpečnostních incidentů podle § 8 odst. 1 ZoKB národnímu CERT)<br>◦ tyto povinnosti musí být splněny do 1. 1. 2016, po tomto datu je možná jejich kontrola ze strany NÚKIB [dle § 29 odst. 2 ZoKB]<br>◦ logicky lze dovozovat tu skutečnost, že pokud by orgán nebo osoba začala nově zajišťovat významnou síť (tj. tato síť by nově vznikla), lhůta pro implementaci povinností by zřejmě činila 1 rok<br>• **provádět detekci kybernetických bezpečnostních událostí** |
| **Povinnosti, které je třeba vykonávat jen za stavu kybernetického nebezpečí a za nouzového stavu** | • **provádět reaktivní opatření** podle § 11 odst. 3 písm. a) ZoKB pouze za stavu kybernetického nebezpečí nebo nouzového stavu (Ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky, ve znění ústavního zákona č. 300/2000 Sb.), vyhlášeného na základě § 21 odst. 6 ZoKB.<br>• **oznámit vládnímu CERT provedení reaktivního opatření a jeho výsledek**<br>◦ oznámení o provedení reaktivních opatření se uskutečňuje jen za stavu kybernetického nebezpečí nebo za nouzového stavu<br>◦ o provedení reaktivního opatření jsou orgány nebo osoby nuceny informovat, formou hlášení, NÚKIB<br>◦ forma a náležitosti hlášení o provedení reaktivního opatření je součástí jedné z příloh vyhlášky o kybernetické bezpečnosti<br>• **strpět kontroly v oblasti kybernetické bezpečnosti ze strany NÚKIB** |
| **Práva a spolupráce** | **Provozovatel národního CERT**<br>• přijímá oznámení kontaktních údajů a tyto údaje eviduje a uchovává [§ 17 odst. 2) písm. a) ZoKB]<br>• přijímá hlášení o kybernetických bezpečnostních incidentech a tyto údaje eviduje, uchovává a chrání [§ 17 odst. 2) písm. b) ZoKB]<br>• vyhodnocuje kybernetické bezpečnostní incidenty [§ 17 odst. 2) písm. c) ZoKB]<br>• poskytuje orgánům a osobám metodickou podporu, pomoc a součinnost při výskytu kybernetického bezpečnostního incidentu [§ 17 odst. 2) písm. d) ZoKB] |

| | |
|---|---|
| | • působí jako kontaktní místo pro orgány a osoby [§ 17 odst. 2) písm. e) ZoKB]<br>• provádí hodnocení zranitelností v oblasti kybernetické bezpečnosti [§ 17 odst. 2) písm. f) ZoKB]<br>• předává Úřadu údaje o kybernetických bezpečnostních incidentech ohlášených podle § 8 odst. 3, bez uvedení ohlašovatele [§ 17 odst. 2) písm. g) ZoKB]<br>• předává na vyžádání Úřadu za stavu kybernetického nebezpečí kontaktní údaje orgánů a osob [§ 17 odst. 2) písm. h) ZoKB]<br><br>**Vládní CERT**<br>• přijímá podněty a údaje od orgánů a osob uvedených v § 3 a od jiných orgánů a osob a tyto podněty a údaje vyhodnocuje [§ 20 písm. f) ZoKB]<br>• provádí hodnocení zranitelností v oblasti kybernetické bezpečnosti [§ 20 písm. j) ZoKB]<br><br>**Úřad (NÚKIB)**<br>• vydá varování, dozví-li se o hrozbě v oblasti kybernetické bezpečnosti [§ 12 odst. 1) ZoKB]<br>• varování Úřad zveřejní na svých internetových stránkách<br>• oznámí je orgánům a osobám uvedeným v § 3 ZoKB |
| **Přestupky** | **§ 25 odst. 1 písm. a) a b) ZoKB**<br>a) nesplní za stavu kybernetického nebezpečí povinnost uloženou Úřadem v rozhodnutí nebo v opatření obecné povahy podle § 13, nebo<br>b) nesplní některou z povinností uloženou nápravným opatřením podle § 24<br><br>**§ 25 odst. 6 ZoKB**<br>• neohlásí kybernetický bezpečnostní incident podle § 8 odst. 1 a 3 ZoKB<br>*Za přestupek lze uložit pokutu do 1 000 000 Kč, jde-li o přestupek podle § 25 odst. 1 písm. a) nebo b) či dle § 25 odst. 6 ZoKB.* |




Obrázek 22: Lhůty pro plnění povinností podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti[282]

**K písm. c)** a **d)**
**Správce a provozovatel informačního systému kritické informační infrastruktury**
**Správce a provozovatel komunikačního systému kritické informační infrastruktury**
K pojmu **Správce informačního systému** viz § 2 písm. e) ZoKB.
K pojmu **Správce komunikačního systému** viz § 2 písm. f) ZoKB.
K pojmu **Provozovatel informačního nebo komunikačního systému** viz § 2 písm. g) ZoKB.
K pojmu **kritická infrastruktura** viz § 2 písm. b) ZoKB - Kritická informační infrastruktura.

282: *Lhůty pro plnění povinností podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti.* [online]. [cit. 21. 8. 2018]. Dostupné z: https://nukib.cz/download/kii-vis/Schema_lhuty.pdf

**Shrnutí aktiv, práv a povinností** dle **ZoKB**:

| | **Správce a provozovatele informačního systému kritické informační infrastruktury** [§ 3 písm. c) ZoKB]<br>**Správce a provozovatel komunikačního systému ktitické informační infrastruktury** [§ 3 písm. d) ZoKB] |
|---|---|
| **Soubor aktiv** | • **informační systém kritické informační infrastruktury** [§ 2 písm. b) ZoKB]<br>• **komunikační systém kritické informační infrastruktury** [§ 2 písm. b) ZoKB] |
| **Povinnosti, které je třeba vykonávat mandatorně za všech okolností** | • **hlásit kontaktní údaje vládnímu CERT**<br>◦ GovCERT.CZ- https://www.govcert.cz/<br>◦ formulář je dostupný na: https://www.govcert.cz/download/kii-vis/hlaseni_kontaktu_v5.xltx či https://www.govcert.cz/cs/kyberneticky-zakon/formulare/<br>◦ kontaktní údaje podle § 16 je třeba nahlásit nejpozději do 30 dnů ode dne určení jejich informačního systému nebo komunikačního systému kritickou informační infrastrukturou<br>• **hlásit vládnímu CERT kybernetické bezpečnostní incidenty**<br>◦ formulář je dostupný na: https://www.govcert.cz/download/kii-vis/container-nodeid-649/incidentreportnckb.pdf<br>◦ e-mailový kontakt: cert.incident@nukib.cz<br>◦ v případě nenadálé a vážné situace, kdy hrozí riziko z prodlení, můžete pro kontaktování týmu GovCERT.CZ v pracovní době využít telefonní spojení na čísle +420 541 110 777<br>◦ mimo standardní pracovní dobu pak na telefonním čísle +420 725 502 878<br>◦ lhůta pro implementaci povinností (hlášení kybernetických bezpečnostních incidentů podle § 8 odst. 1 ZoKB vládnímu CERT) činí 1 rok ode dne určení informačního systému nebo komunikačního systému kritickou informační infrastrukturou<br>• **implementovat a provádět bezpečnostní opatření**<br>◦ provádět bezpečnostní opatření, a to v rozsahu nezbytném pro zajištění kybernetické bezpečnosti jejich informačního nebo komunikačního systému |

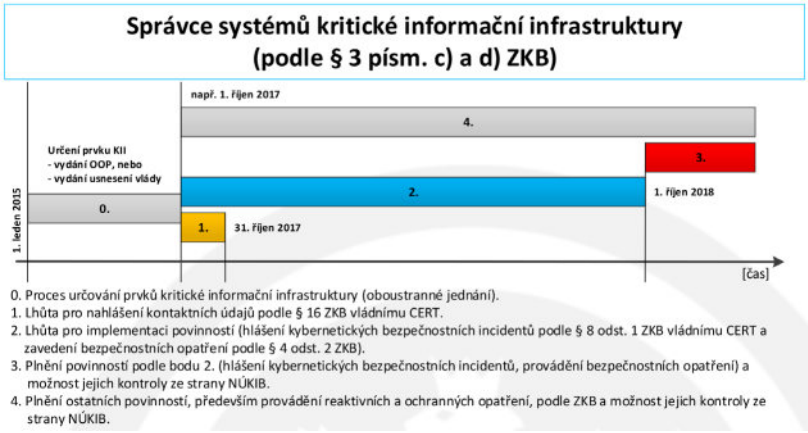
| | |
|---|---|
| | ◦ povinnost vést bezpečnostní dokumentaci o bezpečnostních opatřeních<br>◦ zavést a provádět vhodná a přiměřená bezpečnostní opatření pro sítě elektronických komunikací a informační systémy, které využívá v souvislosti se zajišťováním své služby<br>◦ požadavky na bezpečnostní opatření podle ZoKB jsou obsahem vyhlášky o kybernetické bezpečnosti<br>◦ lhůta pro implementaci povinností (zavedení bezpečnostních opatření podle § 4 odst. 2 ZoKB) činí 1 rok ode dne určení informačního systému nebo komunikačního systému kritickou informační infrastrukturou<br>• **provádět detekci kybernetických bezpečnostních událostí**<br>◦ povinnost řídit se vyhláškou o kybernetické bezpečnosti, která klade speciální požadavky na provoz LOG managementu, IDS / IPS systémů a SIEM systému<br>• **provádět reaktivní opatření**, které jim ukládá NÚKIB na základě informací o probíhajícím bezpečnostním incidentu, k řešení takového incidentu anebo k zabezpečení informačních systémů nebo sítí a služeb před kybernetickým bezpečnostním incidentem<br>◦ reaktivní opatření je vydáváno ve formě rozhodnutí nebo ve formě opatření obecné povahy<br>• **oznámit vládnímu CERT provedení reaktivního opatření a jeho výsledek**<br>◦ o provedení reaktivního opatření jsou orgány nebo osoby nuceny informovat, formou hlášení, NÚKIB<br>◦ forma a náležitosti hlášení o provedení reaktivního opatření je součástí jedné z příloh vyhlášky o kybernetické bezpečnosti<br>• **provádět ochranná opatření**<br>◦ účelem ochranných opatření je dodatečně reagovat na zkušenosti z řešení nastalých kybernetických bezpečnostních incidentů<br>◦ ochranné opatření je vydáváno ve formě opatření obecné povahy<br>• **stanovit požadavky na dodavatele**<br>◦ osoby uvedené v § 3 písm. c) a d) jsou povinny zohlednit požadavky vyplývající z bezpečnostních opatření při výběru dodavatele pro jejich informační nebo komunikační systém |

| | |
|---|---|
| | a tyto požadavky zahrnout do smlouvy, kterou s dodavatelem uzavřou. Zohlednění požadavků vyplývajících z bezpečnostních opatření podle věty první v míře nezbytné pro splnění povinností podle tohoto zákona nelze považovat za nezákonné omezení hospodářské soutěže nebo neodůvodněnou překážku hospodářské soutěži<br>• **strpět kontroly v oblasti kybernetické bezpečnosti ze strany NÚKIB**<br>• správci informačních nebo komunikačních systémů kritické informační infrastruktury, kteří nejsou provozovateli tohoto systému, jsou povinny **neprodleně a prokazatelně informovat provozovatele** systému o této skutečnosti a o tom, že se tento provozovatel stal orgánem nebo osobou podle § 3 písm. c), d) nebo e) ZoKB<br>• **provozovatel** informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury **předá na vyžádání správce tohoto systému** bez zbytečného odkladu a v dohodnutém formátu **data, provozní údaje a informace**, které má k dispozici v souvislosti s provozováním tohoto systému<br>◦ ustanovení právního předpisu upravujícího práva k duševnímu vlastnictví nejsou předáním dat, provozních údajů a informací dotčena<br>• **pokud provozovatel** informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury **nebude tento systém nadále provozovat, předá správci tohoto systému data, provozní údaje a informace**, které má k dispozici v souvislosti s provozováním tohoto systému a které jsou nezbytné pro případné další provozování tohoto informačního systému nebo jeho jiné využití a **bezpečně zlikviduje ve svém digitálním prostředí jejich kopie**<br>◦ způsob likvidace dat, provozních údajů, informací a jejich kopií stanoví prováděcí právní předpis |
| **Práva a spolupráce** | • správce informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury **může pověřit provozováním** informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury **jiný orgán nebo osobu**, pokud to jiný zákon nevylučuje |

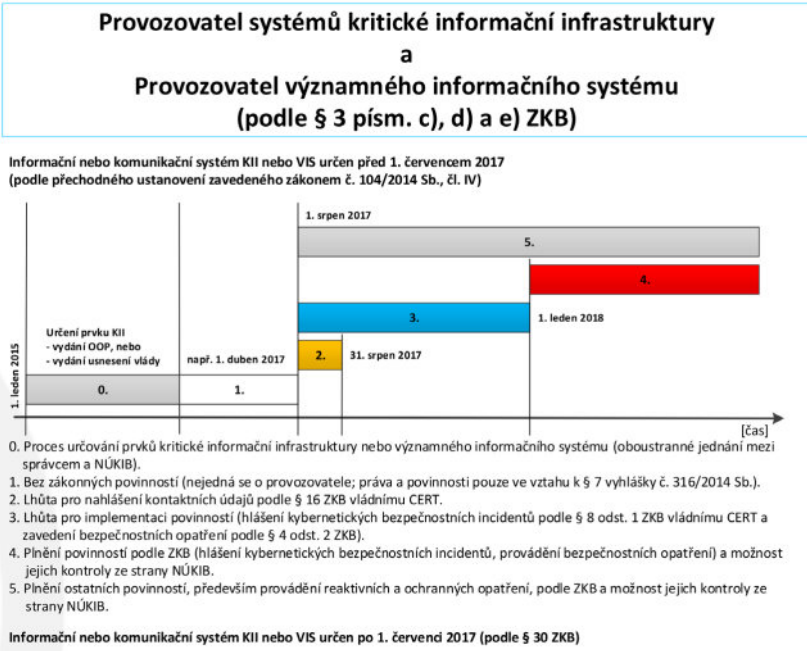
| | |
|---|---|
| | • **provozovatel** informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury **má nárok na úhradu účelně vynaložených nákladů za předání dat, provozních údajů a informací** podle § 6a odst. 2 a 3 ZoKB; náklady provozovateli uhradí správce takového systému.<br><br>**Vládní CERT**<br>• přijímá oznámení kontaktních údajů [§ 20 písm. a) ZoKB]<br>• přijímá hlášení o kybernetických bezpečnostních incidentech a [§ 20 písm. b) ZoKB]<br>• poskytuje orgánům a osobám metodickou podporu, pomoc [§ 20 písm. d) ZoKB]<br>• poskytuje součinnost orgánům a osobám uvedeným v § 3 písm. c) až g) při výskytu kybernetického bezpečnostního incidentu a kybernetické bezpečnostní události [§ 20 písm. e) ZoKB]<br>• přijímá podněty a údaje od orgánů a osob uvedených v § 3 a od jiných orgánů a osob a tyto podněty a údaje vyhodnocuje [§ 20 písm. f) ZoKB]<br>• provádí hodnocení zranitelností v oblasti kybernetické bezpečnosti [§ 20 písm. j) ZoKB]<br><br>**Úřad (NÚKIB)**<br>• vydá varování, dozví-li se o hrozbě v oblasti kybernetické bezpečnosti [§ 12 odst. 1) ZoKB]<br>◦ varování Úřad zveřejní na svých internetových stránkách<br>◦ oznámí je orgánům a osobám uvedeným v § 3 ZoKB<br>◦ je z důvodu ochrany vnitřního pořádku a bezpečnosti, ochrany života a zdraví osob nebo ochrany ekonomiky státu oprávněn po konzultaci s orgánem nebo osobou uvedenými v § 3 písm. c), d), f), g) nebo h), které jsou dotčeny kybernetickým bezpečnostním incidentem, veřejnost o tomto incidentu informovat nebo dotčenému orgánu nebo osobě uložit, aby tak učinil sám<br>• vydá opatření obecné povahy, ve kterém orgánům a osobám uvedeným v § 3 písm. c) až f) stanoví způsob zvýšení ochrany informačních systémů nebo služeb a sítí elektronických komunikací a přiměřenou lhůtu k jeho provedení |

| | |
|---|---|
| **Přestupky** | **§ 25 odst. 2 písm. a) až j) ZoKB**<br>Správce nebo provozovatel informačního nebo komunikačního systému kritické informační infrastruktury se dopustí přestupku tím, že<br>a) v rozporu s § 4 odst. 2 nezavede nebo neprovádí bezpečnostní opatření anebo nevede bezpečnostní dokumentaci,<br>b) neohlásí kybernetický bezpečnostní incident podle § 8 odst. 1 a 4,<br>c) nesplní povinnost uloženou Úřadem v rozhodnutí nebo v opatření obecné povahy podle § 13 nebo 14,<br>d) nesplní povinnost uloženou Úřadem v rozhodnutí podle § 15a odst. 1,<br>e) nepředá data, provozní údaje a informace podle § 6a odst. 2,<br>f) nepředá data, provozní údaje a informace podle § 6a odst. 3,<br>g) nezničí kopie dat, provozních údajů a informací podle § 6a odst. 3,<br>h) neumožní správci dohled nad průběhem zničení dat, provozních údajů a informací podle § 6a odst. 3,<br>i) neoznámí kontaktní údaje nebo jejich změnu Úřadu podle § 16 odst. 2 písm. b) nebo<br>j) nesplní některou z povinností uloženou nápravným opatřením podle § 24.<br>*Za přestupek lze uložit pokutu do 5 000 000 Kč, jde-li o přestupek podle § 25 odst. 2 písm. a) ZoKB.*<br>*Za přestupek lze uložit pokutu do 1 000 000 Kč, jde-li o přestupek podle § 25 odst. 2 písm. b), c), e) ZoKB.*<br>*Za přestupek lze uložit pokutu do 10 000 Kč, jde-li o přestupek podle § 25 odst. 2 písm. d) ZoKB*<br><br>**§ 25 odst. 3 ZoKB**<br>Správce informačního nebo komunikačního systému kritické informační infrastruktury se dopustí přestupku tím, že neinformuje provozovatele systému podle § 4a odst. 1.<br>*Za přestupek lze uložit pokutu do 1 000 000 Kč, jde-li o přestupek podle § 25 odst. 3 ZoKB.*<br><br>**§ 25 odst. 4 ZoKB**<br>Správce nebo provozovatel informačního nebo komunikačního systému kritické informační infrastruktury se dopustí přestupku tím, že neinformuje subjekt zajišťující síť elektronických komunikací podle § 4a odst. 2. |

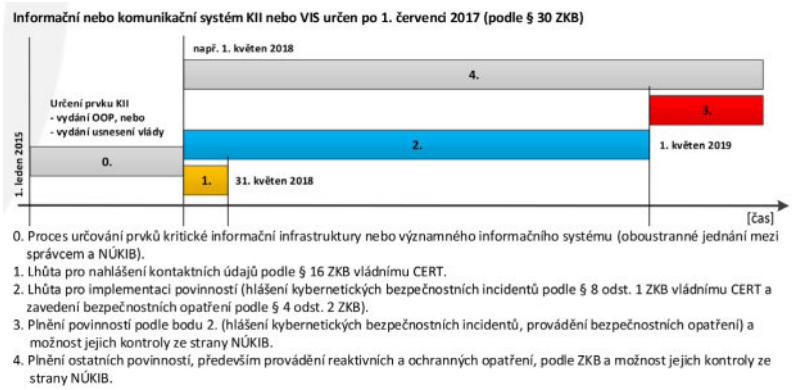
| | |
|---|---|
| | *Za přestupek lze uložit pokutu do 1 000 000 Kč, jde-li o přestupek podle § 25 odst. 4 ZoKB.*<br><br>**§ 25 odst. 5 ZoKB**<br>Provozovatel informačního nebo komunikačního systému kritické informační infrastruktury se dopustí přestupku tím, že<br>a) nesplní povinnost uloženou Úřadem v rozhodnutí podle § 15a odst. 1,<br>a) nepředá data, provozní údaje a informace podle § 6a odst. 2,<br>a) nepředá data, provozní údaje a informace podle § 6a odst. 3,<br>a) nezničí kopie dat, provozních údajů a informací podle § 6a odst. 3, nebo<br>a) neumožní správci dohled nad průběhem zničení dat, provozních údajů a informací podle § 6a odst. 3.<br>*Za přestupek lze uložit pokutu do 1 000 000 Kč, jde-li o přestupek podle § 25 odst. 5 písm. a), c), d) ZoKB.*<br>*Za přestupek lze uložit pokutu do 200 000 Kč, jde-li o přestupek podle § 25 odst. 5 písm. b), e) ZoKB.*<br><br>**§ 25 odst. 8 ZoKB**<br>Správce nebo provozovatel informačního nebo komunikačního systému kritické informační infrastruktury, kteří jsou orgánem veřejné moci, se dopustí přestupku tím, že uzavřou smlouvu s poskytovatelem služeb cloud computingu v rozporu s § 4 odst. 5.<br>*Za přestupek lze uložit pokutu do 1 000 000 Kč, jde-li o přestupek podle § 25 odst. 8 ZoKB.*<br><br>**§ 25 odst. 9 ZoKB**<br>Správce nebo provozovatel informačního nebo komunikačního systému kritické informační infrastruktury se dopustí přestupku tím, že nesplní povinnost informovat veřejnost uloženou Úřadem podle § 12 odst. 3.<br>*Za přestupek lze uložit pokutu do 1 000 000 Kč, jde-li o přestupek podle § 25 odst. 9 ZoKB.* |




Obrázek 23: Lhůty pro plnění povinností podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti[283]




283: *Lhůty pro plnění povinností podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti.* [online]. [cit. 21. 8. 2018]. Dostupné z: https://nukib.cz/download/kii-vis/Schema_lhuty.pdf




Obrázek 24: Lhůty pro plnění povinností podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti[284]

**K písm. e)**
**Správce a provozovatel významného informačního systému**
K pojmu **Správce informačního systému** viz § 2 písm. e) ZoKB.
K pojmu **Významný informační systém** viz § 2 písm. d) ZoKB.

**Shrnutí aktiv, práv a povinností** dle **ZoKB**:

| | **Správce a provozovatel významného informačního systému** [§ 3 písm. e) ZoKB] |
|---|---|
| **Soubor aktiv** | • **významný informační systém** [§ 2 písm. d) ZoKB] |
| **Povinnosti, které je třeba vykonávat mandatorně za všech okolností** | • **hlásit kontaktní údaje vládnímu CERT**<br>◦ GovCERT.CZ- https://www.govcert.cz/<br>◦ formulář je dostupný na: https://www.govcert.cz/download/kii-vis/hlaseni_kontaktu_v5.xltx či https://www.govcert.cz/cs/kyberneticky-zakon/formulare/<br>◦ kontaktní údaje podle § 16 je třeba nahlásit nejpozději do 30 dnů ode dne naplnění určujících kritérií významného informačního systému jejich informačních systémů |

284: *Lhůty pro plnění povinností podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti.* [online]. [cit. 21. 8. 2018]. Dostupné z: https://nukib.cz/download/kii-vis/Schema_lhuty.pdf

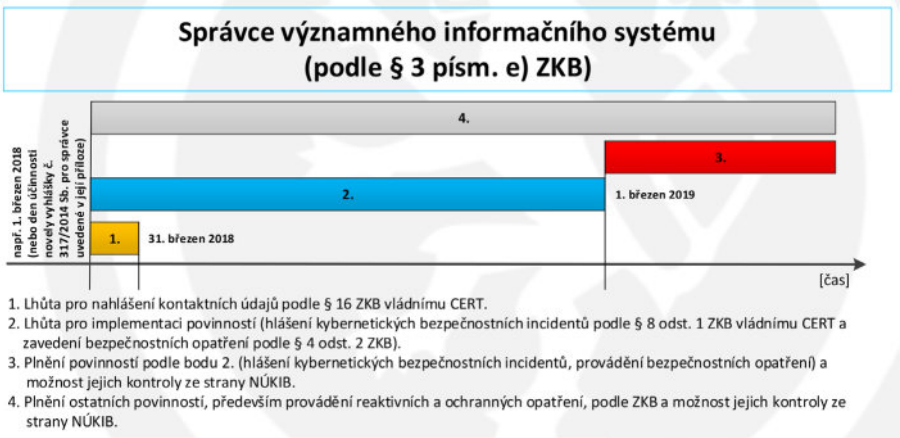
| | |
|---|---|
| | • **hlásit vládnímu CERT kybernetické bezpečnostní incidenty**<br>◦ formulář je dostupný na: https://www.govcert.cz/download/kii-vis/container-nodeid-649/incidentreportnckb.pdf<br>◦ e-mailový kontakt: cert.incident@nukib.cz<br>◦ v případě nenadálé a vážné situace, kdy hrozí riziko z prodlení, můžete pro kontaktování týmu GovCERT.CZ v pracovní době využít telefonní spojení na čísle +420 541 110 777<br>◦ mimo standardní pracovní dobu pak na telefonním čísle +420 725 502 878<br>◦ lhůta pro implementaci povinností (hlášení kybernetických bezpečnostních incidentů podle § 8 odst. 1 ZoKB vládnímu CERT) činí 1 rok ode dne naplnění určujících kritérií významného informačního systému<br>• **implementovat a provádět bezpečnostní opatření**<br>◦ provádět bezpečnostní opatření, a to v rozsahu nezbytném pro zajištění kybernetické bezpečnosti jejich informačního nebo komunikačního systému<br>◦ povinnost vést bezpečnostní dokumentaci o bezpečnostních opatřeních<br>◦ zavést a provádět vhodná a přiměřená bezpečnostní opatření pro sítě elektronických komunikací a informační systémy, které využívá v souvislosti se zajišťováním své služby<br>◦ požadavky na bezpečnostní opatření podle ZoKB jsou obsahem vyhlášky o kybernetické bezpečnosti<br>◦ lhůta pro implementaci povinností (zavedení bezpečnostních opatření podle § 4 odst. 2 ZoKB) činí 1 rok ode dne naplnění určujících kritérií významného informačního systému<br>• **provádět detekci kybernetických bezpečnostních událostí**<br>◦ povinnost řídit se vyhláškou o kybernetické bezpečnosti, která klade speciální požadavky na provoz LOG managementu, IDS / IPS systémů a SIEM systému<br>• **provádět reaktivní opatření,** které jim ukládá NÚKIB na základě informací o probíhajícím bezpečnostním incidentu, k řešení takového incidentu anebo k zabezpečení informačních systémů nebo sítí a služeb před kybernetickým bezpečnostním incidentem |

| | |
|---|---|
| | ◦ reaktivní opatření je vydáváno ve formě rozhodnutí nebo ve formě opatření obecné povahy<br>• **oznámit vládnímu CERT provedení reaktivního opatření a jeho výsledek**<br>◦ o provedení reaktivního opatření jsou orgány nebo osoby nuceny informovat, formou hlášení, NÚKIB<br>◦ forma a náležitosti hlášení o provedení reaktivního opatření je součástí jedné z příloh vyhlášky o kybernetické bezpečnosti<br>• **provádět ochranná opatření**<br>◦ účelem ochranných opatření je dodatečně reagovat na zkušenosti z řešení nastalých kybernetických bezpečnostních incidentů<br>◦ ochranné opatření je vydáváno ve formě opatření obecné povahy<br>• **stanovit požadavky na dodavatele**<br>◦ orgány a osoby uvedené v § 3 písm. e) jsou povinny zohlednit požadavky vyplývající z bezpečnostních opatření při výběru dodavatele pro jejich informační nebo komunikační systém a tyto požadavky zahrnout do smlouvy, kterou s dodavatelem uzavřou. Zohlednění požadavků vyplývajících z bezpečnostních opatření podle věty první v míře nezbytné pro splnění povinností podle tohoto zákona nelze považovat za nezákonné omezení hospodářské soutěže nebo neodůvodněnou překážku hospodářské soutěži<br>• **strpění kontroly v oblasti kybernetické bezpečnosti ze strany NÚKIB**<br>• orgány a osoby, které se **staly správci** významných informačních systémů, **a nejsou provozovateli tohoto systému, jsou povinny neprodleně a prokazatelně informovat provozovatele systému** o této skutečnosti a o tom, že se tento provozovatel stal orgánem nebo osobou podle § 3 písm. c), d) nebo e) ZoKB<br>• **provozovatel** významného informačního systému **předá na vyžádání správce** tohoto systému bez zbytečného odkladu a v dohodnutém formátu **data, provozní údaje a informace**, které má k dispozici v souvislosti s provozováním tohoto systému |

| | |
|---|---|
| | ◦ ustanovení právního předpisu upravujícího práva<br>◦ k duševnímu vlastnictví nejsou předáním dat, provozních údajů a informací dotčena<br>• pokud **provozovatel** významného informačního systému **nebude tento systém nadále provozovat, předá správci tohoto systému data, provozní údaje a informace**, které má k dispozici v souvislosti s provozováním tohoto systému a které jsou nezbytné pro případné další provozování tohoto informačního systému nebo jeho jiné využití a **bezpečně zlikviduje ve svém digitálním prostředí jejich kopie**<br>◦ způsob likvidace dat, provozních údajů, informací a jejich kopií stanoví prováděcí právní předpis |
| **Práva a spolupráce** | • **správce** významného informačního systému **může pověřit provozováním** významného informačního systému **jiný orgán nebo osobu**, pokud to jiný zákon nevylučuje<br>• provozovatel **významného informačního systému** má **nárok na úhradu účelně vynaložených nákladů za předání dat, provozních údajů a informací** podle § 6a odst. 2 a 3 ZoKB; náklady provozovateli uhradí správce takového systému<br><br>**Vládní CERT**<br>• přijímá oznámení kontaktních údajů [§ 20 písm. a) ZoKB]<br>• přijímá hlášení o kybernetických bezpečnostních incidentech a [§ 20 písm. b) ZoKB]<br>• poskytuje orgánům a osobám metodickou podporu, pomoc [§ 20 písm. d) ZoKB]<br>• poskytuje součinnost orgánům a osobám uvedeným v § 3 písm. c) až g) při výskytu kybernetického bezpečnostního incidentu a kybernetické bezpečnostní události [§ 20 písm. e) ZoKB]<br>• přijímá podněty a údaje od orgánů a osob uvedených v § 3 a od jiných orgánů a osob a tyto podněty a údaje vyhodnocuje [§ 20 písm. f) ZoKB]<br>• provádí hodnocení zranitelností v oblasti kybernetické bezpečnosti [§ 20 písm. j) ZoKB]<br><br>**Úřad (NÚKIB)**<br>• vydá varování, dozví-li se o hrozbě v oblasti kybernetické bezpečnosti [§ 12 odst. 1) ZoKB]<br>◦ varování Úřad zveřejní na svých internetových stránkách<br>◦ oznámí je orgánům a osobám uvedeným v § 3 ZoKB |

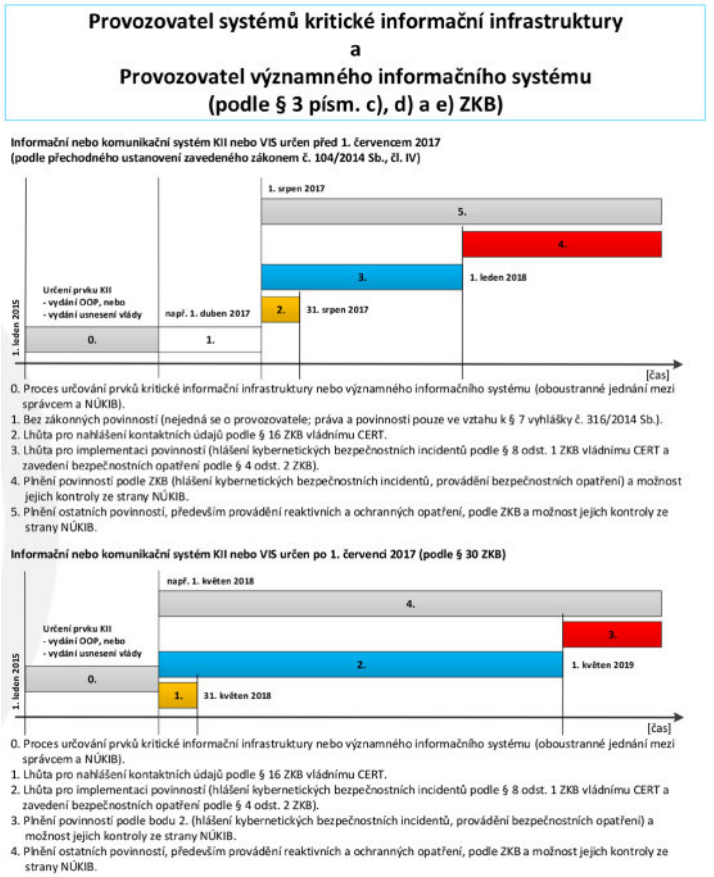
| | |
|---|---|
| | • vydá opatření obecné povahy, ve kterém orgánům a osobám uvedeným v § 3 písm. c) až f) stanoví způsob zvýšení ochrany informačních systémů nebo služeb a sítí elektronických komunikací a přiměřenou lhůtu k jeho provedení |
| **Přestupky** | **§ 25 odst. 2 písm. a) až j) ZoKB**<br>Správce nebo provozovatel významného informačního systému se dopustí přestupku tím, že<br>a) v rozporu s § 4 odst. 2 nezavede nebo neprovádí bezpečnostní opatření anebo nevede bezpečnostní dokumentaci,<br>b) neohlásí kybernetický bezpečnostní incident podle § 8 odst. 1 a 4,<br>c) nesplní povinnost uloženou Úřadem v rozhodnutí nebo v opatření obecné povahy podle § 13 nebo 14,<br>d) nesplní povinnost uloženou Úřadem v rozhodnutí podle § 15a odst. 1,<br>e) nepředá data, provozní údaje a informace podle § 6a odst. 2,<br>f) nepředá data, provozní údaje a informace podle § 6a odst. 3,<br>g) nezničí kopie dat, provozních údajů a informací podle § 6a odst. 3,<br>h) neumožní správci dohled nad průběhem zničení dat, provozních údajů a informací podle § 6a odst. 3,<br>i) neoznámí kontaktní údaje nebo jejich změnu Úřadu podle § 16 odst. 2 písm. b) nebo<br>j) nesplní některou z povinností uloženou nápravným opatřením podle § 24.<br>*Za přestupek lze uložit pokutu do 5 000 000 Kč, jde-li o přestupek podle § 25 odst. 2 písm. a) ZoKB.*<br>*Za přestupek lze uložit pokutu do 1 000 000 Kč, jde-li o přestupek podle § 25 odst. 2 písm. b), c), e) ZoKB.*<br>*Za přestupek lze uložit pokutu do 10 000 Kč, jde-li o přestupek podle § 25 odst. 2 písm. d) ZoKB*<br><br>**§ 25 odst. 3 ZoKB**<br>Správce významného informačního systému se dopustí přestupku tím, že neinformuje provozovatele systému podle § 4a odst. 1.<br>*Za přestupek lze uložit pokutu do 1 000 000 Kč, jde-li o přestupek podle § 25 odst. 3 ZoKB.*<br>*Za přestupek lze uložit pokutu do 1 000 000 Kč, jde-li o přestupek podle § 25 odst. 4 ZoKB.* |

| | |
|---|---|
| | **§ 25 odst. 8 ZoKB**<br>Správce nebo provozovatel významného informačního systému, kteří jsou orgánem veřejné moci, se dopustí přestupku tím, že uzavřou smlouvu s poskytovatelem služeb cloud computingu v rozporu s § 4 odst. 5.<br>*Za přestupek lze uložit pokutu do 1 000 000 Kč, jde-li o přestupek podle § 25 odst. 8 ZoKB.* |




Obrázek 25: Lhůty pro plnění povinností podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti[285]

285: *Lhůty pro plnění povinností podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti.* [online]. [cit. 21. 8. 2018]. Dostupné z: https://nukib.cz/download/kii-vis/Schema_lhuty.pdf




Obrázek 26: Lhůty pro plnění povinností podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti[286]

**K písm. f)**

**Správce a provozovatel informačního systému základní služby**

K pojmu **Správce informačního systému** viz § 2 písm. e) ZoKB.

K pojmu **Provozovatel informačního nebo komunikačního systému** viz § 2 písm. g) ZoKB a § 2 odst. k) ZoKB - Základní služba. Informační systém základní služby. Provozovatel základní služby.

K pojmu **základní služba** viz § 2 písm. i) ZoKB.

286: *Lhůty pro plnění povinností podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti.* [online]. [cit. 21. 8. 2018]. Dostupné z: https://nukib.cz/download/kii-vis/Schema_lhuty.pdf

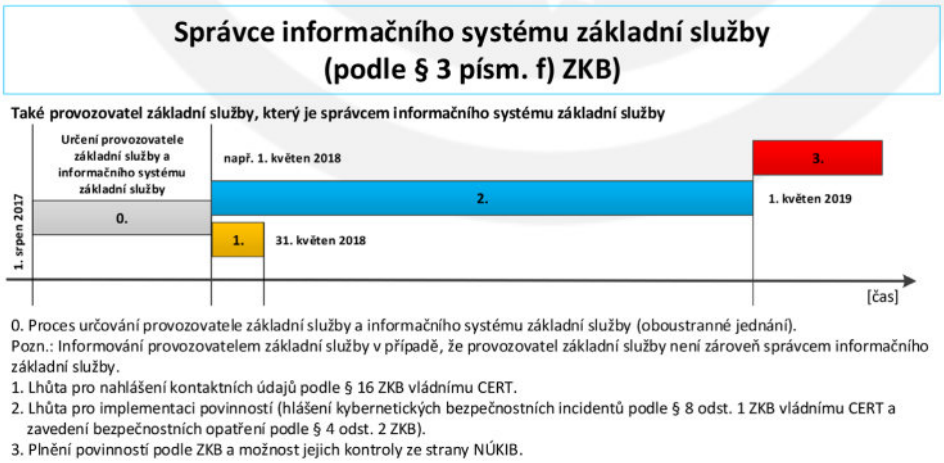
**Shrnutí aktiv, práv a povinností** dle **ZoKB**:

| | **Správce a provozovatel informačního systému základní služby,** pokud nejsou správcem nebo provozovatelem podle písmene c) nebo d) [§ 3 písm. f) ZoKB] |
|---|---|
| **Soubor aktiv** | • **informační systém základní služby** [§ 2 písm. f) a i) ZoKB] |
| **Povinnosti, které je třeba vykonávat mandatorně za všech okolností** | • **hlásit kontaktní údaje vládnímu CERT**<br>◦ GovCERT.CZ - https://www.govcert.cz/<br>◦ formulář je dostupný na: https://www.govcert.cz/download/kii-vis/hlaseni_kontaktu_v5.xltx či https://www.govcert.cz/cs/kyberneticky-zakon/formulare/<br>◦ kontaktní údaje podle § 16 je třeba nahlásit nejpozději do 30 dnů ode dne určení provozovatele základní služby a informačního systému základní služby<br>• **hlásit vládnímu CERT kybernetické bezpečnostní incidenty**<br>◦ formulář je dostupný na: https://www.govcert.cz/download/kii-vis/container-nodeid-649/incidentreportnckb.pdf<br>◦ e-mailový kontakt: cert.incident@nukib.cz<br>◦ v případě nenadálé a vážné situace, kdy hrozí riziko z prodlení, můžete pro kontaktování týmu GovCERT.CZ v pracovní době využít telefonní spojení na čísle +420 541 110 777<br>◦ mimo standardní pracovní dobu pak na telefonním čísle +420 725 502 878<br>◦ lhůta pro implementaci povinností (hlášení kybernetických bezpečnostních incidentů podle § 8 odst. 1 ZoKB vládnímu CERT) činí 1 rok ode dne určení provozovatele základní služby a informačního systému základní služby<br>• **implementovat a provádět bezpečnostní opatření**<br>◦ provádět bezpečnostní opatření, a to v rozsahu nezbytném pro zajištění kybernetické bezpečnosti jejich informačního nebo komunikačního systému<br>◦ povinnost vést bezpečnostní dokumentaci o bezpečnostních opatřeních<br>◦ zavést a provádět vhodná a přiměřená bezpečnostní opatření pro sítě elektronických komunikací a informační systémy, které využívá v souvislosti se zajišťováním své služby |

| | |
|---|---|
| | ◦ požadavky na bezpečnostní opatření podle ZoKB jsou obsahem vyhlášky o kybernetické bezpečnosti<br>◦ lhůta pro implementaci povinností (zavedení bezpečnostních opatření podle § 4 odst. 2 ZoKB) činí 1 rok ode dne určení provozovatele základní služby a informačního systému základní služby<br>• **provádět detekci kybernetických bezpečnostních událostí**<br>◦ povinnost řídit se vyhláškou o kybernetické bezpečnosti, která klade speciální požadavky na provoz LOG managementu, IDS / IPS systémů a SIEM systému<br>• **provádět reaktivní opatření,** které jim ukládá NÚKIB na základě informací o probíhajícím bezpečnostním incidentu, k řešení takového incidentu anebo k zabezpečení informačních systémů nebo sítí a služeb před kybernetickým bezpečnostním incidentem<br>◦ reaktivní opatření je vydáváno ve formě rozhodnutí nebo ve formě opatření obecné povahy<br>• **oznámit vládnímu CERT provedení reaktivního opatření a jeho výsledek**<br>◦ o provedení reaktivního opatření jsou orgány nebo osoby nuceny informovat, formou hlášení, NÚKIB<br>◦ forma a náležitosti hlášení o provedení reaktivního opatření je součástí jedné z příloh vyhlášky o kybernetické bezpečnosti<br>• **provádět ochranná opatření**<br>◦ účelem ochranných opatření je dodatečně reagovat na zkušenosti z řešení nastalých kybernetických bezpečnostních incidentů<br>◦ ochranné opatření je vydáváno ve formě opatření obecné povahy<br>• **stanovit požadavky na dodavatele**<br>◦ osoby uvedené v § 3 písm. c) a d) jsou povinny zohlednit požadavky vyplývající z bezpečnostních opatření při výběru dodavatele pro jejich informační nebo komunikační systém a tyto požadavky zahrnout do smlouvy, kterou s dodavatelem uzavřou. Zohlednění požadavků vyplývajících z bezpečnostních opatření podle věty první v míře nezbytné pro splnění povinností podle tohoto zákona nelze považovat za nezákonné omezení hospodářské soutěže nebo neodůvodněnou překážku hospodářské soutěži |

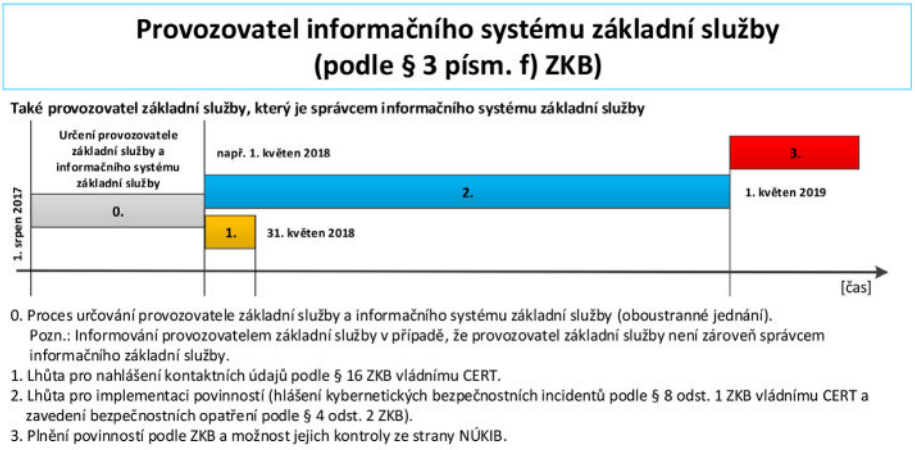
| | |
|---|---|
| | • **strpění kontroly v oblasti kybernetické bezpečnosti ze strany NÚKIB**<br>• orgány a osoby, které byly určené **provozovateli základní služby a nejsou zároveň správci** nebo **provozovateli svých informačních systémů** základní služby, **jsou povinny správce nebo provozovatele tohoto** informačního **systému** základní služby neprodleně a prokazatelně **informovat o svém určení a o tom, že se dotčený správce nebo provozovatel stal orgánem nebo osobou podle § 3 písm. f) ZoKB** |
| **Práva a spolupráce** | **Vládní CERT**<br>• přijímá oznámení kontaktních údajů [§ 20 písm. a) ZoKB]<br>• přijímá hlášení o kybernetických bezpečnostních incidentech a [§ 20 písm. b) ZoKB]<br>• poskytuje orgánům a osobám metodickou podporu, pomoc [§ 20 písm. d) ZoKB]<br>• poskytuje součinnost orgánům a osobám uvedeným v § 3 písm. c) až g) při výskytu kybernetického bezpečnostního incidentu a kybernetické bezpečnostní události [§ 20 písm. e) ZoKB]<br>• přijímá podněty a údaje od orgánů a osob uvedených v § 3 a od jiných orgánů a osob a tyto podněty a údaje vyhodnocuje [§ 20 písm. f) ZoKB]<br>• provádí hodnocení zranitelností v oblasti kybernetické bezpečnosti [§ 20 písm. j) ZoKB]<br><br>**Úřad (NÚKIB)**<br>• vydá varování, dozví-li se o hrozbě v oblasti kybernetické bezpečnosti [§ 12 odst. 1) ZoKB]<br>◦ varování Úřad zveřejní na svých internetových stránkách<br>◦ oznámí je orgánům a osobám uvedeným v § 3 ZoKB<br>◦ je z důvodu ochrany vnitřního pořádku a bezpečnosti, ochrany života a zdraví osob nebo ochrany ekonomiky státu oprávněn po konzultaci s orgánem nebo osobou uvedenými v § 3 písm. c), d), f), g) nebo h), které jsou dotčeny kybernetickým bezpečnostním incidentem, veřejnost o tomto incidentu informovat nebo dotčenému orgánu nebo osobě uložit, aby tak učinil sám<br>• vydá opatření obecné povahy, ve kterém orgánům a osobám uvedeným v § 3 písm. c) až f) stanoví způsob zvýšení ochrany |

| | |
|---|---|
| | informačních systémů nebo služeb a sítí elektronických komunikací a přiměřenou lhůtu k jeho provedení |
| **Přestupky** | **§ 25 odst. 7 písm. a) až f) ZoKB**<br>Správce a provozovatel informačního systému základní služby se dopustí přestupku tím, že<br>a) v rozporu s § 4 odst. 2 nezavede nebo neprovádí bezpečnostní opatření nebo nevede bezpečnostní dokumentaci,<br>b) neohlásí kybernetický bezpečnostní incident podle § 8 odst. 1 a 4,<br>c) nesplní povinnost informovat veřejnost uloženou Úřadem podle § 12 odst. 3,<br>d) nesplní povinnost uloženou Úřadem podle § 13 nebo 14,<br>e) neoznámí kontaktní údaje nebo jejich změnu Úřadu podle § 16 odst. 2 písm. b), nebo<br>f) nesplní některou z povinností uloženou nápravným opatřením podle § 24.<br>*Za přestupek lze uložit pokutu do 5 000 000 Kč, jde-li o přestupek podle § 25 odst. 7 písm. a) ZoKB.*<br>*Za přestupek lze uložit pokutu do 1 000 000 Kč, jde-li o přestupek podle § 25 odst. 7 písm. b) až d) ZoKB.*<br>*Za přestupek lze uložit pokutu do 10 000 Kč, jde-li o přestupek podle § 25 odst. 7 písm. e) ZoKB*<br><br>**§ 25 odst. 8 ZoKB**<br>Správce nebo provozovatel informačního systému základní služby, kteří jsou orgánem veřejné moci, se dopustí přestupku tím, že uzavřou smlouvu s poskytovatelem služeb cloud computingu v rozporu s § 4 odst. 5.<br>*Za přestupek lze uložit pokutu do 1 000 000 Kč, jde-li o přestupek podle § 25 odst. 8 ZoKB.* |




0. Proces určování provozovatele základní služby a informačního systému základní služby (oboustranné jednání).
Pozn.: Informování provozovatelem základní služby v případě, že provozovatel základní služby není zároveň správcem informačního základní služby.
1. Lhůta pro nahlášení kontaktních údajů podle § 16 ZKB vládnímu CERT.
2. Lhůta pro implementaci povinností (hlášení kybernetických bezpečnostních incidentů podle § 8 odst. 1 ZKB vládnímu CERT a zavedení bezpečnostních opatření podle § 4 odst. 2 ZKB).
3. Plnění povinností podle ZKB a možnost jejich kontroly ze strany NÚKIB.

Obrázek 27: Lhůty pro plnění povinností podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti[287]




0. Proces určování provozovatele základní služby a informačního systému základní služby (oboustranné jednání).
Pozn.: Informování provozovatelem základní služby v případě, že provozovatel základní služby není zároveň správcem informačního základní služby.
1. Lhůta pro nahlášení kontaktních údajů podle § 16 ZKB vládnímu CERT.
2. Lhůta pro implementaci povinností (hlášení kybernetických bezpečnostních incidentů podle § 8 odst. 1 ZKB vládnímu CERT a zavedení bezpečnostních opatření podle § 4 odst. 2 ZKB).
3. Plnění povinností podle ZKB a možnost jejich kontroly ze strany NÚKIB.

Obrázek 28: Lhůty pro plnění povinností podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti[288]

287: *Lhůty pro plnění povinností podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti.* [online]. [cit. 21. 8. 2018]. Dostupné z: https://nukib.cz/download/kii-vis/Schema_lhuty.pdf

288: *Lhůty pro plnění povinností podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti.* [online]. [cit. 21. 8. 2018]. Dostupné z: https://nukib.cz/download/kii-vis/Schema_lhuty.pdf

**K písm. g)**

**Provozovatel základní služby**

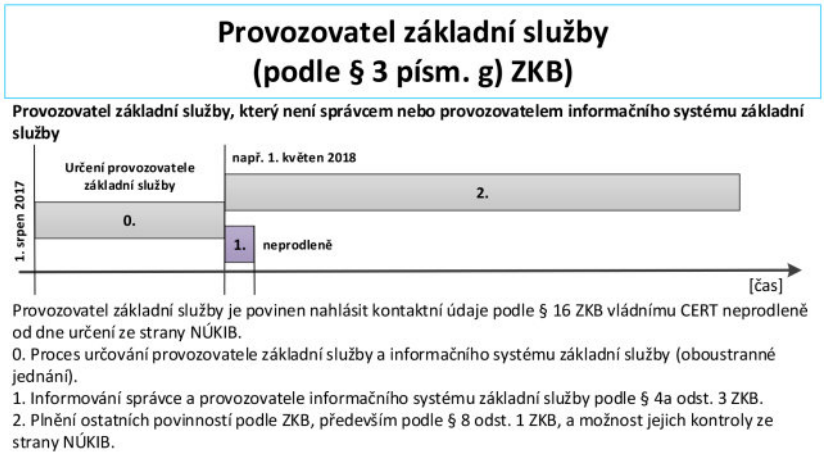
K pojmu **Základní služba**, Informační systém základní služby, Provozovatel základní služby, viz § 2 písm. k) ZoKB.

**Shrnutí aktiv, práv a povinností** dle **ZoKB**:

| | **Provozovatel základní služby**, pokud není správcem nebo provozovatelem podle písmene f) [§ 3 písm. g) ZoKB] |
|---|---|
| **Soubor aktiv** | • **poskytuje základní službu závislou na informačních systémech základní služby** [§ 2 písm. f) a i) ZoKB] |
| **Povinnosti, které je třeba vykonávat mandatorně za všech okolností** | • **hlásit kontaktní údaje vládnímu CERT**<br>◦ GovCERT.CZ - https://www.govcert.cz/<br>◦ formulář je dostupný na: https://www.govcert.cz/download/kii-vis/hlaseni_kontaktu_v5.xltx či https://www.govcert.cz/cs/kyberneticky-zakon/formulare/<br>◦ kontaktní údaje podle § 16 je třeba nahlásit **neprodleně** ode dne určení ze strany NÚKIB<br>• **hlásit vládnímu CERT kybernetické bezpečnostní incidenty v případě, že mají významný dopad na kontinuitu poskytování základní služby**<br>◦ náležitosti hlášení jsou obsaženy ve vyhlášce o kybernetické bezpečnosti<br>◦ formulář je dostupný na: https://www.govcert.cz/download/kii-vis/container-nodeid-649/incidentreportnckb.pdf<br>◦ e-mailový kontakt: cert.incident@nukib.cz<br>◦ v případě nenadálé a vážné situace, kdy hrozí riziko z prodlení, můžete pro kontaktování týmu GovCERT.CZ v pracovní době využít telefonní spojení na čísle +420 541 110 777<br>◦ mimo standardní pracovní dobu pak na telefonním čísle +420 725 502 878<br>◦ implementace povinností (hlášení kybernetických bezpečnostních incidentů podle § 8 odst. 1 ZoKB vládnímu CERT) ode dne určení provozovatele základní služby<br>• **Informovat správce a provozovatele informačního systému základní služby** podle § 4a odst. 3 ZoKB.<br>• **neprodleně** ode dne určení ze strany NÚKIB |

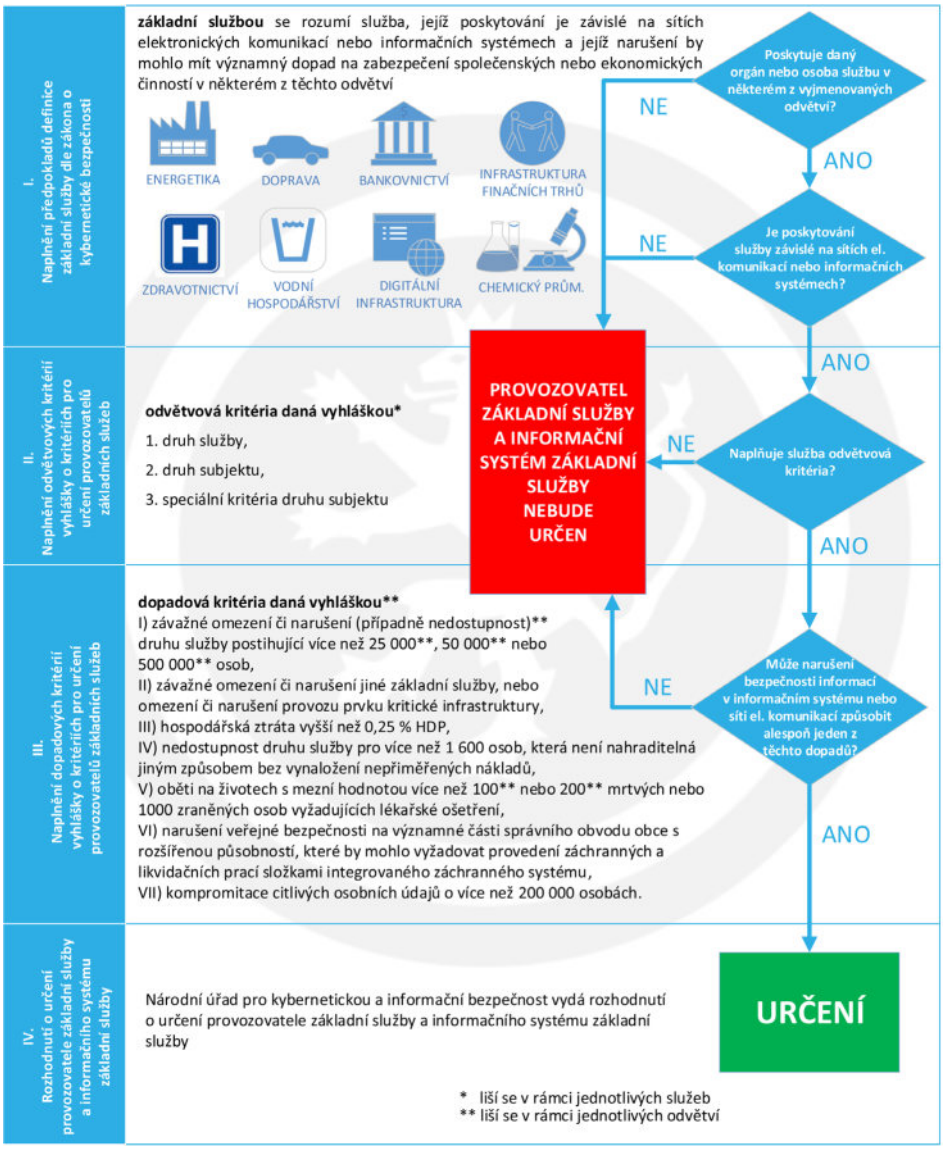
| | |
|---|---|
| | • **strpění kontroly v oblasti kybernetické bezpečnosti ze strany NÚKIB** |
| **Práva a spolupráce** | **Vládní CERT**<br>• přijímá oznámení kontaktních údajů [§ 20 písm. a) ZoKB]<br>• přijímá hlášení o kybernetických bezpečnostních incidentech a [§ 20 písm. b) ZoKB]<br>• poskytuje orgánům a osobám metodickou podporu, pomoc [§ 20 písm. d) ZoKB]<br>• poskytuje součinnost orgánům a osobám uvedeným v § 3 písm. c) až g) při výskytu kybernetického bezpečnostního incidentu a kybernetické bezpečnostní události [§ 20 písm. e) ZoKB]<br>• přijímá podněty a údaje od orgánů a osob uvedených v § 3 a od jiných orgánů a osob a tyto podněty a údaje vyhodnocuje [§ 20 písm. f) ZoKB]<br>• provádí hodnocení zranitelností v oblasti kybernetické bezpečnosti [§ 20 písm. j) ZoKB]<br><br>**Úřad (NÚKIB)**<br>• vydá varování, dozví-li se o hrozbě v oblasti kybernetické bezpečnosti [§ 12 odst. 1) ZoKB]<br>◦ varování Úřad zveřejní na svých internetových stránkách<br>◦ oznámí je orgánům a osobám uvedeným v § 3 ZoKB<br>◦ je z důvodu ochrany vnitřního pořádku a bezpečnosti, ochrany života a zdraví osob nebo ochrany ekonomiky státu oprávněn po konzultaci s orgánem nebo osobou uvedenými v § 3 písm. c), d), f), g) nebo h), které jsou dotčeny kybernetickým bezpečnostním incidentem, veřejnost o tomto incidentu informovat nebo dotčenému orgánu nebo osobě uložit, aby tak učinil sám<br>• **určí provozovatele základní služby a informační systém základní služby** podle § 22a odst. 1 ZoKB, **do 9. listopadu 2018**<br><br>**Další subjekty**<br>• orgány a osoby, které byly určené provozovateli základní služby a nejsou zároveň správci nebo provozovateli svých informačních systémů základní služby, jsou povinny správce nebo provozovatele tohoto informačního systému základní služby neprodleně a prokazatelně informovat o svém určení |

| | |
|---|---|
| | a o tom, že se dotčený správce nebo provozovatel stal orgánem nebo osobou podle § 3 písm. f) ZoKB |
| **Přestupky** | **§ 25 odst. 8 ZoKB**<br>Provozovatel základní služby, který je orgánem veřejné moci, se dopustí přestupku tím, že uzavře smlouvu s poskytovatelem služeb cloud computingu v rozporu s § 4 odst. 5.<br>*Za přestupek lze uložit pokutu do 1 000 000 Kč, jde-li o přestupek podle § 25 odst. 8 ZoKB.*<br><br>**§ 25 odst. 10 ZoKB**<br>Provozovatel základní služby se dopustí přestupku tím, že<br>a) neinformuje správce nebo provozovatele informačního systému základní služby podle § 4a odst. 3,<br>b) nenahlásí významný dopad na kontinuitu poskytování základní služby podle § 8 odst. 1 a 4,<br>c) nenahlásí významný dopad na kontinuitu poskytování základní služby způsobený kybernetickým bezpečnostním incidentem podle § 8 odst. 8,<br>d) nesplní povinnost informovat veřejnost uloženou Úřadem podle § 12 odst. 3, nebo<br>e) neoznámí kontaktní údaje nebo jejich změnu Úřadu podle § 16 odst. 2 písm. b).<br>*Za přestupek lze uložit pokutu do 1 000 000 Kč, jde-li o přestupek podle § 25 odst. 10 písm. a) až d) ZoKB.*<br>*Za přestupek lze uložit pokutu do 10 000 Kč, jde-li o přestupek podle § 25 odst. 10 písm. e) ZoKB.* |




Obrázek 29: Lhůty pro plnění povinností podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti[289]

289: *Lhůty pro plnění povinností podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti.* [online]. [cit. 21. 8. 2018]. Dostupné z: https://nukib.cz/download/kii-vis/Schema_lhuty.pdf




Obrázek 30: Proces určování provozovatelů základních služeb a informačních systémů základních služeb[290]

290: *Proces určování provozovatelů základních služeb a informačních systémů základních služeb.* [online]. [cit. 21. 8. 2018]. Dostupné z: https://nukib.cz/download/kii-vis/Schema_rozhodovani_PZS_v2.1.pdf

**K písm. h)**
**Poskytovatel digitální služby**
K pojmu **Správce informačního systému** viz § 2 písm. e) ZoKB.
K pojmu **Digitální služba** viz § 2 písm. l) ZoKB.

Dle čl. 4 odst. 6 NIS **je poskytovatelem digitálních služeb** „***jakákoli právnická*** *osoba poskytující digitální službu.*" Totožně definuje působnost vůči poskytovateli digitální služby i § 33 odst. 3 ZoKB, kde je uvedeno, že se „*zákon vztahuje* ***pouze na poskytovatele*** *digitální služby,* ***který je právnickou osobou****.*"

**Digitální službou je** (dle NIS i ZoKB) **míněna** služba spočívající v poskytování některé z uvedených služeb:

- on-line tržiště,
- internetový vyhledávač,
- cloud computing.

Vedle pozitivního vymezení poskytovatele digitálních služeb uvádí shodně NIS[291] i ZoKB[292] negativní vymezení, které stanoví, že se tyto předpisy aplikují pouze v případě, že právnická osoba, která digitální službu poskytuje, zároveň není mikropodnikem ani malým podnikem ve smyslu doporučení Komise 2003/361/ES.[293]

Poskytovatelé digitálních služeb by měli zajišťovat bezpečnost sítí a informačních systémů, které používají. Požadavky vztahující se k bezpečnosti a hlášení kybernetických bezpečnostních incidentů by měly pro poskytovatele digitálních služeb platit bez ohledu na to, zda své sítě a informační systémy spravují interně, nebo s pomocí externího dodavatele.[294]

Recitál 57 NIS uvádí, že „***členské státy by neměly určovat poskytovatele digitálních služeb****, neboť tato* ***směrnice by se měla použít na všechny poskytovatele digitálních služeb v oblasti její působnosti.*** *Kromě toho by tato směrnice a prováděcí akty přijaté v souvislosti s ní měly pro poskytovatele digitálních služeb zajišťovat vysokou míru harmonizace, co se týče bezpečnostních požadavků a požadavků na hlášení incidentů.* ***S poskytovateli digitálních služeb v celé Unii by mělo být zacházeno jednotným způsobem a přiměřeně k jejich povaze a míře rizika, kterému by mohli čelit.***"

291: Čl. 4 odst. 6 a 16 odst. 11 NIS

292: § 33 odst. 3 ZoKB

293: Příloha doporučení Komise 2003/361/ES ze dne 6. května 2003 o definici mikropodniků a malých a středních podniků.
Blíže viz také § 33 odst. 3 ZoKB

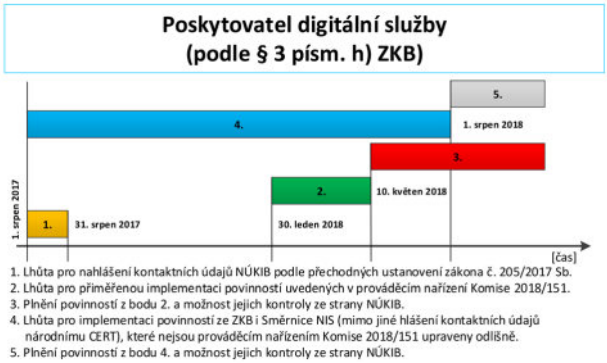
294: Recitál 52 NIS

**Shrnutí aktiv, práv a povinností** dle **ZoKB**:

| | **Poskytovatel digitální služby** [§ 3 písm. h) ZoKB] |
|---|---|
| **Soubor aktiv** | • **digitální služba** [§ 2 písm. l) ZoKB]<br>◦ on-line tržiště<br>◦ internetový vyhledávač<br>◦ cloud computing |
| **Povinnosti, které je třeba vykonávat mandatorně za všech okolností** | • **hlásit kontaktní údaje národnímu CERT**<br>◦ CSIRT.CZ - https://csirt.cz/<br>◦ formulář je dostupný na: https://www.csirt.cz/contactreport/<br>◦ kontaktní údaje podle § 16 je třeba nahlásit nejpozději do 30 dnů ode dne nabytí účinnosti tohoto zákona (tj. do 31. 8. 2017)<br>◦ v případě, že se subjekt stane orgánem nebo osobou uvedenou v § 3 písm. h) ZoKB po výše uvedeném datu, provede nahlášení těchto údajů bezodkladně |
| **Povinnosti, které jsou pro daný orgán nebo osobu z části odlišné** | • **hlásit národnímu CERT (CSIRT.CZ) kybernetické bezpečnostní incidenty**<br>◦ formulář je dostupný na: https://www.csirt.cz/stateincidentreport/<br>◦ e-mailová adresa pro hlášení bezpečnostních incidentů je abuse@csirt.cz<br>◦ je možné využít i telefonický kontakt: +420 910 101 010 (každý pracovní den od 09:00–17:00)<br>◦ v urgentních případech je mimo pracovní dobu možné využít telefonní číslo +420 222 745 111<br>• **implementovat a provádět bezpečnostní opatření**<br>◦ zavést a provádět vhodná a přiměřená bezpečnostní opatření pro sítě elektronických komunikací a informační systémy, které využívá v souvislosti se zajišťováním své služby<br>◦ požadavky na bezpečnostní opatření podle ZoKB jsou obsahem vyhlášky o kybernetické bezpečnosti<br>◦ lhůta pro přiměřenou implementaci povinností uvedených v prováděcím nařízení Komise 2018/151<br>▪ tyto povinnosti musí být splněny do 10. 5. 2018, po tomto datu je možná jejich kontrola ze strany NÚKIB |

| | |
|---|---|
| | ◦ lhůta pro implementaci povinností ze ZoKB i NIS (mimo jiné hlášení kontaktních údajů národnímu CERT)<br>▪ tyto povinnosti musí být splněny nejpozději do 1 roku ode dne nabytí účinnosti tohoto zákona (tj. do 1. 8. 2018), po tomto datu je možná jejich kontrola ze strany NÚKIB<br>• **strpění kontroly ze strany NÚKIB v případě, že je důvodné podezření, že poskytovatel digitální služby neplní povinnosti stanovené tímto zákonem** |
| **Práva a spolupráce** | **Provozovatel národního CERT**<br>• přijímá oznámení kontaktních údajů a tyto údaje eviduje a uchovává [§ 17 odst. 2) písm. a) ZoKB]<br>• přijímá hlášení o kybernetických bezpečnostních incidentech od orgánů a osob a tyto údaje eviduje, uchovává a chrání [§ 17 odst. 2) písm. b) ZoKB]<br>• vyhodnocuje kybernetické bezpečnostní incidenty u orgánů a osob [§ 17 odst. 2) písm. c) ZoKB]<br>• poskytuje orgánům a osobám metodickou podporu, pomoc a součinnost při výskytu kybernetického bezpečnostního incidentu [§ 17 odst. 2) písm. d) ZoKB]<br>• působí jako kontaktní místo pro orgány a osoby [§ 17 odst. 2) písm. e) ZoKB]<br>• provádí hodnocení zranitelností v oblasti kybernetické bezpečnosti [§ 17 odst. 2) písm. f) ZoKB]<br>• předává Úřadu údaje o kybernetických bezpečnostních incidentech ohlášených podle § 8 odst. 3, bez uvedení ohlašovatele [§ 17 odst. 2) písm. g) ZoKB]<br>• předává na vyžádání Úřadu za stavu kybernetického nebezpečí kontaktní údaje orgánů a osob [§ 17 odst. 2) písm. h) ZoKB]<br><br>**Vládní CERT**<br>• přijímá podněty a údaje od orgánů a osob uvedených v § 3 a od jiných orgánů a osob a tyto podněty a údaje vyhodnocuje [§ 20 písm. f) ZoKB]<br>• provádí hodnocení zranitelností v oblasti kybernetické bezpečnosti [§ 20 písm. j) ZoKB]<br><br>**Úřad (NÚKIB)**<br>• vydá varování, dozví-li se o hrozbě v oblasti kybernetické bezpečnosti [§ 12 odst. 1) ZoKB] |

| | |
|---|---|
| | ◦ varování Úřad zveřejní na svých internetových stránkách<br>◦ oznámí je orgánům a osobám uvedeným v § 3 ZoKB<br>◦ je z důvodu ochrany vnitřního pořádku a bezpečnosti, ochrany života a zdraví osob nebo ochrany ekonomiky státu oprávněn po konzultaci s orgánem nebo osobou uvedenými v § 3 písm. c), d), f), g) nebo h), které jsou dotčeny kybernetickým bezpečnostním incidentem, veřejnost o tomto incidentu informovat nebo dotčenému orgánu nebo osobě uložit, aby tak učinil sám |
| **Přestupky** | **§ 25 odst. 11 ZoKB**<br>Poskytovatel digitální služby se dopustí přestupku tím, že<br>a) neustaví svého zástupce podle § 3a odst. 1,<br>b) v rozporu s § 4 odst. 3 nezavede nebo neprovádí bezpečnostní opatření,<br>c) neohlásí kybernetický bezpečnostní incident podle § 8 odst. 2 a 3,<br>d) nesplní povinnost informovat veřejnost uloženou Úřadem podle § 12 odst. 3, nebo<br>e) neoznámí kontaktní údaje nebo jejich změnu podle § 16 odst. 2 písm. a).<br>*Za přestupek lze uložit pokutu do 5 000 000 Kč, jde-li o přestupek podle § 25 odst. 11 písm. b) ZoKB.*<br>*Za přestupek lze uložit pokutu do 1 000 000 Kč, jde-li o přestupek podle § 25 odst. 11 písm. a), c), d) ZoKB.*<br>*Za přestupek lze uložit pokutu do 10 000 Kč, jde-li o přestupek podle § 25 odst. 11 písm. e) ZoKB.* |




Obrázek 31: Lhůty pro plnění povinností podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti[295]

**§ 3a**
**Zástupce poskytovatele digitálních služeb**

**(1) Poskytovatel digitální služby, který poskytuje tuto službu v České republice, nemá sídlo v Evropské unii a neustavil si svého zástupce v jiném členském státě Evropské unie (dále jen „jiný členský stát"), je povinen ustavit si svého zástupce v České republice. Zástupcem poskytovatele digitální služby je osoba, která je usazená v České republice a která je poskytovatelem digitální služby na základě plné moci zmocněná jej zastupovat ve vztahu k povinnostem podle tohoto zákona.**
**(2) V případě, že poskytovatel digitální služby má sídlo mimo Evropskou unii a ustavil si svého zástupce v České republice, má se za to, že je usazen v České republice a vztahují se na něj povinnosti podle tohoto zákona.**
**(3) V případě, že je poskytovatel digitální služby usazen v České republice nebo zde má ustaveného zástupce, ale jím využívané sítě elektronických komunikací a informační systémy se nacházejí v jiném členském státu, Úřad při výkonu státní správy spolupracuje s příslušným orgánem dotčeného členského státu.**

Z důvodové zprávy k novele ZoKB:

*V případě poskytovatelů digitálních služeb může, vzhledem k nehmotné povaze těchto služeb, snadno dojít k tomu, že dotčený podnikatel nemusí být usazen (mít sídlo) v rámci Evropské unie. Směrnice takovou situaci řeší stanovením povinnosti poskytovatele ustavit si v rámci Unie svého zástupce.*

295: *Lhůty pro plnění povinností podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti.* [online]. [cit. 21. 8. 2018]. Dostupné z: https://nukib.cz/download/kii-vis/Schema_lhuty.pdf

*Členský stát Unie, ve kterém je takový zástupce určen, se pak považuje za stát, v němž je poskytovatel digitálních služeb usazen a dopadá na něj tedy regulace příslušného orgánu tohoto členského státu.*

*Směrnice pojem usazení ve svém recitálu 64 vymezuje takto „Usazení předpokládá účinný a skutečný výkon činnosti prostřednictvím stálých struktur. Právní forma takových struktur, ať již jde o pobočku, nebo dceřinou společnost s právní subjektivitou, není v tomto ohledu rozhodující. Uvedené kritérium by nemělo záviset na tom, zda se sítě a informační systémy fyzicky nacházejí na daném místě; sama přítomnost a samotné používání takových sítí a systémů nejsou podstatou primárního usazení, a tudíž ani nejsou kritérii pro jeho určení."*

*Otázkou zaměření služeb na konkrétní členský stát se zaobíral i Soudní dvůr Evropské unie, a to konkrétně ve svých rozhodnutích ve věcech C585/08) a (C144/09). Za účelem určení, zda podnikatel, jehož činnost je prezentována na jeho internetové stránce nebo na internetové stránce jeho zprostředkovatelské společnosti, může být považován za podnikatele „zaměřujícího" činnost na členský stát, na jehož území má spotřebitel své bydliště ve smyslu čl. 15 odst. 1 písm. c) nařízení č. 44/2001, je třeba ověřit, zda před případným uzavřením smlouvy se spotřebitelem z uvedených internetových stránek a celkové činnosti podnikatele vyplývalo, že podnikatel zamýšlel obchodovat se spotřebiteli s bydlištěm v jednom či více členských státech, včetně členského státu, ve kterém má spotřebitel bydliště, v tom smyslu, že byl připraven uzavřít s nimi smlouvu.*

*Následující skutečnosti, jejichž výčet není taxativní, mohou představovat indicie umožňující se domnívat, že činnost podnikatele je zaměřena na členský stát bydliště spotřebitele:*

1) *mezinárodní povaha činnosti,*
2) *popis cesty do sídla podnikatele s počátkem v jiných členských státech,*
3) *použití jiného jazyka nebo jiné měny, než jsou jazyk nebo měna, které jsou obvykle používány v členském státě, ve kterém má podnikatel sídlo s možností provést rezervaci a potvrdit ji v tomto jiném jazyce,*
4) *uvedení telefonického spojení s mezinárodním předčíslím,*
5) *vynaložení nákladů na službu sponzorovaných odkazů na internetu s cílem usnadnit spotřebitelům s bydlištěm v jiných členských státech přístup na stránku podnikatele nebo jeho zprostředkovatele,*
6) *použití jiného jména domény prvního řádu, než je doména členského státu, ve kterém má podnikatel sídlo, a*
7) *uvedení mezinárodní klientely složené ze zákazníků s bydlištěm v jiných členských státech.*

*Naproti tomu pouhá dostupnost internetové stránky podnikatele nebo jeho zprostředkovatelské společnosti v členském státě, na jehož území má spotřebitel bydliště, nepostačuje. Stejně je tomu v případě uvedení elektronické adresy, jakož i dalších kontaktních údajů nebo v případě využití jazyka nebo měny, které jsou obvykle používány v členském státě, ve kterém má podnikatel sídlo.*

*V rozhodnutí ve věci C230/14 Soudní dvůr Evropské unie uvedl, že může soud za účelem určení zaměření služeb na členský stát, zohlednit zejména skutečnost, že činnost správce, v rámci níž k uvedenému zpracování dochází, spočívá v provozování webových stránek s inzeráty na nemovitosti nacházející se na území tohoto členského státu, které jsou v jazyce tohoto státu, a že je tato činnost tedy zaměřena především, nebo dokonce zcela na uvedený členský stát, a dále skutečnost, že tento správce má v uvedeném členském státě zástupce, jehož úkolem je vymáhat pohledávky vyplývající z této činnosti, jakož i zastupovat správce ve správních a soudních řízeních souvisejících se zpracováním předmětných údajů.*

*Směrnice řeší i stav, kdy je poskytovatel digitálních služeb usazen v jednom členském státu Evropské unie (v našem případě tedy v České republice), ale jeho sítě a informační systémy jsou umístěny v jiném členském státu. V takovém případě se zavádí povinnost NBÚ spolupracovat s příslušným úřadem tohoto dotčeného členského státu pro zjištění reálného stavu zajištění bezpečnosti sítí a informačních systémů a řešení případných nedostatků. Tato spolupráce může zahrnovat například výměnu informací mezi příslušnými orgány nebo vyžádání informací potřebných k posouzení bezpečnosti sítí a informačních systémů poskytovatele digitálních služeb, včetně existující bezpečnostní politiky, a v případě zjištění nedostatků uložení povinnosti jejich nápravy.*

*Ustaveným zástupcem musí být vždy osoba, která je usazená v Evropské unii, neboť v případě, že by tomu tak nebylo, ztrácel by institut ustavení zástupce jakýkoliv reálný smysl. Vzhledem k působnosti NBÚ je právní úprava adresována v tomto ustanovení zástupcům usazeným v České republice. Pro větší právní jistotu se stanoví, že zástupce musí být výslovně (doložitelně) pověřen k jednání jménem poskytovatele digitálních služeb.*

**K odst. 1)**
K pojmu **Správce informačního systému** viz § 2 písm. e) ZoKB.
K pojmu **Digitální služba** viz § 2 písm. l) ZoKB.
K pojmu **Poskytovatel digitální služby** viz § 3 písm. g) ZoKB.

Poskytovatelé digitálních služeb mohou své služby nabízet bez ohledu na fyzickou geolokaci svoji nebo uživatele, který tyto služby využívá. Směrnice NIS se snaží zvýšit ochranu kybernetického prostoru a jeho uživatelů mimo jiné i tím, že v případě, že **poskytovatel** digitálních služeb usazený **mimo Unii nabízí služby v rámci Unie**, **měl by ustanovit svého zástupce v některé zemi Unie**. Zástupce musí být doložitelně pověřen k jednání jménem poskytovatele digitálních služeb.

Díky usazení poskytovatele digitálních služeb či jeho zástupce v některé ze zemí Unie by mělo dojít k vyšší garanci vymahatelnosti práva Unie (či členského státu Unie) na poskytovateli.

Ustanovení § 3a odst. 1 ZoKB pak explicitně stanovuje povinnost, spočívající v **ustanovení zástupce poskytovatele digitálních služeb v České republice**, pokud:

- si poskytovatel digitální služby neustavil svého zástupce v jiném členském státě Evropské unie a
- poskytuje digitální službu v České republice.

*„Aby bylo možno určit, zda takový poskytovatel digitálních služeb nabízí služby v rámci Unie, mělo by být ověřeno, zda má dotyčný poskytovatel digitálních služeb zjevně v úmyslu nabízet služby osobám v jednom nebo více členských státech.“* [296]

Pouhý fakt, že je některá z digitálních služeb (on-line tržiště, internetový vyhledávač, cloud computing) poskytovatele digitálních služeb nebo jeho zprostředkovatele v Unii dostupná, k ověření tohoto úmyslu nepostačují.

To, co může napomoci při určení, zda je některá z digitálních služeb nabízena, nebo má být nabízena v Unii, jsou například následující skutečnosti:

- používání jazyka nebo
- měny obecně používaných v jednom nebo více členských státech,
- možnost objednat služby v tomto jiném jazyce,
- zmínka o zákaznících či uživatelích nacházejících se v Unii,
- uvedení telefonického spojení s mezinárodním předčíslím,
- použití jména domény prvního řádu některého ze států Unie,
- vynaložení nákladů na službu sponzorovaných odkazů na Internetu s cílem usnadnit spotřebitelům s bydlištěm v jiných členských státech přístup na stránku podnikatele nebo jeho zprostředkovatele, aj.

Zástupce by měl jednat jménem poskytovatele digitálních služeb a příslušné orgány nebo týmy CERT/CSIRT by měly být oprávněny zástupce kontaktovat. Zástupce by měl být výslovně písemně pověřen poskytovatelem digitálních služeb, aby mohl jednat jeho jménem v otázkách jeho povinností podle této směrnice, včetně hlášení incidentů.[297]

**K odst. 2)**
Pravomoc nad poskytovateli digitálních služeb by měl mít ten členský stát, v němž je daný poskytovatel v rámci Unie primárně **usazen**, **což** v zásadě **odpovídá místu, kde se v Unii nachází jeho sídlo.**

Pojem **usazení** *„předpokládá **účinný a skutečný výkon činnosti prostřednictvím stálých struktur**. Právní forma takových struktur, ať již jde o pobočku, nebo dceřinou společnost s právní subjektivitou, není v tomto ohledu rozhodující. Uvedené kritérium by nemělo záviset na tom, zda se sítě a informační*

296: Recitál 65 NIS
297: Tamtéž

*systémy fyzicky nacházejí na daném místě; sama přítomnost a samotné používání takových sítí a systémů nejsou podstatou primárního usazení, a tudíž ani nejsou kritérii pro jeho určení.“* [298]

**K odst. 3)**
V případě, že je poskytovatel digitálních služeb usazen v jednom členském státu Unie, ale jeho služby či infrastruktura je nabízena ve státě druhém (případně ve více státech), zavádí směrnice NIS i ZoKB povinnost spolupráce mezi příslušnými úřady a bezpečnostními týmy těchto států, za účelem zajištění bezpečnosti sítí a informačních systémů a řešení incidentů.

Poskytovatelé digitálních služeb by dle NIS měli podléhat mírné a reaktivní následné kontrole, odůvodněné povahou jejich služeb a činností.

**Dotčený příslušný orgán by měl** tudíž **jednat pouze v případě, že má k dispozici důkazy**, například přímo od poskytovatele digitálních služeb, od jiného příslušného orgánu, včetně příslušných orgánů jiného členského státu, nebo od uživatele dané služby, **které potvrzují, že některý poskytovatel digitálních služeb nesplňuje požadavky směrnice NIS, a to zejména poté, co již došlo k incidentu.**

Příslušný **orgán by proto neměl mít obecnou povinnost vykonávat** nad poskytovateli digitálních služeb **kontrolu**.[299]

## HLAVA II
## SYSTÉM ZAJIŠTĚNÍ KYBERNETICKÉ BEZPEČNOSTI

### Bezpečnostní opatření
### § 4

**(1) Bezpečnostním opatřením se rozumí souhrn úkonů, jejichž cílem je zajištění bezpečnosti informací v informačních systémech a dostupnosti a spolehlivosti služeb a sítí elektronických komunikací**[300] **v kybernetickém prostoru.**
**(2) Orgány a osoby uvedené v § 3 písm. c) až f) jsou povinny zavést a provádět bezpečnostní opatření v rozsahu nezbytném pro zajištění kybernetické bezpečnosti informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury, informačního systému základní služby a významného informačního systému a vést o nich bezpečnostní dokumentaci.**

298: Recitál 64 NIS

299: Recitál 60 NIS

300: Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů.

**(3) Poskytovatel digitální služby je povinen zavést a provádět vhodná a přiměřená bezpečnostní opatření pro sítě elektronických komunikací a informační systémy, které využívá v souvislosti se zajišťováním své služby, přičemž tato bezpečnostní opatření zohledňují zajištění bezpečnosti informací, zvládání kybernetických bezpečnostních incidentů, řízení kontinuity činností, monitorování, audit, testování a soulad s mezinárodními předpisy.**
**(4) Orgány a osoby uvedené v § 3 písm. c) až f) jsou povinny zohlednit požadavky vyplývající z bezpečnostních opatření při výběru dodavatele pro jejich informační nebo komunikační systém a tyto požadavky zahrnout do smlouvy, kterou s dodavatelem uzavřou. Zohlednění požadavků vyplývajících z bezpečnostních opatření podle věty první v míře nezbytné pro splnění povinností podle tohoto zákona nelze považovat za nezákonné omezení hospodářské soutěže nebo neodůvodněnou překážku hospodářské soutěži.**
**(5) Orgány a osoby uvedené v § 3 písm. c) až g), které jsou orgány veřejné moci, jsou povinny si ve smlouvě s poskytovatelem služeb cloud computingu zejména zajistit, že budou dodržována bezpečnostní pravidla pro poskytování služeb cloud computingu stanovená Úřadem, a že budou mít na základě své žádosti bez zbytečného odkladu k dispozici informace a data, která pro ně poskytovatel služeb cloud computingu uchovává včetně možnosti kontroly uchovávaných informací a dat v reálném čase. Dalšími nezbytnými náležitostmi smlouvy jsou**

- **a) zakotvení povinnosti poskytovatele služeb respektovat bezpečnostní politiku odběratele služeb,**
- **b) stanovení úrovně poskytovaných služeb,**
- **c) systém schvalování subdodavatelů služby cloud computingu,**
- **d) podmínky ukončení smluvního vztahu z pohledu bezpečnosti,**
- **e) řízení kontinuity činností v souvislosti s poskytovanou službou cloud computingu,**
- **f) určení vlastníka uchovávaných dat,**
- **g) dohoda o důvěrnosti smluvního vztahu,**
- **h) stanovení úrovně ochrany dat z pohledu důvěrnosti, dostupnosti a integrity,**
- **i) pravidla zákaznického auditu,**
- **j) stanovení povinnosti poskytovatele služeb informovat odběratele o kybernetických bezpečnostních incidentech souvisejících s plněním smlouvy.**

**(6) Poskytovatel služby cloud computingu a orgány a osoby uvedené v § 3 písm. c) až g), které jsou orgány veřejné moci, si ve smlouvě dále dohodnou způsob a výši úhrady účelně vynaložených nákladů na zavedení bezpečnostních pravidel.**
**(7) Zohlednění požadavků vyplývajících z bezpečnostních pravidel, bezpečnostních opatření a dalších podmínek sjednaných ve smlouvě podle odstavce 5, které jsou nezbytné pro splnění povinností podle tohoto zákona, nelze považovat za nezákonné omezení hospodářské soutěže nebo neodůvodněnou překážku hospodářské soutěži.**

Z důvodové zprávy:

*Návrh ustanovení zakládá povinnost vybraným typům povinných osob zavádět v jimi spravovaných informačních a komunikačních systémech bezpečnostní opatření a vést o tom příslušnou bezpečnostní dokumentaci. Účelem zavedení bezpečnostních opatření je zajištění určité úrovně bezpečnosti informačních a komunikačních systémů. Zavedení standardů má tak zejména preventivní význam, neboť systém, v němž budou příslušná bezpečnostní opatření aplikována, by měl být odolnější vůči kybernetickým útokům a současně by měl být připraven na efektivní zvládání kybernetických bezpečnostních událostí a incidentů.*

*Výběr typů povinných osob podléhajících povinnosti zavést bezpečnostní opatření je veden zákonným principem minimalizace zásahu do autonomie vůle povinných osob. Ze zákona tak plyne povinnost k zabezpečení vlastních informačních a komunikačních systémů jen těm osobám soukromého práva a orgánům veřejné moci, jejichž systémy mají zásadní význam pro kybernetickou bezpečnost České republiky, tj. správcům informačních systémů nebo komunikačních systémů kritické informační infrastruktury a správcům významných informačních systémů.*

Z důvodové zprávy k novele ZoKB:

K § 4 odst. 2
*Čl. 14 odst. 1 a 2 směrnice stanoví, že členské státy zajistí, aby provozovatelé základních služeb přijali vhodná a přiměřená technická a organizační opatření k řízení bezpečnostních rizik, jimž čelí sítě a informační systém, které provozovatelé používají pro výkon své činnosti. Tuto povinnost předkladatel transponuje do ustanovení § 4 odst. 2 zákona tím, že rozšiřuje okruh subjektů, na které se vztahuje povinnost zavést a provádět bezpečnostní opatření a vést o nich bezpečnostní dokumentaci. Vzhledem k tomu, že informační systém základní služby nemusí vždy spravovat, tj. určovat účel zpracování informací a podmínky provozování informačního systému, a provozovat ve smyslu zákona o kybernetické bezpečnosti samotný provozovatel základní služby, adresuje se tato povinnost primárně správcům, potažmo provozovatelům informačního systému ZS. Požadavky na bezpečnostní opatření, jež budou v českém právním řádu začleněna do prováděcí vyhlášky, by dle recitálů směrnice měly být stanoveny přiměřeně k rizikům, aby nebyla uvalena nepřiměřená finanční a administrativní zátěž na provozovatele základních služeb, a to s ohledem na nejnovější technický vývoj a se zachováním principu technologické neutrality.*

K § 4 odst. 3
*V souladu s čl. 16 odst. 1 a 2 směrnice se poskytovateli digitálních služeb ukládá povinnost zavést a provádět vhodná a přiměřená bezpečnostní opatření pro sítě a informační systémy, které využívají v souvislosti s nabízením svých služeb, tak aby byla zajištěna bezpečnost a kontinuální poskytování digitálních služeb. Na rozdíl od provozovatelů základních služeb nebudou poskytovatelé digitálních služeb „svazováni" konkrétními požadavky ze strany státu a bude především na nich, jak zabezpečí*

*kontinuitu poskytování jejich služeb. V souladu s čl. 16 odst. 1 směrnice toto ustanovení vymezuje obecně rozsah a obsah bezpečnostních opatření, jež mají poskytovatelé digitálních služeb přijmout.*

*Směrnice tento přístup podporuje v recitálu 49 „Poskytovatelé digitálních služeb by měli zajišťovat míru bezpečnosti přiměřenou míře rizika, jemuž je vystavena bezpečnost jimi poskytovaných digitálních služeb, a to se zřetelem k významu těchto služeb pro fungování jiných podniků v Unii. Míra rizika, jemuž jsou vystaveni provozovatelé základních služeb, mnohdy nezbytných pro zachování klíčových hospodářských a společenských činností, bývá ovšem v praxi vyšší než v případě poskytovatelů digitálních služeb. Bezpečnostní požadavky na poskytovatele digitálních služeb by tudíž měly být méně náročné. Poskytovatelé digitálních služeb by měli mít i nadále možnost přijímat opatření, jež považují za přiměřená z hlediska řízení rizik, kterým je vystavena bezpečnost jejich sítí a informačních systémů.“*

K § 4 odst. 4

*Navrhovaná úprava reaguje na požadavky z praxe, kdy není zřídkavým jevem, že orgány nebo osoby uvedené v § 3 písm. c) až e) zákona nezahrnou bezpečnostní požadavky pro informační systém kritické informační infrastruktury, komunikační systém kritické informační infrastruktury nebo významný informační systém do smluvních podmínek při uzavírání smlouvy s dodavatelem služeb. Nemusí tak být zajištěna bezpečnost jmenovaných systémů, což se předkladatel snaží napravit tím, že nově ukládá povinnost pod sankcí tyto požadavky do smluvních podmínek začlenit. Tuto povinnost předkladatel vzhledem k systematice zákona a požadavkům směrnice (čl. 14 odst. 1 a 2) ukládá i správci nebo provozovateli informačního systému ZS.*

K § 4 odst. 5

*Proto, aby byl vždy zajištěn přístup k informacím a datům z informačního systému nebo komunikačního systému kritické informační infrastruktury, významného informačního systému a informačního systému základní služby uloženým v cloudu, zavádí se povinnost správce nebo provozovatele takového systému – orgánu veřejné moci začlenit podmínku dostupnosti dat do jeho smlouvy s poskytovatelem služeb cloud computingu. To plně odpovídá recitálu 56, který vysvětluje, že „Tato směrnice by neměla bránit členským státům v přijetí vnitrostátních opatření ukládajících subjektům veřejného sektoru, aby v rámci zakázek, jež na služby cloud computingu zadávají, zajistily uplatnění zvláštních bezpečnostních požadavků. Veškerá takováto vnitrostátní opatření by se měla vztahovat na dotyčný subjekt veřejného sektoru, a nikoli na poskytovatele služeb cloud computingu.“. Požadavku na vyšší míru zabezpečení přitaká i čl. 1 odst. 6 směrnice, jenž umožňuje členským státům přijmout opatření s cílem zabezpečit své základní státní funkce, zejména pokud jde o zajištění národní bezpečnosti, včetně opatření na ochranu informací. Formulace „bez zbytečného odkladu“ odpovídá situaci, kdy po zadání požadavku na přístup k datům nebo jejich kontrolu dojde k jejich zpřístupnění neprodleně a ve velmi blízkém okamžiku.*

*S ohledem na poznatky z praxe, kterými Národní bezpečnostní úřad disponuje, považuje předkladatel za potřebné stanovit zákonem podstatné/nezbytné náležitosti smlouvy, které podle tohoto ustanovení orgány veřejné moci, které jsou povinnými subjekty podle tohoto zákona, uzavírají. To by mělo zajistit zvýšení úrovně těchto smluv a vyšší ochranu dat, která stát uchovává v cloudech. Zároveň považujeme*

*za nutné zdůraznit, že není cílem předkladatele, aby měl orgán veřejné moci přístup k datům spojených s technickým zajištěním provozu cloudu.*

**K odst. 1)**
Pojem **bezpečnostní opatření** je třeba chápat jako **úkony** prováděné v kyberprostoru **směřující k zajištění bezpečnosti** informací v informačních systémech, jakož i dostupnosti a spolehlivosti služeb a sítí elektronických komunikací.
K pojmu **kybernetický prostor** viz kap. 1 Kyberprostor (Cyberspace).
K pojmu **informační systém** viz § 1 ZoKB.
K pojmu **síť elektronických komunikací** viz § 1 ZoKB, § 2 písm. h) ZoEK či čl. 4 odst. 1 písm. a) NIS.

**K odst. 2) a 3)**
**Povinnost zavést a provádět bezpečnostní opatření** není obecně uložena všem orgánům a osobám uvedeným v § 3 ZoKB. Ustanovení § 4 odst. 2 a 3 ZoKB tuto povinnost stanoví pouze orgánům a osobám [viz § 3 písm. c) až f) ZoKB] zajišťujícím:

- informační systém kritické informační infrastruktury,
- komunikační systém kritické informační infrastruktury,
- informační systém základní služby,
- významný informační systém.

Uvedené subjekty jsou povinny zavést a **provádět bezpečnostní opatření** v rozsahu nezbytném pro zajištění kybernetické bezpečnosti **a** současně jsou povinny **vést** o nich **bezpečnostní dokumentaci**.

Nově je zákonem o kybernetické bezpečnosti **uložena povinnost zavést bezpečnostní opatření i poskytovateli digitální služby.**[301] Tento poskytovatel musí **zavést a provádět** vhodná a přiměřená **bezpečnostní opatření pro sítě elektronických komunikací a informační systémy, které využívá v souvislosti se zajišťováním své služby.** Uvedená bezpečnostní opatření zohledňují zajištění bezpečnosti informací, zvládání kybernetických bezpečnostních incidentů, řízení kontinuity činností, monitorování, audit, testování a soulad s mezinárodními předpisy.

*„**Poskytovatelé digitálních služeb by měli zajišťovat míru bezpečnosti přiměřenou míře rizika, jemuž je vystavena bezpečnost jimi poskytovaných digitálních služeb, a to se zřetelem k významu těchto služeb pro fungování jiných podniků v Unii.***

***Bezpečnostní požadavky na poskytovatele digitálních služeb by tudíž měly být méně náročné.***

301: Viz § 4 odst. 3 ZoKB

***Poskytovatelé digitálních služeb by měli mít i nadále možnost přijímat opatření, jež považují za přiměřená z hlediska řízení rizik, kterým je vystavena bezpečnost jejich sítí a informačních systémů.***" [302]

**Omezení povinnosti zavést bezpečnostní opatření** pouze na subjekty uvedené v § 3 písm. c) až f) ZoKB a nově na poskytovatele digitální služby je jednak vyjádřením významnosti uvedených informačních a komunikačních systémů a služeb pro stát samotný (pro zajištění jeho kybernetické bezpečnosti), a jednak respektováním **principu minimalizace státního donucení.** [303]

Právě díky respektování principu minimalizace státního donucení není zasahováno do práv soukromých subjektů ve větší míře, než je nezbytně nutné k naplnění účelu zákona.

**K odst. 4)**
V § 4 odst. 4 ZoKB je znovu zdůrazněn **princip technologické neutrality** spočívající v užití toliko obecných kritérií pro standardní zabezpečení informačních systémů a služeb a sítí elektronických komunikací. Bezpečnostní opatření jsou definována tak, aby mohlo být jejich splnění řešeno za užití různých technologií a postupů.

Subjekty aplikující bezpečnostní opatření, mohou dle vlastního uvážení volit konkrétní způsob zabezpečení jejich informačních struktur, a to včetně volby dodavatelů příslušných bezpečnostních řešení. Nedochází tak k upřednostňování či zvýhodňování konkrétního dodavatele (technologií, aplikací aj.) a ani k narušení standardních tržních mechanismů v oboru bezpečnostních ICT.

Subjekty uvedené v § 3 písm. c) až f) ZoKB jsou však povinny **zohlednit požadavky vyplývající z bezpečnostních opatření** při výběru dodavatele **a** současně **jsou povinny tyto požadavky zahrnout do smlouvy** s dodavatelem.

K pojmům **nezákonné omezení hospodářské soutěže** a **neodůvodněná překážka hospodářské soutěže** viz zákon č. 143/2001 Sb., o ochraně hospodářské soutěže a o změně některých zákonů (zákon o ochraně hospodářské soutěže) a zákon č. 134/2016 Sb., o zadávání veřejných zakázek.

V § 1 zákona č. 143/2001 Sb. je uvedeno, že „*tento zákon upravuje **ochranu hospodářské soutěže** na trhu výrobků a služeb **proti** jejímu **vyloučení, omezení, jinému narušení** nebo ohrožení dohodami soutěžitelů (§ 3 odst. 1), zneužitím dominantního postavení soutěžitelů, spojením soutěžitelů, nebo orgány státní správy při výkonu státní správy, orgány územní samosprávy při výkonu samosprávy a při přeneseném výkonu státní správy a orgány zájmové samosprávy při přeneseném výkonu státní správy (dále jen ‚**orgány veřejné správy**').*"

302: Recitál 49 NIS

303: Viz kap. 4.2 Základní cíle a principy ZoKB

V § 36 odst. 1 zákona č. 134/2016 Sb., o zadávání veřejných zakázek je pak stanoveno, že „***zadávací podmínky nesmí být stanoveny tak, aby*** *určitým dodavatelům* ***bezdůvodně*** *přímo nebo nepřímo* ***zaručovaly konkurenční výhodu nebo vytvářely bezdůvodné překážky hospodářské soutěže.***"

Z ustanovení § 4 odst. 4 věta první ZoKB vyplývá, že **pokud jsou zohledňovány požadavky vyplývající z bezpečnostních opatření při výběru dodavatele** pro informační nebo komunikační systém správce a provozovatele informačního systému kritické informační infrastruktury, správce a provozovatele komunikačního systému kritické informační infrastruktury, správce a provozovatele významného informačního systému, správce a provozovatele informačního systému základní služby **a to v míře nezbytně nutné pro splnění povinností** podle ZoKB **nelze takové zohlednění považovat za nezákonné omezení hospodářské soutěže nebo neodůvodněnou překážku hospodářské soutěži.**

**K odst. 5)**
Zákon č. 205/2014 Sb., který novelizoval zákon o kybernetické bezpečnosti, výrazně modifikoval ustanovení § 4 ZoKB. Konkrétně do něj vložil novou povinnost orgánů a osob uvedených v § 3 písm. c) až g) ZoKB, za podmínky, že jsou orgány veřejné moci.

Těmto osobám je stanoven výčet obligatorních náležitostí, jež musí být smluvně upraveny v případě, že je mezi nimi a poskytovatelem cloud computingu uzavřena smlouva o poskytování této služby.

Mezi tyto náležitosti patří:

- **ustanovení o dodržování bezpečnostních pravidel pro poskytování služeb cloud computingu stanovená Úřadem** (NÚKIB),
- **ustanovení o možnosti disponování s informacemi a daty,** která pro ně poskytovatel služeb cloud computingu uchovává **včetně možnosti kontroly uchovávaných informací a dat v reálném čase a bez zbytečného odkladu**, na základě žádosti orgánů a osob uvedených v § 3 písm. c) až g) ZoKB,
- **zakotvení povinnosti poskytovatele služeb respektovat bezpečnostní politiku odběratele služeb,**
- stanovení úrovně poskytovaných služeb,
- systém schvalování subdodavatelů služby cloud computingu,
- podmínky ukončení smluvního vztahu z pohledu bezpečnosti,
- řízení kontinuity činností v souvislosti s poskytovanou službou cloud computingu,
- určení vlastníka uchovávaných dat,
- dohoda o důvěrnosti smluvního vztahu,
- stanovení úrovně ochrany dat z pohledu důvěrnosti, dostupnosti a integrity,
- pravidla zákaznického auditu,

- stanovení povinnosti poskytovatele služeb informovat odběratele o kybernetických bezpečnostních incidentech souvisejících s plněním smlouvy.

Pojem **bez zbytečného odkladu** odpovídá situaci, kdy po zadání požadavku na přístup k datům nebo jejich kontrolu dojde k jejich zpřístupnění neprodleně a ve velmi blízkém okamžiku.[304]

**K odst. 6 a 7)**
Ustanovení § 4 odst. 6 ZoKB stanoví, že je možné si smluvně dohodnout **způsob a výši úhrady účelně vynaložených nákladů na zavedení bezpečnostních pravidel** při poskytování služby cloud computingu orgánům a osobám uvedeným v § 3 písm. c) až g) ZoKB.

Ustanovení § 4 odst. 7 ZoKB opětovně zdůrazňuje skutečnost uvedenou ve vztahu k jiným službám v § 4 odst. 4 ZoKB. Dle tohoto ustanovení **není možné zohlednění požadavků vyplývajících z bezpečnostních pravidel, bezpečnostních opatření a dalších podmínek sjednaných ve smlouvě o poskytování cloud computingu** [mezi poskytovatelem této služby a orgánem a osobou uvedenou v § 3 písm. c) až g) ZoKB], **které jsou nezbytné pro splnění povinností podle tohoto zákona, považovat za nezákonné** omezení hospodářské soutěže nebo neodůvodněnou překážku hospodářské soutěži.

V případě, že podmínky smluvního vztahu některého z orgánů a osob uvedených v § 3 písm. c) až g) ZoKB s jeho dodavateli nejsou v souladu s požadavky ZoKB nebo jeho prováděcích předpisů, má povinný subjekt povinnost do 1. srpna 2018 uvést podmínky tohoto smluvního vztahu do souladu se ZoKB.

**§ 4a**

**(1) Orgány a osoby, které se staly správci informačních nebo komunikačních systémů kritické informační infrastruktury nebo správci významných informačních systémů, a nejsou provozovateli tohoto systému, jsou povinny neprodleně a prokazatelně informovat provozovatele systému o této skutečnosti a o tom, že se tento provozovatel stal orgánem nebo osobou podle § 3 písm. c), d) nebo e).**
**(2) Orgány a osoby, které se staly správci nebo provozovateli informačních nebo komunikačních systémů kritické informační infrastruktury, jsou povinny neprodleně a prokazatelně informovat subjekt zajišťující síť elektronických komunikací, ke které je jejich předmětný informační nebo komunikační systém kritické informační infrastruktury připojen, o této skutečnosti a o tom, že se tento subjekt stal orgánem nebo osobou podle § 3 písm. b).**

304: Srov. *Důvodová zpráva k návrhu zákona č. 205/2014 Sb.* [online]. [cit. 21. 8. 2018]. Dostupné z: https://apps.odok.cz/veklep-detail?pid=ALBSABVH86O2 s. 45

**(3) Orgány a osoby, které byly podle § 22a určené provozovateli základní služby a nejsou zároveň správci nebo provozovateli svých informačních systémů základní služby, jsou povinny správce nebo provozovatele tohoto informačního systému základní služby neprodleně a prokazatelně informovat o svém určení a o tom, že se dotčený správce nebo provozovatel stal orgánem nebo osobou podle § 3 písm. f).**

Z důvodové zprávy k novele ZoKB:

*Obecně toto ustanovení zakládá povinnosti orgánů nebo osob, které se staly povinnými osobami podle zákona o kybernetické bezpečnosti, a tento fakt má dopad na třetí subjekty, aby tyto subjekty informovaly, tak aby bylo zaručeno, že budou za všech okolností naplňovány požadavky zákona. Způsob informování by měl být ve vlastním zájmu povinných osob prokazatelný.*

*Povinnost informovat se tedy vztahuje na následující*

- *orgány a osoby, které se stanou správcem informačního systému kritické informační infrastruktury nebo komunikačního systému kritické informační infrastruktury nebo významného informačního systému a nejsou provozovateli tohoto systému,*
- *orgány a osoby, které se stanou správcem nebo provozovatelem informačního systému kritické informační infrastruktury nebo komunikačního systému kritické informační infrastruktury, ve vztahu k subjektu zajišťujícímu síť elektronických komunikací, k níž je jejich předmětný informační nebo komunikační systém kritické informační infrastruktury připojen,*
- *subjekt, který Úřad určí jako provozovatele základní služby a který není zároveň správcem nebo provozovatelem svého informačního systému základní služby.*

Ustanovení § 4a ZoKB zavádí **vzájemnou informační povinnost, mezi některými subjekty uvedenými v § 3 ZoKB.** Tato vzájemná informační povinnost je v této monografii již včleněna do tabulky aktiv, práv a povinností jednotlivých subjektů (blíže viz § 3 ZoKB).

Subjekty, kterým je uložena povinnost informovat jiný subjekt o určitých skutečnostech, tak musí učinit **neprodleně** a **prokazatelně**.

Zjednodušeně je možné vzájemnou informační povinnost znázornit v následující tabulce:

| | | |
|---|---|---|
| Orgány a osoby, které jsou **správci informačních nebo komunikačních systémů kritické informační infrastruktury** (v případě, že nejsou provozovateli) | **informují** | **provozovatele** tohoto systému o této skutečnosti a o tom, že se tento provozovatel stal orgánem nebo osobou podle § 3 písm. c), d) nebo e) ZoKB. |
| Orgány a osoby, které jsou **správci významných informačních systémů** (v případě, že nejsou provozovateli) | | **provozovatele** tohoto systému o této skutečnosti a o tom, že se tento provozovatel stal orgánem nebo osobou podle § 3 písm. c), d) nebo e) ZoKB. |
| Orgány a osoby, které se staly **správci nebo provozovateli informačních nebo komunikačních systémů kritické informační infrastruktury** | | **subjekt zajišťující síť elektronických komunikací**, ke které je jejich předmětný informační nebo komunikační systém kritické informační infrastruktury připojen, o této skutečnosti a o tom, že se tento subjekt stal orgánem nebo osobou podle § 3 písm. b) ZoKB. |
| Orgány a osoby, které byly určené **provozovateli základní služby** a nejsou zároveň správci nebo provozovateli svých informačních systémů základní služby | | **správce nebo provozovatele tohoto informačního systému základní služby** o svém určení a o tom, že se dotčený správce nebo provozovatel stal orgánem nebo osobou podle § 3 písm. f) ZoKB. |

Obrázek 32: Vzájemná informační povinnost

**§ 5**

**(1) Bezpečnostními opatřeními jsou**
- **a) organizační opatření a**
- **b) technická opatření.**

**(2) Organizačními opatřeními jsou**
- **a) systém řízení bezpečnosti informací,**
- **b) řízení rizik,**
- **c) bezpečnostní politika,**
- **d) organizační bezpečnost,**
- **e) stanovení bezpečnostních požadavků pro dodavatele,**
- **f) řízení aktiv,**

**g) bezpečnost lidských zdrojů,**
**h) řízení provozu a komunikací kritické informační infrastruktury nebo významného informačního systému,**
**i) řízení přístupu osob ke kritické informační infrastruktuře nebo k významnému informačnímu systému,**
**j) akvizice, vývoj a údržba kritické informační infrastruktury a významných informačních systémů,**
**k) zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů,**
**l) řízení kontinuity činností a**
**m) kontrola a audit kritické informační infrastruktury a významných informačních systémů.**

**(3) Technickými opatřeními jsou**
**a) fyzická bezpečnost,**
**b) nástroj pro ochranu integrity komunikačních sítí,**
**c) nástroj pro ověřování identity uživatelů,**
**d) nástroj pro řízení přístupových oprávnění,**
**e) nástroj pro ochranu před škodlivým kódem,**
**f) nástroj pro zaznamenávání činnosti kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů,**
**g) nástroj pro detekci kybernetických bezpečnostních událostí,**
**h) nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí,**
**i) aplikační bezpečnost,**
**j) kryptografické prostředky,**
**k) nástroj pro zajišťování úrovně dostupnosti informací a**
**l) bezpečnost průmyslových a řídicích systémů.**

Z důvodové zprávy:

*Toto ustanovení podrobněji specifikuje obsah bezpečnostních opatření, k jejichž zavedení mají povinnost správci informačních nebo komunikačních systémů kritické informační infrastruktury a správci významných informačních systémů. Bezpečnostní opatření jsou rozdělena do dvou skupin, a to na organizační opatření a technická opatření. Organizační opatření zahrnují povinnost pořizovat plány a aplikovat řídící, organizační a kontrolní postupy k ošetření procesů souvisejících se zaváděním a provozem informačních a komunikačních systémů spravovaných povinnými osobami. Technická opatření specifikují jednotlivé okruhy technických řešení týkajících se zabezpečení informačních a komunikačních systémů včetně detekce, vyhodnocování a řešení kybernetických bezpečnostních událostí a incidentů. K povinnostem zavést bezpečnostní opatření se váže též povinnost zpracovat jejich bezpečnostní dokumentaci.*

**K odst. 1)**
Ustanovení § 5 ZoKB se zaměřuje na bezpečnostní opatření, která jsou **subjekty** (orgány a osoby) **uvedené v § 3 písm. c) až f) ZoKB** povinny zavést. Poskytovatel digitální služby **[§ 3 písm. h) ZoKB]** je povinen také zavést a provádět vhodná a přiměřená bezpečnostní opatření pro sítě elektronických komunikací a informační systémy, které využívá v souvislosti se zajišťováním své služby. V případě poskytovatele digitální služby tato bezpečnostní opatření zohledňují zajištění bezpečnosti informací, zvládání kybernetických bezpečnostních incidentů, řízení kontinuity činností, monitorování, audit, testování a soulad s mezinárodními předpisy. **Ostatní subjekty** uvedené v § 3 ZoKB **nemají povinnost zavádět bezpečnostní opatření**, na druhou stranu jim však nic nebrání v tom, aby samy a dobrovolně aplikovaly bezpečnostní opatření ve stejném nebo obdobném rozsahu jako subjekty k tomu povinné.

**Zákonný výčet jednotlivých bezpečnostních opatření** uvedený v § 5 ZoKB **je dále konkretizován ve vyhlášce č. 82/2018 Sb.**, o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (**vyhláška o kybernetické bezpečnosti**[305]). Tato vyhláška zapracovává požadavky uvedené ve směrnici NIS a upravuje obsah a strukturu bezpečnostní dokumentace, obsah a rozsah bezpečnostních opatření, typy, kategorie a hodnocení významnosti kybernetických bezpečnostních incidentů, náležitosti a způsob hlášení kybernetického bezpečnostního incidentu, náležitosti oznámení o provedení reaktivního opatření a jeho výsledku, vzor oznámení kontaktních údajů a jeho formu a způsob likvidace dat, provozních údajů, informací a jejich kopií.[306]

V rámci komentáře budou dílčí ustanovení VoKB přiřazena k příslušnému bezpečnostnímu opatření uvedenému v § 5 ZoKB.

Bezpečnostní opatření se dělí na **opatření**:

- **organizační** a
- **technická**.

**Organizační opatření** v sobě zahrnují systém řízení bezpečnosti informací, řízení rizik, bezpečnostní politiku, organizační bezpečnost, stanovení bezpečnostních požadavků pro dodavatele, řízení aktiv, bezpečnost lidských zdrojů, řízení provozu a komunikací kritické informační infrastruktury nebo významného informačního systému, řízení přístupu osob ke kritické informační infrastruktuře nebo k významnému informačnímu systému, akvizici, vývoj a údržbu kritické informační infrastruktury a významných informačních systémů,

305: Vyhláška je dostupná online na:
https://www.zakonyprolidi.cz/cs/2018-82 či https://nukib.cz/download/kii-vis/NovaVKB/VKB_82-2018sb.pdf
306: Viz § 1 VoKB

zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů, řízení kontinuity činností a kontrolu a audit kritické informační infrastruktury a významných informačních systémů.

**Technická opatření** v sobě zahrnují fyzickou bezpečnost, nástroj pro ochranu integrity komunikačních sítí, nástroj pro ověřování identity uživatelů, nástroj pro řízení přístupových oprávnění, nástroj pro ochranu před škodlivým kódem, nástroj pro zaznamenávání činnosti kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů, nástroj pro detekci kybernetických bezpečnostních událostí, nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí, aplikační bezpečnost, kryptografické prostředky, nástroj pro zajišťování úrovně dostupnosti informací a bezpečnost průmyslových a řídicích systémů.

Subjekty (orgány a osoby) uvedené v § 3 písm. c) až f) a h) ZoKB jsou krom bezpečnostních opatření také povinny **zpracovat** jejich **bezpečnostní dokumentaci**.

## Organizační opatření

**K písm. a)**

### Systém řízení bezpečnosti informací

**Systém řízení bezpečnosti informací** (angl. **I**nformation **S**ecurity **M**anagement **S**ystem[307] - **ISMS**) **představuje soubor pravidel**, jejichž cílem je zachovat důvěrnost, integritu a dostupnost[308] informací aplikováním procesu řízení rizik a dát jistotu zainteresovaným stranám, že jsou rizika přiměřeně řízena.[309] V rámci ISMS jsou chráněna aktiva, řízena rizika bezpečnosti informací[310] a již zavedená opatření jsou kontrolována.

Dle § 2 písm. j) VoKB se systémem řízení bezpečnosti informací rozumí ta část systému řízení, která je založená na přístupu k rizikům informačního a komunikačního systému. Tato část systému řízení definuje způsob ustavení, zavádění, provozování, monitorování, přezkoumání, udržování a zlepšování bezpečnosti informací a dat.

I z výše uvedené definice je zřejmé, že **ISMS je součástí procesů a celkového systému řízení organizace a je do těchto systémů integrován**.

307: Dále jen **ISMS**

308: Viz principy kybernetické bezpečnosti – kap. 2.2 Principy kybernetické bezpečnosti, specificky viz kap. 2.2.1 Triáda CIA

309: Srov. úvod ČSN ISO/IEC 27001

310: Viz kap. 2.3 Riziko, aktivum, zranitelnost

ISMS lze aplikovat na organizaci jako celek, jakož i na organizační složku v rámci organizace, či na specificky určený informační a komunikační systém, případně jeho část.

*„ISMS lze zavést a používat v organizaci s deseti pracovníky, a stejně tak i ve velkém holdingu, který může čítat tisíce zaměstnanců. Zjednodušeně lze říci, že ISMS je jen jeden, a to ten, který je popsán v normě ISO/IEC 27001. Interpretace a implementace jednotlivých doporučení se však může výrazně lišit podle rozsahu systému, počtu uživatelů, způsobu zpracování dat, jejich hodnoty a především podle reálných bezpečnostních rizik apod. Strategie ISMS nebývá v malých a středních firmách popsána tak detailně, jako je tomu zvykem ve velkých, zejména nadnárodních organizacích.*

*ISMS se netýká jen průmyslových podniků a privátních organizací, ISMS se týká všech organizací včetně veřejně právních institucí a orgánů státu. Toho důkazem je i existence mnoha národních vládních a resortních usnesení doporučujících anebo vyžadujících implementaci ISMS v organizacích řízených a zřízených státem.“* [311]

Řada norem ISMS má pomoci organizacím všech typů a velikostí zavést a provozovat ISMS. Sestává z následujících mezinárodních norem se společným názvem *Informační technologie – Bezpečnostní techniky*[312] (uvedených dále v číselném pořadí):

- ISO/IEC 27000 *Systémy řízení bezpečnosti informací – Přehled a slovník*
- **ISO/IEC 27001** ***Systémy řízení bezpečnosti informací – Požadavky*** [313]
- ISO/IEC 27002 *Soubor postupů pro opatření bezpečnosti informací*
- ISO/IEC 27003 *Směrnice pro implementaci systému řízení bezpečnosti informací*
- ISO/IEC 27004 *Řízení bezpečnosti informací – Měření*
- ISO/IEC 27005 *Řízení rizik bezpečnosti informací*
- ISO/IEC 27006 *Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací*
- ISO/IEC 27007 *Směrnice pro audit systémů řízení bezpečnosti informací*
- ISO/IEC TR 27008 *Směrnice pro auditory opatření bezpečnosti informací*
- ISO/IEC 27009 *Oborově specifická aplikace ISO/IEC 27001 – Požadavky*
- ISO/IEC 27010 *Řízení bezpečnosti informací pro meziodvětvové komunikace a komunikace mezi organizacemi*
- ISO/IEC 27011 *Směrnice pro řízení bezpečnosti informací pro telekomunikační organizace na základě ISO/IEC 27002*

311: POŽÁR, Josef a Luděk NOVÁK. *Pracovní příručka bezpečnostního manažera.* Praha: AFCEA, 2011. ISBN 978-80-7251-364-2, s. 5 případně: POŽÁR, Josef a Luděk NOVÁK. *Systém řízení informační bezpečnosti.* [online]. [cit. 6. 7. 2018]. Dostupné z: https://www.cybersecurity.cz/data/srib.pdf s. 1

312: Společný název „*Informační technologie – Bezpečnostní techniky*“ označuje, že tyto mezinárodní normy byly vypracovány společnou technickou komisí ISO/IEC JTC 1 *Informační technologie*, subkomisí SC 27 *IT Bezpečnostní techniky*

313: Tato norma je českou verzí mezinárodní normy ISO/IEC 27001:2013

- ISO/IEC 27013 *Pokyn pro integrovanou implementaci ISO/IEC 27001 a ISO/IEC 20000-1*
- ISO/IEC 27014 *Správa a řízení bezpečnosti informací*
- ISO/IEC TR 27015 *Směrnice pro řízení bezpečnosti informací pro finanční služby*
- ISO/IEC TR 27016 *Řízení bezpečnosti informací – Organizační ekonomika*
- ISO/IEC 27017 *Soubor postupů pro opatření bezpečnosti informací pro cloudové služby založený na ISO/IEC 27002*
- ISO/IEC 27018 *Soubor postupů pro ochranu osobně identifikovatelných informací (PII) ve veřejných cloudech vystupujících jako zpracovatelé PII*
- ISO/IEC 27019 *Směrnice pro řízení bezpečnosti informací na základě ISO/IEC 27002 pro systémy řízení procesů specifické pro odvětví energetiky*

Mezinárodní normy, které nejsou uvedeny pod tímto společným názvem, ale jsou také součástí řady norem ISMS, jsou uvedeny dále:

- ISO 27799 *Zdravotnická informatika – Systémy řízení bezpečnosti informací ve zdravotnictví využívající ISO/IEC 2700*15

Řešení ISMS vyžaduje systémový a komplexní přístup, respektující principy a prvky v rámci celého životního cyklu kybernetické bezpečnosti. Systém řízení ISMS je založen na Demingově cyklu, neboli též na **PDCA cyklu** (**P**lan-**D**o-**C**heck-**A**ct; **P**lánuj-**D**ělej-**K**ontroluj-**J**ednej).

PDCA cyklus je jedním ze základních manažerských principů spočívající v postupném zlepšování kvality procesů, služeb, dat, výrobků aj. díky neustálému opakování jeho čtyř základních činností: Plan-Do-Check-Act.

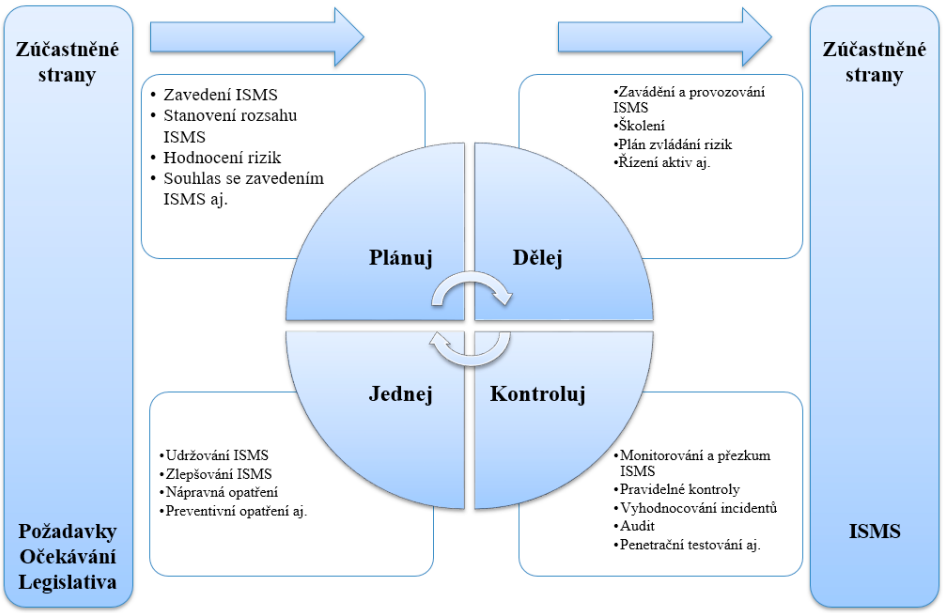
V současné době existuje celá řada variant PDCA cyklu[314], přičemž jednou z vhodných modifikací tohoto cyklu, jež je využitelná i v oblasti kybernetické bezpečnosti, je varianta **OPDCA**, která původní model rozšiřuje o fázi **Observe** (**Pozoruj**/Poznamenej) **předcházející fázi plánování**.

PDCA cyklus, či některé jeho modifikace je možné aplikovat na všechny procesy ISMS. Nejjednodušeji je možné tento model zobrazit jako nikdy nekončící kruh:

314: ROSER, Christoph. *The Many Flavors of the PDCA.* [online]. [cit. 6. 7. 2018]. Dostupné z: https://www.allaboutlean.com/pdca-variants/


Obrázek 33: Model PDCA[315]

Model PDCA byl vyjádřen i v normě ISO/IEC 27001:2005 a znázorňoval, jak ISMS přijímá požadavky bezpečnosti informací a očekávání zainteresovaných stran jako vstup, a jak pomocí nezbytných činností a procesů vytváří výstupy bezpečnosti informací, které splňují tyto požadavky a očekávání.




Obrázek 34: PDCA model aplikovaný na procesy ISMS[316]

315: *PDCA cycle.* [online]. [cit. 6. 7. 2018]. Dostupné z: https://www.creativesafetysupply.com/glossary/pdca-cycle/

316: Upravený a doplněný model PDCA. Původní model byl představen v ISO/IEC 27001:2005 s. 7

| | |
|---|---|
| **Plánuj (ustavení ISMS)** | Ustavení politiky ISMS, cílů, procesů a postupů souvisejících s managementem rizik a zlepšováním bezpečnosti informací tak, aby poskytovaly výsledky v souladu s celkovou politikou a cíli organizace. |
| **Dělej (zavádění a provozování ISMS)** | Zavedení a využívání politiky ISMS, opatření, procesů a postupů. |
| **Kontroluj (monitorování a přezkoumání ISMS)** | Posouzení, kde je to možné, i měření výkonu procesu vůči politice ISMS, cílům a praktickým zkušenostem a hlášení výsledků vedení organizace k přezkoumání. |
| **Jednej (udržování a zlepšování ISMS)** | Přijetí opatření k nápravě a přijetí preventivních opatření, založených na výsledcích interního auditu ISMS a přezkoumání systému řízení ze strany vedení organizace tak, aby bylo dosaženo neustálého zlepšování ISMS. |

Norma ISO/IEC 27001 prosazuje přijetí procesního přístupu pro **ustavení**, **zavádění, provozování**, **monitorování**, **udržování** a **zlepšování ISMS** v organizaci. Důraz je kladen zejména na:

- pochopení požadavků na bezpečnost informací organizace a potřebu stanovení politiky a cílů bezpečnosti informací,
- zavedení a provozování opatření pro management bezpečnosti informací v kontextu s řízením celkových rizik činností organizace,
- monitorování a přezkoumání výkonnosti a účinnosti ISMS,
- neustálé zlepšování založené na objektivním měření.

*„Pro ISMS v rámci organizace musí být jednoznačně popsána organizace řízení, odpovědnost za informační bezpečnost řídících pracovníků všech stupňů, odborných orgánů a rolí v systému bezpečnosti informací.*

*V organizační struktuře organizace musí být informační bezpečnost zohledněna tak, aby pokrývala činnosti a spolupráci vedení, osob odpovědných za aplikační systémy, provozní služby, koncové uživatele a osoby odpovědné za jednotlivé činnosti. Informační bezpečnost předpokládá úzkou spolupráci všech uvedených skupin pracovníků a poskytování školení v oblasti informační bezpečnosti, tak aby kromě osob, které v organizaci odpovídají za informační a další bezpečnost, měli základní znalosti o informační bezpečnosti i pracovníci pracující ve správě informací a všichni uživatelé informační techniky.*“ [317]

317: POŽÁR, Josef a Luděk NOVÁK. *Pracovní příručka bezpečnostního manažera.* Praha: AFCEA, 2011. ISBN 978-80-7251-364-2, s. 7–8 případně: POŽÁR, Josef a Luděk NOVÁK. *Systém řízení informační bezpečnosti.* [online]. [cit. 6. 7. 2018]. Dostupné z: https://www.cybersecurity.cz/data/srib.pdf s. 2

S ohledem na výše uvedené si je možné vydefinovat standardní cíle ISMS v rámci organizace:

- zajištění bezpečnosti informačních a komunikačních systémů a služeb,
- zajištění kontinuity provozu informačních a komunikačních systémů a služeb,
- ochrana dat a informací,
- ochrana dalších aktiv,
- řešení hrozeb, událostí a incidentů včetně prevence,
- zvyšování bezpečnosti informačních a komunikačních systémů a služeb,
- zvyšování obecného podvědomí uživatelů o bezpečnosti a bezpečnostních hrozbách (edukace),
- sdílení zkušeností s dalšími subjekty.

**Zavedení ISMS** v organizaci však **nemůže zajistit naprostou bezpečnost aktiv** organizace. Implementace ISMS však může výrazně snížit rizika zásahu do aktiv na přijatelnou úroveň. Celý systém je tak silný, jak silný je jeho nejslabší článek. V tomto případě je oním nejslabším článkem, a největším nebezpečím pro zabezpečení informací, člověk.

Ustanovení § 3 VoKB stanoví, že povinné osoby v rámci systému řízení bezpečnosti informací:

a) s ohledem na požadavky dotčených stran a organizační bezpečnost **rozsah systému řízení bezpečnosti informací**, ve kterém **určí organizační části a aktiva, jichž se systém** řízení bezpečnosti informací **týká**,

b) **určí cíle** systému řízení bezpečnosti informací,

c) pro stanovený rozsah systému řízení bezpečnosti informací na základě cílů systému řízení bezpečnosti informací, bezpečnostních potřeb a hodnocení rizik **zavedou přiměřená bezpečnostní opatření,**

d) **řídí rizika** podle § 5 VoKB,

e) **vytvoří a schválí bezpečnostní politiku** v oblasti systému řízení bezpečnosti informací, která obsahuje hlavní zásady, cíle, bezpečnostní potřeby, práva a povinnosti ve vztahu k řízení bezpečnosti informací, a na základě bezpečnostních potřeb a výsledků hodnocení rizik stanoví bezpečnostní politiku v dalších oblastech podle § 30 VoKB a **zavedou přiměřená bezpečnostní opatření**,

f) **zajistí provedení auditu kybernetické bezpečnosti** u informačního a komunikačního systému (dále jen „audit kybernetické bezpečnosti“) podle § 16 VoKB,

g) **zajistí pravidelné vyhodnocování účinnosti systému řízení bezpečnosti informací,** které obsahuje hodnocení stavu systému řízení bezpečnosti informací včetně revize hodnocení rizik, posouzení výsledků provedených auditů kybernetické bezpečnosti a dopadů kybernetických bezpečnostních incidentů na systém řízení bezpečnosti informací,

h) **průběžně identifikují a** následně podle § 11 VoKB **řídí významné změny**, které patří do rozsahu systému řízení bezpečnosti informací,

i) **aktualizují systém řízení bezpečnosti informací a příslušnou dokumentaci** na základě zjištění auditů kybernetické bezpečnosti, výsledků vyhodnocení účinnosti systému řízení bezpečnosti informací a v souvislosti s prováděnými významnými změnami a

j) **řídí provoz a zdroje systému řízení bezpečnosti informací a zaznamenávají** činnosti spojené se systémem řízení bezpečnosti informací a řízením rizik.

**K písm. b)**
**Řízení rizik**
K pojmu **riziko** viz kap. 2.3.1.
K pojmu **hrozba** viz kap. 2.4.1.
K pojmu **zranitelnost** viz kap. 2.3.3.

Dle § 2 písm. d) VoKB se **hodnocením rizik** rozumí **celkový proces identifikace, analýzy a vyhodnocení rizik.** Na tento pojem bezprostředně navazuje § 2 písm. i) ZoKB definující **řízení rizik**, jako **činnost zahrnující hodnocení rizik, výběr a zavedení opatření ke zvládání rizik, sdílení informací o riziku a sledování a přezkoumání rizik**.

Ustanovení **§ 5 VoKB** definuje, že subjekty uvedené v § 3 písm. c) až f) a h) ZoKB jsou v rámci systému řízení rizik povinny:

a) **stanovit metodiku pro hodnocení rizik, včetně stanovení kritérií pro akceptovatelnost rizik,**

b) **identifikovat relevantní hrozby a zranitelnosti** s ohledem na aktiva,

V rámci této činnosti musí zejména zvážit kategorie hrozeb a zranitelností.[318]

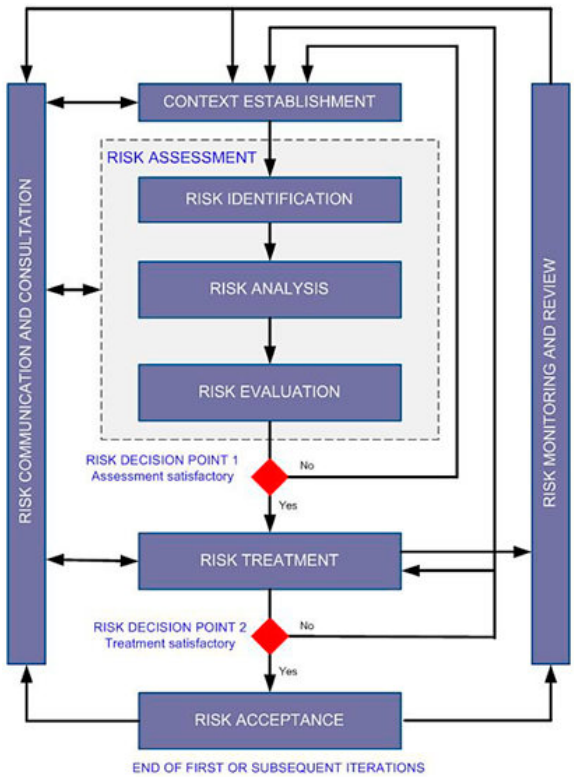
c) **provést hodnocení rizik**,

Hodnocení rizik je prováděno v pravidelných intervalech:

318: Viz příloha č. 3 k VoKB či kap. 2.4.1 Kybernetická hrozba a 2.3.3 Zranitelnost.

- alespoň **1x ročně**, pokud se jedná subjekty uvedené v § 3 písm. c), d) a f) ZoKB:
  - o správce a provozovatele informačního systému kritické informační infrastruktury,
  - správce a provozovatele komunikačního systému kritické informační infrastruktury,
  - správce a provozovatel informačního systému základní služby.
- alespoň **1x za tři roky**, pokud se jedná subjekt uvedené v § 3 písm. e):
  - správce a provozovatel významného informačního systému

Procesu hodnocení rizik se věnuje např. ISO/IEC 27005, kde je tento proces demonstrován.




Obrázek 35: Demonstrace hodnocení rizik v ISMS[319]

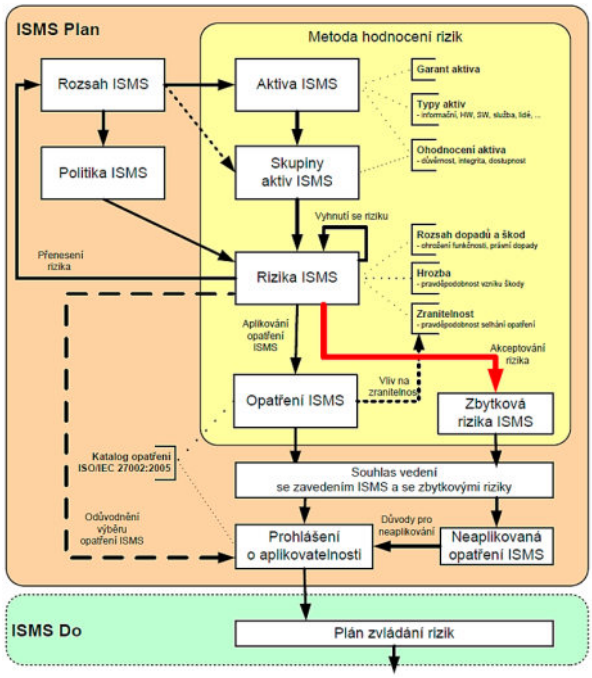
I v rámci procesu hodnocení rizik je třeba respektovat model PDCA, který je však přizpůsoben pro hodnocení rizik.[320]

319: ISO/IEC 27005 s. 8

320: ISO/IEC 27005 s. 9

| ISMS proces | Proces hodnocení rizik v ISMS |
|---|---|
| **Plan** | Vytvoření kontextu<br>Odhad rizika<br>Vypracování plánu zvládání rizika<br>Přijetí rizika |
| **Do** | Implementace plánu zvládání rizika |
| **Check** | Nepřetržité sledování a revize rizik |
| **Act** | Udržování a zlepšování procesu hodnocení a řízení rizik<br>Řídící proces |

Pokud jde o vlastní řízení rizik, pak je možné tento proces graficky znázornit následovně:




Obrázek 36: Řízení rizik v procesu ISMS[321]

321: POŽÁR, Josef a Luděk NOVÁK. *Pracovní příručka bezpečnostního manažera.* Praha: AFCEA, 2011. ISBN 978-80-7251-364-2, s. 12 případně: POŽÁR, Josef a Luděk NOVÁK. *Systém řízení informační bezpečnosti.* [online]. [cit. 6. 7. 2018]. Dostupné z: https://www.cybersecurity.cz/data/srib.pdf s. 5

d) **zohlednit relevantní hrozby a zranitelnosti** v rámci hodnocení rizik a posoudit možné dopady na aktiva,

Rizika jsou hodnocena alespoň v rozsahu přílohy č. 2 k VoKB. Dle této přílohy je třeba při hodnocení rizik **jednoznačně stanovit funkce pro určení rizik.** Toto stanovení funkce je nezbytnou součástí metodiky pro hodnocení rizik podle § 5 VoKB.
**Hodnota rizika je nejčastěji vyjádřena jako funkce, kterou ovlivňuje dopad, hrozba a zranitelnost**. Pro vlastní hodnocení rizika lze dle přílohy č. 2 k VoKB využít například následující funkci:

**Riziko = dopad * hrozba * zranitelnost**

V případě, že povinná osoba využívá metodu pro hodnocení rizik, která nerozlišuje hodnocení hrozby a zranitelnosti, je možné stupnice pro hodnocení hrozeb a zranitelností sloučit. Sloučení stupnic by nemělo vést ke ztrátě schopnosti rozlišení úrovně hrozby a zranitelnosti. Za tímto účelem lze použít například komentář, který zřetelně vyjádří jak úroveň hrozby, tak i úroveň zranitelnosti. Obdobně se postupuje i v případech, kdy povinná osoba používá jiný počet úrovní pro hodnocení dopadů, hrozeb, zranitelností a rizik.[322]

Příloha č. 3 VoKB dále uvádí používané stupnice pro hodnocení hrozeb, zranitelností a rizik.

| **Úroveň** | **Popis** |
|---|---|
| **Nízká** | Hrozba neexistuje nebo je málo pravděpodobná. Předpokládaná realizace hrozby **není častější než jednou za 5 let.** |
| **Střední** | Hrozba je málo pravděpodobná až pravděpodobná. Předpokládaná realizace hrozby je v rozpětí **od 1 roku do 5 let**. |
| **Vysoká** | Hrozba je pravděpodobná až velmi pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od **1 měsíce do 1 roku**. |
| **Kritická** | Hrozba je velmi pravděpodobná až víceméně jistá. Předpokládaná realizace hrozby **je častější než jednou za měsíc**. |

Obrázek 37: Stupnice pro hodnocení hrozeb

322: Viz příloha č. 3 odst. 5 k VoKB

| Úroveň | Popis |
|---|---|
| **Nízká** | **Zranitelnost neexistuje nebo je** zneužití zranitelnosti **málo pravděpodobné**. Jsou zavedena bezpečnostní opatření, která jsou schopna včas detekovat možné zranitelnosti nebo případné pokusy o jejich zneužití. |
| **Střední** | **Zneužití zranitelnosti je málo pravděpodobné až pravděpodobné**.<br>Jsou zavedena bezpečnostní opatření, jejichž účinnost je pravidelně kontrolována.<br>Schopnost bezpečnostních opatření včas detekovat možné zranitelnosti nebo případné pokusy o překonání opatření je omezena.<br>Nejsou známé žádné úspěšné pokusy o překonání bezpečnostních opatření. |
| **Vysoká** | **Zneužití zranitelnosti je pravděpodobné až velmi pravděpodobné**.<br>Bezpečnostní opatření jsou zavedena, ale jejich účinnost nepokrývá všechny potřebné aspekty a není pravidelně kontrolována. Jsou známé dílčí úspěšné pokusy o překonání bezpečnostních opatření. |
| **Kritická** | **Zneužití zranitelnosti je velmi pravděpodobné až víceméně jisté**.<br>Bezpečnostní opatření nejsou realizována nebo je jejich účinnost značně omezena.<br>Neprobíhá kontrola účinnosti bezpečnostních opatření.<br>Jsou známé úspěšné pokusy překonání bezpečnostních opatření. |

Obrázek 38: Stupnice hodnocení zranitelností

| Úroveň | Popis |
|---|---|
| **Nízké** | **Riziko je** považováno za **akceptovatelné**. |
| **Střední** | **Riziko může být sníženo méně náročnými opatřeními** nebo v případě vyšší náročnosti opatření je riziko akceptovatelné. |
| **Vysoké** | **Riziko je dlouhodobě nepřípustné** a musí být zahájeny systematické kroky k jeho odstranění. |
| **Kritické** | **Riziko je nepřípustné** a musí být neprodleně zahájeny kroky k jeho odstranění. |

Obrázek 39: Stupnice pro hodnocení rizik

e) **zpracovat zprávu o hodnocení rizik,**

f) **zpracovat** na základě bezpečnostních potřeb a výsledků hodnocení rizik **prohlášení o aplikovatelnosti,**
Toto prohlášení musí obsahovat přehled bezpečnostních opatření požadovaných vyhláškou o kybernetické bezpečnosti, včetně uvedení toho, která bezpečnostní opatření:
1) **nebyla aplikována** (včetně odůvodnění),
2) **byla aplikována** (včetně způsobu plnění).

g) **zpracovat a zavést plán zvládání rizik,**
Plán zvládání rizik musí obsahovat:
- cíle a přínosy bezpečnostních opatření pro zvládání jednotlivých rizik,
- určení osoby zajišťující prosazování bezpečnostních opatření pro zvládání rizik,
- potřebné finanční, technické, lidské a informační zdroje,
- termín jejich zavedení,
- popis vazeb mezi riziky a příslušnými bezpečnostními opatřeními,
- způsob realizace bezpečnostních opatření.

h) **zohlednit při hodnocení rizik a v plánu,**
1) významné změny,
2) změny rozsahu systému řízení bezpečnosti informací,
3) opatření podle § 11 ZoKB,
1) kybernetické bezpečnostní incidenty, včetně dříve řešených.

i) **zavést bezpečnostní opatření** v souladu s plánem zvládání rizik.

**K písm. c)**

### Bezpečnostní politika

Dle § 2 písm. c) VoKB se **bezpečnostní politikou** rozumí **soubor zásad a pravidel, které určují způsob zajištění ochrany aktiv.**

Ustanovení § 30 VoKB stanoví, že subjekty uvedené v § 3 písm. c) až f) a h) ZoKB jsou povinny:

a) **stanovit bezpečnostní politiku** a **vést bezpečnostní dokumentaci** zahrnující oblasti následující politiky:[323]
- systému řízení bezpečnosti informací,
- řízení aktiv,
- organizační bezpečnosti,
- řízení dodavatelů,

323: Blíže viz příloha č. 5 VoKB

- bezpečnosti lidských zdrojů,
- řízení provozu a komunikací,
- řízení přístupu,
- bezpečného chování uživatelů,
- zálohování a obnovy a dlouhodobého ukládání,
- bezpečného předávání a výměny informací,
- řízení technických zranitelností,
- bezpečného používání mobilních zařízení,
- akvizice, vývoje a údržby,
- ochrany osobních údajů,
- fyzické bezpečnosti,
- bezpečnosti komunikační sítě,
- ochrany před škodlivým kódem,
- nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí,
- bezpečného používání kryptografické ochrany,
- řízení změn,
- zvládání kybernetických bezpečnostních incidentů,
- řízení kontinuity činností.

Dále je stanoven **obsah bezpečnostní dokumentace**, jež musí zahrnovat:

- zprávu z auditu kybernetické bezpečnosti,
- zprávu z přezkoumání systému řízení bezpečnosti informací,
- metodiku pro identifikaci a hodnocení aktiv a pro hodnocení rizik,
- zprávu o hodnocení aktiv a rizik,
- prohlášení o aplikovatelnosti,
- plán zvládání rizik,
- plán rozvoje bezpečnostního povědomí,
- evidenci změn,
- hlášené kontaktní údaje,
- přehled obecně závazných právních předpisů, vnitřních předpisů a jiných předpisů a smluvních závazků,
- další doporučenou dokumentaci (např. topologii infrastruktury, přehled síťových zařízení).

b) **pravidelně přezkoumávat bezpečnostní politiku** a **bezpečnostní dokumentaci,**

c) zajistit, aby byla bezpečnostní politika a bezpečnostní dokumentace aktuální.

**Bezpečnostní politika a bezpečnostní dokumentace musí být:**

- dostupná v listinné nebo elektronické podobě,
- komunikována v rámci povinné osoby,
- přiměřeně dostupná dotčeným stranám,
- řízena,
- chráněna z pohledu důvěrnosti, integrity a dostupnosti,
- vedena tak, aby informace v nich obsažené byly úplné, čitelné, snadno identifikovatelné a snadno vyhledatelné.

**K písm. d)**

## Organizační bezpečnost

Vymezení organizační bezpečnosti a zejména ukotvení kybernetické či ICT bezpečnosti v rámci již fungujících struktur organizace je velmi zásadní pro případné zvládání kybernetických hrozeb či útoků.

Problematika bezpečnosti by měla být v rámci organizaci řešena na operativní, taktické, ale i strategické úrovni z pohledu managementu organizace.

Z pohledu bezpečnosti je významné, aby byl útvar (odbor) kybernetické bezpečnosti oddělen od útvaru (odboru), který zajišťuje provoz ICT.[324]

**Příklad:** *Autor se setkal se správcem sítě, po kterém jeho zaměstnavatel požadoval, aby se stal současně manažerem bezpečnosti. V praxi by to znamenalo, že by si tento správce sám navrhoval směrnice, kterými se má řídit a zároveň by sám kontroloval, zda je dodržuje a jejich dodržování vymáhal. Absurdnost této situace je patrná na první pohled.*

Dle § 6 VoKB spočívá organizační bezpečnost v tom, že subjekty uvedené v § 3 písm. c) až f) a h) ZoKB s ohledem na systém řízení bezpečnosti informací:

- **zajistí stanovení bezpečnostní politiky a cílů ISMS** tak, aby byly slučitelné se strategickým směřováním povinné osoby,
- **zajistí integraci ISMS** do procesů povinné osoby,
- **zajistí dostupnost zdrojů** potřebných **pro ISMS**,
- **informují zaměstnance o významu ISMS** a významu dosažení shody s jeho požadavky se všemi dotčenými stranami,
- **zajistí podporu** k dosažení zamýšlených výstupů **ISMS**,
- **vedou zaměstnance k rozvíjení efektivity ISMS** a podporují je při tomto rozvíjení,
- **prosazují neustálé zlepšování ISMS**,

324: Srov. *Bezpečnostní role a jejich začlenění v organizaci.* [online]. [cit. 21. 8. 2018]. Dostupné z: https://nukib.cz/download/kii-vis/container-nodeid-574/bezpecnostnirolev41.pdf s. 3

- **podporují osoby zastávající bezpečnostní role** při prosazování kybernetické bezpečnosti v oblastech jejich odpovědnosti,
- **zajistí stanovení pravidel pro určení administrátorů** a **osob, které budou zastávat bezpečnostní role**,

  Pojmem **administrátor** se dle § 2 písm. a) VoKB rozumí „*osoba zajišťující správu, provoz, použití, údržbu a bezpečnost technického aktiva.*"

  **Bezpečnostními rolemi** se rozumí:
  - **manažer** kybernetické bezpečnosti,
  - **architekt** kybernetické bezpečnosti,
  - **garant aktiva**,
  - **auditor** kybernetické bezpečnosti.

- **zajistí, aby byla zachována mlčenlivost** administrátorů a osob zastávajících bezpečnostní role,
- **pro osoby zastávající bezpečnostní role zajistí příslušné pravomoci** a zdroje včetně rozpočtových prostředků k naplňování jejich rolí a plnění souvisejících úkolů,
- **zajistí testování plánů kontinuity činností, obnovy a procesů spojených se zvládáním kybernetických bezpečnostních incidentů**.

Subjekty uvedené v § 3 písm. c) až f) a h) ZoKB zajistí založení **výboru pro řízení kybernetické bezpečnosti a určí jeho složení**. Taktéž určí osoby, které budou zastávat bezpečnostní role a vymezí jim jejich práva a povinnosti.

| **Role:** | **Výbor pro řízení kybernetické bezpečnosti** |
|---|---|
| **Klíčové činnosti:** | a) **Odpovědnost za celkové řízení a rozvoj kybernetické bezpečnosti v rámci povinné osoby**.<br>b) **Tvorba rámce kybernetické bezpečnosti**, směrování a zásad kybernetické bezpečnosti povinné osoby (definování strategických cílů a směrování rozvoje v oblasti kybernetické bezpečnosti).<br>c) **Definice rolí a odpovědností** v rámci systému řízení bezpečnosti informací.<br>d) Definice požadavků na podávání zpráv a kontrolu systému řízení bezpečnosti informací.<br>e) Kontrola aktuálního stavu kybernetické bezpečnosti v rámci povinné osoby a zjišťování, zda dochází k naplňování plánovaných cílů. |

| | |
|---|---|
| **Další podmínky:** | a) **Člen výboru pro řízení kybernetické bezpečnosti musí být** alespoň<br>1) **zástupce vrcholového vedení** nebo jím pověřené osoby,<br>2) **manažer kybernetické bezpečnosti**.<br>b) Členové výboru pro řízení kybernetické bezpečnosti se pravidelně scházejí, přičemž průběh a výstupy z jednání jsou uchovávány v listinné nebo elektronické podobě. |

Příloha č. 6 VoKB krom Výboru pro řízení kybernetické bezpečnosti také podrobněji definuje jednotlivé bezpečnostní role.

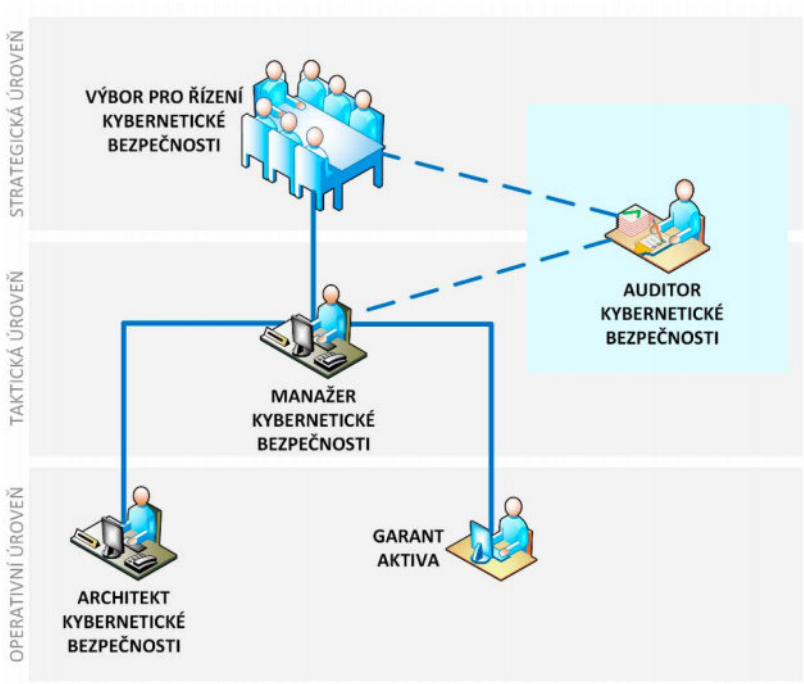
| **Role:** | **Manažer kybernetické bezpečnosti** |
|---|---|
| **Klíčové činnosti:** | a) **Odpovědnost za řízení systému řízení bezpečnosti informací**.<br>b) **Pravidelný reporting** pro vrcholové vedení povinné osoby.<br>c) **Pravidelná komunikace** s vrcholovým vedením povinné osoby.<br>d) Předkládání Zpráv o hodnocení aktiv a rizik, Plánu zvládání rizik a Prohlášení o aplikovatelnosti výboru pro řízení kybernetické bezpečnosti.<br>e) Poskytování pokynů pro zajištění bezpečnosti informací při vytváření, hodnocení, výběru, řízení a ukončení dodavatelských vztahů v oblasti ICT.<br>f) Komunikace s GovCERT/CSIRT.<br>g) Podílení se na procesu řízení rizik.<br>h) Koordinace řízení incidentů.<br>i) Vyhodnocování vhodnosti a účinnosti bezpečnostních opatření. |
| **Znalosti:** | a) Normy řady ISO/IEC 27000 a obdobné normy z oblasti bezpečnosti a ICT.<br>b) Přehled v oblasti ICT (operační systémy, databáze, aplikace, datové sítě) s důrazem na bezpečnost<br>c) Řízení rizik.<br>d) Řízení kontinuity činností.<br>e) Relevantní právní a regulatorní požadavky, zejména zákon.<br>f) Kontext povinné osoby. |
| **Zkušenosti:** | a) Prosazování systému řízení bezpečnosti informací.<br>b) Porozumění definicím rizik a rizikovým scénářům.<br>c) Řízení rizik v rámci povinné osoby.<br>d) Schopnost interpretovat výsledky řízení rizik a koordinovat zvládání rizik. |

| | |
|---|---|
| **Vzdělání a praxe:** | a) **Alespoň 3 roky praxe** v oboru informační nebo kybernetické bezpečnosti, nebo<br>b) absolvování studia na vysoké škole a **alespoň 1 rok praxe** v oboru informační nebo kybernetické bezpečnosti. |
| **Relevantní certifikace*:** | Certified Information Security Manager (CISM), Certified in Risk and Information Systems Control (CRISC), Certified Information Systems Security Professional (CISSP), Manažer BI (akreditační schéma ČIA). |
| **Další podmínky:** | a) Role není slučitelná s rolemi odpovědnými za provoz informačního a komunikačního systému a s dalšími provozními či řídicími rolemi.<br>b) Pro správný výkon této role je zapotřebí zajistit potřebné pravomoci, odpovědnost a rozpočet. |
| | **Architekt kybernetické bezpečnosti** |
| **Klíčové činnosti:** | a) **Odpovědnost za návrh implementace bezpečnostních opatření**.<br>b) **Zajišťování architektury bezpečnosti**. |
| **Znalosti:** | a) Architektura informačních a komunikačních systémů a její navrhování.<br>b) Hardwarové komponenty, nástroje a architektury.<br>c) Operační systémy a software.<br>d) Podnikové procesy a jejich integrace a závislost na ICT.<br>e) Řízení bezpečnosti a rizik.<br>f) Bezpečnost komunikací a sítí.<br>g) Řízení identit a přístupů.<br>h) Hodnocení a testování bezpečnosti.<br>i) Bezpečnost provozu.<br>j) Základní principy bezpečného vývoje softwaru.<br>k) Integrace a závislosti ICT a obchodních procesů. |
| **Zkušenosti:** | a) Navrhování implementace bezpečnostních opatření.<br>b) Navrhování architektury bezpečnosti se zaměřením na cíle a bezpečnost.<br>c) Bezpečnost vývoje softwaru. |
| **Vzdělání a praxe:** | a) Alespoň **3 roky praxe** v oboru informační nebo kybernetické bezpečnosti, nebo<br>b) absolvování studia na vysoké škole a alespoň **1 rok praxe** v oboru informační nebo kybernetické bezpečnosti. |

| | |
|---|---|
| **Relevantní certifikace*:** | Certified Ethical Hacker (CEH), CompTIA Security +, Certified Information Security Manager (CISM), Certified in Risk and Information Systems Control (CRISC), Certified Information Systems Security Professional (CISSP), Manažer BI (akreditační schéma ČIA). |
| **Další podmínky:** | **Role není slučitelná s rolemi odpovědnými za provoz informačních a komunikačních systémů.** |
| | **Auditor kybernetické bezpečnosti** |
| **Klíčové činnosti:** | **Provádění auditu kybernetické bezpečnosti**. |
| **Znalosti:** | a) **Metodologie a rámce auditu** informační bezpečnosti.<br>b) **Procesy a postupy interního auditu**.<br>c) Role a funkce interního auditu.<br>d) Proces provádění auditu ICT bezpečnosti.<br>e) Strategické a taktické řízení ICT.<br>f) Akvizice, vývoj a nasazení ICT.<br>g) Řízení provozu, údržby a služeb ICT.<br>h) Ochrana aktiv.<br>i) Hodnocení kybernetické bezpečnosti, metody testování a vzorkování.<br>j) Relevantní právní předpisy.<br>k) ICT bezpečnost. |
| **Zkušenosti:** | a) Plánování auditů informační nebo kybernetické bezpečnosti.<br>b) Provádění auditů kybernetické bezpečnosti nebo auditů systému řízení bezpečnosti informací.<br>c) Analyzování výsledků auditů.<br>d) Psaní auditních závěrů, jejich prezentace a navrhování doporučení vedoucích k nápravě nálezů.<br>e) Reporting stavu plnění zákonných požadavků.<br>f) Provádění auditů se zaměřením na ICT a informační nebo kybernetickou bezpečnost. |
| **Vzdělání a praxe:** | a) Alespoň **3 roky praxe** v oblasti auditu informační nebo kybernetické bezpečnosti, nebo<br>b) absolvování studia na vysoké škole a alespoň **1 rok praxe** v oblasti auditu informační nebo kybernetické bezpečnosti. |

| | |
|---|---|
| **Relevantní certifikace*:** | Certified Information Systems Auditor (CISA), Certified Internal Auditor (CIA), Certified in Risk and Information Systems Control (CRISC), Lead Auditor Information Security Management Systém (Lead Auditor ISMS), Auditor BI (akreditační schéma ČIA). |
| **Další podmínky:** | a) **Role není slučitelná s rolemi**<br>1) výboru pro řízení kybernetické bezpečnosti,<br>2) manažera kybernetické bezpečnosti,<br>3) architekta kybernetické bezpečnosti,<br>4) garanta aktiva.<br>b) **Role není slučitelná s rolemi odpovědnými za provoz informačních a komunikačních systémů.** |
| | **Garant aktiva** |
| **Klíčové činnosti:** | a) **Odpovědnost za zajištění rozvoje, použití a bezpečnosti aktiva**.<br>b) **Spolupráce s ostatními osobami** zastávajícími bezpečnostní role. |
| **Znalosti:** | a) Dobrá znalost aktiva, jehož je garantem.<br>b) Dobrá znalost interních bezpečnostních politik a metodik (například Metodika pro hodnocení aktiv a rizik). |

Graficky by bylo možné vymezit vztah jednotlivých bezpečnostních rolí dle VoKB a jednotlivých úrovní v organizaci následovně:




Obrázek 40: Hierarchie bezpečnostních rolí[325]

Pro přiřazení a zobrazení (v rámci tabulky) odpovědností jednotlivých osob (bezpečnostních rolí dle VoKB) v rámci organizace je vhodné použít **matici odpovědnosti RACI (matice RACI)**. RACI je akronym z počátečních písmen slov:

| | |
|---|---|
| **R - Responsible** | kdo je odpovědný za vykonání svěřeného úkolu (dané aktivity) |
| **A - Accountable** (či Approver) | kdo je odpovědný za celý úkol, respektive za to, že je daný proces vykonán tak, jak bylo předdefinováno |
| **C - Consulted** | kdo může poskytnout cenou radu či konzultaci k úkolu, avšak nepřebírá odpovědnost za výkon procesu |
| **I - Informed** | kdo má být informován o průběhu úkolu či rozhodnutích v úkolu |

325: *Bezpečnostní role a jejich začlenění v organizaci.* [online]. [cit. 21. 8. 2018]. Dostupné z: https://nukib.cz/download/kii-vis/container-nodeid-574/bezpecnostnirolev41.pdf s. 6

Platí pravidlo, že celkovou odpovědnost (A - Accountability) má k danému úkolu pouze jedna osoba, zapojených lidí (R - Responsibility) by mělo být přiměřeně k danému úkolu. Metoda RACI je jednoduchou formou modelu kompetencí.[326]

| **Procesy:** | **Role:** | **Výbor KB** | **Manažer KB** | **Architekt KB** | **Auditor KB** | **Garant aktiva** |
|---|---|---|---|---|---|---|
| **Celkové řízení a rozvoj KB** | | **A** | **R** | **R** | | **C** |
| **Systém řízení bezpečnosti informací** | | **A** | **R** | **C** | | **C** |
| **Návrh bezpečnostních opatření** | | **C** | **A** | **R** | | **C** |
| **Implementace bezpečnostních opatření** | | **C** | **A** | **R** | | **C** |
| **Zajištění rozvoje, použití a bezpečnostní aktiva** | | | **A** | **C** | | **R** |
| **Audit KB** | | **I** | **C** | **C** | **A/R** | **C** |

Obrázek 41: RACI matice[327]

Subjekty uvedené v § 3 písm. c) až f) a h) ZoKB nemusí určit všechny bezpečnostní role, respektive v některých případech musí určit navíc jejich zastupitelnost. Diferenciace rolí je určena § 6 odst. 4 až 6 VoKB následovně:

326: Blíže viz např. *Matice odpovědnosti RACI (RACI Responsibility Matrix).* [online]. [cit. 21. 8. 2018]. Dostupné z: https://managementmania.com/cs/matice-odpovednosti-raci či *Bezpečnostní role a jejich začlenění v organizaci.* [online]. [cit. 21. 8. 2018]. Dostupné z: https://nukib.cz/download/kii-vis/container-nodeid-574/bezpecnostnirolev41.pdf s. 6

327: RACI matice při popisu základních procesů s pojených s bezpečnostními rolemi. Vztahy jednotlivých bezpečnostních rolí a procesů se v závislosti na dané organizaci mohou lišit. *Bezpečnostní role a jejich začlenění v organizaci.* [online]. [cit. 21. 8. 2018]. Dostupné z: https://nukib.cz/download/kii-vis/container-nodeid-574/bezpecnostnirolev41.pdf s. 7

| Subjekt | Povinné bezpečnostní role | Zajistí zastupitelnost: |
|---|---|---|
| **[§ 3 písm. e) ZoKB]** | • manažer kybernetické bezpečnosti<br>• garant aktiva<br><br>Ostatní bezpečnostní role určí přiměřeně vzhledem k rozsahu a potřebám systému řízení bezpečnosti informací. | • manažera kybernetické bezpečnosti |

**K písm. e)**

**Stanovení bezpečnostních požadavků pro dodavatele**

Další z organizačních opatření spočívá ve stanovení požadavků na dodavatele informačních, komunikačních systémů či služeb. Subjekty uvedené v § 3 písm. c) až f) a h) ZoKB jsou dle § 8 VoKB povinny:

- **stanovit pravidla pro dodavatele, která zohledňují požadavky ISMS**,
- **seznámit** své **dodavatele s těmito pravidly a vyžadovat plnění** těchto pravidel,
- **vést evidenci** svých **významných dodavatelů**,
- prokazatelně písemně **informovat své významné dodavatele o skutečnosti, že jsou vedeni v této evidenci**,
  Pro to, **aby bylo informování prokazatelné**, **musí obsahovat** náležitosti spočívající v identifikaci správce nebo provozovatele, identifikaci informačního a komunikačního systému, identifikaci významného dodavatele, vyrozumění o skutečnosti, že dodavatel je pro správce významným dodavatelem, a popřípadě také o tom, že významný dodavatel je zároveň provozovatelem. Přiložen musí být i obsah pravidel pro dodavatele, která zohledňují požadavky ISMS [viz § 8 odst. 1 písm. a) VoKB].
- **řídit rizika spojená s dodavateli,**
- **zajistit, aby smlouvy** uzavírané s významnými dodavateli **obsahovaly relevantní oblasti uvedené v příloze č. 7 VoKB**,
- pravidelně **přezkoumávat plnění smluv** s významnými dodavateli z hlediska systému řízení bezpečnosti informací.

**U významných dodavatelů** je dále třeba:

- provést hodnocení rizik souvisejících s plněním předmětu výběrového řízení[328] v rámci výběrového řízení a před uzavřením smlouvy,

328: Viz příloha č. 2 VoKB

- stanovit způsoby a úrovně realizace bezpečnostních opatření a určit obsah vzájemné smluvní odpovědnosti za zavedení a kontrolu bezpečnostních opatření v rámci uzavíraných smluvních vztahů,
- provádět pravidelné hodnocení rizik a pravidelnou kontrolu zavedených bezpečnostních opatření u poskytovaných plnění pomocí vlastních zdrojů nebo pomocí třetí strany,
- v reakci na rizika a zjištěné nedostatky zajistit jejich řešení.

**K písm. f)**

### Řízení aktiv

K pojmu **aktivum** viz kap. 2.3.2.
K pojmům **podpůrná** a **primární aktiva** viz § 2 písm. f) a g) VoKB či kap. 2.3.2.

*„V rámci spolehlivého řízení bezpečnosti informací je důležité mít přehled o vazbách a závislostech mezi primárními a podpůrnými aktivy.“* [329]

Subjekty uvedené v § 3 písm. c) až f) a h) ZoKB jsou dle § 4 VoKB povinny:

- **stanovit metodiku pro identifikaci aktiv**,
- stanovit metodiku pro **hodnocení aktiv**,
- **identifikovat a evidovat aktiva**,
- **určit** a evidovat **garanty aktiv**,
- **hodnotit a evidovat primární aktiva** z hlediska důvěrnosti, integrity a dostupnosti a zařadí je do jednotlivých úrovní aktiv,
- **určit a evidovat vazby mezi primárními a podpůrnými aktivy** a hodnotit důsledky závislostí mezi primárními a podpůrnými aktivy,
- **hodnotit podpůrná aktiva** a zohlednit vzájemné závislosti mezi primárními a podpůrnými aktivy,
- stanovit a **zavést pravidla ochrany** nutná pro zabezpečení **jednotlivých úrovní aktiv**,
- stanovit přípustné způsoby používání aktiv a pravidla pro manipulaci s aktivy s ohledem na úroveň aktiv, včetně pravidel pro bezpečné elektronické sdílení a fyzické přenášení aktiv,
- určit způsob likvidace dat, provozních údajů, informací a jejich kopií nebo likvidaci technických nosičů dat s ohledem na úroveň aktiv v souladu s přílohou č. 4 VoKB.

**Při hodnocení významu primárních aktiv je třeba povinně posoudit:**

- rozsah a důležitost osobních údajů, zvláštních kategorií osobních údajů nebo obchodního tajemství,
- rozsah dotčených právních povinností nebo jiných závazků,

329: MAISNER, Martin a Barbora VLACHOVÁ. *Zákon o kybernetické bezpečnosti. Komentář.* Praha: Wolters Kluwer, 2015. s. 85

- rozsah narušení vnitřních řídicích a kontrolních činností,
- poškození veřejných, obchodních nebo ekonomických zájmů a možné finanční ztráty,
- dopady na poskytování důležitých služeb,
- rozsah narušení běžných činností,
- dopady na zachování dobrého jména nebo ochranu dobré pověsti,
- dopady na bezpečnost a zdraví osob,
- dopady na mezinárodní vztahy,
- dopady na uživatele informačního a komunikačního systému.

**K písm. g)**

**Bezpečnost lidských zdrojů**

Subjekty uvedené v § 3 písm. c) až f) a h) ZoKB jsou povinny v rámci ISMS dbát i na bezpečnost lidských zdrojů, jakožto jednoho z aktiv. Jak již bylo uvedeno dříve, člověk bývá zpravidla oním nejslabším článkem v rámci kybernetické bezpečnosti. Z tohoto důvodu je v prováděcím předpise především pamatováno na edukaci uživatelů a nastavení bezpečnostních politik. Vlastní problematika bezpečnosti lidských zdrojů je řešena v § 9 VoKB, podle kterého jsou subjekty uvedené v § 3 písm. c) až f) a h) ZoKB povinny:

- **stanovit plán rozvoje bezpečnostního povědomí** s cílem zajistit odpovídající vzdělávání a zlepšování bezpečnostního povědomí,
  Tento plán obsahuje formu, obsah a rozsah
  - poučení uživatelů, administrátorů, osob zastávajících bezpečnostní role a dodavatelů o jejich povinnostech a o bezpečnostní politice,
  - potřebných teoretických i praktických školení uživatelů, administrátorů a osob zastávajících bezpečnostní role.
- **určit osoby odpovědné** za realizaci jednotlivých činností uvedených v plánu,
- **zajistit poučení** uživatelů, administrátorů, osob zastávajících bezpečnostní role a dodavatelů o jejich povinnostech a o bezpečnostní politice formou vstupních a pravidelných školení,
- **pro osoby zastávající bezpečnostní role zajistit pravidelná odborná školení**,
- zajistit **pravidelné školení** a ověřování bezpečnostního povědomí **zaměstnanců** v souladu s jejich pracovní náplní,
- zajistit **kontrolu dodržování bezpečnostní politiky ze strany uživatelů**, administrátorů a osob zastávajících bezpečnostní role,
- v případě ukončení smluvního vztahu s administrátory a osobami zastávajícími bezpečnostní role **zajistit předání odpovědností**,
- **hodnotit účinnost plánu rozvoje** bezpečnostního povědomí, provedených školení a dalších činností spojených se zlepšováním bezpečnostního povědomí,
- **určit pravidla a postupy pro řešení případů porušení stanovených bezpečnostních pravidel** ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role.

O výše uvedených školeních je povinnost vést přehledy, které obsahují předmět školení a seznam osob, které školení absolvovaly.

**Příklad:** *Protože standardní školení, které uživatelé pouze povinně absolvují, se ukazují jako ne zcela účinná, přistupují některé organizace i k metodám ověřujícím skutečné pochopení informací předaných ve vlastním školení. Může jít například o rozeslání phishingových zpráv uživatelů po školení zaměřeném právě na tuto oblast. Organizace následně sleduje, kolik uživatelů na útok chybně reagovalo. Je však třeba upozornit, že takovéto testy musí být dobře promyšleny a při jejich plánování by neměl chybět právník, který posoudí, zda použitý test nebude například přílišným zásahem do soukromí zaměstnanců.*

**K písm. h)**

### Řízení provozu a komunikací kritické informační infrastruktury nebo významného informačního systému

Povinné subjekty musí dle § 10 VoKB stanovit provozní pravidla a postupy, které obsahují zejména:

- **práva a povinnosti** administrátorů, uživatelů a osob zastávajících bezpečnostní role,
- **postupy pro spuštění a ukončení chodu systému**, pro restart nebo obnovení chodu systému po selhání a pro ošetření chybových stavů nebo mimořádných jevů,
- **postupy pro sledování kybernetických bezpečnostních událostí** a opatření pro ochranu přístupu k záznamům o těchto událostech,
- **pravidla a postupy pro ochranu před škodlivým kódem**,
- řízení technických zranitelností,
- **spojení na kontaktní osoby**, které jsou pověřeny výkonem systémové a technické podpory,
- postupy řízení a schvalování provozních změn,
- postupy pro sledování, plánování a řízení kapacity lidských a technických zdrojů,
- pravidla a postupy pro ochranu informací a dat v průběhu celého životního cyklu,
- **pravidla a postupy pro instalaci technických aktiv**,
- provádění pravidelného zálohování a kontroly použitelnosti provedených záloh,
- pravidla a postupy pro zajištění bezpečnosti síťových služeb.

Povinná osoba též zajistí oddělení vývojového, testovacího a provozního prostředí.

**K písm. i)**

### Řízení přístupu osob ke kritické informační infrastruktuře nebo k významnému informačnímu systému

Řízení přístupu je jedním ze základních principů budování kybernetické bezpečnosti. Byť je tato povinnost ve VoKB primárně směřována pouze na osoby mající přístup ke kritické informační, komunikační infrastruktuře či významnému informačnímu systému, jsme přesvědčeni, že níže

uvedené principy by měly být respektovány jak v každé organizaci, tak uživateli samotnými. Povinné subjekty musí dle § 10 VoKB:

- **řídit přístup na základě skupin a rolí,**
- **přidělit každému uživateli** a administrátorovi přistupujícímu k informačnímu a komunikačnímu systému **přístupová práva a oprávnění a jedinečný identifikátor**,
- **řídit identifikátory, přístupová práva a oprávnění** aplikací a technických účtů,
- **zavádět bezpečnostní opatření pro řízení přístupu** zařízení k prostředkům informačního a komunikačního systému,
- **zavádět bezpečnostní opatření** potřebná **pro bezpečné používání mobilních zařízení** a jiných technických zařízení, popřípadě i bezpečnostní opatření spojená s využitím technických zařízení, která povinná osoba nemá ve své správě,
- **omezit přidělování privilegovaných oprávnění na úroveň nezbytně nutnou** k výkonu náplně práce,
- **omezit a kontrolovat používání programových prostředků, které mohou být schopné překonat systémové nebo aplikační kontroly**,
- **přidělovat a odebírat přístupová oprávnění** v souladu s politikou řízení přístupu,
- **provádět pravidelné přezkoumání nastavení** veškerých přístupových oprávnění včetně rozdělení do přístupových skupin a rolí,
- **využívat nástroj pro správu a ověřování identity a** nástroj pro řízení **přístupových oprávnění**,
- **prosazovat, aby uživatelé** při používání privátních autentizačních informací **dodržovali stanovené postupy**,
- **zajistit odebrání nebo změnu přístupových oprávnění při změně pozice nebo zařazení uživatelů**, administrátorů nebo osob zastávajících bezpečnostní role,
- **zajistit odebrání nebo změnu přístupových oprávnění při ukončení** nebo změně **smluvního vztahu**,
- **dokumentovat přidělování a odebírání přístupových oprávnění**.

**K písm. j)**

## Akvizice, vývoj a údržba kritické informační infrastruktury a významných informačních systémů

„*Informační nebo komunikační systém nemůže zůstat neměnný, ale musí se neustále rozvíjet a přizpůsobovat novým požadavkům. Jakákoliv změna však může představovat potencionální riziko z hlediska kybernetické bezpečnosti.*“ [330]

330: MAISNER, Martin a Barbora VLACHOVÁ. *Zákon o kybernetické bezpečnosti. Komentář.* Praha: Wolters Kluwer, 2015. s. 85

Správce a provozovatel kritické informační infrastruktury a významných informačních systémů je v souvislosti s plánovanou akvizicí, vývojem a údržbou informačního a komunikačního systému povinen dle § 13 VoKB:

- **řídit rizika** (§ 5 VoKB),
- **řídit významné změny** (§ 11 VoKB),
- **stanovit bezpečnostní požadavky**,
- **zahrnout bezpečnostní požadavky do projektu akvizice, vývoje a údržby**,
- zajistit bezpečnost vývojového a testovacího prostředí a zajistí ochranu používaných testovacích dat,
- **provádět bezpečnostní testování** významných změn před jejich zavedením do provozu,
- plnit požadavek spočívající v ověřování uživatelů, administrátorů a aplikací pomocí více faktorové autentizace, je-li cílem provedení akvizice nebo vývoje nástroj pro správu a ověřování identity.

**K písm. k)**

### Zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů,

K pojmu **kybernetická bezpečnostní událost** viz kap. 2.4.2.
K pojmu **kybernetický bezpečnostní incident** viz kap. 2.4.3.

Subjekty uvedené v § 3 písm. c) až f) a h) ZoKB jsou dle § 14 VoKB v rámci zvládání kybernetických bezpečnostních událostí a incidentů povinny:

- **zavést proces detekce a vyhodnocování kybernetických bezpečnostních událostí** a zvládání kybernetických bezpečnostních incidentů,
- **přidělit odpovědnosti a stanovit postupy pro,**
  - **detekci** a vyhodnocování kybernetických bezpečnostních událostí a incidentů,
  - **koordinaci a zvládání kybernetických bezpečnostních incidentů.**
- **definovat a aplikovat postupy pro** identifikaci, **sběr, získání a uchování** věrohodných **podkladů potřebných pro analýzu kybernetického bezpečnostního incidentu**,
- **zajistit detekci kybernetických bezpečnostních událostí**,
- při detekci kybernetických bezpečnostních událostí se dále řídí § 22 a 23 VoKB,
- **zajistit, že uživatelé**, administrátoři, osoby zastávající bezpečnostní role, další zaměstnanci a dodavatelé **budou oznamovat neobvyklé chování informačního a komunikačního systému a podezření na jakékoliv zranitelnosti**,
- **zajistit posuzování kybernetických bezpečnostních událostí**, při kterém musí být rozhodnuto, zda mají být klasifikovány jako kybernetické bezpečnostní incidenty podle § 31 VoKB,
- zajistit zvládání kybernetických bezpečnostních incidentů podle stanovených postupů,

- přijmout opatření pro odvrácení a zmírnění dopadu kybernetického bezpečnostního incidentu,
- **hlásit kybernetické bezpečnostní incidenty** podle § 32 VoKB,
- **vést záznamy o kybernetických bezpečnostních incidentech** a o jejich zvládání,
- **prošetřit a určit příčiny** kybernetického bezpečnostního **incidentu**,
- **vyhodnotit účinnost řešení kybernetického bezpečnostního incidentu** a na základě vyhodnocení stanovit nutná bezpečnostní opatření, popřípadě aktualizovat stávající bezpečnostní opatření k zamezení opakování řešeného kybernetického bezpečnostního incidentu.

**Povinná osoba** uvedená v § 3 písm. c), d) a f) ZoKB při detekci kybernetických bezpečnostních událostí **musí používat nástroj pro sběr a nepřetržité vyhodnocení kybernetických bezpečnostních událostí** (viz § 24 VoKB).

**K písm. l)**

**Řízení kontinuity činností**

Řízení kontinuity činností (**B**usiness **C**ontinuity **M**anagement - **BCM**) představuje proces spočívající identifikaci klíčových prvků (systémů a procesů) v organizaci a následném nastavení procesů a postupů umožňujících zajištění kontinuity či obnovy těchto prvků, na předem definované úrovni, na které bude ještě možno plnit základní úlohy organizace.

V případě řízení kontinuity činností je třeba provést hodnocení rizik a analýzu stávajících informačních a komunikačních systémů a služeb a na základě takto získaných dat stanovit:

- **minimální úroveň poskytovaných služeb**, která je přijatelná pro užívání, provoz a správu informačního a komunikačního systému,
- **dobu obnovení chodu**, během které bude po kybernetickém bezpečnostním incidentu obnovena minimální úroveň poskytovaných služeb informačního a komunikačního systému,
- **bod obnovení dat** jako časové období, za které musí být zpětně obnovena data po kybernetickém bezpečnostním incidentu nebo po selhání.

Povinná osoba dále v rámci řízení kontinuity činností:

- **stanoví práva a povinnosti** administrátorů a **osob** zastávajících bezpečnostní role,
- pomocí hodnocení rizik a analýzy dopadů vyhodnotí a **dokumentuje možné dopady kybernetických bezpečnostních incidentů a posoudí možná rizika** související s ohrožením kontinuity činností,
- **stanoví politiku řízení kontinuity činností**,
- **vypracuje, aktualizuje a pravidelně testuje plány kontinuity činností a havarijní plány** související s provozováním informačního a komunikačního systému a souvisejících služeb,

- **realizuje opatření pro zvýšení odolnosti informačního a komunikačního systému** vůči kybernetickým bezpečnostním incidentům a omezením dostupnosti.

**K písm. m)**
**Kontrola a audit kritické informační infrastruktury a významných informačních systémů**
Subjekty uvedené v § 3 písm. c) až f) a h) ZoKB jsou dle § 16 VoKB povinny:

- **provádět a dokumentovat audit dodržování bezpečnostní politiky**, včetně přezkoumání technické shody,
- **výsledky auditu zohlednit v plánu** rozvoje bezpečnostního povědomí a plánu zvládání rizik,
- **posoudit soulad bezpečnostních opatření s nejlepší praxí**, právními předpisy, vnitřními předpisy, jinými předpisy a smluvními závazky vztahujícími se k informačnímu a komunikačnímu systému a určit případná nápravná opatření pro zajištění souladu.

Audit je prováděn auditorem kybernetické bezpečnosti (viz § 7 odst. 4 VoKB) při významných změnách (v rámci jejich rozsahu), **v pravidelných intervalech alespoň po 3 letech** [v případě osoby uvedené v § 3 písm. e) ZoKB] a **alespoň po 2 letech** [v případě ostatních povinných subjektů].

Audit je v odůvodněných případech možné provádět průběžně po systematických celcích. V takovém případě je nutno audit v celém rozsahu provést nejpozději do 5 let.

Auditor kybernetické bezpečnosti v rámci auditu nezávisle hodnotí správnost a účinnost zavedených bezpečnostních opatření.

## Technická opatření

Technická opatření spolu s opatřeními organizačními představují základní prvky bezpečnostních opatření. Zatímco organizační opatření jsou primárně zaměřena na nastavení pravidel a politik v organizaci, technická opatření se primárně věnují pravidlům pro nastavení informačních a komunikačních systémů a služeb.

V rámci jednotlivých technických opatření budou demonstrovány i možné open source nástroje aplikovatelné pro dané opatření. Kodet uvádí, že *„ačkoli teoreticky lze vyhovět všem požadavkům ZoKB na technická opatření pomocí open source nástrojů, je nutné jejich nasazení uvážit ze všech hledisek, zejména na základě analýz rizik a nákladů spojených s jejich vlastnictvím.*

*Často se totiž zapomíná na to, že open source software sám osobě sice lze získat zdarma, ale komerční podpora k němu již bezplatná nebývá. Stejně jako ke komerčním produktům je možné k nim někdy přikoupit podporu na bázi SLA, ale není to pravidlem.*

*Pokud není komerční podpora k dispozici, je organizace odkázána na podporu na komunitní bázi, případně na schopnosti administrátora těchto nástrojů.*

***Při náležité úrovni znalostí administrátorů však není třeba se open source řešení obávat**, nicméně náklady na vyškolení administrátora též přispívají k navýšení celkových nákladů na vlastnictví.*“ [331]

**K písm. a)**

## Fyzická bezpečnost

Fyzická bezpečnost je primárně zaměřena na ochranu technických aktiv daného subjektu. Maisner k fyzické bezpečnosti uvádí, že „*cílem tohoto opatření je především zamezení přístupu nepovolaných osob k jednotlivým prvkům infrastruktury, do serveroven, pracovišť správců systému apod. Snahou je vyloučit zcizení majetku přímo i nepřímo souvisejícího s informačním systémem, případně zamezit poškození hmotného i nehmotného vybavení nebo vybavení prostor. V neposlední řadě se snaží zamezit úniku informací a dat.*“ [332]

Takto široké vymezení však spíše odpovídá cílům technických opatření dle § 5 odst. 3 ZoKB a § 17 a násl. VoKB.

Dle § 17 VoKB musí povinná osoba v rámci fyzické bezpečnosti

- **předcházet poškození**, krádeži nebo zneužití aktiv nebo přerušení poskytování služeb informačního a komunikačního systému,
- stanovit **fyzický bezpečnostní perimetr** ohraničující oblast, ve které jsou uchovávány a zpracovávány informace a umístěna technická aktiva informačního a komunikačního systému,
- **uplatnit** u fyzického perimetru **prostředky fyzické bezpečnosti:**
  - **k zamezení neoprávněnému vstupu,**
  - **k zamezení poškození a neoprávněným zásahům,**
  - **pro zajištění ochrany na úrovni objektů a v rámci objektů.**

Pojem předcházení poškození zdůrazňuje generální prevenční povinnost[333] stanovenou mimo jiné v občanském zákoníku.

---

331: KODET, Jaroslav. *Kybernetický zákon: Využijte naplno open source nástroje.* [online]. [cit. 25. 4. 2018]. Dostupné z: https://www.nic.cz/files/nic/doc/Securityworld_CSIRTCZ_112015.pdf

332: MAISNER, Martin a Barbora VLACHOVÁ. *Zákon o kybernetické bezpečnosti. Komentář.* Praha: Wolters Kluwer, 2015. 91

333: Blíže viz kap. 3.3.3.3 Náhrada škody a § 2900 OZ

Při definování pojmů perimetr a prostředky fyzické bezpečnosti je vhodné mimo jiné využít např. i vyhlášku č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů.[334]

Pojem fyzický **bezpečnostní perimetr** vymezuje určený prostor, respektive hranice tohoto prostoru. Oním prostorem může být například soubor objektů, objekt samotný či část objektu.

**Objektem** se rozumí budova nebo jiný ohraničený prostor. **Hranicí objektu** se rozumí plášť budovy, fyzická bariéra (oplocení) nebo jinak viditelně vymezená hranice oblasti. **Zabezpečenou oblastí** se rozumí stavebně nebo jinak viditelně ohraničený prostor v objektu.[335]

**Prostředky fyzické bezpečnosti** jsou příkladmo uvedeny v § 3 až 10 vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů. Jedná se o:

- **mechanické zábranné prostředky** (např. zámky, dveře, mříže, folie, skla a další bezpečnostní konstrukční a stavební prvky, skříňové trezory, trezorové dveře a komorové trezory,
- **systém kontroly vstupu do zabezpečené oblasti** [poplachové a elektronické bezpečnostní systémy, detektory (pohybu, tříštění skla aj.) stanovení podmínek pro vstup: identifikační prvek, PIN, biometrie (případně jejich kombinace)],
- **zařízení elektrické zabezpečovací signalizace** (poplachové zabezpečovací a tísňové systémy – ústředny elektrické zabezpečovací signalizace, detektory elektrické zabezpečovací signalizace, otřesové detektory, perimetrické detekční systémy, tísňové systémy aj.),
- **speciální televizní systémy (kamerové systémy,** CCTV sledovací systémy aj.),
- **zařízení elektrické požární signalizace** (napojení do ústředny elektrické požární signalizace, nebo do ústředny elektrické zabezpečovací signalizace,
- **prostředky omezující působení požárů a živelných událostí** (poplachové systémy, detektory kouře, samočinné hasící systémy aj.,
- **zařízení pro zajištění ochrany před selháním dodávky elektrického napájení** (záložní zdroje – UPS, diesel agregáty aj.).

334: [online]. Dostupné z:
https://www.nbu.cz/cs/pravni-predpisy/provadeci-pravni-predpisy/1087-vyhlaska-c-5282005/

335: Viz § 2 písm. a) až c) vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů

Dále lze implementovat například i:

- **zařízeními proti pasivnímu a aktivnímu odposlechu.**[336]

Do prostor, u kterých by z pohledu bezpečnosti informačních a komunikačních systémů měl být omezen, resp. regulován vstup, patří zejména **serverovny** (primární, záložní)**, prostory se síťovými prvky** (router, switch aj.), **úložiště dat** (kartotéky, NAS úložiště aj.), **prostory administrátorů ICT** aj.

**Příklad:** *Fyzická bezpečnost je jednou z oblastí, kde typicky dochází k porušování organizačních pravidel a kde je potřeba provádět periodické audity. Zatímco většinu ostatních činností vykonávají v organizaci administrátoři, správa fyzických přístupů bývá po samotné implementaci zabezpečení svěřena, například z důvodů úspor, méně kvalifikované pracovní síle, která navíc nemusí mít takové povědomí o vlastní problematice bezpečnosti.*

*Autor zažil několik situací, kdy po určité době začala osoba odpovědná za řízení fyzických přístupů udělovat oprávnění ke vstupům osobám, které do daných oblastí (např. serverovny) neměly mít přístup, například jen proto, že o přístup do chráněné oblasti požádal nadřízený manažer, který však k udělení souhlasu neměl dostatečná oprávnění.*

V rámci fyzické bezpečnosti je možné využít i nástroje open source. Zejména půjde o případy *„realizace pultů centrální ochrany včetně kamerových přehledových systémů. Pro tento účel lze využít nástroje určené pro dohled síťových prvků (**Icinga**, **Nagios** a další), doplněné o rozhraní pro odpovídající čidla, propojené s pro gramy pro přenos a zachycení obrazového signálu z bezpečnostních kamer.“*[337]

336: Proti pasivnímu a aktivnímu odposlechu musí být oblast zajištěna dostatečně zvukotěsnými stěnami, dveřmi, podlahou a stropem, okna, větrací otvory nebo prostupy klimatizace musí být chráněny technickými prostředky. Oblast musí být chráněna proti odezírání z míst nacházejících se vně jednací oblasti. Do oblasti nesmí být umístěn jakýkoliv nábytek nebo jakékoliv zařízení, pokud neprošly kontrolou, zda v jednací oblasti nedochází k nedovolenému použití technických prostředků určených k získávání informací. Nábytek a zařízení oblasti musí být evidováno (včetně typu, případně sériového a inventárního čísla), včetně historie pohybu. Umísťovat telefonní přístroje v oblasti není žádoucí. Pokud je jejich instalace bezpodmínečně nutná, musí být vybaveny odpojovačem nebo odpojovány ručně před jednáním. Do oblasti nelze vnášet mobilní telefony, jakákoliv nahrávací zařízení, vysílací zařízení, jakákoliv testovací, měřící a diagnostická zařízení a další elektronická zařízení (toto neplatí v případě, že jde o zařízení používané v rámci prováděné prohlídky s vědomím odpovědné osoby nebo jí pověřené osoby. Pro oblast musí být zpracována pravidla pro evidenci a pohyb osob a zařízení.

337: KODET, Jaroslav. *Kybernetický zákon: Využijte naplno open source nástroje.* [online]. [cit. 25. 4. 2018]. Dostupné z: https://www.nic.cz/files/nic/doc/Securityworld_CSIRTCZ_112015.pdf

**K písm. b)**
**Nástroj pro ochranu integrity komunikačních sítí**

Dle § 17 VoKB musí správce a provozovatel informačního systému kritické informační infrastruktury v rámci fyzické bezpečnosti

- **zajistit segmentaci** komunikační **sítě**,
- zajistit řízení komunikace v rámci komunikační sítě a perimetru komunikační sítě (tj. **řídit bezpečný přístup mezi vnitřní a vnější sítí**),
- **pomocí kryptografie zajistit důvěrnost a integritu dat při vzdáleném přístupu**, vzdálené **správě nebo při přístupu do** komunikační **sítě pomocí bezdrátových technologií** (tj. zajistit pomocí kryptografie například VPN, připojování ICT na Wi-Fi aj.),
- **aktivně blokovat nežádoucí komunikaci** (např. spam filtry aj.),
- pro zajištění segmentace sítě a pro řízení komunikace mezi jejími segmenty využívat nástroj, který zajistí ochranu integrity komunikační sítě.

„*Nástrojem pro ochranu integrity komunikačních sítí se tady rozumí* ***vhodně navržená topologie sítě*** *včetně použití síťových prvků umožňujících požadovanou segmentaci sítě a filtraci provozu mezi jednotlivými prvky. Použitá zařízení pro dosažení těchto požadavků představují ethernetové switche, routery a firewally. Pokud nelze zajistit segmentaci sítě pomocí VLAN na upravovatelném přepínači, je možné ji zabezpečit prostřednictvím několika menších nemanagovatelných switchů, z nich každý realizuje jednu fyzickou LAN.*

*Při segmmentaci některých sítí je možné využít např. i routery Turris (https://www.turris.cz/cs/), kde je garantována vysoká bezpečnost (mj. díky firmwaru, který byl navržen s ohledem na dosažení maximálního možného zabezpečení) a rovněž nízký elektrický příkon.*

*Softwarové* ***routery/firewally****: www.ipcop.org/; https://www.ipfire.org/*
*Ethernetový* ***switch*** *pro virtualizované prostředí: http://www.openvswitch.org/*“.[338]

**K písm. c)**
**Nástroj pro ověřování identity uživatelů**
Dle § 19 VoKB musí povinná osoba používat nástroj pro správu a ověření identity uživatelů, administrátorů a aplikací informačního a komunikačního systému.

Tento nástroj je v současnosti de facto součástí všech běžně používaných operačních systémů (Linux, iOS, Windows). Dle VoKB má tento nástroj zajistit:

338: KODET, Jaroslav. *Kybernetický zákon: Využijte naplno open source nástroje.* [online]. [cit. 25. 4. 2018]. Dostupné z: https://www.nic.cz/files/nic/doc/Securityworld_CSIRTCZ_112015.pdf

- **ověření identity osoby** (před zahájením aktivit v informačním a komunikačním systému),
- řízení počtu možných neúspěšných **pokusů o přihlášení**,
- **odolnost** uložených nebo přenášených **autentizačních údajů proti neoprávněnému odcizení a zneužití**,
- **ukládání autentizačních** údajů ve formě odolné proti off-line útokům,
- **opětovné ověření identity** po určené době nečinnosti,
- **dodržení důvěrnosti autentizačních údajů** při obnově přístupu,
- **centralizovanou správu identit**.

Povinná osoba pro ověření identity uživatelů, administrátorů a aplikací využívá:

1) **autentizační mechanizmus**, který není **založený** pouze na použití identifikátoru účtu a hesla, nýbrž **na vícefaktorové autentizaci s nejméně dvěma různými typy faktorů,**
2) nástroj pro ověření identity uživatelů, administrátorů a aplikací, používat **autentizaci pomocí kryptografických klíčů** a zaručit obdobnou úroveň bezpečnosti[339],
3) nástroj pro ověření identity uživatelů, administrátorů a aplikací, který používá k **autentizaci identifikátor účtu a heslo.**[340]

V případě, že je k autentizaci využito účtu a hesla, musí být splněny následující podmínky:

- minimální délka hesla:
  - **12 znaků u uživatelů** a
  - **17 znaků u administrátorů a aplikací.**
- **možnost zadat heslo o délce alespoň 64 znaků,**
- možnost použít v hesle **malá a velká písmena, číslice a speciální znaky,**
- **možnost změny hesla**, přičemž **doba mezi dvěma změnami** hesla **nesmí být kratší než 30 minut,**
- **neumožnit uživatelům a administrátorům:**
  - **zvolit si nejčastěji používaná hesla,**
  - **tvořit hesla na základě** mnohonásobně opakujících se znaků, přihlašovacího jména, e-mailu, názvu systému nebo obdobným způsobem,
  - opětovné použití dříve používaných hesel **s pamětí alespoň 12 předchozích hesel.**
- pro **povinnou změnu hesla v intervalu maximálně po 18 měsících**, přičemž toto pravidlo se nevztahuje na účty sloužící k obnově systému v případě havárie,
- **vynutí bezodkladnou změnu výchozího hesla po jeho prvním použití,**
- **bezodkladně zneplatní heslo sloužící k obnovení přístupu po jeho prvním použití nebo uplynutím nejvýše 60 minut od jeho vytvoření**,
- **zahrne pravidla tvorby bezpečných hesel do plánu rozvoje bezpečnostního povědomí.**

339: Za předpokladu, že povinná osoba doposud nesplnila první z preferovaných autentizačních mechanismů.

340: Za předpokladu, že povinná osoba doposud nesplnila první či druhý z preferovaných autentizačních mechanismů.

**Příklad:** *Doporučujeme při školení uživatelů využít i praktické ukázky. Například nástroje CEWL, nebo CUPP. Oba lze nalézt například v linuxové distribuci Kali. Nástroj CEWL umí vytvořit slovník pro slovníkový útok na míru konkrétní organizaci a to na základě obsahu jejích webových stránek. Nástroj CUPP pak umí vytvořit slovník konkrétnímu uživateli na míru. Tyto praktické ukázky jsou dle zkušenosti autorů pro uživatele velmi přínosné, neboť na nich prakticky vidí, že jejich dosud používané heslo složené například z data narození a jména rodinného psího mazlíčka lze skutečně vygenerovat, pokud o nich má útočník dostatek informací.*[341]

*„Pro praktické ověřování identity uživatelů nabízí komunita open source dostatek softwaru kompatibilního se svými komerčními protějšky. Jde například o:*

*FreeRADIUS – http://freeradius.org/ /RADIUS*
*OpenLDAP – http://www.openldap.org/ /Microsoft AD, Oracle Internet Directory*
*Kerberos – https://www.gnu.org/software/shishi/*
*OpenDiameter – https://sourceforge.net/projects/diameter/*

*Všechny tyto nástroje poskytují prostředky pro vynucení určené složitosti hesla, jakož i dalších atributů požadovaných ZoKB, buď samy o sobě prostřednictvím* `login.conf`*, nebo s využitím externích mechanismů jako cracklib a slovníků oblíbených „hesel“.*[342]

**K písm. d)**

## Nástroj pro řízení přístupových oprávnění

Dle § 20 VoKB musí povinná osoba používat centralizovaný nástroj pro řízení přístupových oprávnění.

Pojmem **oprávnění** se rozumí právo přístupu k některému z aktiv (typicky informačnímu či komunikačnímu systému, aplikacím aj.). V praxi se jedná o nástroj „správy uživatelů a skupin“ a nástroj nastavování oprávnění k souborům a adresářům. Tyto nástroje jsou proprietární součástí všech standardně využívaných operačních systémů.

Centralizovaný nástroj pro řízení přístupových oprávnění, má dle § 19 VoKB zajistit řízení oprávnění:

- pro přístup k jednotlivým aktivům informačního a komunikačního systému a
- pro čtení dat, zápis dat a změnu oprávnění.

341: Blíže viz kap. 6.2.3 Hesla

342: KODET, Jaroslav. *Kybernetický zákon: Využijte naplno open source nástroje.* [online]. [cit. 25. 4. 2018]. Dostupné z: https://www.nic.cz/files/nic/doc/Securityworld_CSIRTCZ_112015.pdf

**Je vhodné aplikovat nástroje** pro centralizovanou správu přístupových oprávnění, **které budou komunikovat s centrálním AAA** (**A**uthentication, **A**uthorisation, **A**ccounting) **serverem**.

**Příklad:** *Důležité je pamatovat na řízení přístupových oprávnění již při samotném návrhu softwaru. Autor zná aplikaci, která měla velmi obecná oprávnění a v podstatě v ní existovaly pouze role administrátora a uživatele. Administrátor byl oprávněn přidávat další uživatele a administrátory a uživatel byl oprávněn k ostatním činnostem. Tato aplikace však uchovávala důležité informace o zákaznících dané organizace. Protože tato aplikace neumožňovala žádnou granuralitu oprávnění, všichni uživatelé, bez ohledu na jejich skutečné pracovní potřeby, byli oprávněni přistupovat do jakékoliv části informací o zákaznících. Tato situace nakonec vyústila v únik dat týkajících se konkrétní zákaznice.*

**K písm. e)**

**Nástroj pro ochranu před škodlivým kódem**

Povinná osoba uvedená v § 3 písm. c), d) a f) ZoKB v rámci ochrany před škodlivým kódem:

- **zajišťuje** (s ohledem na důležitost aktiv) **použití nástroje pro nepřetržitou automatickou ochranu**
  - koncových stanic,
  - mobilních zařízení,
  - serverů,
  - datových úložišť a výměnných datových nosičů,
  - komunikační sítě a prvků komunikační sítě,
  - obdobných zařízení.
- **monitoruje a řídí používání výměnných zařízení a datových nosičů,**
- **řídí automatické spouštění obsahu** výměnných zařízení a datových nosičů,
- **řídí oprávnění ke spouštění kódu,**
- **provádí pravidelnou a účinnou aktualizaci** nástroje pro ochranu před škodlivým kódem.

Správce a provozovatel významného informačního systému postupuje dle § 20 odst. 1 VoKB přiměřeně.

„***Ochrana před škodlivým softwarem šířeným prostřednictvím emailu.*** *Open source řešením emailové proxy, zajišťujícím ochranu před škodlivým softwarem, je projekt ASSP (AntiSpam SMTP Proxy, https://sourceforge.net/projects/assp/), umožňující komplexní konfiguraci chování mail proxy prostřednictvím webového rozhraní.*

***Ochrana před škodlivým softwarem šířeným prostřednictvím webu.*** *Vhodným řešením je například projekt HTTP AntiVirus Proxy (http://www.havp.org/) nebo www.cacheguard.com. I zde je nutné*

*zajistit také odpovídající ochranu koncových pracovních stanic, protože šifrovaný provoz není možné v reálném čase skenovat v pozici ‚muže uprostřed'.*

*Blokování jeho síťového provozu, a to jak na úrovni datové infrastruktury, tak na úrovni ‚osobních firewallů' koncových stanic. Pravidla síťové komunikace by se měla nastavit ‚paranoidně', tj. povolit jen provoz nezbytný k fungování legitimního softwaru, vše ostatní zakázat. Opatření na straně serveru, proxy serveru či prvku síťové infrastruktury ale v žádném případě plně nenahrazuje ochranu proti škodlivému softwaru na koncových pracovních stanicích, zejména proto, že nemusí být vždy schopné zachytit šifrovaný provoz, který je dešifrován až na klientském programu."* [343]

**K písm. f)**

**Nástroj pro zaznamenávání činnosti kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů**

Dle § 22 VoKB musí povinná osoba:

- **zaznamenávat bezpečnostní a** potřebné **provozní události** důležitých aktiv informačního a komunikačního systému a
- **aktualizovat rozsah aktiv** (na základě hodnocení jejich důležitosti), u kterých je zaznamenávání bezpečnostních a provozních událostí prováděno.

Pro **zaznamenávání bezpečnostních a provozních událostí** je třeba zajistit

- jednoznačnou síťovou identifikaci zařízení původce, je-li v komunikační síti použit nástroj, který mění jeho síťovou identifikaci,
- sběr informací o bezpečnostních a provozních událostech; zejména se zaznamenává:
  - datum a čas včetně specifikace časového pásma,
  - typ činnosti,
  - identifikace technického aktiva, které činnost zaznamenalo,
  - jednoznačná identifikace účtu, pod kterým byla činnost provedena,
  - jednoznačná síťová identifikaci zařízení původce,
  - úspěšnost nebo neúspěšnost činnosti.
- ochranu takto získaných informací před neoprávněným čtením a jakoukoli změnou,
- zaznamenávání:
  - přihlašování a odhlašování ke všem účtům, a to včetně neúspěšných pokusů,
  - činností provedených administrátory,
  - úspěšné i neúspěšné manipulace s účty, oprávněními a právy,
  - neprovedení činností v důsledku nedostatku přístupových práv a oprávnění,

343: KODET, Jaroslav. *Kybernetický zákon: Využijte naplno open source nástroje.* [online]. [cit. 25. 4. 2018]. Dostupné z: https://www.nic.cz/files/nic/doc/Securityworld_CSIRTCZ_112015.pdf

  - činnosti uživatelů, které mohou mít vliv na bezpečnost informačního a komunikačního systému,
  - zahájení a ukončení činností technických aktiv,
  - kritických i chybových hlášení technických aktiv,
  - přístupů k záznamům o událostech, pokusy o manipulaci se záznamy o událostech a změny nastavení nástrojů pro zaznamenávání událostí.
- synchronizaci jednotného času technických aktiv nejméně jednou za 24 hodin.

Povinná osoba uvedená v § 3 písm. c), d) a f) ZoKB **uchovává záznamy událostí** po dobu **18 měsíců**.

Povinná osoba uvedená v § 3 písm. e) ZoKB **uchovává záznamy událostí** po dobu **12 měsíců**.

*„Pro zajištění jejich použitelnosti pro případ vyšetřování kybernetických bezpečnostních incidentů je třeba zajistit synchronizaci času všech prvků pomocí protokolu NTP (Network Time Protocol), který je implementovaný na všech běžných operačních systémech. Dále je třeba zajistit konfiguraci logovacích systémů (ať už unixových syslogů či Windows eventlogů), tak aby obsahovaly všechny požadované náležitosti specifikované v jednotlivých odstavcích tohoto paragrafu.*

*Použitelnými open source nástroji jsou v tomto případě syslog, syslogng (*`syslog-ng.org`*) a rsyslog (*`rsyslog.com`*). Bývají užitečné zejména v roli centralizovaných syslog serverů, na nichž se koncentrují veškeré relevantní logy ze všech prvků na jednom místě. Takto shromážděné logy se následně zpracovávají softwarem IDS/IPS/SIEM pro včasnou detekci kybernetických bezpečnostních incidentů, jakož i k omezení jejich dopadů a prevenci jejich opakování.“* [344]

**K písm. g)**

### Nástroj pro detekci kybernetických bezpečnostních událostí

Dle § 23 VoKB musí povinná osoba v rámci komunikační sítě, jejíž součástí je informační a komunikační systém, používat nástroj pro detekci kybernetických bezpečnostních událostí, který zajistí:

- **ověření a kontrolu přenášených dat v rámci komunikační sítě** a mezi komunikačními sítěmi,
- **ověření a kontrolu přenášených dat na perimetru** komunikační sítě a
- **blokování nežádoucí komunikace**.

Povinná osoba uvedená v § 3 písm. c), d) a f) ZoKB zajistí detekci kybernetických bezpečnostních událostí přiměřeně s ohledem na důležitost aktiv v rámci koncových stanic, mobilních zařízení,

344: KODET, Jaroslav. *Kybernetický zákon: Využijte naplno open source nástroje.* [online]. [cit. 25. 4. 2018]. Dostupné z: https://www.nic.cz/files/nic/doc/Securityworld_CSIRTCZ_112015.pdf

serverů, datových úložišť a výměnných datových nosičů, síťových aktivních prvků a obdobných aktiv.

Zákonodárce v tomto případě de facto požaduje nasazení intrusion detection systémů (IDS), a to jak v rámci vnitřní sítě, tak na perimetru sítě.

*„K detekci kybernetických bezpečnostních událostí lze využít výstupů z mnoha softwarových nástrojů, například prohledávačů logů Logwatch (https://sourceforge.net/projects/logwatch/files/), Epylog (https://fedoraproject.org/wiki/Infrastructure/Fedorahosted-retirement), intrusion detection systémů jako OpenVAS (http://openvas.org/), Suricata (https://suricata-ids.org/), Snort (https://www.snort.org/) nebo Samhain (lasamhna.de/Samoin).“* [345]

**K písm. h)**

### Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí

Povinná osoba dle § 3 písm. c), d) a f) ZoKB musí používat **nástroj pro sběr a nepřetržité vyhodnocení kybernetických bezpečnostních událostí**, který umožní:

- **sběr a vyhodnocování událostí** zaznamenaných podle § 22 a 23 VoKB,
- **vyhledávání a seskupování souvisejících záznamů,**
- **poskytování informací pro určené bezpečnostní role** o detekovaných kybernetických bezpečnostních událostech,
- **vyhodnocování kybernetických bezpečnostních událostí** s cílem identifikace kybernetických bezpečnostních incidentů, včetně včasného varování určených bezpečnostních rolí,
- omezení případů nesprávného vyhodnocení událostí pravidelnou aktualizací nastavení pravidel pro:
  - vyhodnocování kybernetických bezpečnostních událostí,
  - včasné varování,
- využívání informací získaných nástrojem pro sběr a vyhodnocení kybernetických bezpečnostních událostí pro optimální nastavení bezpečnostních opatření informačního a komunikačního systému.

Nástrojem pro sběr a vyhodnocení kybernetických bezpečnostních událostí se rozumí nástroje, které jsou označovány jako **SIEM** (**S**ecurity **I**ncident and **E**vent **M**anagement).[346]

345: KODET, Jaroslav. *Kybernetický zákon: Využijte naplno open source nástroje.* [online]. [cit. 25. 4. 2018]. Dostupné z: https://www.nic.cz/files/nic/doc/Securityworld_CSIRTCZ_112015.pdf

346: Blíže viz kap. 6.1.3.5

V rámci open source řešení SIEM je možné využít například OSSIM/USM (https://www.alienvault.com/products/usm-anywhere/try-it-now), OSSEC (www.ossec.net/) nebo logalyze (www.logalyze.com).[347]

**K písm. i)**

## Aplikační bezpečnost

V případě aplikační bezpečnosti je pozornost věnována aplikacím, které jsou využívané v informačních systémech (ať již v rámci počítačového systému, mobilního zařízení, či jako webová aplikace). Aplikační bezpečnost je mimo jiné zajišťována penetračním testováním aplikací, či aplikačními firewally.

Dle § 23 VoKB musí povinná osoba provádět **penetrační testy** informačního a komunikačního systému se zaměřením na důležitá aktiva, a to:

- **před** jejich **uvedením do provozu a**
- **v souvislosti s významnou změnou** podle § 11 odst. 3 VoKB.

Povinná osoba v rámci aplikační bezpečnosti dále musí **zajistit trvalou ochranu aplikací, informací a transakcí před:**

- neoprávněnou činností,
- popřením provedených činností.

*„Z aplikačních firewallů je možné uvést například bezpečnostní moduly webserveru (www.modsecurity.org) nebo OWASP Web Application Firewall. Z komerčních nástrojů pro testování aplikační bezpečnosti jde zejména o nástroj Nessus (www.tenable.com/products/nessusvulnerabilityscanner). Jeho open source alternativou je pak projekt OpenVAS (http://www.openvas.org/).“*[348]

**K písm. j)**

## Kryptografické prostředky

Kryptografie (šifrování) je vědní obor, který se zabývá převodem informací srozumitelných do podoby nesrozumitelné pro příjemce, pokud tento nevlastní klíče, kterým je možné provést rozšifrování dané informace.

S přesunem značného množství dat a informací do systémů ICT je nezbytné věnovat zvýšenou pozornost právě možnostem šifrování (utajování obsahu) přenášených dat.

---

347: KODET, Jaroslav. *Kybernetický zákon: Využijte naplno open source nástroje.* [online]. [cit. 25. 4. 2018]. Dostupné z: https://www.nic.cz/files/nic/doc/Securityworld_CSIRTCZ_112015.pdf

348: Tamtéž

Dle § 26 VoKB musí povinná osoba pro ochranu aktiv informačního a komunikačního systému:

- používat aktuálně odolné kryptografické algoritmy a kryptografické klíče,
- používat systém správy klíčů a certifikátů, který:
  - zajistí generování, distribuci, ukládání, změny, omezení platnosti, zneplatnění certifikátů a likvidaci klíčů,
  - umožní kontrolu a audit.
- prosazovat bezpečné nakládání s kryptografickými prostředky,
- zohledňovat doporučení v oblasti kryptografických prostředků vydaná Úřadem (NÚKIB), zveřejněná na jeho internetových stránkách.

*„Pro účely zajištění dostatečně odolného šifrování síťového provozu se používají knihovny OpenSSL (https://www.openssl.org/), avšak je třeba mít zajištěnou jejich aktuálnost a správnou konfiguraci, tak aby se vyhovělo podmínkám této vyhlášky. Je nutné sledovat aktuální zprávy o zranitelnostech a nevyhovující verze knihoven bez otálení upgradovat na varianty bez známých zranitelností. V tomto ohledu lze doporučit projekt bettercrypto (https://bettercrypto.org/), který má administrátorům pomoci s co nejlepším zabezpečením jimi používaných služeb a používané kryptografie.“* [349]

**K písm. k)**

## Nástroj pro zajišťování úrovně dostupnosti informací

Dle § 27 VoKB musí povinná osoba zavést opatření pro zajišťování úrovně dostupnosti, kterými zajistí:

- **dostupnost informačního a komunikačního systému** pro splnění cílů podle § 15 VoKB,
- **odolnost informačního a komunikačního systému** vůči kybernetickým bezpečnostním incidentům, které by mohly snížit jeho dostupnost,
- **dostupnost důležitých technických aktiv** informačního a komunikačního systému,
- **redundanci aktiv** nezbytných pro zajištění dostupnosti informačního a komunikačního systému.

Implementací nástroje pro zajišťování úrovně dostupnosti informací dochází k naplňování organizačního aktiva: řízení kontinuity činností (**B**usiness **C**ontinuity **M**anagement – **BCM**).

*„Pro dosažení předepsané úrovně dostupnosti lze použít clusterové a cloudové technologie vyvíjené jako open source (KVM, OpenStack), případně zajistit dostupnost náhradního aktiva v určeném čase prostřednictvím backup/restore softwaru (https://sourceforge.net/projects/bacula/).“* [350]

349: KODET, Jaroslav. *Kybernetický zákon: Využijte naplno open source nástroje.* [online]. [cit. 25. 4. 2018]. Dostupné z: https://www.nic.cz/files/nic/doc/Securityworld_CSIRTCZ_112015.pdf

350: Tamtéž

**K písm. l)**

**Bezpečnost průmyslových a řídicích systémů**

Posledním technickým opatřením je zajištění kybernetické bezpečnosti průmyslových, řídicích a obdobných specifických systémů. Dle § 28 VoKB musí povinná osoba používat nástroje a opatření, které zajistí:

- **použití** technických a programových **prostředků, které jsou určeny do specifického prostředí,**
- **omezení fyzického přístupu k zařízením** těchto systémů a ke komunikační síti,
- **vyčlenění komunikační sítě určené pro tyto systémy od ostatní infrastruktury,**
- **omezení a řízení vzdáleného přístupu** k těmto systémům,
- **ochranu jednotlivých technických aktiv** těchto systémů před využitím známých zranitelností,
- obnovení chodu těchto systémů po kybernetickém bezpečnostním incidentu.

**§ 6**

**Prováděcí právní předpis stanoví**

**a) obsah bezpečnostních opatření,**
**b) obsah a strukturu bezpečnostní dokumentace,**
**c) rozsah bezpečnostních opatření pro orgány a osoby uvedené v § 3 písm. c) až f),**
**d) významné informační systémy a jejich určující kritéria,**
**e) obsah a rozsah bezpečnostních pravidel pro orgány veřejné moci využívající služby poskytovatelů cloud computingu.**

Z důvodové zprávy:

*Z důvodu zachování právní jistoty povinných osob je třeba dále jednotlivé komponenty bezpečnostních opatření konkretizovat. Rovněž je třeba zajistit, aby byla tato konkretizace dostatečně flexibilní ve vztahu k budoucímu vývoji techniky. V tomto ustanovení je tedy provedeno zmocnění k realizaci podmíněné omezené legislativní kompetence správní orgánu, tj. v tomto případě NBÚ, ke specifikaci obsahu a rozsahu bezpečnostních opatření, přičemž se předpokládá stanovení úrovně bezpečnostních opatření v závislosti na důležitosti a bezpečnostní expozici příslušné kategorie informačních nebo komunikačních systémů. V zásadě platí, že správci informačních nebo komunikačních systémů kritické informační infrastruktury budou v těchto systémech zavádět bezpečnostní opatření v širším rozsahu než správci významných informačních systémů, u nichž bude rozsah zavedení bezpečnostních opatření v jimi spravovaných systémech užší.*

*Rovněž je tímto ustanovením založeno právo a povinnost NBÚ upravit prováděcím předpisem strukturu bezpečnostní dokumentace. Účelem technické specifikace náležitostí bezpečnostní dokumentace je usnadnit povinným osobám její zpracování a zefektivnit její následné užití včetně kontroly.*

Z důvodové zprávy k novele ZoKB:

*Rozšiřuje se vymezení adresátů prováděcího právního předpisu, který stanoví rozsah bezpečnostních opatření, o správce a provozovatele informačního systému základních služeb. Návrh ustanovení reflektuje čl. 14 odst. 1 a 2 směrnice.*

Ustanovení § 6 ZoKB explicitně odkazuje na prováděcí předpisy, které mají konkretizovat některé obecné požadavky či principy stanovené tímto zákonem. Důvodem ukotvení těchto specifických požadavků do prováděcích předpisů ve formě vyhlášek je mimo jiné i možnost jejich mnohem snazší novelizace, než jak by tomu bylo v případě vymezení těchto požadavků přímo v zákoně.

Prováděcími právními předpisy k zákonu o kybernetické bezpečnosti jsou:

- **nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury**;
- **vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích**;
- **vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby**;
- **vyhláška č. 82/2018 Sb.**, o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (**vyhláška o kybernetické bezpečnosti**).

Výše uvedené vyhlášky a v nich specifikované požadavky jsou zapracovány do textu této publikace (zejména v rámci komentáře k ZoKB) průběžně.

**§ 6a**

**(1) Správce informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému může pověřit provozováním informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému jiný orgán nebo osobu, pokud to jiný zákon nevylučuje.**
**(2) Provozovatel informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému předá na vyžádání správce tohoto systému bez zbytečného odkladu a v dohodnutém formátu data, provozní údaje a informace, které má k dispozici v souvislosti s provozováním tohoto**

**systému. Ustanovení právního předpisu upravujícího práva k duševnímu vlastnictví nejsou předáním dat, provozních údajů a informací dotčena.**
**(3) Pokud provozovatel informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému nebude tento systém nadále provozovat, předá správci tohoto systému data, provozní údaje a informace, které má k dispozici v souvislosti s provozováním tohoto systému a které jsou nezbytné pro případné další provozování tohoto informačního systému nebo jeho jiné využití a bezpečně zlikviduje ve svém digitálním prostředí jejich kopie. Způsob likvidace dat, provozních údajů, informací a jejich kopií stanoví prováděcí právní předpis.**
**(4) Provozovatel informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému má nárok na úhradu účelně vynaložených nákladů za předání dat, provozních údajů a informací podle odstavců 2 a 3; náklady provozovateli uhradí správce takového systému.**

Z důvodové zprávy k novele ZoKB:

*V souvislosti s novelou zákona o informačních systémech veřejné správy se do zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), zavádí nová kategorie povinných osob – provozovatel informačního nebo komunikačního systému.*

*Dopady jsou přitom podobné, tedy rozšířit okruh povinných orgánů a osob i na provozovatele systémů, kteří provozují informační systémy nebo komunikační systémy pro kritickou informační infrastrukturu, resp. významné informační systémy, avšak bez zahrnutí těch osob, které dodávají části systémů nebo nemají na provoz informačního systému takový vliv, jako osoby podřaditelné pod novou definici provozovatele.*

*Tato novela je potřebná zejména z toho důvodu, že řada povinných orgánů a osob neprovozuje systémy, které spravují. Je sice tedy možno zprostředkovaně i proti provozovatelům těchto systémů uplatnit kontrolní pravomoci, ale provozovatelé nemají přímé zákonné povinnosti a nedopadá na ně sankční režim zákona o kybernetické bezpečnosti. Outsourcing je navíc často realizován na základě starých smluv, jejichž obsah mnohdy již neodpovídá současné situaci, přičemž je pak z hlediska povinných orgánů a osob obvykle problematické operativně řešit rozpor příslušných systémů s požadavky zákona.*

*Současně se návrhem provádí dílčí úpravy, které mají zabránit tomu, aby nastalo duplicitní hlášení o incidentech v oblasti kybernetické bezpečnosti v případě, že byl incident již nahlášen provozovatelem.*

*Dále se zavádí, shodně jako v návrhu novely zákona o informačních systémech veřejné správy, povinnost předat data a informace mezi provozovatelem a správcem informačního systému. Tato povinnost může být rovněž uložena na základě návrhu správce rozhodnutím Národního bezpečnostního úřadu, a to*

*v případě hrozícího kybernetického bezpečnostního incidentu. Tato povinnost je předmětem úhrady účelně a prokazatelně vynaložených nákladů.*

*Návrh rovněž reaguje na stav, kdy správci nemají např. v důsledku neshod s provozovateli informačních nebo komunikačních systémů nebo při skončení smlouvy s provozovatelem přístup k datům a informacím, které správce potřebuje pro výkon své pravomoci. Absence smluvních povinností migrovat data a případně poskytnout další součinnost při změně dodavatele v těchto případech vede k tomu, že je správcům de facto znemožněno vybrat lepšího dodavatele technologií nebo služeb. Zákon o kybernetické bezpečnosti by měl tedy především ošetřit případy, kdy tento „lock-in" efekt může představovat bezpečnostní riziko pro systémy a sítě spadající pod jeho věcný rozsah.*

Novelizace provedená zákonem č. 104/2017 Sb.,[351] s účinností od 1. července 2017 zavedla nové kategorie povinných osob (provozovatel informačního nebo komunikačního systému) spadajících pod ZoKB o provozovatele informačních systémů.

**K odst. 1)**
K pojmu **informační systém** viz § 1 ZoKB.
K pojmu **Správce a provozovatel informačního systému kritické informační infrastruktury** viz § 3 písm. c) ZoKB.
K pojmu **Správce a provozovatel komunikačního systému kritické informační infrastruktury** viz § 3 písm. d) ZoKB.
K pojmu **Správce a provozovatel významného informačního systému** viz § 3 písm. e) ZoKB.

V ustanovení § 6a odst. 1 ZoKB je výslovně umožněna delegace činností ze strany správce informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému na subjekt, který bude zastávat pouze roli provozovatele takovéhoto systému.

Ve své podstatě jde o outsourcing činností, služeb či systémů, které správce výše uvedených sytémů nezajišťuje (nespravuje), nebo je nemusí zajišťovat.

Podmínkou pro to, **aby bylo možné pověřit provozováním** uvedených **systémů jiný orgán nebo osobu je ta skutečnost, že to jiný zákon nevylučuje.**

351: Zákon č. 104/2017 Sb., kterým se mění zákon č. 365/2000 Sb., **o informačních systémech veřejné správy** a o změně některých dalších zákonů, ve znění pozdějších předpisů, zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), a některé další zákony. [online]. Dostupné z: https://www.zakonyprolidi.cz/cs/2017-104

**K odst. 2)**
Zákon o kybernetické bezpečnosti nově zavádí povinnost předat data a informace mezi provozovatelem a správcem informačního systému.

Provozovatel uvedeného informačního systému je povinen předat na vyžádání správce tohoto systému **bez zbytečného odkladu** a **v dohodnutém formátu data, provozní údaje a informace, které má k dispozici v souvislosti s provozováním tohoto systému.**

Ustanovení § 6a odst. 2 ZoKB také zdůrazňuje tu skutečnost, že **práva k duševnímu vlastnictví nejsou předáním dat, provozních údajů a informací dotčena.**[352]

Jednotlivá práva a povinnosti správců i provozovatelů uvedených informačních systémů jsou v této publikaci uvedeny v rámci § 3 ZoKB.

**K odst. 3) a 4)**
Ustanovení § 6a odst. 3 ZoKB se věnuje situaci, kdy provozovatel jednoho z výše uvedených informačních systémů de facto ukončuje svoji činnost (ať již zcela, či v této specifické oblasti) a dále již nebude tyto systémy provozovat.

V takovém případě je povinen:

- **předat správci tohoto systému data, provozní údaje a informace:**
  - **které má k dispozici v souvislosti s provozováním tohoto systému,**
  - **a které jsou nezbytné pro případné další provozování tohoto informačního systému nebo jeho jiné využití.**

- **bezpečně zlikvidovat ve svém digitálním prostředí jejich kopie.**

Provozovatel uvedených informačních systémů **má nárok na úhradu účelně vynaložených nákladů za předání dat**. Takto vzniklé náklady je povinen provozovateli uhradit správce.

352: Blíže viz zejména:
- Zákon č. 121/2000 Sb., autorský zákon;
- Zákon č. 89/2014 Sb., občanský zákoník;
- Zákon č. 14/1993 Sb., o opatřeních na ochranu průmyslového vlastnictví;
- Zákon č. 441/2003 Sb., o ochranných známkách;
- Zákon č. 527/1990 Sb., o vynálezech, průmyslových vzorech a zlepšovacích návrzích.

## § 7
## Kybernetická bezpečnostní událost a kybernetický bezpečnostní incident

**(1) Kybernetickou bezpečnostní událostí je událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací.**[353]
**(2) Kybernetickým bezpečnostním incidentem je narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací**[354] **v důsledku kybernetické bezpečnostní události.**
**(3) Orgány a osoby uvedené v § 3 písm. b) až f) jsou povinny detekovat kybernetické bezpečnostní události v jejich významné síti, informačním systému kritické informační infrastruktury, komunikačním systému kritické informační infrastruktury, informačním systému základní služby nebo významném informačním systému.**

Z důvodové zprávy:

*Rozdělení skutkových stavů, na něž zákon reaguje konstrukcí specifických povinností, na kybernetické bezpečnostní události a kybernetické bezpečnostní incidenty, sleduje účel odlišení potenciálně problematických situací vykazujících stanovené formální znaky a situací, které na základě vyhodnocení formálních podmínek v kontextu aktuálních okolností, představují reálné bezpečnostní riziko. Zatímco kybernetickou bezpečnostní událostí je událost bez reálného negativního následku pro daný komunikační nebo informační systém, kybernetickým bezpečnostním incidentem je pak již taková událost, která s sebou nese reálné narušení informačního nebo komunikačního systému negativním dopadem. Detekční povinnosti zákon váže ke kybernetickým bezpečnostním událostem, oproti tomu povinnosti reagovat formou hlášení příslušnému dohledovému pracovišti resp. formou provedení protiopatření jsou navázány až k situaci, kdy je příslušná událost vyhodnocena povinnou osobou jako kybernetický bezpečnostní incident.*

*Toto ustanovení zakládá vybraným povinným osobám detekční povinnost vzhledem ke kybernetickým bezpečnostním událostem, které se vyskytly v jejich významné síti, informačním nebo komunikačním systému kritické informační infrastruktury anebo ve významném informačním systému. Povinnost hlásit kybernetický bezpečností incident je pak založena v následujícím ustanovení.*

*Cizojazyčný pojem „incident" byl použit z důvodu zachování souladu zákonného pojmového aparátu s mezinárodní technickou terminologií. Ze stejného důvodu je použit i pojem „detekovat", jehož český ekvivalent, tj. „odhalovat" nebo „zjišťovat" navíc není sémanticky zcela adekvátní.*

353: Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů.
354: Tamtéž

Z důvodové zprávy k novele ZoKB:

*V souladu s čl. 14 odst. 2 směrnice se povinnost detekovat kybernetické bezpečnostní události nově vztahuje i na správce a provozovatele informačního systému základních služeb.*

K pojmu **informační systém** viz § 1 ZoKB.
K pojmu **bezpečnost informací** viz kap. 2.1.
K pojmu **síť elektronických komunikací** viz § 1 odst. 2 ZoKB.

**K odst. 1)**
K pojmu **kybernetická bezpečnostní událost** blíže viz kap. 2.4.2.

Kybernetická bezpečnostní událost představuje **událost bez zatím reálného negativního následku** pro daný komunikační nebo informační systém. Ve své podstatě **se jedná pouze o hrozbu**, která však musí být reálná.

Domníváme se, že pojem kybernetická bezpečnostní událost by bylo vhodnější a zřejmě i srozumitelnější označovat a vykládat jako **kybernetickou hrozbu**, neboť zde skutečně pouze existuje potenciální příčina, která může způsobit nežádoucí událost.

K pojmu **kybernetická hrozba** blíže viz kap. 2.4.1.

Povinnost **detekovat kybernetické bezpečnostní události** má:

- orgán nebo osoba zajišťující významnou síť [§ 3 písm. b) ZoKB],
- správce a provozovatel informačního systému kritické informační infrastruktury [§ 3 písm. c) ZoKB],
- správce a provozovatel komunikačního systému kritické informační infrastruktury [§ 3 písm. d) ZoKB],
- správce a provozovatel významného informačního systému [§ 3 písm. e) ZoKB],
- správce a provozovatel informačního systému základní služby [§ 3 písm. f) ZoKB].

**K odst. 2)**
K pojmu **kybernetický bezpečnostní incident** blíže viz kap. 2.4.3.

Kybernetický bezpečnostní incident představuje **skutečné narušení** bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací, **tj. narušení informačního nebo komunikačního systému s negativním dopadem**.

Za určitou část kybernetických bezpečnostních incidentů jsou zodpovědné i náhodné jevy, chyby hardwaru, softwaru, chyby učiněné při konfiguraci administrátory, chyby uživatelů systémů aj.

Povinnost **hlásit kybernetické bezpečnostní incidenty:**

- **národnímu CERT týmu:**
  - orgán nebo osoba zajišťující významnou síť [§ 3 písm. b) ZoKB],
  - poskytovatel digitální služby [§ 3 písm. g) ZoKB].

- **vládnímu CERT týmu:**
  - správce a provozovatel informačního systému kritické informační infrastruktury [§ 3 písm. c) ZoKB],
  - správce a provozovatel komunikačního systému kritické informační infrastruktury [§ 3 písm. d) ZoKB],
  - správce a provozovatel významného informačního systému [§ 3 písm. e) ZoKB],
  - správce a provozovatel informačního systému základní služby [§ 3 písm. f) ZoKB],
  - provozovatel základní služby [§ 3 písm. g) ZoKB].

Ustanovení § 31 VoKB se věnuje kategorizaci kybernetických bezpečnostních incidentů, přičemž vlastní kategorizace je provedena na základě zohlednění dopadů obsažených v dopadových určujících kritériích, podle kterých byly povinné osoby určeny; počtu dotčených uživatelů; způsobené nebo předpokládané škody; důležitosti dotčených aktiv informačního a komunikačního systému; dopadů na poskytované služby informačního a komunikačního systému; dopadů na služby poskytované jinými informačními a komunikačními systémy; délky trvání incidentu; zeměpisného rozsahu dotčené oblasti a dalších dopadů.

I pro potřeby hlášení kybernetických bezpečnostních incidentů jsou v § 31 odst. 2 VoKB kybernetické bezpečnostní incidenty rozděleny do následujících tří kategorií:

**Kategorie III - velmi významný kybernetický bezpečnostní incident**
Při tomto incidentu je **přímo a významně** narušena bezpečnost poskytovaných **služeb nebo aktiv.** Vyřešení takovéhoto incidentu **vyžaduje neprodlené zásahy obsluhy s tím, že musí být všemi dostupnými prostředky zabráněno dalšímu šíření** kybernetického bezpečnostního incidentu včetně minimalizace vzniklých i potenciálních škod.

**Kategorie II - významný kybernetický bezpečnostní incident**
Při významném kybernetickém incidentu je narušena bezpečnost poskytovaných **služeb nebo aktiv**. Jeho řešení **vyžaduje neprodlené zásahy obsluhy s tím, že musí být vhodnými prostředky zabráněno dalšímu šíření** kybernetického bezpečnostního incidentu včetně minimalizace vzniklých škod.

**Kategorie I - méně významný kybernetický bezpečnostní incident**
Posledním, nejméně závažným incidentem, je méně významný kybernetický bezpečnostní incident, při kterém **dochází k méně významnému narušení bezpečnosti** poskytovaných **služeb nebo aktiv**. Vyřešení takovéhoto incidentu **vyžaduje zásahy obsluhy s tím, že musí být vhodnými prostředky omezeno další šíření** kybernetického bezpečnostního incidentu včetně minimalizace vzniklých škod.

Vyhláška o kybernetické bezpečnosti také v § 31 odst. 3 kategorizuje kybernetické bezpečnostní incidenty dle jejich dopadu. Konkrétně se jedná o kybernetický bezpečnostní incident způsobující narušení:

- **důvěrnosti aktiv**,
- **integrity aktiv**,
- **dostupnosti aktiv**,
- **kombinaci** tří výše **uvedených dopadů**.

Ustanovení § 31 VoKB o kategorizaci kybernetických bezpečnostních incidentů se nevztahuje na kybernetické bezpečnostní incidenty u poskytovatele digitálních služeb [§ 3 písm. h) ZoKB].

**§ 8**
**Hlášení kybernetického bezpečnostního incidentu**

**(1) Orgány a osoby uvedené v § 3 písm. b) až f) jsou povinny hlásit kybernetické bezpečnostní incidenty v jejich významné síti, informačním systému kritické informační infrastruktury, komunikačním systému kritické informační infrastruktury, informačním systému základní služby nebo významném informačním systému, a to bezodkladně po jejich detekci; tím není dotčena informační povinnost podle jiného právního předpisu[355] nebo přímo použitelného předpisu Evropské unie upravujícího ochranu osobních údajů.[356] V případě, že kybernetický bezpečnostní incident má významný dopad na kontinuitu poskytování základní služby, oznámí to provozovatel základní služby Úřadu.**
**(2) Poskytovatel digitální služby je povinen bez zbytečného odkladu hlásit kybernetický bezpečnostní incident s významným dopadem na poskytování jeho služeb, pokud má přístup k informacím nezbytným pro posouzení významnosti tohoto dopadu.**
**(3) Orgány a osoby uvedené v § 3 písm. b) a h) hlásí kybernetické bezpečnostní incidenty provozovateli národního CERT.**

355: Například § 98 odst. 4 a § 99 odst. 4 zákona č. 127/2005 Sb., ve znění pozdějších předpisů.
356: Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

**(4) Orgány a osoby uvedené v § 3 písm. c) až g) hlásí kybernetické bezpečnostní incidenty Úřadu.**
**(5) Povinnost podle odstavce 1 je správcem informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému splněna i tehdy, pokud byl kybernetický bezpečnostní incident hlášen provozovatelem tohoto systému. Provozovatel informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému informuje správce tohoto systému o hlášených kybernetických bezpečnostních incidentech bez zbytečného odkladu.**
**(6) Orgány a osoby neuvedené v § 3 mohou hlásit kybernetické bezpečnostní incidenty provozovateli národního CERT, nebo Úřadu.**
**(7) Prováděcí právní předpis stanoví**
- **a) typy, kategorie a hodnocení významnosti dopadu kybernetického bezpečnostního incidentu a**
- **b) náležitosti a způsob hlášení kybernetického bezpečnostního incidentu.**

**(8) Pokud má kybernetický bezpečnostní incident, který postihnul poskytovatele digitální služby, významný dopad na kontinuitu poskytování základní služby, je její provozovatel povinen tuto skutečnost Úřadu nahlásit.**

Z důvodové zprávy:

*Navržené ustanovení zakládá vybraným povinným osobám povinnost hlásit kybernetické bezpečnostní incidenty dohledovým pracovištím. Účelem tohoto ustanovení je umožnit dohledovým pracovištím vykonávat jejich primární běžnou funkci, tj. koordinovat ochranu kritické informační infrastruktury, významných informačních systémů a významných sítí.*

*Vybrané povinné osoby budou povinny hlásit kybernetické bezpečnostní incidenty, které se vyskytly v jejich významné síti, informačním nebo komunikačním systému kritické informační infrastruktury anebo ve významném informačním systému, bezodkladně po jejich zjištění, tj. po vyhodnocení kybernetické bezpečnostní události jako kybernetického bezpečnostního incidentu. Toto ustanovení je komplementární úpravou k existujícím informačním a ohlašovacím povinnostem, tj. splněním ohlašovací povinnosti podle toho ustanovení se povinné osoby nezbavují informačních povinností založených jinými právními předpisy např. zákonem o elektronických komunikacích.*

*Vzhledem k zásadní důležitosti informačních a komunikačních systémů zařazených do kritické informační infrastruktury a významných informačních systémů jsou jejich správci povinni hlásit výskyt kybernetických bezpečnostních incidentů NBÚ, respektive jím provozovanému veřejnoprávnímu dohledovému pracovišti – vládnímu CERT. Kybernetické bezpečnostní incidenty ve významných sítích jsou vybrané povinné osoby povinny hlásit národnímu CERT.*

*Účelem tohoto ustanovení je založit povinnost hlásit kybernetické bezpečnostní incidenty detekované na základě povinnosti založené v předchozím ustanovení. Tato ustanovení však nevylučují možnost hlášení kybernetických bezpečnostních událostí nebo možnost obracet se na národní CERT nebo vládní CERT s podněty anebo jinými oznámeními souvisejícími s kybernetickou bezpečností nemajícími charakter kybernetického bezpečnostního incidentu.*

*Vzhledem k tomu, že je třeba upravit technické podrobnosti k výkonu povinnosti hlásit kybernetické bezpečnostní incidenty, tj. zejména je třeba v návaznosti na technický vývoj a na aktuální poznatky z oboru informatiky průběžně definovat konkrétní technické parametry typů a kategorií hlášených kybernetických bezpečnostních incidentů, jakož i stanovovat technické náležitosti a formu jednotlivých hlášení, je v tomto ustanovení rovněž provedeno zákonné zmocnění NBÚ k vydání prováděcího předpisu.*

Z důvodové zprávy k novele ZoKB:

K § 8 odst. 1
*Toto ustanovení je transpoziční k čl. 14 odst. 3 a 4 směrnice. Dle stávajícího systému zákona o kybernetické bezpečnosti jsou hlášeny všechny kybernetické bezpečnostní incidenty, přičemž náležitosti a způsob hlášení kybernetického bezpečnostního incidentu upravuje prováděcí právní předpis. Nově se stanoví, že v souladu s tímto předpisem incidenty hlásí také správci a provozovatelé informačních systémů základní služby. Je zapotřebí zdůraznit, že kybernetický bezpečnostní incident, jak je vymezen v § 7 odst. 2 zákona, plně odpovídá pojmu incident, s nímž pracuje směrnice. Jako nadstavbovou informaci poskytne Úřadu provozovatel základní služby informaci o případném závažném dopadu na kontinuitu poskytování základní služby, pokud k takovému dojde, neboť pouze on je schopen posoudit reálné dopady kybernetického bezpečnostního incidentu. Kontinuitou se rozumí plynulost poskytování dané služby. Významnost dopadu incidentu bude posuzována na základě prováděcího právního předpisu.*

*Zároveň návrh tohoto ustanovení reaguje na čl. 33 Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).*

K § 8 odst. 2
*Tento novelizační bod transponuje čl. 16 odst. 3 a 4 směrnice. Zakládá se povinnost poskytovatelů digitálních služeb bezodkladně ohlásit provozovateli národního CERT kybernetické bezpečnostní incidenty se závažným dopadem na jejich služby. Tato povinnost je zmírněna podmínkou, že poskytovatelé digitálních služeb jsou povinni incident hlásit jen v případě, že mají k dispozici informace, které jim umožní posoudit závažnost dopadu incidentu. Kritéria pro určení závažnosti incidentu bude stanovovat prováděcí právní předpis, který již v současnosti stanoví kritéria incidentů pro ostatní povinné osoby podle tohoto zákona.*

K § 8 odst. 3
*Navrženou úpravou ustanovení § 8 odst. 4 se transponuje čl. 16 odst. 3 směrnice, kdy se za tým CSIRT, jemuž poskytovatel digitálních služeb hlásí kybernetický bezpečnostní incident, určuje národní CERT.*

K § 8 odst. 4
*Navrženou úpravou ustanovení § 8 odst. 5 se transponuje čl. 14 odst. 3 směrnice, kdy se adresátem hlášení kybernetického bezpečnostního incidentu, který nastal u provozovatele základních služeb, určuje NBÚ. Zároveň se text ustanovení legislativně technicky upravuje, neboť legislativní zkratka „Úřad" byla zavedena již v § 2.*

K § 8 odst. 6
*Navrhované ustanovení, že i orgány a osoby neuvedené v § 3 mohou v případě svého zájmu hlásit kybernetické bezpečnostní incidenty, a to dle vlastního vyhodnocení situace buď provozovateli národního CERT, nebo NBÚ. Náležitosti a způsob hlášení bude stanovovat prováděcí právní předpis.*

K § 8 odst. 7
*Upravuje se zmocňovací k vydání prováděcího právního předpisu, který bude stanovovat významnost dopadu kybernetického bezpečnostního incidentu.*

K § 8 odst. 8
*Toto ustanovení zavádí do českého právního řádu článek 16 odst. 5 směrnice. Navrhovaný odstavec 5 tedy řeší situaci, kdy kybernetickým bezpečnostním incidentem je postižen poskytovatel digitálních služeb, na jehož službách je závislé provozování základních služeb. V tomto případě se ukládá povinnost provozovatele základních služeb informovat o významném dopadu incidentu na kontinuitu poskytování těchto základních služeb NBÚ, neboť právě pouze poskytovatel základní služby je schopen posoudit míru dopadu incidentu.*

K pojmu **kybernetický bezpečnostní incident** blíže viz kap. 2.4.3.

**K odst. 1)**
K pojmu **Významná síť** elektronických komunikací viz § 2 písm. h) ZoKB.
K pojmu **informační systém** viz § 1 ZoKB.
K pojmům **informační systém kritické informační infrastruktury**, **komunikační systém kritické informační infrastruktury**, **informační systém základní služby nebo významný informační systém** viz § 2 písm. b), d), j) ZoKB.

Hlásit kybernetický bezpečnostní incident musí osoby uvedené v § 3 písm. b) až f) buď národnímu, či vládnímu CERT, dle stanovení ohlašovací povinnosti (viz § 7 ZoKB).

Kybernetický bezpečností incident musí být nahlášen **bezodkladně po jeho detekci.**

Pojem **bezodkladně** je třeba vykládat tak, že **lhůta bez zbytečného odkladu přímo neurčuje, v jakém konkrétním časovém okamžiku je třeba konat.**

Bezodkladně tedy **nemusí nutně znamenat, že je třeba konat ihned**, na druhou stranu **u jakéhokoliv odkladu konání, který nastane, je třeba vždy v každém jednotlivém případě zjistit, zda se nejedná o odklad zbytečný, a to s přihlédnutím ke konkrétním okolnostem daného případu.**[357]

Z pohledu kybernetické bezpečnosti by lhůta bezodkladně byla zřejmě dodržena i v okamžiku, kdy by povinná osoba nahlásila požadované informace o kybernetickém bezpečnostním incidentu teprve tehdy, až by zamezila probíhajícímu incidentu. V takovém případě by se bylo možné odkázat i na kategorizaci kybernetických bezpečnostních incidentů, konkrétně na významný kybernetický bezpečnostní incident, který vyžaduje neprodlené zásahy obsluhy s tím, že musí být všemi dostupnými prostředky zabráněno dalšímu šíření kybernetického bezpečnostního incidentu včetně minimalizace vzniklých i potenciálních škod.

Podmínkou pro neporušení dikce zákona by v daném případě byla i ta skutečnost, že tento konkrétní incident by byl směřován na zájmy výhradně napadeného subjektu a nikoho jiného.

Pokud by docházelo současně i k napadání zájmů jiných subjektů, respektive by hrozily jiné potencionální škody, pak se jako vhodný postup jeví realizace neprodlených zásahů obsluhy současně s předáváním informací o kybernetickém bezpečnostním incidentu týmu CERT, a to i například telefonicky (pokud to časová tíseň, závažnost, či jiná okolnost vyžaduje).

Vedle povinnosti reportovat kybernetický bezpečnostní incident národnímu či vládnímu CERT zde existují i povinnosti vyplývající z jiného právního předpisu.

Zákon o kybernetické bezpečnosti explicitně odkazuje na § 98 odst. 4 ZoEK, kde je uvedeno, že *„**o závažném narušení bezpečnosti a ztrátě integrity sítě, rozsahu a důvodech přerušení** poskytování služby nebo odepření přístupu k ní, přijatých opatřeních a o předpokládaném termínu odstranění příčiny **je podnikatel** zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací **povinen bezodkladně informovat Úřad (ČTÚ), subjekty provozující pracoviště pro příjem tísňového volání a** vhodným způsobem i **uživatele.**“* Dále je také odkázáno na § 99 odst. 4 ZoKB, kde je řešena situace ohrožení nebo narušení bezpečnosti a integrity sítě a bezpečnosti služeb za krizového stavu. V takovém případě je podnikatel zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací, u nějž se ohrožení nebo narušení bezpečnosti a integrity sítě a bezpečnosti služeb vyskytne, povinen

357: Blíže viz např. Rozsudek Nejvyššího soudu 30 Cdo 530/2014, ze dne 30. 7. 2015. [online]. [cit. 8. 7. 2016]. Dostupné z: https://www.mfcr.cz/assets/cs/media/Metodika-Pr-002_2016_Rozsudek-Nejvyssiho-soudu-CR-ze-dne-30-7-2015.pdf

o této skutečnosti bezodkladně informovat Úřad (ČTÚ). Český telekomunikační úřad musí být dále informován o přijatých nebo zamýšlených opatřeních k nápravě a o předpokládaném termínu odstranění příčiny.

Obdobně je stanovena povinnost oznamovat případy porušení zabezpečení osobních údajů subjektu údajů (viz čl. 34 GDPR) a dozorovému úřadu (viz čl. 33 GDPR a recitál 85).

V případě, že **kybernetický bezpečnostní incident má významný dopad na kontinuitu poskytování základní služby, oznámí to provozovatel základní služby Úřadu** (NÚKIB).

K pojmu **významný dopad** viz § 7 odst. 2) ZoKB.

**K odst. 2)**
Ustanovení § 8 odst. 2 ZoKB reaguje na povinnosti uložené směrnicí NIS v čl. 16 odst. 3 a 4 poskytovatelům digitálních služeb. Konkrétně se jedná o:

- povinnost hlásit příslušnému orgánu nebo týmu CERT/CSIRT incidenty, které mají významný dopad na poskytování digitální služby, kterou nabízejí poskytovatelé těchto služeb v rámci Unie.

Vlastní hlášení musí obsahovat takové informace umožňující posoudit (příslušnému orgánu nebo týmu CERT/CSIRT) významnost případného přeshraničního dopadu daného incidentu.[358]

Směrnice NIS současně stanoví parametry, ke kterým se přihlédne při posuzování toho, zda je dopad incidentu významný. Dle čl. 16 odst. 4 NIS se jedná o:
- počet uživatelů postižených incidentem, zejména těch uživatelů, kteří na službu spoléhají při poskytování vlastních služeb,
- délku trvání incidentu,
- zeměpisný rozsah oblasti dotčené incidentem,
- rozsah, v jakém bylo narušeno fungování služby,
- rozsah dopadu na společenské a ekonomické činnosti.

Jak ve směrnici NIS, tak v ZoKB je ohlašovací povinnost zmírněna podmínkou, dle které jsou poskytovatelé digitálních služeb povinni incident hlásit pouze v případě, že mají přístup k informacím, které jsou nezbytné k posouzení dopadu incidentu na základě výše uvedených parametrů.

358: Čl. 16 odst. 3 NIS

**K odst. 3) a 4)**
**Ohlašovací povinnost** jednotlivých subjektů viz § 7 ZoKB a § 3 ZoKB.

**K odst. 5)**
Ustanovení § 8 odst. 5 ZoKB navazuje na možnost uvedenou v § 6a ZoKB, dle které je možné pověřit provozováním informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému jiný orgán nebo osobu, pokud to jiný zákon nevylučuje.

V případě, že takovýto systém je provozován jinou osobou než správcem, je nanejvýš vhodné, aby nahlášení kybernetického bezpečnostního incidentu Úřadu (vládnímu CERT) či národnímu CERT provedl právě provozovatel.

Nicméně § 8 odst. 5 ZoKB tuto povinnost explicitně nepřenáší na provozovatele systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému, ale uvádí, že pokud tento provozovatel ohlásí kybernetický bezpečnostní incident dotčenému CERT týmu, tak je povinnost správce splněna.

Pokud však provozovatel ohlášení neprovede, je na správci, aby tak učinil. **Provozovateli systému** kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému **je** v § 8 odst. 5 věta druhá ZoKB **uložena povinnost o ohlášených kybernetických bezpečnostních incidentech bez zbytečného odkladu informovat správce těchto systémů.**

Vlastní delegace ohlašovací povinnosti mezi správcem a provozovatelem výše uvedených systémů by měla být ošetřena smluvně.

**K odst. 6)**
**Zákon o kybernetické bezpečnosti umožňuje i jiným subjektům** (fyzickým či právnickým osobám) než uvedeným v § 3 ZoKB **hlásit kybernetické bezpečnostní incidenty národnímu či vládnímu CERT.**

**K odst. 7)**
Ustanovení § 31 VoKB stanovuje typy, kategorie a hodnocení významnosti dopadu kybernetického bezpečnostního incidentu.[359] Forma a náležitosti hlášení kybernetických bezpečnostních incidentů jsou uvedeny v § 32 VoKB.

Pokud se kybernetický bezpečnostní incident **hlásí Úřadu (vládní CERT)**, je třeba jej hlásit:

359: Blíže viz § 7 odst. 2 ZoKB

- pomocí formuláře zveřejněného na internetových stránkách Úřadu (vládní CERT)
- na adresu elektronické pošty Úřadu určenou pro příjem hlášení kybernetických bezpečnostních incidentů, zveřejněnou na internetových stránkách Úřadu,
- do datové schránky Úřadu,
- prostřednictvím datového rozhraní, pokud je používáno, jehož popis je zveřejněn na internetových stránkách Úřadu.

Ustanovení § 32 odst. 3 VoKB umožňuje zaslat hlášení kybernetického bezpečnostního incidentu i v listinné podobě, avšak pouze v případech, kdy nelze využít žádný z výše uvedených způsobů.

**Náležitostmi hlášení kybernetického bezpečnostního incidentu jsou identifikace odesílatele, identifikace informačního a komunikačního systému, datum a čas zjištění incidentu a popis incidentu.**

**Doplňující informace:**

- formulář je dostupný na: https://www.govcert.cz/download/kii-vis/container-nodeid-649/incidentreportnckb.pdf
- hlášení incidentů: cert.incident@nukib.cz
- v případě nenadálé a vážné situace, kdy hrozí riziko z prodlení, lze pro kontaktování týmu GovCERT.CZ v pracovní době využít telefonní spojení na čísle +420 541 110 777
- mimo standardní pracovní dobu pak na telefonním čísle +420 725 502 878
- Podávání písemností: Národní úřad pro kybernetickou a informační bezpečnost, P. O. Box 17, Brno 16, 616 00
- Podávání utajovaných písemností pouze přes podatelnu v Praze: NÚKIB, Na Popelce 2/16, Praha 5 – Smíchov, 150 00
- IČ: 05800226
- ID datové schránky: zzfnkp3
- Bankovní spojení: 3031881 / 0710
- E-mailová adresa elektronické podatelny: posta@nukib.cz

Pokud se kybernetický bezpečnostní incident **hlásí provozovateli národního CERT** (sdružení CZ.NIC), je třeba jej hlásit:

- pomocí formuláře zveřejněného na internetových stránkách provozovatele národního CERT
  - na adresu elektronické pošty provozovatele národního CERT určenou pro příjem hlášení kybernetických bezpečnostních incidentů, zveřejněnou na internetových stránkách,
  - do datové schránky provozovatele národního CERT,
  - prostřednictvím internetových stránek provozovatele národního CERT.

Ustanovení § 32 odst. 3 VoKB umožňuje zaslat hlášení kybernetického bezpečnostního incidentu i v listinné podobě, avšak pouze v případech, kdy nelze využít žádný z výše uvedených způsobů.

**Náležitostmi hlášení kybernetického bezpečnostního incidentu jsou identifikace odesílatele, identifikace informačního a komunikačního systému, datum a čas zjištění incidentu a popis incidentu.**

- **Doplňující informace:**
  - formulář je dostupný na: https://www.csirt.cz/stateincidentreport/
  - e-mailová adresa pro hlášení bezpečnostních incidentů: abuse@csirt.cz
  - je možné využít i telefonický kontakt: +420 910 101 010 (každý pracovní den od 09:00–17:00 hod.)
  - v urgentních případech je mimo pracovní dobu možné využít telefonní číslo +420 222 745 111
- popis týmu dle RFC2350 platný od 6. 8. 2018 je dostupný na: https://www.nic.cz/files/csirt/rfc2350_CSIRT.CZ.2018_06_08.pdf
- PGP klíč:
  - User ID: CSIRT.CZ Abuse team abuse@csirt.cz
  - KeyID: 0x6622 A373
  - Key size: 4096
  - Key fingerprint = 7071 8BB4 0939 AB7D 4E39 4EFD 63A1 D634 6622 A373
- Podávání písemností: CZ.NIC, zájmové sdružení právnických osob, Milešovská 1136/5, 130 00 Praha 3
- IČ: 67985726
- ID datové schránky: h4axdn8
- Bankovní spojení: 276463778/0300
- Další kontaktní údaje: https://www.nic.cz/page/357/

**K odst. 8)**
Ustanovení § 8 odst. 8 ZoKB řeší situaci, kdy je kybernetickým bezpečnostním incidentem postižen poskytovatel digitálních služeb, na jehož službách je závislé provozování základních služeb.

V takovém případě, je povinnost informovat o kybernetickém bezpečnostním incidentu delegována na provozovatele základních služeb, neboť pouze tento provozovatel je schopen posoudit míru dopadu incidentu.

Provozovatel základních služeb informuje výše popsaným způsobem vládní CERT.

**Evidence**
**§ 9**

**(1) Úřad vede evidenci kybernetických bezpečnostních incidentů (dále jen „evidence incidentů"), která obsahuje**
- **a) hlášení kybernetického bezpečnostního incidentu,**
- **b) identifikační údaje systému, ve kterém se kybernetický bezpečnostní incident vyskytl,**
- **c) údaje o zdroji kybernetického bezpečnostního incidentu a**
- **d) postup při řešení kybernetického bezpečnostního incidentu a jeho výsledek.**

**(2) Součástí evidence incidentů jsou údaje podle § 20 písm. f) až h) a l).**
**(3) Úřad poskytuje údaje z evidence incidentů orgánům veřejné moci pro výkon jejich působnosti.**
**(4) Úřad může poskytovat údaje z evidence incidentů provozovateli národního CERT, orgánům vykonávajícím působnost v oblasti kybernetické bezpečnosti v zahraničí a jiným osobám působícím v oblasti kybernetické bezpečnosti v rozsahu nezbytném pro zajištění ochrany kybernetického prostoru.**

Z důvodové zprávy:

*Účelem tohoto ustanovení je založit právo a povinnost NBÚ vést evidenci kybernetických bezpečnostních incidentů. Struktura údajů taxativním výčtem je zvolena tak, aby umožňovala evidovat údaje nutné k následné formální a obsahové analýze kybernetických bezpečnostních incidentů. Výstupy této analýzy budou sloužit jako důležitý podklad pro činnosti NBÚ v oblasti kybernetické bezpečnosti upravenými tímto zákonem.*

*Údaje v evidenci kybernetických bezpečnostních incidentů mají velkou vypovídací hodnotu o činnosti dohledových pracovišť a o kybernetické bezpečnostní situaci České republiky, jakož i o jednotlivých povinných osobách. Současně mohou být tyto údaje vysoce důležité pro výkon funkcí orgánů veřejné moci, národního dohledového pracoviště nebo pro činnost zahraničních spolupracujících soukromoprávních nebo veřejnoprávních institucí působících v oblasti kybernetické bezpečnosti. Předávání údajů z evidence kybernetických bezpečnostních incidentů je proto zákonem regulováno, respektive omezeno. Orgánům veřejné moci (typicky např. orgánům činným v trestním řízení, Českému telekomunikačnímu úřadu, zpravodajským službám) lze údaje z evidence kybernetických bezpečnostních incidentů poskytnout pouze pro plnění úkolů v rámci jejich působnosti. Předávání těchto údajů dalším subjektům, (např. národnímu CERT, zahraničním subjektům působícím v oblasti kybernetické bezpečnosti) pak lze na základě správního uvážení NBÚ, a to pouze v rozsahu nezbytném pro ochranu kybernetického prostoru.*

*Toto ustanovení upravuje další poskytování údajů z evidence kybernetických bezpečnostních incidentů ze strany NBÚ v případech vyjma předávání těchto údajů orgánům veřejné moci, provozovateli národního CERT, orgánům vykonávajícím působnost v oblasti kybernetické bezpečnosti v zahraničí*

*a jiným subjektům působícím v oblasti kybernetické bezpečnosti a dopadá tedy na případy, kdy má NBÚ právo nebo povinnost předávat tyto údaje na základě jiných právních předpisů.*

*Jak je uvedeno výše, údaje vedené v evidenci kybernetických bezpečnostních incidentů mají mimo jiné též velký význam pro bezpečnostní reputaci a pro fungování bezpečnostních opatření jednotlivých povinných osob. Aby nedošlo k nedůvodnému zásahu do oprávněných zájmů povinných osob nebo ke zmaření účelu bezpečnostních opatření podle tohoto zákona, je poskytování těchto údajů omezeno jen na takové, z nichž nelze určit totožnost oznamovatele. NBÚ je dále oprávněn omezit poskytování údajů z evidence kybernetických bezpečnostních incidentů v případech, kdy by důsledek jejich poskytnutí představoval riziko pro faktickou realizaci protiopatření.*
Z důvodové zprávy k novele ZoKB:

K § 9 odst. 2
*Podle současné právní úpravy uchovává Úřad v evidenci incidentů informace o incidentech hlášených povinnými osobami podle zákona o kybernetické bezpečnosti. Vzhledem k tomu, že se nově v § 20 odst. 2 písm. l) rozšiřuje kompetence vládního CERT o přijímání dobrovolných hlášení kybernetických bezpečnostních incidentů, začleňují se informace o těchto hlášeních i do evidence vedené Úřadem podle § 9.*

**K odst. 1)**
Národní úřad pro kybernetickou a informační bezpečnost má na základě § 9 ZoKB povinnost vést evidenci kybernetických bezpečnostních incidentů.

K pojmu **kybernetický bezpečnostní incident** blíže viz kap. 2.4.3.

Tato evidence obsahuje:

- vlastní **hlášení kybernetického bezpečnostního incidentu** obsahující:
  - identifikaci odesílatele,
  - datum a čas zjištění incidentu,
  - popis incidentu.

- **identifikační údaje** počítačového **systému**, ve kterém se kybernetický bezpečnostní incident vyskytl,

- údaje o zdroji či příčině kybernetického bezpečnostního **incidentu,**

- **postup popisující** řešení kybernetického bezpečnostního **incidentu** a jeho výsledek.

Tento výčet je taxativní.

Evidovat výše uvedené údaje je významné z několika hledisek. Relevantní informace o kybernetickém bezpečnostním incidentu (zpravidla bez uvedení informací o oběti incidentu) je možné předat dalším bezpečnostním týmům typu CERT/CSIRT či jiným dotčeným subjektům. Dále je možné na základě těchto informací vydat například varování. V neposlední řadě mohou údaje z evidence sloužit ke stanovení dalších postupů a strategií vedoucích k zajištění kybernetické bezpečnosti v ČR.

*„Evidence záznamů o výskytu a řešení kybernetických bezpečnostních incidentů nesměřuje k identifikaci jednotlivých osob. Právní úprava je konstruována tak, aby detekční nebo obranné mechanismy nebylo možné zneužít ke sledování uživatelů služeb informační společnosti. Toto řešení je v souladu se zásadou práva na informační sebeurčení* [360]*, na kterém je zákon o kybernetické bezpečnosti založen.“* [361]

Vzhledem k obsahu evidence je zřejmé, že obsahuje řadu dat, která lze považovat za osobní údaje.[362] Národní úřad pro kybernetickou a informační bezpečnost je povinen takováto data chránit a zacházet s nimi v souladu s podmínkami a pravidly stanovenými v GDPR.[363]

**K odst. 2)**
Součástí evidence, která je NÚKIB vedena jsou i následující údaje:

- podněty a údaje od orgánů a osob uvedených v § 3 ZoKB,
- podněty a údaje od jiných orgánů a osob,
- údaje od provozovatele národního CERT,
- údaje od orgánů, které vykonávají působnost v oblasti kybernetické bezpečnosti v zahraničí,
- hlášení o kybernetickém bezpečnostním incidentu od orgánů a osob neuvedených v § 3 ZoKB.

**K odst. 3)**
Národní úřad pro kybernetickou a informační bezpečnost je na základě tohoto zákonného zmocnění oprávněn poskytovat údaje ze své evidence jiným orgánům veřejné moci pouze pro výkon jejich působnosti.

Vlastní regulace možnosti poskytnout data a informace z evidence NÚKIB je opět postavena na principu ochrany informačního sebeurčení člověka. Na druhou stranu existují situace, za

360: Blíže viz kap. 4.2 Základní cíle a principy ZoKB

361: MAISNER, Martin a Barbora VLACHOVÁ. *Zákon o kybernetické bezpečnosti. Komentář.* Praha: Wolters Kluwer, 2015. 106

362: Blíže viz kap. 3.3.1.2 Osobní údaj

363: Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

kterých je třeba krom řešení kybernetických bezpečnostních incidentů realizovat i další kroky ze strany státu spočívající například v dohledání a potrestání útočníka, který takovýto incident inicializoval.

Mezi orgány veřejné moci, kterým lze údaje z evidence kybernetických bezpečnostních incidentů poskytnout patří např. orgány činné v trestním řízení (policejní orgán, státní zástupce, soud), Policie ČR, GIBS, Celní správa, zpravodajské služby, Český telekomunikační úřad, Úřad pro ochranu osobních údajů aj.

**Nezbytnou podmínkou** pro **poskytnutí těchto údajů je, že** dotčené **orgány** veřejné moci **potřebují takové údaje pro výkon své působnosti.**

**K odst. 4)**
Vedle poskytnutí údajů z evidence orgánům veřejné moci připouští ZoKB fakultativní možnost spočívající v poskytnutí takovýchto údajů i dalším subjektům, mezi které patří:

- **provozovatel národního CERT,**
- **orgány vykonávající působnost v oblasti kybernetické bezpečnosti v zahraničí,**
- **jiné osoby působící v oblasti kybernetické bezpečnosti.**

**Těmto subjektům mohou být poskytnuty informace v takovém rozsahu, který je nezbytný pro zajištění ochrany kybernetického prostoru.**

V tomto případě je zpravidla ještě více respektován princip ochrany informačního sebeurčení člověka, než jak tomu je v případě § 9 odst. 3 ZoKB.

**§ 10**

**(1) Zaměstnanci České republiky zařazení k výkonu práce v Úřadu, kteří se podílejí na řešení kybernetického bezpečnostního incidentu, jsou vázáni povinností mlčenlivosti o údajích z evidence incidentů. Povinnost mlčenlivosti trvá i po skončení pracovněprávního vztahu k Úřadu.**
**(2) Ředitel Úřadu může osoby podle odstavce 1 zprostit povinnosti mlčenlivosti o údajích z evidence incidentů, s uvedením rozsahu údajů a rozsahu zproštění.**

Z důvodové zprávy:

*Návrh ustanovení upravuje individuální povinnost mlčenlivosti zaměstnanců NBÚ vzhledem k údajům tvořícím evidenci kybernetických bezpečnostních incidentů. Účelem tohoto ustanovení je zamezit možnému úniku těchto údajů prostřednictvím zaměstnanců NBÚ, kteří s nimi budou přicházet do styku, a tím umožnit předávání a další užití těchto údajů výlučně způsoby upravenými*

*v předchozích ustanoveních. V odůvodněných případech je ředitel NBÚ oprávněn zbavit zaměstnance mlčenlivosti, a to ve vztahu ke konkrétně určeným údajům a ke konkrétním způsobům jejich dalšího užití.*

**K odst. 1)**
Ustanovení § 10 odst. 1 ZoKB specificky **zavazuje zaměstnance NÚKIB, kteří se podílejí na řešení kybernetického bezpečnostního incidentu, povinností mlčenlivosti o těchto incidentech a dalších údajích z evidence údajů**.

Obecná povinnost mlčenlivosti pro pracovníky NÚKIB při jiných činnostech než je řešení kybernetického bezpečnostního incidentu vyplývá i z § 303 dost. 1 písm. a) zákona č. 262/2006 Sb., zákoník práce[364], kde je uvedeno, že zaměstnanci ve správních úřadech jsou s odkazem na § 303 odst. 2 písm. b) zákoníku práce povinni „***zachovávat mlčenlivost o skutečnostech, o nichž se dozvěděli při výkonu zaměstnání a které v zájmu zaměstnavatele nelze sdělovat jiným osobám…***"

Specifické rozšíření povinnosti mlčenlivosti uvedené v § 10 odst. 1 ZoKB, nad rámec obecné povinnosti stanovené zákoníkem práce, je dle našeho názoru na místě, neboť pracovníci podílející se na řešení kybernetických bezpečnostních incidentů se mohou dostat k informacím či datům, která mohou být pro oběť tohoto incidentu velmi citlivá. Takováto data je třeba chránit a zamezit jejich případnému zneužití i v případě, že se nebude jednat o data podléhající ochraně podle jiného právního předpisu (např. GDPR aj.)

**Povinnost mlčenlivosti trvá i po skončení pracovněprávního vztahu k NÚKIB.**

K pojmu **evidence** viz § 9 ZoKB.

**K odst. 2)**
„*Zproštění mlčenlivosti bývá typicky vyžadováno v případech, kdy může svědectví zaměstnance vést k objasnění skutečností, typicky například ve správních, trestních či občanskoprávních řízeních.*" [365]

Ustanovení § 303 odst. 2 písm. b) věta druhá zákoníku práce umožňuje, aby byli zaměstnanci ve správních úřadech zproštěni povinnosti mlčenlivosti. Zbavit povinnosti mlčenlivosti je oprávněn statutární orgán nebo jím pověřený vedoucí zaměstnanec, nestanoví-li zvláštní právní předpis jinak.

364: Dále jen **zákoník práce**

365: MAISNER, Martin a Barbora VLACHOVÁ. *Zákon o kybernetické bezpečnosti. Komentář.* Praha: Wolters Kluwer, 2015. s. 107

V případě ustanovení § 10 odst. 2 ZoKB **mohou být zaměstnanci** NÚKIB, kteří se podílejí na řešení kybernetického bezpečnostního incidentu, **zproštěni povinnosti mlčenlivosti toliko ředitelem NÚKIB.** Ředitel též stanoví rozsah údajů a rozsah zproštění.

Povinnost mlčenlivosti trvá i po skončení pracovněprávního vztahu k NÚKIB. V případě, že je třeba zprostit povinnosti mlčenlivosti osobu, která již není v pracovně právním vztahu k NÚKIB, řeší se tato situace obdobně.

**§ 10a**

**Informace, jejichž zpřístupnění by mohlo ohrozit zajišťování kybernetické bezpečnosti nebo účinnost opatření vydaného podle tohoto zákona, nebo informace, které jsou vedené v evidenci incidentů, ze kterých by bylo možné identifikovat orgán nebo osobu, která kybernetický bezpečnostní incident ohlásila, se podle předpisů upravujících svobodný přístup k informacím neposkytují.**

Z důvodové zprávy k novele ZoKB:

*Navržená úprava vychází ze stávající právní úpravy omezující poskytování informací podle zákona o svobodném přístupu k informacím. Tato úprava obsažená v § 11 odst. 4 zmiňovaného zákona však cílí pouze na úzký okruh informací, konkrétně na informace z evidence incidentů vedené podle § 9 zákona o kybernetické bezpečnosti.*

*Tato úprava byla dle předkladatele tohoto návrhu zákona velmi omezená již v době přijímání zákona o kybernetické bezpečnosti. V současné době, kdy již bylo určeno 155 významných informačních systémů, spravovaných 58 subjekty, a 48 systémů kritické informační infrastruktury, jejichž správci jsou orgány veřejné správy, tedy potenciálních povinných subjektů podle zákona o svobodném přístupu k informacím, a kdy roste počet útoků v kybernetickém prostoru, je zapotřebí přistoupit k opatření i v obecnější rovině zajišťování kybernetické bezpečnosti. Je zapotřebí zdůraznit, že v současnosti účinná výjimka uvedená v § 11 odst. 4 písm. f) zákona o svobodném přístupu k informacím nenaplňuje požadavky na ochranu citlivých informací, zejména těch, které se vztahují k přijatým bezpečnostním opatřením podle zákona o kybernetické bezpečnosti. Potenciální útočník by tak v současné době mohl požádat podle tohoto zákona správce informačních nebo komunikačních systémů kritické informační infrastruktury nebo správce významných informačních systémů o poskytnutí informací o přijatých bezpečnostních opatřeních, přičemž tento povinný subjekt by byl povinen je poskytnout. Z tohoto důvodu se předkladatel rozhodl, i v souladu s čl. 1 odst. 6 směrnice (Touto směrnicí nejsou dotčena opatření, jež členské státy přijímají s cílem zabezpečit své základní státní funkce, zejména pokud jde o zajištění národní bezpečnosti, včetně opatření na ochranu informací, jejichž zpřístupnění členské státy považují za neslučitelné s podstatnými zájmy své bezpečnosti, a zachování veřejného pořádku, zejména pokud jde o umožnění vyšetřování, odhalování a stíhání trestné činnosti.) a recitály 2 (Rostoucí rozsah, četnost výskytu a dopad bezpečnostních incidentů představují pro fungování sítí a informačních systémů významnou*

*hrozbu. Uvedené systémy se rovněž mohou stát snadným cílem úmyslných škodlivých akcí za účelem poškození nebo narušení provozu systémů. ...) a č. 8 (Touto směrnicí by neměla být dotčena možnost jednotlivých členských států přijmout nezbytná opatření, aby zajistily ochranu podstatných zájmů své bezpečnosti, ochranu veřejného pořádku a veřejné bezpečnosti a umožnily vyšetřování, odhalování a stíhání trestných činů. …) směrnice pro doplnění výjimky z povinnosti poskytovat informace na základě zákona o svobodném přístupu k informacím o údaje, které se týkají zajišťování kybernetické bezpečnosti podle zákona o kybernetické bezpečnosti.*

*Informace, které není v zájmu zajišťování kybernetické bezpečnosti možné poskytovat, mohou být například následující:*

- *schémata, plány budov,*
- *technické specifikace (např. topologie sítě),*
- *konfigurační parametry,*
- *havarijní plány.*

*Podle tohoto návrhu zákona se také neposkytují informace, jejichž zpřístupnění by mohlo ohrozit účinnost opatření vydaného podle tohoto zákona. Těmito opatřeními jsou varování, reaktivní opatření a ochranná opatření. Jedná se o instituty, jejichž zveřejnění ne vždy může ohrozit jejich účinnost, případně mít dopad na zajišťování kybernetické bezpečnosti, z tohoto důvodu jsou v návrhu ustanovení § 10a uvedeny zvlášť.*

*Předkladatel návrhu zákona se domnívá, že toto omezení práva na informace je plně v souladu s čl. 17 odst. 4 Listiny základních práv a svobod, když dospěl k názoru, že v oblasti kybernetické bezpečnosti, která hraje v oblasti bezpečnosti státu stále důležitější roli, převážil požadavek na zajištění bezpečnosti státu a veřejné bezpečnosti, přičemž považuje za nutné konstatovat, že povinný subjekt bude vždy při rozhodování o žádosti o poskytnutí informací povinen posoudit, zda by opravdu poskytnutí požadované informace mohlo ohrozit zajišťování kybernetické bezpečnosti a pečlivě v daném případě zvažovat potřebu omezení práva na informace.*

*Vzhledem ke specifičnosti oblasti kybernetické bezpečnosti byla výjimka z povinnosti poskytovat informace podle zákona o svobodném přístupu k informacím nově začleněna, obdobně jako je tomu i v některých dalších právních předpisech (srov. např. § 40 zákona o obcích, § 3b zákona o České národní bance, § 27 odst. 2 krizového zákona), přímo do zákona o kybernetické bezpečnosti.*

Obecná povinnost poskytovat fyzickým či právnickým osobám informace vyplývá ze zákona č. 106/1999 Sb., o svobodném přístupu k informacím, kde je v § 2 odst. 1 uvedeno, že povinná osoba (tomto případě: státní orgány, územní samosprávné celky a jejich orgány a veřejné instituce) má podle tohoto zákona povinnost poskytovat informace vztahující se k jejich působnosti.

Nicméně i v ustanovení § 2 odst. 3 zákona č. 106/1999 Sb., o svobodném přístupu k informacím je uvedeno, že tento *„zákon se nevztahuje na poskytování informací … **dalších informací, pokud zvláštní zákon upravuje jejich poskytování**, zejména vyřízení žádosti včetně náležitostí a způsobu podání žádosti, lhůt, opravných prostředků a způsobu poskytnutí informací.“*

Dále je specificky v § 11 odst. 4 písm. f) zákona č. 106/1999 Sb., o svobodném přístupu k informacím uvedeno, že *„povinné subjekty dále **neposkytnou informace o údajích vedených v evidenci incidentů podle zákona o kybernetické bezpečnosti**, ze kterých bylo možné identifikovat orgán nebo osobu, která kybernetický bezpečnostní incident ohlásila, nebo jejichž poskytnutí by ohrozilo účinnost reaktivního nebo ochranného opatření podle zákona o kybernetické bezpečnosti.“*

Dle § 10a ZoKB se neposkytují informace, které by:

- umožnily identifikovat orgán nebo osobu, která kybernetický bezpečnostní incident ohlásila,
- mohly ohrozit zajišťování kybernetické bezpečnosti nebo účinnost opatření vydaného podle ZoKB.

Vzhledem k právu neposkytnout informace žádajícímu subjektu je třeba zdůraznit tu skutečnost, že **neposkytnutí informací musí být řádně a prokazatelně odůvodněno** a musí vycházet ze zákonných důvodů.

*„Národní úřad pro kybernetickou a informační bezpečnost má za to, že **pro posouzení a správné užití první části ustanovení § 10a ZoKB** (tedy možné ohrožení zajišťování kybernetické bezpečnosti nebo možné ohrožení účinnosti opatření vydaného podle ZoKB) **je velmi vhodným institutem správně provedená vnitřní klasifikace informací v rámci hodnocení aktiv podle vyhlášky č. 82/2018 o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat.**“* [366]

V rámci posuzování, zda požadované informace (aktiva) poskytnout či nikoliv, by mělo primárně dojít ke kvalifikaci důvěrnosti informací dle přílohy č. 1 VoKB.[367] Dle této vyhlášky jsou aktiva z hlediska důvěrnosti rozčleněny do 4 kategorií:

1) nízká,
2) střední,
3) vysoká,
4) kritická.

366: *Doporučení NÚKIB k ustanovení § 10a zákona o kybernetické bezpečnosti.* [online]. [cit. 1.8.2018]. Dostupné z: https://nukib.cz/download/kii-vis/Ustanoven%C3%AD_para10a_ZKB_a_utajovane_informace_v1-1_web.pdf s. 4

367: Blíže viz kap. 2.2.1 Triáda CIA

Dle doporučení NÚKIB **je vhodné uvažovat o použití § 10a ZoKB v případě, že je informace** z hlediska důvěrnosti **hodnocena jako vysoká či kritická** a zpřístupněním takové informace by mohlo dojít k narušení kybernetické bezpečnosti. Tímto způsobem je vhodné ohodnotit například technickou či bezpečnostní dokumentaci.

*„Pokud informace není hodnocena z pohledu důvěrnosti na úroveň vysoká nebo kritická, nabízejí se dvě varianty.* ***První je, že informace takového významu*** *z pohledu zajišťování kybernetické bezpečnosti* ***nedosahuje, tedy není možné využít ustanovení § 10a ZoKB a není možné ji z tohoto důvodu neposkytnout. Druhou je, že informace reálně může ohrozit zajišťování kybernetické bezpečnosti, ale není příslušně hodnocena*** *a tedy lze předpokládat, že byla nevhodně hodnocena důležitost aktiv, v důsledku čehož došlo k neplnění nebo nedostatečnému plnění povinností uložených § 4 odst. 2 ZoKB.*

*Je potřeba upozornit, že* ***při případném soudním řízení o oprávněnosti neposkytnutí informace podle § 10a ZoKB jsou předmětem soudního přezkumu zejména důvody neposkytnutí informací, tedy také to, zda informace naplní definici tohoto ustanovení zákona****. Argumentace prostřednictvím klasifikace informací při hodnocení aktiv se tak prima vista jeví jako nezbytná. Avšak vzhledem k tomu, že dosud neexistuje soudní praxe k uplatňování této výjimky z práva na informace ve vztahu ke kybernetické bezpečnosti, lze jen stěží předpokládat, zda soudy zaujmou restriktivní výklad při využití § 10a ZoKB nebo budou naopak akcentovat bezpečností aspekty chráněných bezpečnostních zájmů, a to nejen u hraničních případů.“* [368]

Poslední možností, uváděnou NÚKIB, jak citlivé nebo důležité informace chránit, je jejich utajení na základě zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti a nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací.[369]

### § 11
### Opatření

**(1) Opatřeními se rozumí úkony, jichž je třeba k ochraně informačních systémů nebo služeb a sítí elektronických komunikací[370] před hrozbou v oblasti kybernetické bezpečnosti nebo před kybernetickým bezpečnostním incidentem anebo k řešení již nastalého kybernetického bezpečnostního incidentu.**
**(2) Opatřeními jsou**
- **a) varování,**
- **b) reaktivní opatření a**

368: *Doporučení NÚKIB k ustanovení § 10a zákona o kybernetické bezpečnosti.* [online]. [cit. 1. 8. 2018]. Dostupné z: https://nukib.cz/download/kii-vis/Ustanoven%C3%AD_para10a_ZKB_a_utajovane_informace_v1-1_web.pdf s. 4–5

369: Tamtéž s. 6 a násl.

370: Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů.

**c) ochranné opatření.**

**(3) Reaktivní opatření jsou povinny provádět**

**a) orgány a osoby uvedené v § 3 písm. a) a b) za stavu kybernetického nebezpečí nebo za nouzového stavu[371] vyhlášeného na základě žádosti podle § 21 odst. 6 a**

**b) orgány a osoby uvedené v § 3 písm. c) až f).**

**(4) Ochranné opatření jsou povinny provádět orgány a osoby uvedené v § 3 písm. c) až f).**

Z důvodové zprávy:

*Ustanovení upravuje definici protiopatření jako součásti systému k zajištění kybernetické bezpečnosti. Definice protiopatření je provedena za užití obsahového kritéria, tj. účelu ochrany kybernetického prostoru před hrozbou v oblasti kybernetické bezpečnosti nebo před kybernetickým bezpečnostním incidentem anebo k řešení kybernetického bezpečnostního incidentu, který již nastal.*

*Cílem takto stanovené struktury protiopatření je pokrýt jednak formou varování potřebu oficiálního preventivního působení NBÚ vzhledem k aktuálním kybernetickým bezpečnostním hrozbám ještě před tím, než se tyto hrozby projeví v kybernetickém prostoru. Smyslem reaktivních protiopatření pak je působit k dosažení smyslu a účelu zákona v situaci trvajícího kybernetického bezpečnostního incidentu a účelem ochranných protiopatření je dodatečně reagovat na zkušenosti z řešení nastalých kybernetických bezpečnostních incidentů.*

*Zákon ukládá povinným osobám povinnost provádět reaktivní a ochranná protiopatření. Povinné osoby jsou vzhledem k této povinnosti rozděleny do dvou skupin, přičemž bezprostředně tato povinnost zavazuje správce informačních a komunikačních systémů zařazených do kritické informační infrastruktury a správce významných informačních systémů, tj. subjekty zajišťující chod informačních systémů, služeb a sítí vitálně důležitých pro fungování základních společenských funkcionalit státu. Ostatní povinné osoby, tj. poskytovatelé služeb elektronických komunikací a subjekty zajišťující sítě elektronických komunikací včetně subjektů zajišťujících významné sítě, mají povinnost provádět reaktivní protiopatření jen výjimečně, a to za vyhlášeného stavu kybernetického nebezpečí anebo za nouzového stavu.*

*Rozdělení povinných osob vzhledem k povinnostem provádět reaktivní a ochranná protiopatření odpovídá principu minimalizace zásahu do autonomie vůle povinných osob a zakládá možnost NBÚ autoritativně regulovat chování povinných osob jen v nezbytně nutné míře. Za běžné kybernetické bezpečnostní situace by totiž k ochraně vitálních zájmů státu na fungování základních funkcionalit informační společnosti před kybernetickými bezpečnostními incidenty měla postačit implementace protiopatření správců informačních nebo komunikačních systémů kritické informační infrastruktury anebo správců významných informačních systémů. Až v případě, že dojde k výjimečné kybernetické bezpečnostní situaci, kterou nebude možno řešit standardními prostředky zákona, a v jejímž důsledku*

371: Ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky, ve znění ústavního zákona č. 300/2000 Sb.

*bude vyhlášen stav kybernetického nebezpečí nebo nouzový stav, je důvod zavázat k dodržování protiopatření stanovených NBÚ též ostatní povinné osoby.*

Z důvodové zprávy k novele ZoKB:

K § 11 odst. 3 písm. b) a 4
*V souladu s čl. 14 směrnice se rozšiřuje povinnost provádět reaktivní a ochranná opatření i na správce a provozovatele informačního systému základní služby.*

**K odst. 1) a 2)**
K pojmu **bezpečnostní opatření** blíže viz § 4 odst. 1 a násl. ZoKB

V ustanovení § 4 odst. 1 ZoKB je uvedeno, že *„bezpečnostním opatřením se rozumí souhrn úkonů, jejichž cílem je zajištění bezpečnosti informací v informačních systémech a dostupnosti a spolehlivosti služeb a sítí elektronických komunikací v kybernetickém prostoru.*" Jedná se tedy o **úkony** prováděné v kyberprostoru **směřující k zajištění bezpečnosti informací** v informačních systémech, **jakož i dostupnosti a spolehlivosti služeb a sítí elektronických komunikací.**

V porovnání se změním ustanovení § 11 odst. 1 ZoKB je možné nalézt významné změny v definování vlastního pojmu **opatření**. Konkrétně se jedná o to, že:

- úkony **směřují k ochraně informačních systémů nebo služeb a sítí elektronických komunikací**,
  Oproti ustanovení § 4 ZoKB kde jsou jako **aktiva** chráněny **informace a dostupnost a spolehlivost služeb**, jsou v § 11 ZoKB chráněna primárně **aktiva v podobě informačních a komunikačních systémů jako takových.**

- **aktiva jsou chráněna před hrozbami či před kybernetickým bezpečnostním incidentem** (reálně hrozícím či již nastalým).
  V **§ 11 ZoKB se jedná o reakci či protiopatření na nastalou či hrozící situaci**, kdežto **v § 4 a násl. ZoKB dochází k implementaci preventivních opatření**, která mají minimalizovat možnosti výskytu nežádoucích jevů atp.

Opatřeními dle § 11 odst. 2 ZoKB jsou:

- **varování** (blíže viz § 12 ZoKB),
- **reaktivní opatření** (blíže viz § 13 – 15a ZoKB),
- **ochranné opatření** (blíže viz § 13 – 15a ZoKB).

**K odst. 3)**
Ustanovení § 11 odst. 3 ZoKB definuje, **jaká opatření a za jakého stavu mají orgány a osoby** uvedené v § 3 ZoKB **provádět**.
**Reaktivní opatření** je povinen **provádět:**

- **vždy:**
  - správce a provozovatel informačního systému kritické informační infrastruktury [§ 3 písm. c) ZoKB],
  - správce a provozovatel komunikačního systému kritické informační infrastruktury [§ 3 písm. d) ZoKB],
  - správce a provozovatel významného informačního systému [§ 3 písm. e) ZoKB],
  - správce a provozovatel informačního systému základní služby [§ 3 písm. f) ZoKB].
- **za stavu kybernetického nebezpečí nebo za nouzového stavu:**
  - poskytovatel služby elektronických komunikací a subjekt zajišťující síť elektronických komunikací [§ 3 písm. a) ZoKB],
  - orgán nebo osoba zajišťující významnou síť [§ 3 písm. b) ZoKB].

**Ochranné opatření** je povinen provádět **vždy**:

- správce a provozovatel informačního systému kritické informační infrastruktury [§ 3 písm. c) ZoKB],
- správce a provozovatel komunikačního systému kritické informační infrastruktury [§ 3 písm. d) ZoKB],
- správce a provozovatel významného informačního systému [§ 3 písm. e) ZoKB],
- správce a provozovatel informačního systému základní služby [§ 3 písm. f) ZoKB].

K pojmu **kybernetické nebezpečí** blíže viz § 21 ZoKB.

Kybernetické nebezpečí představuje **stav, ve kterém je ve velkém rozsahu ohrožena bezpečnost informací** v informačních systémech **nebo bezpečnost služeb elektronických komunikací anebo** bezpečnost a **integrita sítí elektronických komunikací, čímž by mohlo dojít k porušení nebo ohrožení zájmu České republiky.** Stav kybernetického nebezpečí je oprávněn vyhlásit pouze ředitel NÚKIB.

Pojmem **nouzový stav** je vymezen v Ústavním zákoně č. 110/1998 Sb., o bezpečnosti České republiky,[372] konkrétně v čl. 2, 5 a 6.

Dle čl. 2 tohoto ústavního zákona je možné, pokud je „***bezprostředně ohrožena*** *svrchovanost, územní celistvost, demokratické základy České republiky* ***nebo ve značném rozsahu*** *vnitřní pořádek*

372: Dále jen **ZoBČR**

*a bezpečnost, životy a zdraví, majetkové hodnoty nebo životní prostředí* ***anebo je-li třeba plnit mezinárodní závazky*** *o společné obraně,* ***může se vyhlásit podle intenzity, územního rozsahu a charakteru situace nouzový stav****, stav ohrožení státu nebo válečný stav.*"

V čl. 5 tohoto ústavního zákona je dále uvedeno, že nouzový stav se může vyhlásit v „*případě živelních pohrom, ekologických nebo průmyslových havárií, nebod* ***nebo jiného nebezpečí, které ve značném rozsahu ohrožují životy, zdraví nebo majetkové hodnoty anebo vnitřní pořádek a bezpečnost.***"

Nouzový stav je možné vyhlásit nejdéle na dobu 30 dnů, kterou lze prodloužit jen po předchozím souhlasu Poslanecké sněmovny.[373]

**Ředitel NÚKIB neprodleně požádá vládu o vyhlášení nouzového stavu v případě, že není možné odvrátit ohrožení** bezpečnosti informací v informačních systémech nebo bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací **v rámci stavu kybernetického nebezpečí.**[374]

**§ 12**
**Varování**

**(1) Úřad vydá varování, dozví-li se zejména z vlastní činnosti nebo z podnětu provozovatele národního CERT anebo od orgánů, které vykonávají působnost v oblasti kybernetické bezpečnosti v zahraničí, o hrozbě v oblasti kybernetické bezpečnosti.**
**(2) Varování Úřad zveřejní na svých internetových stránkách a oznámí je orgánům a osobám uvedeným v § 3, jejichž kontaktní údaje jsou vedeny v evidenci podle § 16 odst. 4.**
**(3) Úřad je z důvodu ochrany vnitřního pořádku a bezpečnosti, ochrany života a zdraví osob nebo ochrany ekonomiky státu oprávněn po konzultaci s orgánem nebo osobou uvedenými v § 3 písm. c), d), f), g) nebo h), které jsou dotčeny kybernetickým bezpečnostním incidentem, veřejnost o tomto incidentu informovat nebo dotčenému orgánu nebo osobě uložit, aby tak učinil sám.**

Z důvodové zprávy:

*Účelem varování podle tohoto ustanovení je oficiální publikace informací o bezpečnostní hrozbě, tj. preventivní informování povinných osob. Vzhledem k technickému charakteru některých kybernetických bezpečnostních hrozeb lze očekávat, že v některých případech bude možno takovou hrozbu ze strany NBÚ po obdržení informací o její existenci pro účely okamžitého vydání varování pouze popsat. Bude-li mít NBÚ k dispozici též informace o technickém řešení, může tyto informaci připojit k varování.*

373: Čl. 6 odst. 2 ZoBČR
374: Blíže viz § 21 odst. 6 ZoKB

*Varování bude publikováno prostřednictvím internetových stránek vládního CERT, aby byla zajištěna informovanost dotčených subjektů, včetně široké veřejnosti. Povinným osobám bude varování rovněž oznamováno formou kontaktních údajů, které mají povinné osoby povinnost hlásit do evidence kontaktních údajů.*

Z důvodové zprávy k novele ZoKB:

K § 12 odst. 3
*Pokud je z taxativně vyjmenovaných důvodů nezbytná informovanost veřejnosti, zavádí se oprávnění NBÚ informovat veřejnost, nebo uložit povinnému subjektu, aby veřejnost informoval sám. NBÚ při rozhodování o zveřejnění informací o kybernetickém bezpečnostním incidentu vezme v rámci správního uvážení do úvahy potřebu zachování rovnováhy mezi zájmem veřejnosti být informovanou o hrozbách a možným poškozením pověsti či obchodních zájmů provozovatelů základních služeb a poskytovatelů digitálních služeb, kteří incidenty ohlašují.*

*Důvody, kdy může být oprávnění svěřená NBÚ podle tohoto ustanovení aplikováno, jsou obdobná jako ta, která definují infrastrukturu jako kritickou ve smyslu § 2 písm. g) krizového zákona, jenž transponuje směrnici Rady 200/114/ES o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu.*

*Vzhledem k tomu, že i provozovatelé základních služeb budou určováni pouze ze subjektů, které zajišťují činnosti z hlediska bezproblémového fungování státu nejdůležitější, bude NBÚ toto ustanovení využívat jen za okolností, kdy je pro zajištění dalšího fungování státu i v situaci, kdy některý z provozovatelů základních služeb bude napaden kybernetickým bezpečnostním incidentem, nezbytně nutná informovanost veřejnosti. Ustanovení § 12 odst. 3 návrhu zákona nevylučuje možnost konzultací věcně příslušeného gestora. Je tedy možné, aby se na něj dotčený subjekt, případně i NBÚ, ještě před samotným informováním veřejnosti obrátil s žádostí o sdělení informací, které mohou být pro informování veřejnosti relevantní. Uvedeme-li konkrétní příklad finančního sektoru, kde by informace o incidentu v rámci jedné banky mohla ovlivnit celý finanční sektor a způsobit dokonce i jeho kolaps, bylo by v takovém případě relevantní stanovisko České národní banky. V takovém případě je NBÚ zřejmé, že provázanost celého odvětví je značně komplexní a stanovisko gestora je nenahraditelné.*

*V případě, že NBÚ uložení dotčenému subjektu, aby takovouto informaci zveřejnil sám, umožní mu zároveň, aby si zvolit konkrétní podobu této informace.*

**K odst. 1) a 2)**
K pojmu **hrozba** blíže viz kap. 2.4.1.

V případě že se **NÚKIB** dozví o hrozbě v oblasti kybernetické bezpečnosti**, vydá varování.**

Varování je zveřejněno na internetových stránkách NÚKIB a současně je oznámeno všem subjektům uvedeným v § 3 ZoKB (jejichž kontaktní údaje jsou vedeny v evidenci NÚKIB).

V současnosti jsou jednotlivé hrozby s jejich stručným popisem, uvedením postižených systémů, návodem jak se jim bránit, případnými odkazy a dalšími informacemi zveřejňovány na: https://nukib.cz/cs/informacni-servis/hrozby/.
Smyslem varování je preventivně informovat jednak subjekty uvedené v § 3 ZoKB a jednak i běžné uživatele či administrátory ICT, kteří tak mají možnost se dozvědět informace o případných hrozbách, zranitelnostech aj.

Informaci o hrozbě v oblasti kybernetické bezpečnosti se NÚKIB může dozvědět:

- z vlastní činnosti,
- z podnětu provozovatele národního CERT,
- od orgánů vykonávajících působnost v oblasti kybernetické bezpečnosti v zahraničí,
- od jiných subjektů.

**K odst. 3)**
V případech, kdy existuje důvod spočívající v:

- ochraně vnitřního pořádku a bezpečnosti,
- ochraně života a zdraví osob,
- ochraně ekonomiky státu,

**je NÚKIB po konzultaci** s orgánem nebo osobou uvedenými v § 3 písm. c), d), f), g) nebo h), které jsou dotčeny kybernetickým bezpečnostním incidentem, **oprávněn informovat o tomto incidentu veřejnost.**

**NÚKIB je také oprávněn orgánu nebo osobě** uvedené v § 3 písm. c), d), f), g) nebo h), které jsou dotčeny kybernetickým bezpečnostním incidentem, **nařídit, aby o tomto incidentu informoval veřejnost sám.**

### § 13
### Reaktivní a ochranné opatření

**(1) Úřad vydá rozhodnutí, ve kterém uloží provést reaktivní opatření k řešení kybernetického bezpečnostního incidentu anebo k zabezpečení informačních systémů nebo sítí a služeb elektronických komunikací**[375] **před kybernetickým bezpečnostním incidentem, které je**

375: Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů.

**prvním úkonem ve věci. Nepodaří-li se rozhodnutí adresátovi doručit do vlastních rukou do 3 dnů ode dne jeho vydání, doručí se mu tak, že se vyvěsí na úřední desce Úřadu a tímto okamžikem je vykonatelné. Rozhodnutí podle věty první může Úřad vydat i v řízení na místě podle správního řádu.**
**(2) Rozklad podaný proti rozhodnutí podle odstavce 1 nemá odkladný účinek.**
**(3) Má-li se reaktivní opatření k řešení kybernetického bezpečnostního incidentu anebo k zabezpečení informačních systémů nebo sítí a služeb elektronických komunikací[376] před kybernetickým bezpečnostním incidentem týkat blíže neurčeného okruhu orgánů nebo osob, vydá je Úřad formou opatření obecné povahy.**
**(4) Orgány a osoby uvedené v § 3 písm. a) až f) jsou povinny bez zbytečného odkladu oznámit Úřadu provedení reaktivního opatření a jeho výsledek. Náležitosti oznámení stanoví prováděcí právní předpis.**

Z důvodové zprávy:

*Účelem reaktivního protiopatření je okamžitá reakce na výskyt kybernetického bezpečnostního incidentu. Obsahem protiopatření tedy mohou být povinnosti provést konkrétní úkony nutné k odvrácení kybernetického bezpečnostního incidentu nebo ke zmírnění jeho následků.*

*Zákon rozlišuje dvě formy reaktivních protiopatření, a to rozhodnutí a opatření obecné povahy. Smyslem tohoto dělení je pokrýt oba typické případy vyskytující se při ochraně před kybernetickými bezpečnostními incidenty. První možností je výskyt kybernetického bezpečnostního incidentu v určitém informačním nebo komunikačním systému. Reaktivní protiopatření lze v takovém případě vydat formou rozhodnutí konkrétně specifikujícím povinnosti pro určeného adresáta – povinnou osobu. Druhou možností je výskytu incidentu, jehož rozsah je větší nebo jehož rozsah nelze kvůli složitosti incidentu nebo jeho rychlému vývoji přesně určit – takový incident pak je možno řešit vydáním reaktivního protiopatření formou opatření obecné povahy, v němž budou specifikovány konkrétní povinnosti k jeho odvrácení neurčitému okruhu povinných osob definovanému za užití generických znaků odpovídajících jeho charakteru.*

*Charakter kybernetických bezpečnostních incidentů vyžaduje k úspěšnosti reaktivního protiopatření reakci v co nejkratším čase. Jakákoli časová prodleva, byť v řádu hodin, může znamenat exponenciální rozvoj kybernetického bezpečnostního incidentu a násobení jeho škodlivého účinku. Z tohoto důvodu je zákonem speciálně upravena vykonatelnost rozhodnutí jeho doručením povinné osobě, respektive vyvěšením na úřední desce NBÚ a výslovně založena možnost vydání rozhodnutí v řízení na místě podle správního řádu. Z téhož důvodu nelze přiznat odkladný účinek rozkladu podanému proti rozhodnutí a nelze vést ani přezkumné řízení, je-li reaktivní protiopatření vydáno opatřením obecné povahy.*

376: Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů.

*Z důvodu potřeby zpětné vazby pro vyhodnocení efektivnosti vydaných protiopatření se formuluje povinným osobám povinnost informovat NBÚ o provedených protiopatřeních a o jejich účinku. Pro zjednodušení této povinnosti a nezatěžování povinných osob přílišnými administrativními povinnostmi pak NBÚ stanoví prováděcím právním předpisem náležitosti tohoto oznámení. Prováděcím právním předpisem budou rovněž stanoveny nejběžnější příklady reaktivních protiopatření, které bude NBÚ vydávat.*

Z důvodové zprávy k novele ZoKB:

K § 13 odst. 4
*Legislativně technické zpřesnění povinných subjektů, které odpovídá úpravě § 11 odst. 3 ZoKB.*

**K odst. 1)**
K pojmu **kybernetický bezpečnostní incident** blíže viz kap. 2.4.3, § 7 odst. 2 ZoKB.
K pojmu **informační systém** viz § 2 písm. j) ZoKB.
K pojmu **síť elektronických komunikací** viz § 1 ZoKB, § 2 písm. h) ZoEK či čl. 4 odst. 1 písm. a) NIS.
K pojmu **služba elektronických komunikací** viz § 2 písm. a) ZoKB, § 2 písm. n) ZoEK.

Smyslem reaktivního opatření dle § 13 odst. 1 ZoKB je zajistit ochranu **konkrétních (specifikovaných) informačních a komunikačních systémů** před kybernetickými bezpečnostními incidenty. Vlastní opatření může být zaměřeno na:

- **zabezpečení informačních systémů nebo sítí a služeb elektronických komunikací** před kybernetickým bezpečnostním incidentem (preventivní opatření),
- vlastní **řešení kybernetického bezpečnostního incidentu.**

Reaktivní opatření dle § 13 odst. 1 ZoKB má **formu rozhodnutí**, které je oprávněn vydat NÚKIB.

Náležitosti rozhodnutí jsou upraveny § 67 a násl. zákona č. 500/2004 Sb., správní řád[377], ve znění pozdějších předpisů. Dle 67 odst. 1 SŘ *„rozhodnutím správní orgán v **určité věci zakládá**, **mění** **nebo ruší práva anebo povinnosti jmenovitě určené osoby nebo** v určité věci **prohlašuje, že taková** **osoba práva nebo povinnosti má anebo nemá**, nebo v zákonem stanovených případech rozhoduje o procesních otázkách.“*

Rozhodnutí je v případě reaktivního opatření prvním úkonem ve věci a nedochází tak k oznámení o zahájení správního řízení dle § 46 SŘ.

377: Dále jen správní řád, či **SŘ**

*„Charakter kybernetických bezpečnostních incidentů vyžaduje k úspěšnosti reaktivního protiopatření reakci v co nejkratším čase.* ***Jakákoli časová prodleva****, byť v řádu hodin,* ***může znamenat exponenciální rozvoj kybernetického bezpečnostního incidentu a násobení jeho škodlivého účinku.*** *Z tohoto důvodu je zákonem speciálně upravena vykonatelnost rozhodnutí jeho doručením povinné osobě, respektive vyvěšením na úřední desce NÚKIB a* ***výslovně založena možnost vydání rozhodnutí v řízení na místě podle správního řádu****."* [378]

V případě, že se nepodaří rozhodnutí doručit adresátovi do vlastních rukou do 3 dnů ode dne jeho vydání, doručí se[379] mu tak, že se vyvěsí na úřední desce NÚKIB a tímto okamžikem je vykonatelné.[380]

**Rozhodnutí** o provedení reaktivního opatření **může NÚKIB vydat i v řízení na místě** podle § 143 SŘ. Dle tohoto ustanovení je možné vydat rozhodnutí na místě, pokud

- hrozí životu nebo zdraví osob bezprostřední nebezpečí,
- hrozí bezprostředně někomu vážná majetková újma,
- dojde k náhlé havárii,
- existuje důvodná obava, že by se osoba, jíž má být uložena povinnost, vyhýbala jejímu splnění,
- jde o uložení záruky za splnění povinnosti (§ 147 SŘ), předběžného opatření (§ 61 SŘ) nebo pořádkového opatření (§ 62 a 63 SŘ),
- je vedeno řízení navazující na výkon dozoru.

Podmínkou pro uložení povinnosti na místě je **zjištění stavu věci**.

V případě rozhodnutí na místě se rozhodnutí vyhlašuje ústně a jeho písemné vyhotovení se bez zbytečného odkladu doručuje dodatečně. Pokud zvláštní zákon nestanoví jinak, nemá odvolání proti takto vyhlášenému rozhodnutí odkladný účinek.

O ústním vyhlášení rozhodnutí se vždy na místě vydá písemné potvrzení (§ 67 odst. 3 SŘ), které obdrží účastník.[381]

378: *Důvodová zpráva.* [online]. [cit. 21. 8. 2018]. Dostupné z: https://www.govcert.cz/download/legislativa/container-nodeid-708/nbu-zkb-navrh-130415-duvodzprava.pdf s. 70

379: Způsoby doručování jsou upraveny v § 19 a násl. SŘ

380: Jedná se o předběžně vykonatelné rozhodnutí – blíže viz § 74 SŘ

381: § 143 odst. 2 SŘ

**K odst. 2)**
Proti rozhodnutí, které v prvním stupni řízení vydává ústřední správní úřad (NÚKIB) je řádným opravným prostředkem **rozklad**.[382] O rozkladu rozhoduje dle § 152 odst. 2 SŘ vedoucí jiného ústředního správního úřadu (ředitel NÚKIB).

Ředitel NÚKIB v souladu s § 152 odst. 6 SŘ může v řízení o rozkladu rozhodnout tak, že:

- rozhodnutí zruší nebo změní, pokud se tím plně vyhoví rozkladu a jestliže tím nemůže být způsobena újma žádnému z účastníků, ledaže s tím všichni, jichž se to týká, vyslovili souhlas, nebo
- rozklad zamítne.

V případě zákona o kybernetické bezpečnosti **nemá rozklad** proti rozhodnutí o provedení reaktivních opatření **odkladný účinek.**

**K odst. 3)**
Smyslem reaktivního opatření dle § 13 odst. 3 ZoKB je zajistit ochranu **předem blíže neurčeného okruhu orgánů nebo osob (nespecifikovaných) a jejich informačních a komunikačních systémů** před kybernetickými bezpečnostními incidenty. Vlastní opatření může být zaměřeno na:

- **zabezpečení informačních systémů nebo sítí a služeb elektronických komunikací** před kybernetickým bezpečnostním incidentem (preventivní opatření),
- vlastní **řešení kybernetického bezpečnostního incidentu.**

Reaktivní opatření dle § 13 odst. 2 ZoKB má **formu opatření obecné povahy**, které je oprávněn vydat NÚKIB.

Opatření obecné povahy je upraveno v § 171 a násl. SŘ.

**K odst. 4)**
Orgány a osoby uvedené v § 3 písm. a) až f) ZoKB jsou povinny bez zbytečného odkladu **oznámit NÚKIB provedení reaktivního opatření a jeho výsledek.**

Důvodem této povinnosti je potřeba vyhodnocení zpětné vazby ze strany NÚKIB na provedená reaktivní opatření.

Orgány a osoby uvedené v § 3 písm. a) až f) ZoKB, kterým NÚKIB uložil provést reaktivní opatření:

382: Viz § 152 SŘ

- posoudí očekávané dopady reaktivního opatření na informační a komunikační systém a na zavedená bezpečnostní opatření a vyhodnotí možné negativní účinky a
- stanoví způsob rychlého provedení tohoto opatření, který minimalizuje jeho možné negativní účinky, a určí časový plán jeho provedení.[383]

Tyto osoby také oznámí způsob provedení reaktivního opatření a jeho výsledek ve formě uvedené na internetových stránkách Úřadu.

**§ 14**
(Ochranné opatření)

**Úřad za účelem zvýšení ochrany informačních systémů nebo služeb a sítí elektronických komunikací[384] a na základě analýzy již vyřešeného kybernetického bezpečnostního incidentu jako ochranné opatření vydá opatření obecné povahy, ve kterém orgánům a osobám uvedeným v § 3 písm. c) až f) stanoví způsob zvýšení ochrany informačních systémů nebo služeb a sítí elektronických komunikací[385] a přiměřenou lhůtu k jeho provedení.**

Z důvodové zprávy:

*Důvodem vydání ochranného protiopatření je nutnost reagovat na vyřešený kybernetický bezpečnostní incident a na základě získaných zkušeností obecně zvýšit kvalitu ochrany informačních systémů, služeb a sítí elektronických komunikací u povinných osob. Vzhledem k tomu, že ochranné protiopatření směřuje k obecnému zvýšení rezistence kybernetického prostoru vůči kybernetickým bezpečnostním incidentům, je vydáváno formou opatření obecné povahy, kterým je možno uložit konkrétní povinnosti (tj. povinnosti vedoucí ke zvýšení ochrany před určitým typem kybernetického bezpečnostního incidentu) neurčitému okruhu subjektů. Okruh adresátů tedy bude v tomto případě určen podle toho, u kterých povinných osob spadajících pod možný rozsah osobní působnosti ochranného protiopatření je nutno zlepšení ochrany realizovat, vždy však půjde o povinné osoby zavádějící standardizaci, tj. o správce informačních nebo komunikačních systémů kritické informační infrastruktury anebo o správce významných informačních systémů.*

*Oproti bezpečnostním opatřením se v tomto případě jedná o řešení prováděné v bezprostřední návaznosti na poznatky získané řešením konkrétního kybernetického bezpečnostního incidentu. Ochranného protiopatření tedy bude použito v situaci, kdy nelze z legislativně-technických důvodů realizovat požadavek na zvýšení úrovně zabezpečení informačních systémů, sítí nebo služeb elektronických komunikací formou aktualizace prováděcích předpisů stanovících technické parametry bezpečnostních opatření.*

383: § 33 odst. 1 VoKB

384: Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů.

385: Tamtéž

Z důvodové zprávy k novele ZoKB:

*Ustanovení bylo nově formulováno tak, aby nemohlo vést ke dvojímu výkladu, a mezi adresáty opatření obecné povahy byli doplněni správci a provozovatelé informačního systému základní služby.*

K pojmu **kybernetický bezpečnostní incident** blíže viz kap. 2.4.3, § 7 odst. 2 ZoKB.
K pojmu **informační systém** viz § 2 písm. j) ZoKB.
K pojmu **síť elektronických komunikací** viz § 1 ZoKB, § 2 písm. h) ZoEK či čl. 4 odst. 1 písm. a) NIS.
K pojmu **služba elektronických komunikací** viz § 2 písm. a) ZoKB, § 2 písm. n) ZoEK.

Smyslem ochranného opatření dle § 14 ZoKB je zajistit ochranu **informačních a komunikačních systémů** před kybernetickými bezpečnostními incidenty. Vlastní opatření je zaměřeno na **stanovení způsobu zvýšení ochrany informačních systémů nebo služeb a sítí elektronických komunikací** (preventivní opatření).

Toto ochranné opatření je vydáváno ve **formě opatření obecné povahy**[386] a je reakcí na již vyřešený kybernetický bezpečnostní incident a jeho analýzu. Smyslem je do budoucna zvýšit ochranu ICT a zabránit tak úspěšnému opakování již známého kybernetického bezpečnostního incidentu.

**V § 15 ZoKB jsou stanoveny odchylky od obecného postupu** v řízení o opatření obecné povahy.

Opatření obecné povahy dle § 14 ZoKB je oprávněn vydat NÚKIB, přičemž současně s vydaným opatřením **stanoví přiměřenou lhůtu k jeho provedení.**

**§ 15**

**(1) Opatření obecné povahy podle § 13 nebo 14 nabývá účinnosti okamžikem jeho vyvěšení na úřední desce Úřadu; ustanovení § 172 správního řádu se nepoužije. O vydání opatření obecné povahy Úřad rovněž vyrozumí orgány a osoby uvedené v § 3, jejichž kontaktní údaje jsou vedeny v evidenci podle § 16 odst. 4.**
**(2) Připomínky k opatření obecné povahy vydanému podle § 13 nebo 14 lze uplatnit ve lhůtě 30 dnů ode dne jeho vyvěšení na úřední desce Úřadu. Úřad může na základě uplatněných připomínek opatření obecné povahy změnit nebo zrušit.**

386: Viz § 171 a násl. SŘ

Z důvodové zprávy:

*Toto ustanovení je společné pro opatření obecné povahy, jejichž prostřednictvím se vydávají reaktivní nebo ochranná protiopatření. Z důvodu naléhavé nutnosti reagovat na probíhající nebo vyřešený kybernetický bezpečnostní incident v co nejkratším čase je upravena účinnost těchto opatření obecné povahy dnem zveřejnění na úřední desce NBÚ, přičemž vydání těchto opatření obecné povahy nebude předcházet řízení o návrhu opatření obecné povahy podle § 172 správního řádu, při němž by mohly být proti návrhu podávány oprávněnými osobami námitky nebo připomínky. Povinným osobám je oprávnění uplatnit připomínky podle § 172 odst. 4 správního řádu modifikováno, a to tak, že budou oprávněny podat připomínky směřující přímo proti vydanému opatření obecné povahy, a to ve lhůtě 15 dnů od jeho zveřejnění na úřední desce NBÚ. V případě vyhodnocení připomínek jako důvodných, lze příslušné opatření obecné povahy změnit nebo zrušit.*

*Aby byla zajištěna co nejširší informovanost povinných osob i veřejnosti, je upravena též povinnost zveřejnit tato opatření obecné povahy na internetových stránkách vládního CERT. Lze totiž očekávat, že reaktivní a ochranná protiopatření vydaná ve formě opatření obecné povahy budou iniciativně realizovat i povinné osoby nespadající pod rozsah jejich osobní působnosti a rovněž tak i další osoby nespadající do osobní působnosti tohoto zákona. Současně z důvodu zajištění co možná nejrychlejšího a nejefektivnějšího informování povinných osob o protiopatřeních vydaných formou opatření obecné povahy NBÚ vyrozumí povinné osoby o vydání těchto protiopatření prostřednictvím kontaktních údajů, které mají povinné osoby povinnost hlásit do evidence kontaktních údajů.*

*Vyloučení přezkumného řízení odůvodňuje potřeba reakce na nastalý kybernetický bezpečnostní incident v co nejkratším čase, jakož i potřeba zamezit prodlevě mezi získáním poznatků z řešení kybernetického bezpečnostního incidentu a jejich implementací povinnými osobami.*

**K odst. 1)**
Ustanovení § 15 ZoKB stanoví postup při vydávání opatření obecné povahy.

**Obecný postup vydávání opatření obecné povahy** je uveden v § 172 a násl. SŘ, tento postup **se** však v případě vydávání opatření obecné povahy dle § 13 nebo 14 ZoKB **nepoužije**.

Dle § 15 ZoKB **nabývá opatření obecné povahy účinnosti okamžikem jeho vyvěšení na úřední desce NÚKIB.**

Jde o postup odlišný oproti řízení o opatření obecné povahy dle § 172 a násl. SŘ. V § 172 odst. 1 SŘ je uvedeno, že *„návrh opatření obecné povahy s odůvodněním správní orgán po projednání s dotčenými orgány uvedenými*[387] *doručí veřejnou vyhláškou*[388]*, kterou vyvěsí na své úřední desce*

387: Viz § 136 SŘ
388: Dle § 25 SŘ

*a na úředních deskách obecních úřadů v obcích, jejichž správních obvodů se má opatření obecné povahy týkat, a vyzve dotčené osoby, aby k návrhu opatření podávaly připomínky nebo námitky. V případě potřeby se návrh zveřejní i jiným způsobem, v místě obvyklým. Návrh opatření obecné povahy musí být zveřejněn nejméně po dobu 15 dnů.*"

Řízení o návrhu opatření obecné povahy dle správního řádu je písemné, pokud zákon nestanoví nebo správní orgán neurčí, že se koná veřejné projednání návrhu. Dobu a místo konání veřejného projednání správní orgán oznámí na úřední desce nejméně **15 dnů předem**. **Hrozí-li nebezpečí z prodlení**, je možné tuto dobu zkrátit; nestanoví-li zákon jinak, musí zkrácená doba činit **nejméně 5 dní**.[389]

Důvodem pro nerespektování správního řádu a specifickou úpravu v ZoKB je ta skutečnost, že **je třeba aktivně a ve velmi krátké době reagovat na kybernetické bezpečnostní incidenty, ať již formou reaktivních** (§ 13 ZoKB) **či ochranných** (§ 14 ZoKB) **opatření.** Pokud by byl respektován postup uvedený v správním řádu, pak by procedurální podmínky uvedené v § 172 SŘ de facto tuto aktivní a rychlou reakci na kybernetické bezpečnostní incidenty znemožnily.

NÚKIB **je povinen vyrozumět všechny subjekty uvedené v § 3 ZoKB** (jejichž kontaktní údaje jsou vedeny v evidenci NÚKIB) **o vydání opatření obecné povahy** dle § 13 nebo 14 ZoKB.

**K odst. 2)**
Správní řád stanoví, že **každý, jehož práva, povinnosti nebo zájmy mohou být opatřením** obecné povahy přímo **dotčeny, může uplatnit u správního orgánu** písemné **připomínky** nebo na veřejném projednání ústní připomínky **k návrhu opatření obecné povahy**. Správní orgán je povinen se připomínkami zabývat jako podkladem pro opatření obecné povahy a vypořádat se s nimi v jeho odůvodnění.[390]

**V § 15 odst. 2 ZoKB je připomínkové řízení stanoveno odlišně.**

**Připomínky** k opatření obecné povahy vydanému podle § 13 nebo 14 ZoKB **je možné uplatnit ve lhůtě 30 dnů ode dne jeho vyvěšení na úřední desce NÚKIB.**

**Úřad může na základě uplatněných připomínek opatření obecné povahy změnit nebo zrušit.**

Ustanovení § 174 odst. 2 SŘ stanoví, že „***soulad opatření obecné povahy s právními předpisy lze posoudit v přezkumném řízení.*** *Usnesení o zahájení přezkumného řízení lze vydat do 1 roku od účinnosti opatření. Účinky rozhodnutí v přezkumném řízení nastávají ode dne jeho právní moci.*"

389: § 172 odst. 3 SŘ
390: § 172 odst. 1 SŘ

Vlastní přezkumné řízení je upraveno v § 94 a násl. SŘ.

**§ 15a**

**(1) Úřad může v případě hrozícího kybernetického bezpečnostního incidentu na návrh správce informačního systému, který marně vyzval provozovatele ke splnění povinnosti předat správci data, provozní údaje a informace, které má k dispozici v souvislosti s provozováním tohoto systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému, rozhodnutím uložit provozovateli tohoto systému povinnost předat správci data, provozní údaje a informace, které má k dispozici v souvislosti s provozováním tohoto systému; návrh musí obsahovat odůvodnění požadavku s ohledem na hrozící kybernetický bezpečnostní incident, podrobný popis předchozího jednání mezi provozovatelem a správcem tohoto systému zejména s ohledem na nesplnění smluvní povinnosti provozovatele a možné následky, pokud nedojde k předání požadovaných dat, provozních údajů a informací.**
**(2) Rozhodnutí o uložení povinnosti předat data, provozní údaje a informace podle odstavce 1 je prvním úkonem v řízení, je vykonatelné dnem doručení rozhodnutí a rozklad proti němu nemá odkladný účinek.**
**(3) Pro úhradu nákladů vynaložených provozovatelem informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému na předání dat, provozních údajů a informací podle odstavce 1 se ustanovení § 6a odst. 4 použije obdobně.**

**K odst. 1)**
V případě, kdy **hrozí kybernetický bezpečnostní incident a provozovatel nesplnil povinnosti dle § 6a** ZoKB může NÚKIB na návrh správce informačního systému uložit provozovateli rozhodnutím povinnost předat data, provozní údaje a informace, která provozovatel má v souvislosti s provozováním:

- **systému kritické informační infrastruktury**,
- **komunikačního systému kritické informační infrastruktury**,
- **významného informačního systému**.

**Vlastnímu rozhodnutí** ze strany NÚKIB však **musí předcházet marná výzva** správce vůči provozovateli, aby splnil svoji povinnost dle § 6a ZoKB.

**Návrh správce** informačního systému **musí obsahovat:**

- **odůvodnění požadavku s ohledem na hrozící kybernetický bezpečnostní incident,**
- **podrobný popis předchozího jednání mezi provozovatelem a správcem tohoto systému** zejména s ohledem na nesplnění smluvní povinnosti provozovatele,

- **možné následky, pokud nedojde k předání požadovaných dat, provozních údajů a informací.**

**K odst. 2) a 3)**
K pojmu **rozhodnutí** viz § 13 odst. 1 ZoKB.

Rozhodnutí dle § 15a odst. 2 ZoKB je prvním úkonem ve věci a nedochází tak k oznámení o zahájení správního řízení dle § 46 SŘ.

Rozhodnutí **je vykonatelné dnem doručení a rozklad** proti němu **nemá odkladný účinek.**

K **úhradě nákladů vynaložených provozovatelem informačního systému** viz § 6a odst. 4 ZoKB.

**§ 16**
**Kontaktní údaje**

**(1) Kontaktními údaji jsou**
**a) u právnické osoby obchodní firma nebo název, adresa sídla, identifikační číslo osoby nebo obdobné číslo přidělované v zahraničí,**
**b) u podnikající fyzické osoby obchodní firma nebo jméno včetně odlišujícího dodatku nebo dalšího označení, adresa sídla a identifikační číslo osoby,**
**c) u orgánu veřejné moci jeho název, adresa sídla, identifikační číslo osoby, bylo-li přiděleno, a identifikátor orgánu veřejné moci, pokud mu není přiděleno identifikační číslo osoby,**
**a údaje o fyzické osobě, která je za orgán nebo osobu uvedené v § 3 oprávněna jednat ve věcech upravených tímto zákonem, a to jméno, příjmení, telefonní číslo a adresa elektronické pošty.**
**(2) Kontaktní údaje a jejich změny oznamují**
**a) orgány a osoby uvedené v § 3 písm. a), b) a h) provozovateli národního CERT a**
**b) orgány a osoby uvedené v § 3 písm. c) až g) Úřadu.**
**(3) Orgány a osoby uvedené v § 3 písm. c) až g) oznamují změny pouze těch údajů podle odstavce 1, které nejsou referenčními údaji vedenými v základních registrech, a to neprodleně.**
**(4) Úřad vede evidenci kontaktních údajů, která obsahuje údaje uvedené v odstavci 1.**
**(5) Úřad je za stavu kybernetického nebezpečí oprávněn vyžadovat kontaktní údaje shromážděné provozovatelem národního CERT podle odstavce 2 písm. a).**
**(6) Úřad je dále oprávněn si pro účely kontroly vyžádat od provozovatele národního CERT kontaktní údaje orgánů a osob uvedených v § 3 písm. h).**
**(7) Vzor oznámení kontaktních údajů a jeho formu stanoví prováděcí právní předpis.**

Z důvodové zprávy:

*Návrh ustanovení vymezuje kontaktní údaje povinných osob, upravuje podmínky jejich evidence vedené NBÚ a notifikační povinnost povinných osob. Poskytovatelé služeb elektronických komunikací, subjekty zajišťující sítě elektronických komunikací a subjekty zajišťující významné sítě jsou povinny oznamovat kontaktní údaje a jejich změny provozovateli národního CERT. Správci informačních a komunikačních systémů kritické informační infrastruktury a správci významných informačních systémů pak tyto údaje oznamují NBÚ. Vzhledem k tomu, že za stavu kybernetického nebezpečí se okruh povinných osob, které mohou být povinny provádět reaktivní a ochranná protiopatření, rozšiřuje též o osoby, které kontaktní údaje oznamují provozovateli národního CERT, upravuje se pro tento případ předání kontaktních údajů těchto osob NBÚ.*

*Institut kontaktních údajů slouží kromě jmenovité evidence povinných osob též ke komunikaci neformálních informací, oficiálních informací (např. varování) a závazných individuálních právních aktů vydávaných NBÚ (ochranných a reaktivních protiopatření). Komunikace prostřednictvím kontaktních údajů má zajistit nikoli jen formální informovanost povinné osoby, ale i skutečný kontakt dohledových pracovišť na konkrétní pracovníky fakticky odpovídající u povinných osob za otázky kybernetické bezpečnosti – prostřednictvím těchto kontaktních údajů tedy bude možno vedle oficiální komunikace řešit též neformální kontakt výkonných pracovníků povinných osob s dohledovými pracovišti, běžnou neformální metodiku, technické konzultace apod.*

*S ohledem na právní úpravu základních registrů, podle které není žádný orgán veřejné moci až na zákonem formulované výjimky oprávněn vyžadovat od osob referenční údaje vedené v základních registrech, byly z notifikační povinnosti povinných osoby oznamujících kontaktní údaje NBÚ vyňaty změny referenčních údajů evidovaných v základních registrech.*

*Vzhledem k tomu, že je třeba zajistit efektivní zpracování velkého množství kontaktních údajů povinných osob, počítá zákon s vydáním formulářového vzoru oznámení kontaktních údajů prováděcím právním předpisem, který bude reflektovat shora uvedenou úpravu základních registrů, tj. nebude vyžadovat od povinných osob referenční údaje vedené v základních registrech.*

Z důvodové zprávy k novele ZoKB:

K § 16 odst. 2 písm. a)
*Zavádí se povinnost poskytovatelů digitálních služeb předávat své kontaktní údaje provozovateli národního CERT. Institut kontaktních údajů slouží například ke komunikaci neformálních informací, závazných individuálních právních aktů vydávaných NBÚ (ochranných a reaktivních opatření). Komunikace prostřednictvím kontaktních údajů má zajistit nikoli jen formální informovanost orgánů a osob, ale i skutečný kontakt pracovišť CERT na konkrétní pracovníky fakticky odpovídající u poskytovatelů digitálních služeb za otázky kybernetické bezpečnosti – prostřednictvím těchto*

*kontaktních údajů tedy bude možno vedle oficiální komunikace řešit též neformální kontakt výkonných pracovníků orgánů a osob s pracovišti CERT, běžnou neformální metodiku, technické konzultace apod.*

K § 16 odst. 2 písm. b) a odst. 3
*Zavádí se povinnost provozovatele základní služby a správců a provozovatelů informačního systému základní služby předávat pro výkon státní správy a kontroly kontaktní údaje NBÚ a ohlašovat jejich změny, nejedná-li se o údaje, které jsou referenčními údaji vedenými v základních registrech.*

K § 16 odst. 6
*Rozšiřuje se okruh důvodů, za kterých může Úřad požadovat předání informací, jež sbírá provozovatel národního CERT, a to o účely kontroly plnění zákonných povinností podle § 24 zákona.*

**K odst. 1) a 4)**
Institut kontaktních údajů upravený v § 16 ZoKB slouží jak k evidenci orgánů a osob uvedených v § 3 ZoKB, tak *„má zajistit nikoli jen formální informovanost povinné osoby, ale i skutečný kontakt dohledových pracovišť na konkrétní pracovníky fakticky odpovídající u povinných osob za otázky kybernetické bezpečnosti – prostřednictvím těchto kontaktních údajů tedy bude možno vedle oficiální komunikace řešit též neformální kontakt výkonných pracovníků povinných osob s dohledovými pracovišti, běžnou neformální metodiku, technické konzultace apod.“* [391]

**Kontaktními údaji jsou:**

- **u právnické osoby** obchodní firma nebo název, adresa sídla, identifikační číslo osoby nebo obdobné číslo přidělované v zahraničí,
- **u podnikající fyzické osoby** obchodní firma nebo jméno včetně odlišujícího dodatku nebo dalšího označení, adresa sídla a identifikační číslo osoby,
- **u orgánu veřejné moci** jeho název, adresa sídla, identifikační číslo osoby, bylo-li přiděleno, a identifikátor orgánu veřejné moci, pokud mu není přiděleno identifikační číslo osoby,
- **údaje o fyzické osobě, která je za orgán nebo osobu uvedené v § 3 oprávněna jednat** ve věcech upravených tímto zákonem, a to jméno, příjmení, telefonní číslo a adresa elektronické pošty.0

**Obchodní firma** dle § 423 OZ označuje jméno (název), pod kterým je podnikatel zapsán do obchodního rejstříku. Podnikatel nesmí mít víc obchodních firem.

**Identifikační číslo osoby** (**IČO**) je unikátní osmimístné identifikační číslo právnické osoby, podnikající fyzické osoby nebo organizační složky státu.

391: *Důvodová zpráva.* [online]. [cit. 21. 8. 2018]. Dostupné z:
https://www.govcert.cz/download/legislativa/container-nodeid-708/nbu-zkb-navrh-130415-duvodzprava.pdf s. 72

**Evidenci kontaktních údajů vede NÚKIB.**

**K odst. 2) a 3)**
**Kontaktní údaje a jejich změny oznamují:**

- **národnímu CERT**, pokud je orgánem nebo osobou:
  - poskytovatel služby elektronických komunikací a subjekt zajišťující síť elektronických komunikací [§ 3 písm. a) ZoKB],
  - orgán nebo osoba zajišťující významnou síť [§ 3 písm. b) ZoKB],
  - poskytovatel digitální služby [§ 3 písm. h) ZoKB].

- **vládnímu CERT**, pokud je orgánem nebo osobou:
  - správce a provozovatel informačního systému kritické informační infrastruktury [§ 3 písm. c) ZoKB],
  - správce a provozovatel komunikačního systému kritické informační infrastruktury [§ 3 písm. d) ZoKB],
  - správce a provozovatel významného informačního systému [§ 3 písm. e) ZoKB],
  - správce a provozovatel informačního systému základní služby [§ 3 písm. f) ZoKB],
  - provozovatel základní služby [§ 3 písm. g) ZoKB].

  Zde uvedené osoby oznamují změnu kontaktních údajů **neprodleně, nemusí však hlásit změny v referenčních údajích vedených v základních registrech**.

  Referenčním údajem se dle § 2 písm. b) zákona č. 111/2009 Sb., o základních registrech rozumí *„údaj vedený v základním registru, který je označen jako referenční údaj"*.

  Referenční údaj je *„**státem garantovaný správný údaj obsažený v příslušném základním registru**, který orgán veřejné moci využívá při své činnosti a to, aniž by ověřoval jejich správnost. Od osob, po kterých je jiným právním předpisem doložení takových údajů požadováno, **je orgán veřejné moci oprávněn požadovat poskytnutí takových údajů pouze, pokud nejsou v základním registru obsaženy, nebo jsou označeny jako nesprávné**, nebo vznikne oprávněná pochybnost o správnosti referenčního údaje, nebo jsou nezbytné pro bezpečnostní řízení podle jiného právního předpisu."* [392]

**K odst. 5) a 6)**
NÚKIB je oprávněn, za stavu kybernetického nebezpečí, vyžadovat kontaktní údaje, které shromáždil národní CERT.

392: *Referenční údaj.* [online]. [cit. 30. 8. 2018]. Dostupné z: http://www.szrcr.cz/referencni-udaj

Z důvodu kontroly je NÚKIB oprávněn vyžádat od národního CERT kontaktní údaje týkající se poskytovatele digitální služby.

**K odst. 7)**
Ustanovení § 34 VoKB definuje způsob oznamování kontaktních údajů:

- **vládnímu CERT** na elektronickém formuláři zveřejněném na internetových stránkách NÚKIB zaslaném:
  - na adresu elektronické pošty tohoto CERT určenou pro příjem oznámení kontaktních údajů, zveřejněnou na internetových stránkách NÚKIB
    GovCERT.CZ - https://www.govcert.cz/
    formulář je dostupný na:
    https://www.govcert.cz/download/kii-vis/hlaseni_kontaktu_v5.xltx
    či https://www.govcert.cz/cs/kyberneticky-zakon/formulare/
  - do datové schránky NÚKIB
    ID datové schránky: zzfnkp3
  - prostřednictvím datového rozhraní, pokud je používáno, jehož popis je zveřejněn na internetových stránkách Úřadu
  - Hlášení kontaktních údajů je možné zaslat i v listinné podobě, avšak pouze v případech, kdy nelze využít žádný z výše uvedených způsobů.
  - Podávání písemností: Národní úřad pro kybernetickou a informační bezpečnost, P. O. Box 17, Brno 16, 616 00
  - Podávání utajovaných písemností pouze přes podatelnu v Praze: NÚKIB, Na Popelce 2/16, Praha 5 – Smíchov, 150 00

- **národnímu CERT** na elektronickém formuláři zveřejněném na internetových stránkách provozovatele národního CERT zaslaném
  - na adresu elektronické pošty provozovatele národního CERT určenou pro příjem oznámení kontaktních údajů, zveřejněnou na jeho internetových stránkách
    CSIRT.CZ - https://csirt.cz/ formulář je dostupný na: https://www.csirt.cz/contactreport/
  - do datové schránky provozovatele národního CERT
    ID datové schránky: h4axdn8
  - prostřednictvím internetových stránek provozovatele národního CERT
    Další kontaktní údaje: https://www.nic.cz/page/357/
  - Hlášení kontaktních údajů je možné zaslat i v listinné podobě, avšak pouze v případech, kdy nelze využít žádný z výše uvedených způsobů.
  - Podávání písemností: CZ.NIC, zájmové sdružení právnických osob, Milešovská 1136/5, 130 00 Praha 3

K doplňujícím kontaktním informacím na národní či vládní CERT viz blíže § 8 ZoKB.

Dle § 34 odst. 5 VoKB je povinná osoba uvedená v § 3 písm. c) až f) ZoKB, která je provozovatelem, dále povinna přiložit k hlášení kontaktních údajů podle § 34 odst. 1 VoKB dokument, kterým ji správce prokazatelně informuje podle § 8 odst. 1 písm. c) VoKB.

### § 17
### Národní CERT

**(1) Národní CERT zajišťuje v rozsahu stanoveném tímto zákonem sdílení informací na národní a mezinárodní úrovni v oblasti kybernetické bezpečnosti.**
**(2) Provozovatel národního CERT**

- **a) přijímá oznámení kontaktních údajů od orgánů a osob uvedených v § 3 písm. a), b) a h) a tyto údaje eviduje a uchovává,**
- **b) přijímá hlášení o kybernetických bezpečnostních incidentech od orgánů a osob uvedených v § 3 písm. b) a h) a tyto údaje eviduje, uchovává a chrání,**
- **c) vyhodnocuje kybernetické bezpečnostní incidenty u orgánů a osob uvedených v § 3 písm. b) a h),**
- **d) poskytuje orgánům a osobám uvedeným v § 3 písm. a), b) a h) metodickou podporu, pomoc a součinnost při výskytu kybernetického bezpečnostního incidentu,**
- **e) působí jako kontaktní místo pro orgány a osoby uvedené v § 3 písm. a), b) a h),**
- **f) provádí hodnocení zranitelností v oblasti kybernetické bezpečnosti,**
- **g) předává Úřadu údaje o kybernetických bezpečnostních incidentech ohlášených podle § 8 odst. 3, bez uvedení ohlašovatele,**
- **h) předává Úřadu na vyžádání údaje podle § 16 odst. 5 a 6,**
- **i) plní roli týmu CSIRT podle příslušného předpisu Evropské unie[393],**
- **j) informuje bez uvedení identifikačních údajů ohlašovatele příslušný orgán jiného členského státu o kybernetickém bezpečnostním incidentu s významným dopadem na kontinuitu poskytování základní nebo digitální služby v tomto členském státě a zároveň o tom informuje Úřad, přičemž zachovává bezpečnost a obchodní zájmy ohlašovatele,**
- **k) spolupracuje s týmy CSIRT jiných členských států a**
- **l) přijímá hlášení o kybernetických bezpečnostních incidentech od orgánů a osob neuvedených v § 3, a pokud to jeho kapacity umožňují, zpracovává je a poskytuje orgánům nebo osobám dotčeným kybernetickým bezpečnostním incidentem metodickou podporu, pomoc a součinnost.**

**(3) Provozovatel národního CERT může vlastním jménem a na vlastní odpovědnost vykonávat i další hospodářskou činnost v oblasti kybernetické bezpečnosti neupravenou tímto zákonem, pokud tato činnost nenaruší plnění povinností uvedených v odstavci 2.**
**(4) Provozovatel národního CERT při plnění povinností uvedených v odstavci 2 koordinuje svou činnost s Úřadem.**

393: Čl. 9 NIS

**(5) Provozovatel národního CERT musí při plnění povinností podle odstavce 2 postupovat nestranně.**

Z důvodové zprávy:

*Toto ustanovení definuje instituci národního dohledového pracoviště, pro které je použito legislativní zkratky národní CERT a vymezuje jeho činnost. Zákon předpokládá, že národní CERT bude provozován zpravidla osobou soukromého práva, která uzavře s NBÚ veřejnoprávní smlouvu, a bude sloužit zejména jako společné kontaktní a koordinační místo pro povinné osoby soukromého práva. Vůči národnímu dohledovému pracovišti budou poskytovatelé služeb elektronických komunikací, subjekty zajišťující sítě elektronických komunikací a subjekty zajišťující významné sítě realizovat svou zákonnou notifikační povinnost.*

*Model standardně soukromoprávního výkonu funkcí národního CERT usnadňuje komunikaci mezi národním CERT a povinnými osobami využívajícími jej povinně jako kontaktní místo. Tyto osoby budou mít totiž rovněž zpravidla soukromoprávní povahu. Národní CERT se bude také moci zapojit do mezinárodních sítí obdobných soukromoprávních národních dohledových pracovišť a těžit z poznatků, které se v rámci těchto sítí neformálně předávají.*

*Předpokládaný soukromoprávní charakter národního CERT je vzhledem ke smyslu a účelu zákona vhodný i z toho důvodu, že provozovatel národního CERT může, jedná-li se o osobu soukromého práva, vyvíjet iniciativně k dosažení účelu zákona též aktivity na základě tacitního dovolení, tj. libovolné aktivity podle své soukromé vůle neporušující zákonné povinnosti. Provozovatel národního CERT tak bude moci například poskytovat metodickou a informační pomoc i subjektům stojícím mimo osobní působnost zákona, tj. osobám mimo definice jednotlivých kategorií povinných osob, které o to projeví zájem. Národní CERT bude moci dále vyvíjet vlastní vzdělávací, publikační, výzkumnou nebo vývojovou činnost apod. Podmínkou omezující iniciativně vykonávané činnosti národního CERT k dosažení účelu tohoto zákona je jejich bezrospornost s plněním povinností vyčtených v zákoně taxativně.*

Z důvodové zprávy k novele ZoKB:

K § 17 odst. 2 písm. a), b), d) a e)
*Mezi subjekty, se kterými komunikuje a spolupracuje provozovatel národního CERT, se doplňují poskytovatelé digitálních služeb.*

K § 17 odst. 2 písm. c)
*Mezi subjekty, se kterými spolupracuje provozovatel národního CERT, v tomto případě, u nichž vyhodnocuje kybernetické bezpečnostní incidenty, se doplňují poskytovatelé digitálních služeb. Toto ustanovení je v obráceném gardu k ustanovení, které stanoví povinnost poskytovatelů digitálních služeb hlásit kybernetické bezpečnostní incidenty provozovateli národního CERT.*

K § 17 odst. 2 písm. g)
*Jedná se o jazykovou úpravu ustanovení a výslovného vztažení povinnosti předávání informací na incidenty nahlášené povinnými subjekty.*

K § 17 odst. 2 písm. h)
*Zpřesňuje se znění ustanovení a ruší se omezení situací, za kterých národní CERT předává Úřadu kontaktní údaje povinných osob.*

K § 17 odst. 2 písm. i) až l)
*Národní CERT (Computer Emergency Response Team) na základě směrnice v tomto ustanovení získává nová kompetence a s nimi související povinnosti. Toto ustanovení je úzce provázáno s § 8, který mimo jiné upravuje hlášení kybernetických bezpečnostních incidentů, které postihly informační systém poskytovatele digitálních služeb. Národní CERT se v tomto ohledu mimo jiné určuje jako jeden z týmů CSIRT (Computer Security Incident Response Team) v České republice; vládní CERT (Národní centrum kybernetické bezpečnosti, jež je součástí NBÚ) je druhým týmem CSIRT ve smyslu směrnice pro incidenty proti bezpečností sítí a informačních systémů určených provozovatelů základních služeb.*

*Týmy CSIRT musí naplňovat požadavky přílohy I směrnice, to je v případě národního CERT provozovaným sdružením CZ.NIC naplněno jednak požadavky na provozovatele národního CERT stanovené § 18 zákona a obsahem veřejnoprávní smlouvy, kterou s ním dle § 19 NBÚ uzavřel. Tato smlouva dle odstavce 1 tohoto ustanovení má zajistit plnění činností podle § 17, tedy i nových požadavků vyplývajících ze směrnice.*

*Konkrétně úkolům týmu CSIRT podle směrnice odpovídá zákon takto:*
*Národní CERT: přijímá hlášení o kybernetických bezpečnostních incidentech, vyhodnocuje je, poskytuje dotčeným subjektů metodickou podporu, pomoc a součinnost, působí jako kontaktní místo, provádí hodnocení zranitelnosti v oblasti kybernetické bezpečnosti, předává NBÚ údaje o incidentech, plní roli týmu CSIRT podle směrnice, spolupracuje s jinými týmy CSIRT, komunikuje s příslušnými orgány jiných členských států a v neposlední řadě přijímá dobrovolná hlášení o kybernetických bezpečnostních incidentech. Tím naplňuje požadavky přílohy I směrnice:*

- *Monitorování incidentů na vnitrostátní úrovni – § 17 odst. 2 písm. b), c), l)*
- *Vydávání včasných varování a upozornění, oznamování a šíření informací o rizicích a incidentech příslušným zúčastněným stranám – § 17 odst. 2 písm. d), e), g), j)*
- *Reakce na incidenty – § 17 odst. 2 písm. c), d)*
- *Poskytování dynamické analýzy rizik a incidentů a přehledu o situaci – § 17 odst. 2 písm. f)*
- *Účast v síti CSIRT – na uvážení provozovatele národního CERT, viz dále komentář k § 20.*

K pojmu **CERT** blíže viz kap. 7 CERT/CSIRT týmy.

Zkratky **CERT** (**C**omputer **E**mergency **R**esponse **T**eam) či **CSIRT** (**C**omputer **S**ecurity **I**ncident **R**esponse **T**eam) jsou využívány pro označení týmů, které jsou zodpovědné za řešení bezpečnostních incidentů, z pohledu uživatelů nebo jiných bezpečnostních týmů. Podstatné je, aby tyto týmy měly předem jasně vymezenou oblast své působnosti.[394]

**První tým typu CERT** vznikl jako reakce na malware (Morris worm) Roberta Tappana Morrise ze dne 2. listopadu 1988.[395] *„Zástupci univerzit, výpočetních center a agentury se shodli, že* ***hlavním problémem je neexistující koordinace a komunikace*** *– chyběl varovný systém a pravidla, jak v případě podobného incidentu postupovat. DARPA se proto rozhodla, že poskytne finance na vytvoření koordinačního centra pro bezpečnostní incident.* ***To vzniklo 17. listopadu 1988 v rámci institutu SEI (Software Engineering Institute) na Carnegie Mellonově univerzitě****.* ***Do vínku dostalo název****, který se posléze rozšířil coby obecné označení podobných oddělení či skupin:* ***Computer Emergency Response Team (CERT)****, posléze bylo označení koordinačního centra změněno na CERT/CC.“*[396]

Vlastní termín **CERT**, je chráněnou značkou v držení Carnegie-Mellon University, která stanoví pravidla pro použití tohoto termínu.[397] V praxi tak došlo k té skutečnosti, že týmy, které vykonávají výše uvedené činnosti, avšak nechtějí procházet procesem stanoveným Carnegie-Mellon University, využívají spíše pojem **CSIRT**.

Povinnost zřídit alespoň jeden bezpečnostní tým typu CSIRT, který by byl odpovědný za zvládání rizik a řešení incidentů podle řádně vymezených postupů a splňují požadavky na bezpečnostní týmy typu CSIRT vyplývá z čl. 9 odst. 1 NIS.

Směrnice NIS stanoví, že tento povinně zřízený tým musí pokrýt svojí činností alespoň odvětví uvedená v příloze č. II (druhy subjektů[398]) a služby uvedené v příloze III (druhy digitálních služeb[399]).

394: Srov. KROPÁČOVÁ, Andrea. *CERT/CSIRT týmy a jejich role.* [online]. [cit. 1. 7. 2018]. Dostupné z: https://www.root.cz/clanky/cert-csirt-tymy-a-jejich-role/

395: Blíže viz např. *Příchod Hackerů: červ Roberta Morrise.* [online]. [cit. 1. 7. 2018]. Dostupné z: https://www.root.cz/clanky/prichod-hackeru-cerv-roberta-morrise/

396: *Příchod hackerů: zrod CERT a CSIRT.* [online]. [cit. 1. 7. 2018]. Dostupné z: https://www.root.cz/clanky/prichod-hackeru-zrod-cert-a-csirt/

397: Blíže viz *Authorization to Use the CERT Mark.* [online]. [cit. 1. 7. 2018]. Dostupné z: https://www.sei.cmu.edu/education-outreach/license-sei-materials/authorization-to-use-cert-mark/index.cfm

398: viz také § 2 ZoKB - kritéria pro určení provozovatele základní služby

399: viz také § 2 písm. l) ZoKB – Digitální služba

V příloze č. I směrnice NIS jsou definovány úkoly a požadavky na bezpečnostní týmy typu CSIRT. Mezi tyto úkoly a povinnosti dle přílohy č. I NIS patří:

1) **Požadavky na týmy CSIRT**

- Týmy CSIRT zajistí, aby v jejich komunikačních službách nebyla žádná kritická místa (tzv. single points of failure), a tyto služby tak byly široce dostupné, a disponují několika způsoby, jimiž budou kontaktovat ostatní a jimiž bude možné kontaktovat je, a to kdykoli. Komunikační kanály musí být navíc jasně specifikované a spolupracujícím partnerům a subjektům spadajícím do působnosti týmů dobře známé.
- Pracoviště týmů CSIRT a jejich podpůrné informační systémy se nacházejí na bezpečném místě.
- Kontinuita činnosti:
  - týmy CSIRT jsou vybaveny vhodnými systémy řízení a směrování požadavků, které usnadní předávání,
  - týmy CSIRT jsou náležitě personálně obsazeny tak, aby byly kdykoli k dispozici,
  - týmy CSIRT musí pracovat s infrastrukturou, jejíž kontinuita je zaručena. Za tímto účelem musí být k dispozici záložní systémy a pracoviště.
- Týmy CSIRT musí mít možnost účastnit se mezinárodních sítí pro spolupráci, pokud chtějí být jejich součástí.

2) **Úkoly týmů CSIRT**

- Úkoly týmů CSIRT zahrnují alespoň:
  - monitorování incidentů na vnitrostátní úrovni,
  - vydávání včasných varování a upozornění, oznamování a šíření informací o rizicích a incidentech příslušným zúčastněným stranám,
  - reakce na incidenty,
  - poskytování dynamické analýzy rizik a incidentů a přehledu o situaci,
  - účast v síti CSIRT.
- Týmy CSIRT naváží spolupráci se soukromým sektorem.
- V zájmu usnadnění spolupráce týmy CSIRT prosazují přijetí a používání společných či standardních postupů v oblasti:
  - řešení incidentů a rizik,
  - klasifikace incidentů, rizik a informací.

Na základě zákona o kybernetické bezpečnosti **jsou v ČR povinně zřízeny dva týmy** typu CERT/CSIRT, **a to národní a vládní**. Každý z těchto týmů má zákonem (§ 17 a násl. ZoKB) přesně stanovené práva a povinnosti.

**Vznik dalších týmů** typu **CERT/CSIRT není zákonem nijak omezen ani regulován.**

Sdružení CZ.NIC provozuje **národní tým CSIRT České republiky – CSIRT.CZ** (blíže viz https://csirt.cz/).

**K odst. 1), 2) a 4)**
Dle zákona o kybernetické bezpečnosti provozovatel národního CERT:

- **přijímá oznámení kontaktních údajů** od orgánů a osob uvedených v § 3 písm. a), b) a h) ZoKB a tyto údaje eviduje a uchovává,

  K pojmu **kontaktní údaje** viz § 16 ZoKB.

- **přijímá hlášení o kybernetických bezpečnostních incidentech** od orgánů a osob uvedených v § 3 písm. b) a h) ZoKB a tyto údaje eviduje, uchovává a chrání,

  K pojmu **kybernetický bezpečnostní incident** blíže viz kap. 2.4.3, § 7 odst. 2 ZoKB.

- **vyhodnocuje kybernetické bezpečnostní incidenty** u orgánů a osob uvedených v § 3 písm. b) a h) ZoKB,

- **poskytuje orgánům a osobám** uvedeným v § 3 písm. a), b) a h) ZoKB **metodickou podporu, pomoc a součinnost při výskytu kybernetického bezpečnostního incidentu**,

  Polem působnosti týmu CSIRT.CZ je celý adresní rozsah České republiky. O pomoc s řešením incidentů se na CSIRT.CZ mohou obrátit všichni správci sítí, kteří potřebují pomoci s řešením incidentu vyžadujícím koordinaci řešení nebo mají podezření, že by incident mohl mít celoplošný dopad. Bližší informace a pokyny k hlášení incidentů je možné nalézt zde.[400] **Tým CSIRT.CZ nemá výkonné pravomoci** a při řešení incidentů působí v roli koordinátora, který může poskytnout také metodickou pomoc při jejich řešení.[401]

- **působí jako kontaktní místo** pro orgány a osoby uvedené v § 3 písm. a), b) a h) ZoKB,

- **provádí hodnocení zranitelností** v oblasti kybernetické bezpečnosti,

- **předává NÚKIB údaje o kybernetických bezpečnostních incidentech** ohlášených podle § 8 odst. 3 ZoKB, bez uvedení ohlašovatele,

- **předává NÚKIB na vyžádání kontaktní údaje** podle § 16 odst. 5 a 6 ZoKB,

400: *Kdy nás kontaktovat.* [online]. [cit. 7. 7. 2018]. Dostupné z: https://www.csirt.cz/page/2632/kdy-nas-kontaktovat/
401: *Služby CSIRT.CZ.* [online]. [cit. 7. 7. 2018]. Dostupné z: https://csirt.cz/page/2764/sluzby/

- **plní roli týmu CSIRT podle směrnice NIS**,

- **informuje** bez uvedení identifikačních údajů ohlašovatele **příslušný orgán jiného členského státu o kybernetickém bezpečnostním incidentu s významným dopadem** na kontinuitu poskytování základní nebo digitální služby v tomto členském státě a zároveň o tom informuje NÚKIB, přičemž zachovává bezpečnost a obchodní zájmy ohlašovatele,

- **spolupracuje s týmy CSIRT jiných členských států**,

- **přijímá hlášení o kybernetických bezpečnostních incidentech od dalších osob,** neuvedených v § 3 ZoKB, a pokud to jeho kapacity umožňují, zpracovává je a poskytuje orgánům nebo osobám dotčeným kybernetickým bezpečnostním incidentem metodickou podporu, pomoc a součinnost.

**Sdružení CZ.NIC je** dle § 17 odst. 4 ZoKB **povinno koordinovat činnost národního CSIRT týmu s činností NÚKIB**.
Vedle povinností explicitně stanovených zákonem o kybernetické bezpečnosti si národní CSIRT stanovil i další úkoly[402], mezi které patří:

- **Informování o nákaze v doméně .CZ**
  Pro účely centrálního monitoringu a řešení hrozeb v doméně druhého řádu vyvinul CSIRT.CZ open source tracker: Malicious Domain Manager.

  Aplikace slouží jako centrální bod pro sběr a analýzu informací o škodlivých URL v doméně .CZ.

  Aplikace podporuje historii hrozeb v doméně a přímé kontaktování jejich držitele. Držitelé domén jsou kontaktováni z dedikované adresy malware@nic.cz.

- **Skener webu**
  Pro neziskový a veřejný sektor primárně je poskytována služba penetračního testování webových stránek. Testování spočívá v automatických a ručních testech zaměřených na hledání bezpečnostních slabin v aplikaci. Každý bezpečnostní nález je označený odhadnutou mírou potencionálního rizika a obsahuje popis doporučení pro jeho případnou opravu.

  Blíže viz https://www.skenerwebu.cz.

402: Všechny úkoly jsou převzaty z: *Služby CSIRT.CZ*. [online]. [cit. 7. 7. 2018]. Dostupné z: https://csirt.cz/page/2764/sluzby/

- **Vzdělávaní a přednášky**
  Ve spolupráci s Akademií CZ.NIC jsou pravidelně realizovány školení Bezpečnost a soukromí na Internetu a Základy fungování CSIRT týmu. CSIRT.CZ také realizuje specializované kurzy pro bezpečnostní složky, státní i vzdělávací instituce či přednášky ad hoc.

- **Pomoc při zřizovaní CERT/CSIRT týmu**

- **Pracovní skupiny**
  Tým CSIRT.CZ pořádá pravidelné setkání bezpečnostních týmů a členů bezpečnostní komunity v České republice.

- **Zátěžové testy**
  Po DDoS útocích z roku 2013, které byly zaměřené na významné služby v České republice, připravily Laboratoře CZ.NIC zátěžové testy dosahující stejné a vyšší intenzity, jako zmiňované DDoS útoky. Ve spolupráci s CSIRT.CZ se tato služba poskytuje bezplatně pro všechny zájemce, kteří splní vstupní podmínky.

- **Intrusion Detection System**
  Ve spolupráci se sdružením CESNET provozuje CSIRT.CZ systém detekující podezřelé chování systémů připojených do sítě Internet.

  V případě zaznamenání podezřelých pokusů o připojení z konkrétních IP adres, jsou o takové události ihned informování zodpovědní administrátoři (prostřednictvím e-mailové adresy ids@csirt.cz).

- **Provozování honeypotů**
  V rámci bezpečnostního výzkumu provozuje CSIRT.CZ ve spolupráci s Laboratořemi CZ.NIC řadu honeypotů. Nově zachycené vzorky malwaru jsou analyzovány.

- **PROKI**
  Rozesílání informací o bezpečnostních incidentech, jež mají původ v rozsahu českých IP adres.[403]

**K odst. 3) a 5)**
Ustanovení § 17 odst. 2 ZoKB umožňuje, aby sdružení CZ.NIC vlastním jménem a na vlastní odpovědnost vykonávalo i další hospodářskou činnost v oblasti kybernetické bezpečnosti, která není přímo upravena zákonem o kybernetické bezpečnosti. Podmínkou však je, že tato další hospodářská činnost nenaruší plnění úkolů národního CSIRT.

403: Blíže viz kap. 6.10.2 Cyber Threat Intelligence Project - PROKI

Sdružení CZ.NIC je povinno při plnění povinností národního CSIRT týmu postupovat nestranně.

**§ 18**
**Provozovatel národního CERT**

**(1) Provozovatelem národního CERT se může stát pouze právnická osoba,**
- **a) která splňuje podmínky uvedené v odstavci 2 a**
- **b) se kterou Úřad uzavřel veřejnoprávní smlouvu podle § 19.**

**(2) Provozovatelem národního CERT může být pouze právnická osoba, která**
- **a) nevyvíjí ani nevyvíjela činnost proti zájmu České republiky ve smyslu zákona upravujícího ochranu utajovaných informací,**
- **b) provozuje nebo spravuje informační systémy nebo služby a sítě elektronických komunikací[404] anebo se na jejich provozu a správě podílí, a to nejméně po dobu 5 let,**
- **c) má technické předpoklady v oblasti kybernetické bezpečnosti,**
- **d) je členem nadnárodní organizace působící v oblasti kybernetické bezpečnosti,**
- **e) nemá v evidenci daní u orgánů Finanční správy České republiky ani orgánů Celní správy České republiky ani v evidenci daní, pojistného na sociální zabezpečení a pojistného na veřejné zdravotní pojištění evidovány nedoplatky,**
- **f) nebyla pravomocně odsouzena za spáchání trestného činu uvedeného v § 7 zákona o trestní odpovědnosti právnických osob a řízení proti nim,**
- **g) není zahraniční osobou podle jiného právního předpisu a**
- **h) nebyla založena nebo zřízena výlučně za účelem dosažení zisku; tím není dotčena možnost provozovatele národního CERT postupovat podle § 17 odst. 3.**

**(3) Zájemce prokazuje splnění podmínek předložením**
- **a) čestného prohlášení v případě odstavce 2 písm. a) až d), g) a h) a**
- **b) potvrzení orgánu Finanční správy České republiky a Celní správy České republiky v případě odstavce 2 písm. e).**

**(4) Z obsahu čestného prohlášení podle odstavce 3 písm. a) musí být zřejmé, že uchazeč splňuje příslušné předpoklady. Potvrzení podle odstavce 3 písm. b), že uchazeč nemá v evidenci daní u orgánů Finanční správy České republiky ani orgánů Celní správy České republiky ani v evidenci daní, pojistného na sociální zabezpečení a pojistného na veřejné zdravotní pojištění evidovány nedoplatky, nesmí být starší než 30 dnů. Za účelem prokázání podmínky uvedené v odstavci 2 písm. f) si Úřad vyžádá výpis z evidence Rejstříku trestů podle jiného právního předpisu.**[405]

404: Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů.

405: Zákon č. 269/1994 Sb., o Rejstříku trestů, ve znění pozdějších předpisů.

**(5) Provozovatel národního CERT vykonává činnosti podle § 17 odst. 2 písm. a) až c), e) a g) až l) bezúplatně. Provozovatel národního CERT je povinen vynaložit k řádnému a účelnému výkonu činností uvedených v § 17 odst. 2 nezbytné náklady.**
**(6) Úřad zveřejní na svých internetových stránkách údaje o provozovateli národního CERT, a to jeho obchodní firmu nebo název, adresu sídla, identifikační číslo osoby, identifikátor datové schránky a adresu jeho internetových stránek.**

Z důvodové zprávy:

*Toto ustanovení stanoví obecné podmínky pro výběr provozovatele národního CERT. Současně je upraven způsob založení jeho závazku k provozování národního CERT formou veřejnoprávní smlouvy uzavřené s NBÚ. Užití institutu veřejnoprávní smlouvy odpovídá předpokladu, že provozovatelem národního CERT bude osoba soukromého práva. Závazky provozovatele národního CERT vykonávat činnosti uvedené v tomto zákoně mají sice převážně charakter soukromoprávní, ve vztahu k poskytovatelům služeb elektronických komunikací, subjektům zajišťující sítě elektronických komunikací a subjektům zajišťující významné sítě však bude provozovatel národního CERT vystupovat jako subjekt, prostřednictvím jehož činnosti tyto povinné osoby plní některé své zákonné povinnosti, typicky povinnost oznamovat kontaktní údaje a v případě subjektů zajišťujících významné sítě též povinnost hlásit výskyt kybernetických bezpečnostních incidentů.*

*Vzhledem k tomu, že národní CERT je pracovištěm velkého významu pro systém kybernetické bezpečnosti České republiky, vyžaduje se, aby měl jeho provozovatel sídlo na území České republiky. S ohledem na bezpečnostní expozici národního CERT tedy není možno vnímat tento požadavek jako diskriminační vůči osobám se sídlem v ostatních státech Evropské unie. Bezúhonnost, transparentní vlastnická struktura a neexistence splatných finančních závazků vůči státu jsou v případě spolupráce státu a osoby soukromého práva standardně požadovanými formálními podmínkami. Zákon rovněž formuluje materiální podmínky výkonu funkce provozovatele národního CERT, přičemž se požaduje, aby provozovatel národního CERT prokázal faktické schopnosti, zkušenosti a technické možnosti schopnost vykonávat činnosti uložené mu tímto zákonem, jakož i schopnost pracovat v součinnosti se zahraničními subjekty působícími na úseku kybernetické bezpečnosti. Zákon dále požaduje, aby provozovatel národního CERT vykonával činnosti svěřené mu tímto zákonem nestranně, bez ohledu na jeho případný smluvní či jiný vztah s povinnými osobami.*

Z důvodové zprávy k novele ZoKB:

K § 18 odst. 5
*Toto ustanovení reaguje na rozšíření kompetencí provozovatele národního CERT v § 17 a rozšiřuje adekvátně okruh činností, jež provozovatel národního CERT vykonává bezplatně.*

K § 18 odst. 5
*Legislativně technická úprava z důvodu rozšíření kompetencí provozovatele národního CERT. Pro zajištění důsledného naplňování povinností vyplývajících ze směrnice a následně ze zákona o kybernetické bezpečnosti se zakotvuje povinnost národního CERT vynaložit na zajištění výkonu kompetencí adekvátní finanční prostředky.*

K pojmu **CERT** blíže viz kap. 7 CERT/CSIRT týmy a § 17 ZoKB.

**K odst. 1) a 2)**
**Provozovatelem národního CERT týmu je sdružení CZ.NIC.**

Ustanovení § 18 ZoKB definuje podmínky, za kterých se může subjekt stát provozovatelem národního CERT.

Provozovatelem národního CERT může být pouze **právnická osoba**[406]**, s níž NÚKIB** (či dříve NBÚ) **uzavřel veřejnoprávní smlouvu**[407] (dle § 19 ZoKB), a **která splňuje následující podmínky:**

a) **nevyvíjí ani nevyvíjela činnost proti zájmu České republiky** ve smyslu zákona upravujícího ochranu utajovaných informací,

   Dle § 2 písm. b) ZoOUI je „*zájmem České republiky zachování její ústavnosti, svrchovanosti a územní celistvosti, zajištění vnitřního pořádku a bezpečnosti, mezinárodních závazků a obrany, ochrana ekonomiky a ochrana života nebo zdraví fyzických osob.*"

b) **provozuje nebo spravuje informační systémy nebo služby a sítě** elektronických komunikací anebo se na jejich provozu a správě podílí, **a to nejméně po dobu 5 let,**

c) **má technické předpoklady v oblasti kybernetické bezpečnosti,**

d) **je členem nadnárodní organizace působící v oblasti kybernetické bezpečnosti,**

---

406: Dle § 20 odst. 1 OZ se právnickou osobou rozumí „***organizovaný útvar, o kterém zákon stanoví, že má právní osobnost, nebo jehož právní osobnost zákon uzná.*** *Právnická osoba může bez zřetele na předmět své činnosti mít práva a povinnosti, které se slučují s její právní povahou.*" Stát se v oblasti soukromého práva považuje za právnickou osobu. (§ 21 OZ).
**Právnickou osobou může být osoba soukromého či veřejného práva** podle toho v jakém zájmu je právnická osoba ustanovena (§ 144 OZ). Z pohledu občanského práva jsou právnickou osobou korporace (viz § 210 a násl. OZ), fundace (viz § 303 a násl. OZ) a ústavy (viz § 402 a násl.).
407: Využití institutu veřejnoprávní smlouvy dle § 160 a násl. SŘ odpovídá předpokladu, že provozovatelem národního CERT bude osoba soukromého práva.

Požadavek na provozování některého ze systémů uvedených pod písmenem c), na existenci technických předpokladů v oblasti kybernetické bezpečnosti a členství v nadnárodní organizaci působící v oblasti kybernetické bezpečnosti dává státu garanci, že se daná osoba dostatečně dlouho a kvalitně věnuje problematice kybernetické bezpečnosti, řešení incidentů aj. De facto jde o prokázání faktické schopnosti, zkušenosti a technické možnosti vykonávat činnosti uložené mu ZoKB.

e) **nemá** v evidenci daní u orgánů Finanční správy České republiky ani orgánů Celní správy České republiky ani **v evidenci daní, pojistného na sociální zabezpečení a pojistného na veřejné zdravotní pojištění evidovány nedoplatky,**

f) **nebyla pravomocně odsouzena za spáchání trestného** činu uvedeného v § 7 zákona o trestní odpovědnosti právnických osob a řízení proti nim,

Neexistence splatných finančních závazků vůči státu, stejně jako prokázání bezúhonnosti je v případě spolupráce státu a osoby soukromého práva standardně požadovanou formální podmínkou pro uzavření smlouvy.

Zákon o kybernetické bezpečnosti se v § 18 odst. 2 písm. f) dopouští faktické nepřesnosti, která je způsobena novelizací zákona č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim.[408] V tomto zákoně byly původně v § 7 vymezeny ty trestné činy, jichž se může dopustit právnická osoba. V současné účinné právní úpravě je v § 7 uvedeno negativní vymezení trestných činů.

Ustanovení § 7 TOPO (s účinností od 1. 12. 2016) stanoví, že právnická osoba může být trestně odpovědná za spáchání všech trestných činů s výjimkou trestných činů v tomto ustanovení taxativně uvedených.

Vedle vymezení okruhu trestných činů je třeba v případě trestně právní odpovědnosti právnických osob řešit i otázku přičitatelnosti. *„Přestože právnická osoba je fiktivní konstrukt, právo obecně ve vztahu k právnickým osobám uznává jejich způsobilost právně (tedy i protiprávně) jednat, včetně toho, že se jim přičítá zavinění. Zavinění jakožto podmínka trestní odpovědnosti se právnické osobě přičítá, jestliže nastaly okolnosti dle § 8 odst. 2 zákona o TOPO.“* [409]

Dle § 8 odst. 1 zákona o TOPO se trestným činem spáchaným právnickou osobou rozumí protiprávní čin spáchaný v jejím zájmu nebo v rámci její činnosti, jednal-li tak

408: Dále jen **TOPO**.

409: NOVOTNÝ, František a kolektiv. *Trestní právo hmotné*. 4. aktualizované a doplněné vydání. Plzeň: Aleš Čeněk, 2017. s. 334

a) statutární orgán nebo člen statutárního orgánu, anebo jiná osoba ve vedoucím postavení v rámci právnické osoby, která je oprávněna jménem nebo za právnickou osobu jednat,
b) osoba ve vedoucím postavení v rámci právnické osoby, která u této právnické osoby vykonává řídící nebo kontrolní činnost, i když není osobou uvedenou v písmenu a),
c) ten, kdo vykonává rozhodující vliv na řízení této právnické osoby, jestliže jeho jednání bylo alespoň jednou z podmínek vzniku následku zakládajícího trestní odpovědnost právnické osoby, nebo
d) zaměstnanec nebo osoba v obdobném postavení (dále jen „zaměstnanec“) při plnění pracovních úkolů, i když není osobou uvedenou v písmenech a) až c),
jestliže lze právnické osobě jednání výše uvedené osoby přičítat podle § 8 odst. 2 TOPO.

g) **není zahraniční osobou** podle jiného právního předpisu,

Za zahraniční osobu se dle § 3024 OZ považuje fyzická osoba s bydlištěm nebo právnická osoba se sídlem mimo území České republiky.

Vzhledem k významnosti národního CERT týmu v oblasti kybernetické bezpečnosti ČR je požadováno, aby provozovatel tohoto týmu měl sídlo na území ČR. Tento požadavek nelze vnímat jako diskriminaci vůči jiným osobám se sídlem v jiném členském státu Unie.

h) **nebyla založena nebo zřízena výlučně za účelem dosažení zisku**; tím není dotčena možnost provozovatele národního CERT postupovat podle § 17 odst. 3 ZoKB.

**K odst. 3) a 4)**
Právnická osoba, která se chce stát provozovatelem národního CERT, prokazuje splnění podmínek předložením čestného prohlášení [v případě § 18 odst. 2 písm. a) až d), g), h) ZoKB] a potvrzením orgánu Finanční správy České republiky a Celní správy České republiky [v případě § 18 odst. 2 písm. e) ZoKB].

***Z obsahu čestného prohlášení musí být zřejmé, že uchazeč splňuje příslušné předpoklady.*** **Potvrzení**, že uchazeč nemá v evidenci daní u orgánů Finanční správy České republiky ani orgánů Celní správy České republiky ani v evidenci daní, pojistného na sociální zabezpečení a pojistného na veřejné zdravotní pojištění evidovány nedoplatky, **nesmí být starší než 30 dnů.**

Z důvodu **prokázání té skutečnosti, že právnická osoba nebyla pravomocně odsouzena za spáchání trestného** činu **si NÚKIB vyžádá výpis z evidence Rejstříku trestů.**

**K odst. 5)**
Provozovatel národního CERT **vykonává činnosti uvedené v § 17 odst. 2 ZoKB bezúplatně**. Výjimkou z podmínky bezplatnosti jsou pouze následující činnosti:

- **poskytuje orgánům a osobám** uvedeným v § 3 písm. a), b) a h) ZoKB **metodickou podporu, pomoc a součinnost při výskytu kybernetického bezpečnostního incidentu,**
- **provádí hodnocení zranitelností** v oblasti kybernetické bezpečnosti.

Provozovatel národního CERT je povinen vynaložit k řádnému a účelnému výkonu činností uvedených v § 17 odst. 2 ZoKB nezbytné náklady.

**K odst. 6)**
Z důvodu možnosti kontaktovat provozovatele národního CERT týmu jsou údaje o tomto provozovateli zveřejněny na internetových stránkách NÚKIB. Zveřejněny jsou následující informace: obchodní firma nebo název, adresa sídla, identifikační číslo osoby, identifikátor datové schránky a adresa jeho internetových stránek.

**§ 19**
**Veřejnoprávní smlouva**

**(1) Úřad uzavírá veřejnoprávní smlouvu (dále jen „smlouva") s právnickou osobou vybranou postupem podle § 163 odst. 4 správního řádu za účelem spolupráce v oblasti kybernetické bezpečnosti a zajištění činností podle § 17 odst. 2. Řízení o výběru žádosti vyhlašuje Úřad.**
**(2) Smlouva obsahuje alespoň**
**a) označení smluvních stran,**
**b) vymezení předmětu smlouvy,**
**c) práva a povinnosti smluvních stran,**
**d) podmínky spolupráce smluvních stran,**
**e) způsob a podmínky odstoupení smluvních stran od smlouvy,**
**f) výpovědní lhůtu a výpovědní důvody,**
**g) zákaz zneužití údajů získaných v souvislosti s výkonem činností uvedených v § 17 odst. 2,**
**h) vymezení podmínek pro výkon činnosti národního CERT podle § 17 odst. 3 a**
**i) způsob předání a rozsah údajů předávaných Úřadu v případě zániku závazku.**
**(3) Smlouvu uzavřenou podle odstavce 1 Úřad zveřejňuje ve Věstníku Úřadu, s výjimkou těch částí smlouvy, jejichž zveřejnění neumožňuje jiný právní předpis.**
**(4) Není-li uzavřena smlouva podle odstavce 1, nebo v případě zániku závazku, vykonává činnost národního CERT Úřad.**

Z důvodové zprávy:

*Toto ustanovení upravuje způsob výběru provozovatele národního CERT, účel a podstatné náležitosti veřejnoprávní smlouvy, kterou bude NBÚ uzavírat s provozovatelem národního CERT. Zákon předpokládá, že tato veřejnoprávní smlouva bude zveřejněna ve Věstníku NBÚ. Zveřejní obsahu této smlouvy společně s institutem výběru provozovatele národního CERT v řízení o výběru žádosti*

*podle správního řádu a institutem zveřejnění výsledku výběru přitom představuje projev principu transparentnosti výkonu veřejné správy.*

*Vzhledem k tomu, že může dojít k situaci, kdy nebude uzavřena veřejnoprávní smlouva s provozovatelem národního CERT nebo kdy uzavřená veřejnoprávní smlouva pozbude účinnosti (např. pokud provozovatel národního CERT přestane splňovat zákonné podmínky), je třeba pro tento výjimečný případ upravit provizorní fungování národního CERT. V takovém případě pak bude funkce národního CERT vykonávat NBÚ.*

**K odst. 1)**
Za účelem spolupráce v oblasti kybernetické bezpečnosti a zajištění činností podle § 17 odst. 2 ZoKB uzavírá NÚKIB s provozovatelem národního CERT veřejnoprávní smlouvu. Ustanovení § 19 ZoKB upravuje způsob výběru tohoto provozovatele, účel a podstatné náležitosti veřejnoprávní smlouvy.

*„Veřejnoprávní smlouva je dvoustranné nebo vícestranné právní jednání, které zakládá, mění nebo ruší veřejnoprávní poměry. Alespoň jednou ze stran veřejnoprávní smlouvy je vždy orgán veřejné správy. Veřejnoprávní smlouva musí být vždy v souladu s veřejným zájmem a právními předpisy, které nesmí ani žádným způsobem obcházet."* [410]

Veřejnoprávní smlouva je s vybranou právnickou osobou uzavřena postupem podle § 163 odst. 4 SŘ, které odkazuje na řízení o výběru žádosti (§ 146 SŘ).

V ustanovení § 146 SŘ se stanoví, že řízení prováděné na základě zvláštního zákona formou výběru žádosti nejlépe odpovídající stanoveným požadavkům, popřípadě výběru více takových žádostí, se vede jako společné řízení o všech žádostech. Žádnou ze žádostí nelze ze společného řízení vyloučit.

Vlastní řízení se zahajuje vyhlášením veřejnou vyhláškou na úřední desce NÚKIB (dříve NBÚ) a současně se oznamuje prostřednictvím hromadných sdělovacích prostředků.

Lhůta pro podávání žádostí nesmí být kratší než 30 dnů.

Národní úřad pro kybernetickou a informační bezpečnost (dříve NBÚ) je povinen zveřejnit kritéria hodnocení podaných žádostí, pravidla postupu (v případě, že řízení formou výběru bude probíhat ve více kolech).

410: MAISNER, Martin a Barbora VLACHOVÁ. *Zákon o kybernetické bezpečnosti. Komentář.* Praha: Wolters Kluwer, 2015. s. 125

**K odst. 2)**
Ustanovení § 19 odst. 2 ZoKB definuje minimální náležitosti obsahu veřejnoprávní smlouvy, mezi které patří:

- označení smluvních stran,
- práva a povinnosti smluvních stran,
- vymezení předmětu smlouvy,
- podmínky spolupráce smluvních stran,
- způsob a podmínky odstoupení od smlouvy,
- výpovědní lhůtu a důvody,
- zákaz zneužití údajů získaných v souvislosti s výkonem činností provozovatele národního CERT (viz § 17 odst. 2 ZoKB),
- vymezení podmínek pro výkon další hospodářské činnosti v oblasti kybernetické bezpečnosti (viz § 17 odst. 3 ZoKB),
- způsob předání a rozsah údajů předávaných NÚKIB v případě zániku závazku.

**K odst. 3) a 4)**
Uzavřené veřejnoprávní smlouvy jsou zveřejněny ve Věstníku NÚKIB. Nemusí být zveřejněny ty části smlouvy, jejichž zveřejnění neumožňuje jiný právní předpis.

Doposud byla uzavřena jen jedna smlouva a tu uzavíral NBÚ, který byl gestorem kybernetické bezpečnosti před vznikem NÚKIB. Smlouva je dostupná na: https://www.govcert.cz/download/uredni-deska/vestnik/NBU-Smlouva-narodni-cert-201512.pdf

**K odst. 5)**
Dne 19. prosince 2012 podepsali zástupci sdružení CZ.NIC a Národního bezpečnostního úřadu memorandum[411] (navazující na předchozí memoranda) týkající se provozu agendy Národního bezpečnostního týmu CSIRT.CZ sdružením CZ.NIC. Toto memorandum vstoupilo v platnost 1. ledna 2013 a platilo po dobu tří let.

V srpnu 2015 byl na základě požadavků stanovených v ZoKB vybrán provozovatel Národního CERT týmu. Tímto provozovatelem se stalo sdružení CZ.NIC.[412] Dne 18. prosince 2015 pak došlo k podpisu Veřejnoprávní smlouvy o zajištění činnosti Národního CERT a o spolupráci v oblasti kybernetické bezpečnosti.[413] Tato smlouva byla uzavřena na dobu neurčitou.

411: *Memorandum o Computer Emergency Response Team/Computer Security Incident Response Team České republiky.* [online]. Dostupné z: https://www.nic.cz/files/nic/NBU_Memorandum_12-12.pdf

412: Viz https://www.nic.cz/page/351/

413: Blíže viz [online]. Dostupné z: https://www.nic.cz/files/nic/doc/NBU-Smlouva-narodni-cert-201512.pdf

V případě, že by nedošlo k uzavření veřejnoprávní smlouvy, či by došlo k zániku závazku mezi vybranou právnickou osobou provozující národní CERT a NÚKIB, začne NÚKIB vykonávat činnost národního CERT.

**§ 20**
**Vládní CERT**

**Vládní CERT jako součást Úřadu**

**a) přijímá oznámení kontaktních údajů od orgánů a osob uvedených v § 3 písm. c) až g),**
**b) přijímá hlášení o kybernetických bezpečnostních incidentech od orgánů a osob uvedených v § 3 písm. c) až g),**
**c) vyhodnocuje údaje o kybernetických bezpečnostních událostech a kybernetických bezpečnostních incidentech z kritické informační infrastruktury, informačního systému základní služby, významných informačních systémů a dalších informačních systémů veřejné správy,**
**d) poskytuje orgánům a osobám uvedeným v § 3 písm. c) až g) metodickou podporu a pomoc,**
**e) poskytuje součinnost orgánům a osobám uvedeným v § 3 písm. c) až g) při výskytu kybernetického bezpečnostního incidentu a kybernetické bezpečnostní události,**
**f) přijímá podněty a údaje od orgánů a osob uvedených v § 3 a od jiných orgánů a osob a tyto podněty a údaje vyhodnocuje,**
**g) přijímá údaje od provozovatele národního CERT a tyto údaje vyhodnocuje,**
**h) přijímá údaje od orgánů, které vykonávají působnost v oblasti kybernetické bezpečnosti v zahraničí, a tyto údaje vyhodnocuje,**
**i) poskytuje podle § 9 odst. 4 provozovateli národního CERT, orgánům vykonávajícím působnost v oblasti kybernetické bezpečnosti v zahraničí a jiným osobám působícím v oblasti kybernetické bezpečnosti údaje z evidence incidentů,**
**j) provádí hodnocení zranitelností v oblasti kybernetické bezpečnosti,**
**k) informuje bez uvedení identifikačních údajů ohlašovatele příslušný orgán jiného členského státu o kybernetickém bezpečnostním incidentu, který má významný dopad na kontinuitu poskytování základních služeb v tomto členském státě nebo se dotýká poskytování digitálních služeb v tomto členském státě, přičemž zachovává bezpečnost a obchodní zájmy ohlašovatele,**
**l) přijímá hlášení o kybernetickém bezpečnostním incidentu od orgánů a osob neuvedených v § 3; vládní CERT hlášení zpracovává, a pokud to jeho kapacity umožňují a jedná se o kybernetický bezpečnostní incident s významným dopadem, poskytuje orgánům nebo osobám dotčeným kybernetickým bezpečnostním incidentem metodickou podporu, pomoc a součinnost,**
**m) plní roli týmu CSIRT podle příslušného předpisu Evropské unie[414] a**

414: Viz čl. 9 NIS

**n) spolupracuje s týmy CSIRT jiných členských států.**

Z důvodové zprávy:

*Vládní CERT je součástí NBÚ, respektive Národního centra kybernetické bezpečnosti, jež je organizačním celkem NBÚ, který zajišťuje jeho činnost. Vládní CERT je koncipován jako centrální veřejnoprávní pracoviště a veřejnoprávní „single point of contact" pro oblast kybernetické bezpečnosti. Jeho činnost zahrnuje příjem kontaktních údajů od vybraných povinných osob, příjem informací o kybernetické bezpečnostní situaci, a to zejména příjem povinných a iniciativních hlášení kybernetických bezpečnostních incidentů a dalších údajů o kybernetické bezpečnostní situaci od tuzemských a zahraničních orgánů veřejné moci a spolupracujících subjektů a jejich vyhodnocování. Vládní CERT dále poskytuje součinnost vybraným typům povinných osob při výskytu kybernetického bezpečnostního incidentu, zajišťuje součinnost s ostatními orgány a subjekty zajišťujícími kybernetickou bezpečnost v České republice a ve spolupracujících nebo spojeneckých státech a rovněž provádí hodnocení zranitelností v oblasti kybernetické bezpečnosti.*

Z důvodové zprávy k novele ZoKB:

K § 20 písm. a), b), d) a e)
*Mezi subjekty, se kterými komunikuje a s nimiž spolupracuje vládní CERT, se doplňují nové povinné subjekty – provozovatelé základních služeb a správci a provozovatelé informačních systémů základních služeb.*

K § 20 písm. c)
*Mezi informační systémy, u nichž vládní CERT vyhodnocuje údaje o kybernetických bezpečnostních událostech a kybernetických bezpečnostních incidentech, se doplňují informační systémy, na jejichž provozování je závislé poskytování základních služeb.*

K § 20 písm. i)
*Legislativně technická úprava vyplývající z potřeby doplnění nových písmen do tohoto ustanovení.*

K § 20 písm. j) a písm. k) až n)
*Vládní CERT na základě směrnice v tomto ustanovení získává nové kompetence a s nimi související povinnosti. Toto ustanovení je úzce provázáno s § 8, který upravuje hlášení kybernetických bezpečnostních incidentů.*

*Vládní CERT podle zákona ve znění tohoto návrhu: přijímá hlášení o kybernetických bezpečnostních incidentech, vyhodnocuje je, poskytuje dotčeným subjektů metodickou podporu, pomoc a součinnost, působí jako kontaktní místo, provádí hodnocení zranitelnosti v oblasti kybernetické bezpečnosti, předává NBÚ údaje o incidentech, plní roli týmu CSIRT podle směrnice, spolupracuje s jinými týmy*

*CSIRT, komunikuje s příslušnými orgány jiných členských států a v neposlední řadě přijímá dobrovolná hlášení o kybernetických bezpečnostních incidentech.*
*Tím naplňuje požadavky přílohy I směrnice:*

- *Monitorování incidentů na vnitrostátní úrovni – § 20 písm. b), c), f), g), l).*
- *Vydávání včasných varování a upozornění, oznamování a šíření informací o rizicích a incidentech příslušným zúčastněným stranám – § 20 písm. d), e), i), n).*
- *Reakce na incidenty – § 20 písm. d), e).*
- *Poskytování dynamické analýzy rizik a incidentů a přehledu o situaci – § 20 písm. j).*
- *Účast v síti CSIRT – § 20 písm. m).*

*Tím, že vládní CERT, který je součástí NBÚ, plní roli týmu CSIRT, bude i naplňovat požadavky směrnice na účast týmu CSIRT v síti CSIRT podle článku 12 směrnice. Účast zástupců národního CERT bude ponechána na jejich uvážení.*

*Směrnice stanoví ve svém článku 9, že každý členský stát zřídí jeden nebo více týmu CSIRT, neřeší však, že by se měli zástupci všech týmů CSIRT členského státu povinně účastnit práce sítě CSIRT. Postačuje tak plně účast alespoň jednoho týmu CSIRT, což naplní zástupci vládního CERT. Ustanovení upravuje postup vládního CERT v případě, že má nahlášený kybernetický bezpečnostní incident významný dopad na kontinuitu poskytování základních služeb, nebo dopad na poskytování digitálních služeb v jiném členském státu Evropské unie. V takovém případě se v souladu s čl. 14 odst. 5, potažmo čl. 16 odst. 6 směrnice zakotvuje oprávnění vládního CERT informovat o daném incidentu příslušné orgány jiných členských států.*

*Směrnice předvídá ve svém čl. 20 situaci, kdy subjekt, který nebyl určen jako provozovatel základních služeb a není ani poskytovatelem digitálních služeb, zaregistruje napadení bezpečnosti jeho informačních systémů a má snahu tuto situaci řešit. V tomto případě může tento kybernetický bezpečnostní incident dobrovolně nahlásit vládnímu CERT a ve spolupráci s ním situaci řešit. Vládní CERT v tomto případě hlášení zpracuje, a pokud to jeho kapacity umožňují a jedná se o kybernetický bezpečnostní incident s významným dopadem, poskytuje přiměřeně, jako když je mu nahlášen kybernetický bezpečnostní incident u provozovatele základních služeb.*

Na základě zákona o kybernetické bezpečnosti **jsou v ČR povinně zřízeny dva týmy** typu CERT/CSIRT, **a to národní a vládní**.

Provozovatelem národní CERT je právnická osoba s níž NÚKIB (dříve NBÚ) uzavřel veřejnoprávní smlouvu (viz § 19 ZoKB).

Vládní CERT (**GovCERT.CZ** – blíže viz https://www.govcert.cz/) je zřízen na základě zákona jakožto součást Národního úřadu pro kybernetickou a informační bezpečnost (dříve v gesci NBÚ).

K pojmu **CERT** blíže viz kap. 7 CERT/CSIRT týmy a § 17 ZoKB.

Dle zákona o kybernetické bezpečnosti vládní CERT:

- **přijímá oznámení kontaktních údajů** od orgánů a osob uvedených v § 3 písm. c) až g) ZoKB,

  K pojmu **kontaktní údaje** viz § 16 ZoKB.

- **přijímá hlášení o kybernetických bezpečnostních incidentech** od orgánů a osob uvedených v § 3 písm. c) až g) ZoKB,

  K pojmu **kybernetický bezpečnostní incident** blíže viz kap. 2.4.3, § 7 odst. 2 ZoKB.

- **vyhodnocuje údaje** o kybernetických bezpečnostních **událostech** a kybernetických bezpečnostních **incidentech** z kritické informační infrastruktury, informačního systému základní služby, významných informačních systémů a dalších informačních systémů veřejné správy,

  K pojmu **kybernetická bezpečnostní událost** blíže viz kap. 2.4.2, § 7 odst. 1 ZoKB.

- **poskytuje orgánům a osobám** uvedeným v § 3 písm. c) až g) ZoKB **metodickou podporu a pomoc,**

- **poskytuje součinnost** orgánům a osobám uvedeným v § 3 písm. c) až g) ZoKB **při výskytu kybernetického bezpečnostního incidentu a kybernetické bezpečnostní události,**

  Řešení bezpečnostních incidentů patří k hlavním činnostem vládního týmu. Při nahlášení kybernetického bezpečnostního incidentu je vládní tým GovCERT.CZ připraven pomoci IT specialistům po technické stránce, včetně poskytnutí rad pro další preventivní opatření. V případě, že dojde ke zjištění, že některý z incidentů cílí na více subjektů, je vládní tým GovCERT.CZ připraven koordinovat společný postup na jeho řešení.[415]

- **přijímá podněty a údaje** od orgánů a osob uvedených v § 3 ZoKB a od jiných orgánů a osob **a tyto** podněty a údaje **vyhodnocuje,**

- **přijímá údaje od provozovatele národního CERT** a tyto údaje vyhodnocuje,

415: *Poskytované služby.* [online]. [cit. 1. 8. 2018]. Dostupné z: https://www.govcert.cz/cs/vladni-cert/poskytovane-sluzby/

- **přijímá údaje od orgánů, které vykonávají působnost v oblasti kybernetické bezpečnosti v zahraničí**, a tyto údaje vyhodnocuje,

- **poskytuje podle údaje z evidence incidentů** (viz § 9 odst. 4 ZoKB) provozovateli národního CERT, orgánům vykonávajícím působnost v oblasti kybernetické bezpečnosti v zahraničí a jiným osobám působícím v oblasti kybernetické bezpečnosti údaje z evidence incidentů,

- **provádí hodnocení zranitelností** v oblasti kybernetické bezpečnosti,

- **informuje bez uvedení identifikačních údajů ohlašovatele příslušný orgán jiného členského státu o kybernetickém bezpečnostním incidentu, který má významný dopad** na kontinuitu poskytování základních služeb v tomto členském státě nebo se dotýká poskytování digitálních služeb v tomto členském státě, přičemž zachovává bezpečnost a obchodní zájmy ohlašovatele,

- **přijímá hlášení o kybernetickém bezpečnostním incidentu od orgánů a osob neuvedených v § 3 ZoKB**; vládní CERT hlášení zpracovává, a pokud to jeho kapacity umožňují a jedná se o kybernetický bezpečnostní incident s významným dopadem, poskytuje orgánům nebo osobám dotčeným kybernetickým bezpečnostním incidentem metodickou podporu, pomoc a součinnost,

- **plní roli týmu CSIRT** podle čl. 9 NIS,

- **spolupracuje s týmy CSIRT jiných členských států**.

Vedle povinností explicitně stanovených zákonem o kybernetické bezpečnosti si vládní CERT stanovil i další úkoly[416], mezi které patří:

- **Sdílení dat**
  GovCERT.CZ získává v rámci spolupráce s různými nadnárodními organizacemi, které se zabývají kybernetickou bezpečností, množství reportů a dat, které se týkají potenciálně infikovaných informačních systémů v ČR. Tyto informace v rámci proaktivní činnosti poskytuje dalším subjektům. Sdílená data jsou rozdělena do následujících projektů:
  - **BotnetFeed** – pomocí tohoto nástroje jsou zpracovávána data z převzatých C&C serverů o koncových stanicích zapojených do sítí botnetů. Pro identifikaci případně nakaženého počítačového systému je správci IP rozsahu předána IP adresa a informace o botnetu, do kterého je začleněna.

416: Všechny úkoly jsou převzaty z: *Poskytované služby.* [online]. [cit. 7. 7. 2018]. Dostupné z: https://www.govcert.cz/cs/vladni-cert/poskytovane-sluzby/

- **IHAP** (Incident Handling Automation Project), **MDM** (Malicious Domain Manager) – v rámci těchto projektů jsou sbírány fragmenty indikátorů kompromitace (IoC) z různých serverů. Mezi nejčastější indikátory patří phishing, útoky hrubou silou, ids alerty, spam, pokusy o skenování, zneužívání zranitelností, výskyt malware a mnoho dalších typů. Na základě těchto dat jsou připravovány krátké reporty, které vždy obsahují IP adresu kompromitovaného stroje a stručné shrnutí, o jaký typ incidentu se jedná.

- **Shadowserver** – projekt je zaměřen na průběžné vyhledávání relevantních informací o zranitelnostech v kyberprostoru a o výskytech těchto zranitelností na konkrétních IP adresách.

- **Nasazování Honeypotů**

- **Penetrační testování**
  Jedná se o legální pokus o průnik do testovaných systémů. Výsledkem je zpráva o chybách v zabezpečení testovaného subjektu, která je určena výhradně jeho vlastníkovi, který na základě zprávy učiní příslušná bezpečnostní opatření.

  Další možností je provedení skenování zranitelností podle OWASP (Open Web Application Security Project).

- **Informační HUB**
  Na webových stránkách govcert.cz je možné nalézt informace, rešerše, analýzy a články týkající se aktuálních hrozeb a zranitelností se vztahem k systémům v České republice. Uvedené dokumenty jsou doplňovány o pravidelné měsíční bulletiny shrnující významné bezpečnostní incidenty v CŘ i zahraničí.

- **Vzdělávání a výzkumná činnost**

- **Forenzní laboratoř a SCADA laboratoř**

## HLAVA III
## STAV KYBERNETICKÉHO NEBEZPEČÍ

### § 21
### Stav kybernetického nebezpečí

**(1) Stavem kybernetického nebezpečí se rozumí stav, ve kterém je ve velkém rozsahu ohrožena bezpečnost informací v informačních systémech nebo bezpečnost služeb elektronických**

**komunikací anebo bezpečnost a integrita sítí elektronických komunikací[417], a tím by mohlo dojít k porušení nebo došlo k ohrožení zájmu České republiky ve smyslu zákona upravujícího ochranu utajovaných informací.**
**(2) O vyhlášení stavu kybernetického nebezpečí rozhoduje ředitel Úřadu. Rozhodnutí o vyhlášení stavu kybernetického nebezpečí se vyhlašuje vyvěšením na úřední desce Úřadu. Informace o vyhlášení stavu kybernetického nebezpečí se zveřejňuje v celoplošném rozhlasovém a televizním vysílání. Provozovatel celoplošného televizního nebo rozhlasového vysílání je povinen bez náhrady nákladů na základě žádosti Úřadu neprodleně a bez úpravy obsahu a smyslu uveřejnit informace o vyhlášení stavu kybernetického nebezpečí.**
**(3) Rozhodnutí o vyhlášení stavu kybernetického nebezpečí nabývá účinnosti okamžikem, který se v rozhodnutí stanoví. Stav kybernetického nebezpečí se vyhlašuje na dobu nezbytně nutnou, nejdéle však na 7 dnů. Uvedenou dobu může ředitel Úřadu prodloužit; souhrnná doba trvání vyhlášeného stavu kybernetického nebezpečí nesmí být delší než 30 dnů.**
**(4) V průběhu vyhlášeného stavu kybernetického nebezpečí ředitel Úřadu informuje vládu o postupech při řešení stavu kybernetického nebezpečí a o aktuálním stavu hrozeb, které vedly k vyhlášení stavu kybernetického nebezpečí. Za stavu kybernetického nebezpečí a za nouzového stavu[418] v případech podle odstavce 6 je Úřad oprávněn vydat rozhodnutí nebo opatření obecné povahy podle § 13 rovněž orgánům a osobám uvedeným v § 3 písm. a) a b).**
**(5) Stav kybernetického nebezpečí nelze vyhlásit v případě, kdy ohrožení bezpečnosti informací v informačních systémech nebo bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací[419] lze odvrátit činností Úřadu podle tohoto zákona.**
**(6) Není-li možné odvrátit ohrožení bezpečnosti informací v informačních systémech nebo bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací[420] v rámci stavu kybernetického nebezpečí, ředitel Úřadu neprodleně požádá vládu o vyhlášení nouzového stavu.[421] Rozhodnutí a opatření obecné povahy vydaná Úřadem podle § 13 před vyhlášením nouzového stavu zůstávají v platnosti, pokud tato opatření nejsou v rozporu s krizovými opatřeními vyhlášenými vládou.**
**(7) Stav kybernetického nebezpečí končí uplynutím doby, na kterou byl vyhlášen, pokud ředitel Úřadu nerozhodne o jeho zrušení před uplynutím této doby, nebo vyhlášením nouzového stavu.[422]**

417: Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů.
418: Ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky, ve znění ústavního zákona č. 300/2000 Sb.
419: Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů).
420: Tamtéž.
421: Ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky, ve znění ústavního zákona č. 300/2000 Sb.
422: Tamtéž.

Z důvodové zprávy:

*Toto ustanovení upravuje vyhlašování stavu kybernetického nebezpečí. Vzhledem k tomu, že zákon je postaven na principu minimalizace zásahu do autonomie vůle subjektů působících v kybernetickém prostoru, jsou zákonné povinnosti týkající se zavádění a dokumentace bezpečnostních opatření, provádění protiopatření, hlášení kybernetických bezpečnostních incidentů a spolupráce s vládním resp. národním CERT za normální situace ukládány pouze těm povinným osobám, jejichž systémy jsou vysoce bezpečnostně exponovány, tj. správcům informačních nebo komunikačních systémů kritické informační infrastruktury a správcům významných informačních systémů a v omezeném případě pak subjektům zajišťujícím významné sítě. Zahraniční zkušenosti však ukazují, že může dojít k tak masivnímu ohrožení nebo narušení kybernetické bezpečnosti, že v jeho důsledku mohou být ohroženy nebo dokonce poškozeny fundamentální národní zájmy. Nelze-li takový incident zvládnout za užití standardních mechanismů zákona, tj. činností dohledových pracovišť, může předseda vlády na návrh ředitele NBÚ vyhlásit stav kybernetického nebezpečí, v němž dojde k rozšíření osobní působnosti zákona na poskytovatele služeb elektronických komunikací, subjekty zajišťující sítě elektronických komunikací a subjekty zajišťující významné sítě, které budou za stavu kybernetického nebezpečí povinny provádět reaktivní protiopatření vydaná NBÚ.*

*Vyhlášení stavu kybernetického nebezpečí se netýká uživatelů informačních systémů, sítí a služeb elektronických komunikací a ve stavu kybernetického nebezpečí rovněž nedochází ani k rozšíření kompetencí orgánů veřejné moci působících na úseku kybernetické bezpečnosti. Vyhlášením stavu kybernetického nebezpečí dojde pouze k rozšíření okruhu povinných osob uvedených výše, které budou povinny provádět reaktivní protiopatření vydaná NBÚ. Vzhledem k tomu, že se stav kybernetického nebezpečí nedotýká práv nebo povinností občanů, není vhodné jej z legislativně-technických důvodů upravovat v obecném předpisu týkajícím se krizového řízení, tj. v krizovém zákoně.*

*Proces vyhlašování stavu kybernetického nebezpečí je upraven analogicky s krizovým zákonem, přičemž jeho vyhlášení je vzhledem k potřebě okamžité reakce na závažný kybernetický bezpečnostní incident kompetenčně svěřeno předsedovi vlády, který stav kybernetického nebezpečí vyhlásí na návrh ředitele NBÚ. Vyhlášení je pak oznámeno analogicky s úpravou krizového zákona. Do 24 hodin je třeba, aby o vyhlášeném stavu kybernetického nebezpečí rozhodla vláda. Vláda jako nejvyšší exekutivní orgán státu pak rozhoduje rovněž o prodloužení stavu kybernetického nebezpečí, přičemž ten může být prodloužen nejdéle tak, aby souhrnná doba vyhlášeného stavu kybernetického nebezpečí nepřekročila dobu 30 dnů.*

*Pro vyhlášení i prodloužení stavu kybernetického nebezpečí platí vedle obecných právních principů též konkrétní materiální omezení uvedená v tomto ustanovení. Stav kybernetického nebezpečí lze vyhlásit, respektive prodloužit pouze ze zákonného důvodu, na dobu nezbytně nutnou k vyřešení ohrožení, které bylo důvodem jeho vyhlášení, a pouze tehdy, nelze-li důvod jeho vyhlášení řešit běžnou činností dohledových pracovišť.*

*Za situace, kdy nebude možno zajistit bezpečnost informací v informačních systémech nebo bezpečnost služeb nebo sítí elektronických komunikací v rámci vyhlášeného stavu kybernetického nebezpečí, je ředitel NBÚ povinen požádat předsedu vlády o vyhlášení nouzového stavu podle ústavního zákona č. 110/1998 Sb., o bezpečnosti České republiky, ve znění ústavního zákona č. 300/2000 Sb. V rámci takto vyhlášeného nouzového stavu lze vedle opatření stanovených krizovým zákonem nadále vydávat reaktivní protiopatření NBÚ se shora uvedenou rozšířenou osobní působností. Ačkoliv vyhlášením nouzového stavu končí stav kybernetického nebezpečí, protiopatření, která byla v jeho rámci vydána, zůstávají v platnosti, pokud nebudou v rozporu s krizovými opatřeními vydanými vládou v rámci vyhlášeného nouzového stavu.*

Z důvodové zprávy k novele ZoKB:

K § 21 odst. 1
*Technická úprava textu z důvodu nutnosti sjednocení tohoto ustanovení s ostatním částmi zákona o kybernetické bezpečnosti a terminologie zákona o elektronických komunikacích.*

**K odst. 1) a 5)**
Ustanovení § 21 odst. 1 ZoKB definuje vlastní pojem stav kybernetického nebezpečí.
Stav **kybernetického nebezpečí** představuje situaci, při které je ve velkém rozsahu ohrožena bezpečnost informací v informačních systémech nebo bezpečnost služeb elektronických komunikací anebo bezpečnost a integrita sítí elektronických komunikací.

Pro to, aby se jednalo o stav kybernetického nebezpečí, však **musí být předmětná hrozba natolik zásadní, aby díky ní mohlo dojít k porušení nebo došlo k ohrožení zájmu České republiky.**

**Stav kybernetického nebezpečí nelze vyhlásit v případě, kdy ohrožení bezpečnosti** informací v informačních systémech nebo bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací **lze odvrátit činností NÚKIB podle zákona o kybernetické bezpečnosti.**

Z výše uvedeného jasně vyplývá, že **stav kybernetického nebezpečí představuje krajní prostředek** (*ultima ratio*) využitelný v případech, kdy nastalou situaci není možné řešit jinými prostředky uvedenými v zákoně o kybernetické bezpečnosti.

Využití tohoto prostředku současně koresponduje se základními cíli a principy zákona o kybernetické bezpečnosti, konkrétně s principem **ochrany nedistributivních (veřejných) práv**. Na základě tohoto principu má stát právo na zajištění vnitřní bezpečnosti, na ochranu základních funkcionalit státu a na ochranu před škodlivými následky výjimečných stavů. V oblasti kybernetické bezpečnosti jde především o zajištění veřejného zájmu na bezpečnosti kritické informační infrastruktury a významných informačních systémů a v otázce úpravy stavu kybernetického nebezpečí.

Dle § 2 písm. b) ZoOUI **mezi zájmy České republiky patří** *„zachování její ústavnosti, svrchovanosti a územní celistvosti, zajištění vnitřního pořádku a bezpečnosti, mezinárodních závazků a obrany, ochrana ekonomiky a ochrana života nebo zdraví fyzických osob.“*

K pojmu **informační systém** viz § 1 ZoKB.
K pojmu **síť elektronických komunikací** viz § 1 ZoKB, § 2 písm. h) ZoEK či čl. 4 odst. 1 písm. a) NIS.
K pojmu **služba elektronických komunikací** viz § 2 písm. a) ZoKB, § 2 písm. n) ZoEK.

**K odst. 2)**
Ustanovení § 21 odst. 1 ZoKB se vymezuje osobu oprávněnou vyhlásit stav kybernetického nebezpečí a také stanoví, jakým způsobem je tento stav vyhlašován.

**Vyhlásit stav kybernetického nebezpečí může pouze ředitel NÚKIB.**

**Rozhodnutí** o vyhlášení stavu kybernetického nebezpečí **se musí vyhlásit vyvěšením na úřední desce NÚKIB. Současně se informace** vyhlášení stavu kybernetického nebezpečí **zveřejňuje v celoplošném rozhlasovém a televizním vysílání**.

Provozovatelé celoplošného televizního nebo rozhlasového vysílání jsou povinni bez náhrady nákladů, neprodleně a bez úpravy obsahu a smyslu uveřejnit informace o vyhlášení stavu kybernetického nebezpečí na základě žádosti NÚKIB.

Důvodem zveřejnění informace o stavu kybernetického nebezpečí prostřednictvím celoplošného rozhlasového a televizního vysílání je skutečnost, aby se o tomto výjimečném stavu dozvěděl co nejširší okruh osob.

Požadavek na nezasahování do vlastního sdělení NÚKIB ze strany provozovatelů vysílání představuje větší míru záruky, že nedojde případné mis či desinterpretaci vlastního sdělení.

**Provozovatelem celoplošného televizního nebo rozhlasového vysílání** se dle ustanovení § 2 písm. g) zákona č. 231/2001 Sb., o provozování rozhlasového a televizního vysílání a o změně dalších zákonů rozumí *„právnická nebo fyzická osoba, která sestavuje program, včetně služeb přímo souvisejících s programem, určuje způsob organizace rozhlasového a televizního vysílání a má za toto vysílání redakční odpovědnost, a pod zvukovým nebo obrazovým označením, jež program a služby přímo související s programem nezaměnitelně identifikuje, tento program a služby přímo související s programem prvotně šíří nebo prostřednictvím třetích osob nechává šířit.“*

**K odst. 3) a 7)**
Ustanovení § 21 odst. 3 ZoKB definuje lhůty vztahující se ke stavu kybernetického nebezpečí.

Vlastní rozhodnutí o vyhlášení stavu kybernetického nebezpečí nabývá účinnosti okamžikem, který je v něm stanoven.

Stav kybernetického nebezpečí **se vyhlašuje na dobu nezbytně nutnou**, **nejdéle** však **na 7 dnů**. Tuto dobu je možné prodloužit, avšak **souhrnná doba** trvání vyhlášeného stavu kybernetického nebezpečí **nesmí být delší než 30 dnů**. O prodloužení stavu kybernetického nebezpečí rozhoduje ředitel NÚKIB.

Stav **kybernetického nebezpečí končí:**

- **uplynutím doby, na kterou byl vyhlášen,**
- **rozhodnutím ředitele NÚKIB o jeho zrušení i před uplynutím takto stanovené doby,**
- **vyhlášením nouzového stavu.**

Pojmem **nouzový stav** se dle čl. 5 odst. 1 ZoBČR rozumí případ živelních pohrom, ekologických nebo průmyslových havárií, nehod nebo **jiného nebezpečí, které ve značném rozsahu ohrožují životy, zdraví nebo majetkové hodnoty anebo vnitřní pořádek a bezpečnost**.

Nouzový stav je možné vyhlásit nejdéle na dobu 30 dnů, kterou lze prodloužit jen po předchozím souhlasu Poslanecké sněmovny.[423]

**K odst. 4) a 6)**
Ustanovení § 21 odst. 4 a 6 ZoKB vymezuje informační povinnost a možnost využití reaktivních a ochranných opatření vůči dalším povinným orgánům a osobám.

V případě, že je vyhlášen stav kybernetického nebezpečí, informuje průběžně ředitel NÚKIB vládu o postupech při řešení stavu kybernetického nebezpečí a o aktuálním stavu hrozeb, které vedly k vyhlášení stavu kybernetického nebezpečí.

Za stavu kybernetického nebezpečí a za nouzového stavu (viz § 31 odst. 6 ZoKB) je NÚKIB oprávněn vydat rozhodnutí nebo opatření obecné povahy spočívající v reaktivním a ochranném opatření (blíže viz § 13 ZoKB) rovněž vůči poskytovateli služby elektronických komunikací a subjektu zajišťující síť elektronických komunikací a orgánu nebo osobě zajišťující významnou síť [§ 3 písm. a) a b) ZoKB].

**V situaci, kdy není možné odvrátit ohrožení bezpečnosti** informací v informačních systémech nebo bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací **v rámci stavu kybernetického nebezpečí, požádá ředitel NÚKIB neprodleně vládu o vyhlášení nouzového stavu.**

423: Čl. 6 odst. 2 ZoBČR

Rozhodnutí a opatření obecné povahy vydaná NÚKIB dle § 13 ZoKB (reaktivní a ochranná opatření) před vyhlášením nouzového stavu zůstávají v platnosti, pokud nejsou v rozporu s krizovými opatřeními vyhlášenými vládou.

HLAVA IV
VÝKON STÁTNÍ SPRÁVY

**Úřad**
**§ 21a**

**(1) Zřizuje se Úřad se sídlem v Brně jako ústřední správní úřad pro oblast kybernetické bezpečnosti a pro vybrané oblasti ochrany utajovaných informací podle zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti. Příjmy a výdaje Úřadu tvoří samostatnou kapitolu státního rozpočtu.**
**(2) V čele Úřadu je ředitel, kterého jmenuje po projednání ve výboru Poslanecké sněmovny příslušném ve věcech bezpečnosti vláda, která ho též odvolává.**
**(3) Ředitel Úřadu je odpovědný předsedovi vlády nebo pověřenému členovi vlády.**

Ustanovení § 21a ZoKB přenáší pravomoci, které byly v souvislosti se zajištěním kybernetické bezpečnosti delegovány na NBÚ, na nově zřízený ústřední správní orgán pro kybernetickou bezpečnost: **Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB).**

Národní úřad pro kybernetickou a informační bezpečnost má též na starost ochranu utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany a problematiku neveřejné služby v rámci družicového systému Galileo.

Tento orgán vznikl 1. srpna 2017 na základě zákona č. 205/2017 Sb., kterým se změnil zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).

**V čele NÚKIB je ředitel**, kterého jmenuje vláda, která ho též odvolává. Ředitel NÚKIB je odpovědný předsedovi vlády nebo pověřenému členovi vlády.

**Sídlem NÚKIB je Brno**, konkrétně: Mučednická 1125/31, 616 00 Brno – Žabovřesky.

**§ 22**

**Úřad**
**a) stanoví bezpečnostní opatření,**
**b) vydává opatření,**
**c) plní stanovené úkoly ve vybraných oblastech ochrany utajovaných informací,**
**d) vede evidence podle tohoto zákona a podle zákona o ochraně utajovaných informací,**

**e) ukládá správní tresty za nedodržení povinností stanovených tímto zákonem a zákonem o ochraně utajovaných informací a o bezpečnostní způsobilosti,**
**f) působí jako koordinační orgán ve stavu kybernetického nebezpečí,**
**g) spolupracuje s orgány a osobami, které působí v oblasti kybernetické bezpečnosti a kybernetické obrany, zejména s veřejnoprávními korporacemi, výzkumnými a vývojovými pracovišti a s ostatními pracovišti typu CERT, a s orgány a osobami, které působí ve vybraných oblastech ochrany utajovaných informací,**
**h) zajišťuje mezinárodní spolupráci v oblasti kybernetické bezpečnosti a ve vybraných oblastech ochrany utajovaných informací,**
**i) sjednává a uzavírá smlouvy o mezinárodní spolupráci v oblasti kybernetické bezpečnosti a ve vybraných oblastech ochrany utajovaných informací,**
**j) zajišťuje prevenci, vzdělávání a metodickou podporu v oblasti kybernetické bezpečnosti a ve vybraných oblastech ochrany utajovaných informací,**
**k) zajišťuje výzkum a vývoj v oblasti kybernetické bezpečnosti a ve vybraných oblastech ochrany utajovaných informací,**
**l) uzavírá veřejnoprávní smlouvu s provozovatelem národního CERT,**
**m) zasílá podle krizového zákona Ministerstvu vnitra návrh prvků kritické infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti, jejichž provozovatelem je organizační složka státu,**
**n) určuje podle krizového zákona prvky kritické infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti, pokud nejde o prvky uvedené v písmeni m),**
**o) ověřuje každé 2 roky aktuálnost určení prvků kritické infrastruktury podle písmen m) a n),**
**p) určuje provozovatele základní služby a informační systém základní služby,**
**q) zpracovává a vládě ke schválení předkládá národní strategii kybernetické bezpečnosti**[424] **a akční plán k jejímu naplňování a tuto strategii aktualizuje nejméně každých 5 let,**
**r) je jednotným kontaktním místem pro zajištění přeshraniční spolupráce v oblasti kybernetické bezpečnosti v rámci Evropské unie,**
**s) je příslušným orgánem v České republice a plní informační povinnosti vůči Evropské komisi a skupině pro spolupráci podle příslušného předpisu Evropské unie,**[425]
**t) informuje veřejnost o kybernetickém bezpečnostním incidentu podle § 12 odst. 3,**
**u) provádí analýzu a monitoring kybernetických hrozeb a rizik,**
**v) vykonává působnost v oblasti veřejné regulované služby Evropského programu družicové navigace Galileo,**
**w) vydává Věstník Úřadu, který zveřejňuje na svých internetových stránkách,**
**x) plní další úkoly v oblasti kybernetické bezpečnosti stanovené tímto zákonem a ve vybraných oblastech ochrany utajovaných informací podle zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti.**

---

424: Čl. 7 NIS

425: Například čl. 5 odst. 3, čl. 7 odst. 3 a čl. 8 NIS

Z důvodové zprávy:

*Tímto ustanovením je zřízen stálý poradní orgán ředitele NBÚ, s nímž ředitel NBÚ konzultuje běžnou činnost NBÚ v oblasti kybernetické bezpečnosti tak, aby byla zajištěna co nejefektivnější prevence důvodů, které by mohly vést k vyhlášení stavu kybernetického nebezpečí. Dojde-li k nástupu těchto důvodů a k vyhlášení stavu kybernetického nebezpečí, působí Komise pro kybernetickou bezpečnost jako poradní orgán ředitele NBÚ za účelem co nejefektivnějšího řešení stavu kybernetického nebezpečí, respektive důvodů, které vedly k jeho vyhlášení.*

*Tímto ustanovením je obecně svěřen NBÚ výkon státní správy na úseku kybernetické bezpečnosti. Ve výčtu činností, k jejichž výkonu má NBÚ právo a povinnost jsou vedle správních, evidenčních, kontrolních a legislativních kompetencí s ohledem na povahu NBÚ jako orgánu veřejné moci, pro který nepůsobí tacitní zákonné dovolení, explicitně uvedeny i činnosti nemající autoritativní povahu, tj. činnosti výzkumné a vývojové, koordinační, kooperační, preventivní a činnosti vedoucí k realizaci mezinárodní spolupráce na úseku kybernetické bezpečnosti.*

*Vzhledem k tomu, že na úseku informačních systémů veřejné správy je ústředním správním úřadem Ministerstvo vnitra, je mu specificky svěřena též kontrola plnění zákonné povinnosti spočívající v zavedení bezpečnostních opatření a vedení bezpečnostní dokumentace správci významných informačních systémů.*

Z důvodové zprávy k novele ZoKB:

K § 22 odst. 2 písm. n)
*Legislativně technická úprava vyplývající z potřeby doplnění nových písmen do tohoto ustanovení.*

K § 22 odst. 2 písm. n) a písm. o) až u)
*S ohledem na přijetí směrnice a z ní vyplývající nové úkoly pro orgány působící v oblasti kybernetické bezpečnosti rozšiřují se přiměřeně kompetence NBÚ tak, aby tento ústřední orgán státní správy splňoval všechny požadavky směrnice.*

*Vzhledem k tomu, že správci nebo provozovatelé komunikačních nebo informačních systémů kritické informační infrastruktury se na základě § 22a odst. 3 považují za provozovatele základních služeb, je nutné v souladu se směrnicí pravidelně přezkoumávat aktuálnost jejich určení.*

*Informačními povinnostmi vůči Evropské komisi a skupině pro spolupráci podle směrnice (EU) 2016/1148 uvedenými v nově navrhovaném písmenu s) se rozumí tyto povinnosti vyplývajícími ze směrnice:*

- *povinnost nahlásit působnost týmů CSIRT (čl. 9 odst. 4 směrnice),*
- *povinnost ve stanoveném termínu a následně každé dva roky předkládat Evropské komisi informace (čl. 5 odst. 7 směrnice), které zahrnují nejméně*

*a) způsob určení provozovatelů základních služeb,*
*b) seznam základních služeb,*
*c) počet provozovatelů základních služeb určených v každém odvětví a jejich význam ve vztahu k dotyčnému odvětví,*
*d) mezní hodnoty, existují-li, pro stanovení příslušné zásobovací úrovně podle počtu uživatelů závislých na dané službě nebo význam konkrétního provozovatele základních služeb.*

- *povinnost ve stanoveném termínu předložit a poté každý rok předkládat skupině pro spolupráci ustavené v souladu s čl. 11 směrnice souhrnnou zprávu o hlášeních kybernetických bezpečnostních incidentů, jejich počtu, povahy ohlášených kybernetických bezpečnostních incidentů a přijatých opatření (čl. 10 odst. 3 směrnice).*

*NBÚ se v tomto směru stává rovněž jednotným kontaktním místem, které bude poskytovatel informace jednotným kontaktním místům jiných členských států.*

*Směrnice ve svém článku 7 ukládá členským státům povinnost zpracovat národní strategii pro bezpečnost sítí a informačních systémů a vymezuje její minimální obsah. Žádá také po členských státech, aby své schválené strategie hlásily Evropské komisi. Předkladatel tuto kompetenci svěřil v § 22 NBÚ s odkazem na požadovaný rozsah strategie podle směrnice.*

Ustanovení § 22 ZoKB definuje pravomoci Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB) jakožto ústředního správního orgánu a gestora kybernetické a informační bezpečnosti v ČR.

V rámci výkonu státní správy Národní úřad pro kybernetickou a informační bezpečnost:

a) **stanoví bezpečnostní opatření,**

K pojmu **bezpečnostní opatření** viz § 4 až § 6a ZoKB.

b) **vydává opatření,**

K procesu **vydávání opatření** viz § 11 až § 15a ZoKB.

c) **plní stanovené úkoly ve vybraných oblastech ochrany utajovaných informací,**

K plnění úkolů ve vybraných oblastech ochrany utajovaných informací dle zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

Do působnosti NÚKIB dle tohoto zákona patří především:

- bezpečnost informačních a komunikačních systémů (§ 33a až 35a ZoOUI),
- ochrana utajovaných informací při zpracování v elektronické podobě v zařízení, které není součástí informačního nebo komunikačního systému (§ 36 ZoOUI),
- kryptografická ochrana (§ 36a až 45 ZoOUI),
- certifikace (§ 45a až 53 ZoOUI).

d) **vede evidence podle tohoto zákona a podle zákona o ochraně utajovaných informací,**

K pojmu **evidence** viz § 9 až § 10a ZoKB. K podmínkám vedení evidence dle ZoOUI viz § 21 a násl. tohoto zákona.

e) **ukládá správní tresty za nedodržení povinností stanovených tímto zákonem a zákonem o ochraně utajovaných informací a o bezpečnostní způsobilosti,**

K **ukládání správních trestů** viz § 25 až § 27 ZoKB. K podmínkám vedení evidence dle ZoOUI viz § 148 a násl. tohoto zákona.

f) **působí jako koordinační orgán ve stavu kybernetického nebezpečí,**

K pojmu **stav kybernetického nebezpečí a činnosti NÚKIB** viz § 21 ZoKB.

g) **spolupracuje s orgány a osobami, které působí v oblasti kybernetické bezpečnosti a kybernetické obrany, zejména s veřejnoprávními korporacemi, výzkumnými a vývojovými pracovišti a s ostatními pracovišti typu CERT, a s orgány a osobami, které působí ve vybraných oblastech ochrany utajovaných informací,**

h) **zajišťuje mezinárodní spolupráci v oblasti kybernetické bezpečnosti a ve vybraných oblastech ochrany utajovaných informací,**

i) **sjednává a uzavírá smlouvy o mezinárodní spolupráci v oblasti kybernetické bezpečnosti a ve vybraných oblastech ochrany utajovaných informací,**

Částečně k problematice **spolupráce** viz § 20 ZoKB a úkoly vládního CERT. Nicméně vlastní spolupráci není možné omezit jen na úkoly vymezené v § 20 písm. k) až n) ZoKB, neboť se jedná primárně o spolupráci v rámci plnění povinností týmu typu CERT/CSIRT.

Národní úřad pro kybernetickou a informační bezpečnost je oprávněn dle § 22 písm. g) a j) ZoKB sám aktivně navazovat kontakty a spolupráci s jinými subjekty, které se věnují problematice kybernetické bezpečnosti a ve vybraných oblastech ochrany utajovaných informací.

Cílem této spolupráce má být zvyšování kybernetické bezpečnosti, urychlení procesu řešení incidentů, předávání informací o nich aj.

Obdobně tomu je i v případech zajišťování prevence, edukace, metodické podpory, oblasti výzkumu a vývoje [viz § 22 písm. j) a k) ZoKB].

j) **zajišťuje prevenci, vzdělávání a metodickou podporu v oblasti kybernetické bezpečnosti a ve vybraných oblastech ochrany utajovaných informací,**

k) **zajišťuje výzkum a vývoj v oblasti kybernetické bezpečnosti a ve vybraných oblastech ochrany utajovaných informací,**

l) **uzavírá veřejnoprávní smlouvu s provozovatelem národního CERT,**

K pojmu **veřejnoprávní smlouva a její náležitosti** viz § 19 ZoKB.

m) **zasílá podle krizového zákona Ministerstvu vnitra návrh prvků kritické infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti, jejichž provozovatelem je organizační složka státu,**

V případě informačních a komunikačních systémů veřejné správy je ústředním správním úřadem Ministerstvo vnitra.

K pojmu **kritická infrastruktura** viz § 2 písm. b) ZoKB.

n) **určuje podle krizového zákona prvky kritické infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti, pokud nejde o prvky uvedené v písmeni m),**

NÚKIB je oprávněn určovat prvky kritické infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti dle zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů. Tyto prvky není NÚKIB oprávněn určit, pokud se jedná o prvky kritické infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti, jejichž provozovatelem je organizační složka státu.

K pojmu **kritická infrastruktura** viz § 2 písm. b) ZoKB.

o) **ověřuje každé 2 roky aktuálnost určení prvků kritické infrastruktury podle písmen m) a n),**

Cílem tohoto oprávnění je ověřit, zda již určené prvky nadále splňují průřezová a odvětvová kritéria dle krizového zákona, případně ověřit, zda tyto podmínky nesplňují jiné (dosud neurčené) informační a komunikační systémy.

K pojmu **kritická infrastruktura** viz § 2 písm. b) ZoKB.

p) **určuje provozovatele základní služby a informační systém základní služby,**

K pojmu **základní služba** viz § 2 písm. i) ZoKB. K pojmu **provozovatel základní služby** viz § 3 písm. a) ZoKB. K určení provozovatele základní služby viz vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby.

q) **zpracovává a vládě ke schválení předkládá národní strategii kybernetické bezpečnosti a akční plán k jejímu naplňování a tuto strategii aktualizuje nejméně každých 5 let,**

Článek 7 NIS stanoví, že každý členský stát přijme národní strategii pro bezpečnost sítí a informačních systémů. V této strategii musí být vymezeny strategické cíle a politická a regulační opatření s cílem dosáhnout vysoké úrovně bezpečnosti sítí a informačních systémů a udržovat ji, přičemž tato strategie musí pokrývat alespoň základní a digitální služby. Předmětem národní strategie pro bezpečnost sítí a informačních systémů jsou především následující cíle a opatření:

- cíle a priority národní strategie pro bezpečnost sítí a informačních systémů,
- správní rámec pro naplnění cílů a priorit vnitrostátní strategie pro bezpečnost sítí a informačních systémů, včetně úlohy a povinností vládních orgánů a dalších relevantních subjektů,
- stanovení opatření týkající se připravenosti, reakce a obnovy, včetně spolupráce veřejného a soukromého sektoru,
- vymezení vzdělávacích, informačních a školicích programů souvisejících s vnitrostátní strategií pro bezpečnost sítí a informačních systémů,
- vymezení výzkumných a rozvojových plánů souvisejících s národní strategií pro bezpečnost sítí a informačních systémů,
- plán posouzení rizik pro určení rizik,
- seznam různých subjektů zapojených do provádění národní strategie pro bezpečnost sítí a informačních systémů.

r) **je jednotným kontaktním místem pro zajištění přeshraniční spolupráce v oblasti kybernetické bezpečnosti v rámci Evropské unie,**

s) **je příslušným orgánem v České republice a plní informační povinnosti vůči Evropské komisi a skupině pro spolupráci podle příslušného předpisu Evropské unie,**

t) **informuje veřejnost o kybernetickém bezpečnostním incidentu,**

NÚKIB je oprávněn vydávat **varování**, blíže viz § 12 ZoKB.

u) **provádí analýzu a monitoring kybernetických hrozeb a rizik,**

K pojmu **kybernetická hrozba** viz kap. 2.4.1. K pojmu **riziko** viz kap. 2.3.1.

v) **vykonává působnost v oblasti veřejné regulované služby Evropského programu družicové navigace Galileo,**

K projektu Galileo blíže viz např. https://www.gsa.europa.eu/.

w) **vydává Věstník Úřadu, který zveřejňuje na svých internetových stránkách,**

Věstník je dostupný na: https://www.govcert.cz/cs/uredni-deska/vestnik/.

x) **plní další úkoly v oblasti kybernetické bezpečnosti stanovené tímto zákonem a ve vybraných oblastech ochrany utajovaných informací podle zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti.**

**§ 22a**
**Určení provozovatele základní služby a informačního systému základní služby**

**(1) Úřad rozhodnutím určí provozovatele základní služby a informační systém základní služby, pokud naplní odvětvová a dopadová kritéria, která zohledňují významnost**
- **a) služeb poskytovaných v jednotlivých odvětvích uvedených v § 2 písm. i) a**
- **b) dopad kybernetického bezpečnostního incidentu zejména na**
  - **1) rozsah a kvalitu poskytování základní služby uživatelům, kteří jsou na ní závislí,**
  - **2) ekonomické a společenské činnosti a veřejnou bezpečnost,**
  - **3) vzájemnou závislost odvětví uvedených v § 2 písm. i).**

**Dopadová a odvětvová kritéria pro určení provozovatele základní služby a vymezení významnosti dopadu narušení základní služby na zabezpečení společenských nebo ekonomických činností stanoví prováděcí právní předpis.**

**(2) V případě, že Úřad zjistí, že orgán nebo osoba, které hodlá určit podle odstavce 1 jako provozovatele základní služby, poskytují danou službu i v jiném členském státě, provede před rozhodnutím ve věci konzultaci s příslušným orgánem dotčeného členského státu.**
**(3) Proti rozhodnutí Úřadu o určení provozovatele základní služby a informačního systému základní služby není rozklad přípustný.**
**(4) Úřad ověřuje nejméně každé 2 roky ode dne vydání rozhodnutí o určení provozovatele základní služby, zda jsou splněny podmínky pro určení provozovatele základní služby a informačního systému základní služby.**

Z důvodové zprávy k novele ZoKB:

*Navržené ustanovení transponuje čl. 4 bod 4 a čl. 5 odst. 2 a 4 směrnice. Zmocňuje NBÚ k vydání prováděcího právního předpisu (vyhlášky), který stanoví odvětvová a průřezová kritéria, na jejichž základě budou možné určovat rozhodnutím ve věci provozovatele základních služeb a informační systémy základních služeb. Zákon pro větší právní jistotu vymezuje okruh kritérií, která budou vyhláškou určována. Jak vyplývá i z definice informačního systému obsaženého ve směrnici, nemusí být informační systém tvořen pouze jedním zařízením, ale jeho fungování může záviset na vícero propojených (přiřazených) zařízení – technických prostředků, z nichž ne všechny musí nutně provádět automatické zpracování digitálních dat. Přičemž obecně lze konstatovat, že zpracováním dat se v širším kontextu čl. 4 odst. 1 písm. c) myslí jak samotné zpracování, tak i uchovávání, opětovné vyhledávání nebo předávání dat. Zároveň tato vyhláška stanovením dopadových určovacích kritérií vymezí významnost dopadu narušení základní služby na zabezpečení společenských nebo ekonomických činností.*

*Vzhledem k zájmům, jejichž ochrana je určováním provozovatelů základních služeb sledována (zejména národní bezpečnosti a ochrana obyvatelstva), je nutné, aby proces určování probíhal pokud možno bez výraznějšího zpoždění. Z toho důvodu nebude možné podávat proti rozhodnutí o určení provozovatele základní služby a informačního systému základní služby rozklad. Právní moc rozhodnutí tedy nastane jeho oznámením. Rozhodnutí bude obsahovat lhůty pro nahlášení kontaktních údajů podle § 16 zákona a přijetí bezpečnostních opatření podle § 4 zákona.*

*Základní služby, jak jsou definovány směrnicí a jí nastavenými kritérii, jsou zpravidla služby značného významu a rozsahu v daném členském státě Evropské unie a je tedy více než pravděpodobné, že provozovatelé těchto služeb se nebudou omezovat na působení pouze v jednom členském státě. Tuto situaci směrnice předvídá a zavádí proto povinnost příslušného orgánu (tedy NBÚ) konzultovat určení provozovatele základních služeb s příslušnými orgány dalších členských států, v nichž podnikatel působí. Předkladatel návrhu zákona tuto povinnost konzultace upravuje v odstavci 3 nového § 22a.*

*Pro zajištění toho, že seznam provozovatelů základních služeb je vždy aktuální a vychází z reálného stavu, ukládá se povinnost Úřadu pravidelně aktuálnost rozhodnutí ve dvouletých cyklech ověřovat.*

**K odst. 1)**
K pojmu **základní služba** viz § 2 písm. i) ZoKB.
K pojmu **provozovatel základní služby** viz § 3 písm. a) ZoKB.

**K určení provozovatele základní služby** viz vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby.

NÚKIB je oprávněn rozhodnutím určit provozovatele základní služby. Náležitosti rozhodnutí jsou upraveny § 67 a násl. SŘ. Dle § 67 odst. 1 SŘ *„rozhodnutím správní orgán v **určité věci zakládá, mění nebo** ruší práva anebo povinnosti jmenovitě určené osoby nebo v určité věci **prohlašuje, že taková osoba práva nebo povinnosti má anebo nemá**, nebo v zákonem stanovených případech rozhoduje o procesních otázkách.“*

**Základní službou je služba, která je závislá na informačních systémech nebo sítích elektronických komunikací v odvětvích:**

1) energetika,
2) doprava,
3) bankovnictví,
4) infrastruktura finančních trhů,
5) zdravotnictví,
6) vodní hospodářství,
7) digitální infrastruktura nebo
8) chemický průmysl.

Vymezení jednotlivých základních služeb, jakož i stanovení kritérií pro určení provozovatele základní služby a informačního systému základní služby, je uvedeno ve **vyhlášce č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby**.[426] Tato vyhláška vstoupila v účinnost 1. února 2018.

Při určení toho zda je daná služba **základní službou** se užijí **odvětvová a dopadová kritéria** [viz § 28 odst. 2 písm. e) ZoKB]. **Odvětvová a dopadová kritéria současně musejí zohledňovat významnost:**

**a) služeb poskytovaných v jednotlivých odvětvích uvedených v § 2 písm. i) ZoKB,**
**b) dopad kybernetického bezpečnostního incidentu zejména na**

**1) rozsah a kvalitu poskytování základní služby uživatelům, kteří jsou na ní závislí,**
**2) ekonomické a společenské činnosti a veřejnou bezpečnost,**

426: [online]. Dostupné z: https://www.zakonyprolidi.cz/cs/2017-437

**3) vzájemnou závislost odvětví uvedených v § 2 písm. i) ZoKB.**

**Odvětvová kritéria** jsou určena:

- druhem služby,
- druhem subjektu a
- speciálním kritériem druhu subjektu.

Speciální kritérium druhu subjektu dle § 2 odst. 2 vyhlášky č. 437/2017 Sb. zohledňuje **významnost subjektu v jednotlivém odvětví**.

**Dopadová kritéria stanovují hranice možných škod** způsobených kybernetickým bezpečnostním incidentem v informačních systémech a sítích elektronických komunikací, kterých musí být pro určení dosaženo. Dopadová kritéria jsou ve vyhlášce č. 347/2017 Sb. stanovena následovně:

Kybernetický bezpečnostní incident v informačním systému či síti elektronických komunikací by mohl způsobit:

I. závažné omezení či narušení (či nedostupnost) druhu služby postihující více než 25000, 50000 nebo 500000 osob[427],
II. závažné omezení či narušení jiné základní služby, nebo omezení či narušení provozu prvku kritické infrastruktury,
III. hospodářskou ztrátu vyšší než 0,25 % HDP,
IV. nedostupnost druhu služby pro více než 1600 osob, která není nahraditelná jiným způsobem bez vynaložení nepřiměřených nákladů,
V. oběti na životech s mezní hodnotou více než 100 nebo 200[428] mrtvých nebo 1000 zraněných osob vyžadujících lékařské ošetření,
VI. narušení veřejné bezpečnosti na významné části správního obvodu obce s rozšířenou působností, které by mohlo vyžadovat provedení záchranných a likvidačních prací složkami integrovaného záchranného systému nebo
VII. kompromitaci citlivých osobních údajů o 200000 osobách.

**Pokud subjekt naplní odvětvová kritéria a kybernetický bezpečnostní incident v jeho systému či systémech naplní dopadová kritéria, bude určen jako provozovatel základní služby a předmětný systém jako informační systém základní služby.**

427: Hodnoty se liší v rámci jednotlivých odvětví nebo pododvětví.

428: Hodnoty se liší v rámci jednotlivých odvětví nebo pododvětví.

Proces určení provozovatele základní služby a informačního systému základní služby je vhodně znázorněn v diagramu vydaném NÚKIB.[429]

V příloze č. 1 vyhlášky č. 437/2017 jsou definována jednotlivá odvětvová a dopadová kritéria pro určení provozovatele základní služby.

**K odst. 2)**
Pokud NÚKIB zjistí, že orgán nebo osoba, kterou hodlá určit jako provozovatele základní služby, poskytuje danou službu i v jiném členském státě, provede před rozhodnutím ve věci konzultaci s příslušným orgánem dotčeného členského státu.

Tato povinnost konzultace vyplývá z čl. 5 odst. 4 NIS, kde je uvedeno, že „*v případě, že jeden subjekt poskytuje základní službu ve dvou či více členských státech, zahájí tyto členské státy vzájemné konzultace.* ***Tyto konzultace proběhnou před přijetím rozhodnutí o určení provozovatele základní služby.***"

**K odst. 3)**
Základní služby jsou jedněmi z prioritních služeb, k jejichž ochraně má mimo jiné sloužit i zákon o kybernetické bezpečnosti. Díky této skutečnosti je nutné, aby proces určování probíhal pokud možno co nejrychleji.

Z toho důvodu není možné podávat proti rozhodnutí o určení provozovatele základní služby a informačního systému základní služby rozklad.

Právní moc rozhodnutí nastane jeho oznámením.

Rozhodnutí obsahuje lhůty pro nahlášení kontaktních údajů podle § 16 ZoKB a přijetí bezpečnostních opatření podle § 4 ZoKB.

**K odst. 4)**
Na základě čl. 5 odst. 5 NIS je třeba alespoň **každé dva roky** ode dne 9. května 2018 **přezkoumávat, případně aktualizovat seznam určených provozovatelů základních služeb.**

V ustanovení § 22a odst. 4 ZoKB je pak uvedeno, že **NÚKIB toto ověřování provádí nejméně každé dva roky ode dne vydání rozhodnutí o určení provozovatele základní služby.**

429: *Proces určování provozovatelů základních služeb a informačních systémů základních služeb.* [online]. [cit. 7. 8. 2018]. Dostupné z: https://nukib.cz/download/kii-vis/Schema_rozhodovani_PZS_v2.1.pdf

**§ 22b**

**(1) Úřadu jsou poskytovány pro výkon působnosti podle tohoto zákona ze základního registru obyvatel referenční údaje, kterými jsou**

**a) příjmení,**
**b) jméno, popřípadě jména,**
**c) adresa místa pobytu,**
**d) datum, místo a okres narození; u subjektu údajů, který se narodil v cizině, datum, místo a stát, kde se narodil,**
**e) datum, místo a okres úmrtí; jde-li o úmrtí subjektu údajů mimo území České republiky, datum úmrtí, místo a stát, na jehož území k úmrtí došlo,**
**f) státní občanství, popřípadě více státních občanství,**
**g) záznam o zřízení datové schránky a identifikátor datové schránky, je-li tato datová schránka zpřístupněna.**

**(2) Úřadu jsou poskytovány pro výkon působnosti podle tohoto zákona z agendového informačního systému evidence obyvatel o státních občanech České republiky údaje, kterými jsou**

**a) jméno, popřípadě jména, příjmení, včetně předchozích příjmení, rodné příjmení,**
**b) rodné číslo, pokud není přiděleno, datum narození,**
**c) adresa místa trvalého pobytu, včetně předchozích adres místa trvalého pobytu, popřípadě adresa, na kterou mají být doručovány písemnosti podle jiného právního předpisu,**
**d) omezení svéprávnosti, jméno, popřípadě jména, příjmení a rodné číslo opatrovníka; nebylo-li opatrovníkovi rodné číslo přiděleno, datum, místo a okres narození; je-li opatrovníkem ustanoven orgán místní správy, název a adresa sídla,**
**e) datum, místo a okres úmrtí; jde-li o úmrtí občana mimo území České republiky, datum úmrtí, místo a stát, na jehož území k úmrtí došlo,**
**f) den, který byl v rozhodnutí soudu o prohlášení za mrtvého uveden jako den smrti, popřípadě jako den, který občan prohlášený za mrtvého nepřežil.**

**Údaje, které jsou vedeny jako referenční údaje v základním registru obyvatel, se využijí z agendového informačního systému evidence obyvatel, pouze pokud jsou ve tvaru předcházejícím současný stav.**

**(3) Úřadu jsou poskytovány pro výkon působnosti podle tohoto zákona z informačního systému cizinců o cizincích údaje, kterými jsou**

**a) jméno, popřípadě jména, příjmení, rodné příjmení,**
**b) datum narození,**
**c) rodné číslo,**
**d) státní občanství, popřípadě více státních občanství,**
**e) druh a adresa místa pobytu,**
**f) číslo a platnost oprávnění k pobytu,**
**g) omezení svéprávnosti,**

**h) datum, místo a okres úmrtí; jde-li o úmrtí mimo území České republiky, stát, na jehož území k úmrtí došlo, popřípadě datum úmrtí,**
**i) den, který byl v rozhodnutí soudu o prohlášení za mrtvého uveden jako den smrti, popřípadě jako den, který cizinec prohlášený za mrtvého nepřežil.**

**Údaje, které jsou vedeny jako referenční údaje v základním registru obyvatel, se využijí z informačního systému cizinců, pouze pokud jsou ve tvaru předcházejícím současný stav.**

**(4) Úřadu jsou poskytovány pro výkon působnosti podle tohoto zákona z registru rodných čísel o fyzických osobách, kterým bylo přiděleno rodné číslo, avšak nejsou vedeny v agendovém informačním systému evidence obyvatel, údaje, kterými jsou**

**a) jméno, popřípadě jména, příjmení, popřípadě rodné příjmení,**
**b) rodné číslo,**
**c) v případě změny rodného čísla původní rodné číslo,**
**d) den, měsíc a rok narození,**
**e) místo a okres narození; u fyzické osoby narozené v cizině stát, na jehož území se narodila.**

**(5) Úřadu jsou poskytovány pro výkon působnosti podle tohoto zákona ze základního registru právnických osob, podnikajících fyzických osob a orgánů veřejné moci údaje, kterými jsou**

**a) obchodní firma nebo název právnické osoby nebo jméno, popřípadě jména, a příjmení podnikající fyzické osoby,**
**b) datum vzniku nebo datum zápisu do evidence podle zvláštních právních předpisů,**
**c) datum zániku nebo datum výmazu z evidence podle zvláštních právních předpisů,**
**d) právní forma,**
**e) záznam o zřízení datové schránky a identifikátor datové schránky, je-li tato datová schránka zpřístupněna,**
**f) statutární orgán vyjádřený referenční vazbou na registr obyvatel anebo na registr osob nebo údajem o jménu, popřípadě jménech, příjmení a bydlišti u zahraniční fyzické osoby,**
**g) právní stav,**
**h) adresa sídla právnické osoby nebo adresa místa podnikání fyzické osoby ve formě referenční vazby (kódu adresního místa) na referenční údaj o adrese v registru územní identifikace.**

**(6) K údajům podle odstavců 2 až 5 vedeným v agendových informačních systémech jsou Úřadu poskytovány i jejich předchozí změny.**

**(7) Z poskytovaných údajů lze v konkrétním případě použít vždy jen takové údaje, které jsou nezbytné ke splnění daného úkolu.**

Ustanovení § 22b ZoKB zakotvuje Národnímu úřadu pro kybernetickou a informační bezpečnost **právo získávat taxativně uvedené údaje** (včetně informací o předchozích změnách těchto údajů) **z:**

- **základního registru obyvatel,**
- **agendového informačního systému evidence obyvatel,**
- **informačního systému cizinců,**
- **registru rodných čísel,**
- **základního registru právnických osob, podnikajících fyzických osob a orgánů veřejné moci.**

Údaje z výše uvedených systémů mohou být použity NÚKIB pouze v rámci plnění daného úkolu a to pouze v nezbytně nutné míře i vzhledem k rozsahu použitých údajů. Toto ustanovení tak plně odpovídá principu informačního sebeurčení člověka a minimalizaci státního zásahu do práv jedince.[430]

## HLAVA V
## KONTROLA, NÁPRAVNÁ OPATŘENÍ A PŘESTUPKY

### § 23
### Kontrola

**(1) Úřad vykonává kontrolu v oblasti kybernetické bezpečnosti. Při výkonu kontroly Úřad zjišťuje, jak orgány a osoby uvedené v § 3 písm. a) až g) plní povinnosti stanovené tímto zákonem a rozhodnutími a opatřeními obecné povahy vydanými Úřadem podle tohoto zákona, a dodržují prováděcí právní předpisy v oblasti kybernetické bezpečnosti. Je-li důvodné podezření, že poskytovatel digitální služby neplní povinnosti stanovené tímto zákonem, provede u něj Úřad kontrolu.**
**(2) Při výkonu kontroly se postupuje přiměřeně podle kontrolního řádu.**
**(3) Kontrolu vykonávají pověření zaměstnanci Úřadu.**

Z důvodové zprávy:

*Kontrolní pravomoci specifikované tímto ustanovením jsou rozděleny mezi NBÚ a Ministerstvo vnitra. Předmětem kontroly, při jejímž výkonu se primárně postupuje podle zákona č. 255/2012 Sb., o kontrole (kontrolní řád), je dodržování povinností stanovenými tímto zákonem, reaktivními a ochrannými protiopatřeními, jakož i dodržování prováděcích právních předpisů. Rozsah kontrolovaných povinností se liší v závislosti na typu povinné osoby, u které je kontrola vykonávána. Ve vztahu k poskytovatelům služeb elektronických komunikací, subjektům zajišťujícím sítě elektronických komunikací a subjektům zajišťujícím významné sítě kontroluje NBÚ pouze dodržování povinností stanovených reaktivními protiopatřeními za stavu kybernetického nebezpečí. Nad správci informačních nebo komunikačních systémů kritické informační infrastruktury je výkon kontroly prováděný NBÚ nejširší. Předmětem kontroly těchto povinných osob je plnění povinností spočívajících v zavedení bezpečnostních opatření,*

430: Blíže viz kap. 4.2 Základní cíle a principy ZoKB

*vedení bezpečnostní dokumentace, hlášení kybernetických bezpečnostních incidentů NBÚ, provádění reaktivních a ochranných protiopatření a oznamování kontaktních údajů a jejich změn NBÚ. Rozsah kontroly správců významných informačních systémů je totožný, liší se však v orgánech veřejné moci, které kontrolu vykonávají. Vzhledem k tomu, že Ministerstvo vnitra je ústředním správním úřadem na úseku informačních systémů veřejné správy, vykonává kontrolní pravomoci ohledně zavádění a dokumentace bezpečnostních opatření správci těchto systémů. Kontrolu dodržování ostatních povinností správci významných informačních systémů pak vykonává NBÚ.*
Z důvodové zprávy k novele ZoKB:

K § 23 odst. 1
*Vymezuje se rozsah subjektů, u nichž může NBÚ provádět kontrolu, a to rozšířením o nové povinné osoby – provozovatele základní služby, správce a provozovatele informačního systému základní služby.*

K § 23 odst. 1
*V případě poskytovatelů digitálních služeb se zavádí speciální režim kontroly, neboť v souladu s čl. 17 odst. 1 směrnice může být kontrolováno plnění povinností u těchto subjektů pouze v případě, že má příslušný orgán důvodné podezření, že poskytovatel digitálních služeb nesplňuje požadavky stanovené zákonem. Nelze tedy u těchto subjektů vykonávat kontrolu „preventivně".*

K § 23 odst. 2
*Z důvodu nadbytečnosti se vypouští druhý odstavec, jenž pouze rozváděl odstavec první, stanovující rozsah plnění povinností, které může Úřad kontrolovat.*

**K odst. 1)**
**Národní úřad pro kybernetickou a informační bezpečnost je oprávněn kontrolovat, zda a jak plní orgány a osoby uvedené v** § 3 písm. a) až g) ZoKB (tj. poskytovatelé služeb elektronických komunikací a subjekty zajišťující síť elektronických komunikací, orgány nebo osoby zajišťující významnou síť, správci a provozovatelé informačního systému kritické informační infrastruktury, správci a provozovatelé komunikačního systému kritické informační infrastruktury, správci a provozovatelé významného informačního systému, správci a provozovatelé informačního systému základní služby, provozovatelé základní služby) **povinnosti stanovené tímto zákonem a rozhodnutími a opatřeními obecné povahy vydanými NÚKIB podle tohoto zákona, a dodržují prováděcí právní předpisy v oblasti kybernetické bezpečnosti.**

Oproti předchozímu znění zákona o kybernetické bezpečnosti **se rozsah kontrolovaných povinností neliší** v závislosti na typu povinné osoby, u které je kontrola vykonávána. Kontrolováno je, zda jsou:

- **plněny povinnosti stanovené ZoKB,**
  K plnění povinností jednotlivými orgány a osobami viz § 3 ZoKB.

- **plněny povinnosti stanovené rozhodnutími a opatřeními obecné povahy vydanými NÚKIB dle ZoKB,**
  K plnění povinností na základě rozhodnutí viz např. § 13 a násl. ZoKB (reaktivní a ochranné opatření).
- **dodržovány prováděcí právní předpisy v oblasti kybernetické bezpečnosti.**
  Prováděcími předpisy k ZoKB jsou zejména:
  - **vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích**;
  - **vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby**;
  - **vyhláška č. 82/2018 Sb.**, o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (**vyhláška o kybernetické bezpečnosti**).

**Standardní** („preventivní") **kontrolní činnost není** ze strany NÚKIB **prováděna u poskytovatelů digitálních služeb.** U těchto poskytovatelů může NÚKIB přistoupit ke kontrole existuje-li důvodné podezření, že poskytovatel digitální služby neplní povinnosti stanovené tímto zákonem.

**K odst. 2) a 3)**
Vlastní výkon kontrolní činnosti se řídí zákonem č. 255/2012 Sb., o kontrole (kontrolní řád). Na základě tohoto zákona zjišťuje kontrolní orgán při kontrole, jak kontrolovaná osoba plní povinnosti, které jí vyplývají z jiných právních předpisů nebo které jí byly uloženy na základě těchto předpisů.[431]

Kontrola je prováděna z moci úřední.[432] Vlastní kontrola je zahájena prvním kontrolním úkonem, kterým je dle § 5 odst. 2 zákona č. 255/2012 Sb., o kontrole:

a) **předložení pověření ke kontrole kontrolované osobě** nebo jiné osobě, která kontrolované osobě dodává nebo dodala zboží nebo ho od ní odebrala či odebírá, koná nebo konala pro ni práce, anebo jí poskytuje nebo poskytovala služby nebo její služby využívala či využívá, případně se na této činnosti podílí nebo podílela (dále jen „povinná osoba"), jež je přítomna na místě kontroly,

b) **doručení oznámení o zahájení kontroly kontrolované osobě**; součástí oznámení musí být pověření ke kontrole, anebo seznam kontrolujících,

431: Viz § 2 zákona č. 255/2012 Sb., o kontrole

432: § 5 odst. 1 zákona č. 255/2012 Sb., o kontrole

c) **první z kontrolních úkonů bezprostředně předcházejících předložení pověření ke kontrole kontrolované osobě** nebo povinné osobě, jež je přítomna na místě kontroly, pokud je provedení takových kontrolních úkonů k výkonu kontroly třeba.

Kontrolu vykonává fyzická osoba, která je zaměstnancem NÚKIB[433] a je k této činnosti pověřena.[434] O kontrole je vyhotoven protokol, mimo jiné s uvedením kontrolního zjištění. Stejnopis protokolu o kontrole doručí NÚKIB kontrolované osobě ve lhůtě 30 dnů ode dne provedení posledního kontrolního úkonu, ve zvláště složitých případech do 60 dnů.[435]

Proti kontrolnímu zjištění uvedenému v protokolu o kontrole může kontrolovaná osoba podat námitky. Námitky se podávají písemně a musí z nich být zřejmé, proti jakému kontrolnímu zjištění směřují, a musí obsahovat odůvodnění nesouhlasu s tímto kontrolním zjištěním. Lhůta pro podání námitek činí 15 dnů ode dne doručení protokolu o kontrole, pokud není stanovena v protokolu o kontrole lhůta delší.[436]

V případě, že NÚKIB zjistí při kontrole nedostatky, má možnost kontrolovanému uložit nápravná opatření dle § 24 ZoKB.

**§ 24**
**Nápravná opatření**

**(1) Zjistí-li Úřad při kontrole nedostatky, uloží kontrolovanému orgánu nebo osobě, aby je ve stanovené lhůtě odstranila, popřípadě určí, jakým způsobem.**
**(2) Pokud je informační systém kritické informační infrastruktury, komunikační systém kritické informační infrastruktury, informační systém základní služby nebo významný informační systém pro zjištěné nedostatky bezprostředně ohrožen kybernetickým bezpečnostním incidentem, který jej může významně poškodit nebo zničit, může kontrolní orgán zakázat kontrolovanému orgánu nebo osobě používání tohoto systému anebo jeho části do doby, než bude zjištěný nedostatek odstraněn.**

Z důvodové zprávy:

*Toto ustanovení upravuje podmínky, za nichž lze uložit povinným osobám při výkonu kontroly nápravná opatření. Účelem nápravných opatření je odstranění nedostatků zjištěných při kontrole, tj. především dodatečné řádné splnění některé z povinností stanovených tímto zákonem nebo na jeho základě (typicky doplnění nedostatečně vedené bezpečnostní dokumentace, aktualizace kontaktních*

433: § 3 ZoKB
434: § 4 zákona č. 255/2012 Sb., o kontrole
435: § 12 zákona č. 255/2012 Sb., o kontrole
436: § 13 zákona č. 255/2012 Sb., o kontrole

*údajů). Obsahem nápravných opatření však mohou být i jiné povinnosti, a to v závislosti na charakteru zjištěných nedostatků a jejich možných následků. Pokud by pro zjištěné nedostatky byl informační nebo komunikační systém kritické informační infrastruktury anebo významný informační systém bezprostředně ohrožen kybernetickým bezpečnostním incidentem, který by jej mohl poškodit či zničit, byl by kontrolní orgán oprávněn povinné osobě uložit povinnost zabezpečit takový systém, v krajním případě pak dočasně zakázat jeho používání či používání jeho části, a to do doby, než budou zjištěné nedostatky odstraněny.*

*Nesplnění některé z povinností uložených nápravným opatřením pak zakládá skutkovou podstatu správního deliktu podle tohoto zákona, za nějž lze uložit pokutu do výše 100 000 Kč.*

*Zákon dále výslovně stanoví, že náklady spojené s provedením nápravných opatření uložených kontrolním orgánem, tj. NBÚ anebo Ministerstvem vnitra, nese povinná osoba, které byla nápravná opatření uložena.*

Z důvodové zprávy k novele ZoKB:

K § 24 odst. 2
*Mezi informační systémy, jejichž provozování může NBÚ zakázat v případě, že nebyly napraveny zjištěné nedostatky, se zařazují informační systémy, na jejichž provozování je závislé poskytování základní služby, tak aby jejich správci a provozovatelé byli v nejnutnějším případě donuceni nedostatky napravit.*

**K odst. 1)**
V případě, že NÚKIB v rámci prováděné kontroly dle § 23 ZoKB zjistí nedostatky, uloží kontrolovanému orgánu nebo osobě, aby je ve stanovené lhůtě odstranila. NÚKIB je také oprávněn určit, jakým způsobem budou zjištěné nedostatky odstraněny.

Cílem nápravných opatření je především zajištění dodatečného a řádného splnění některé z povinností stanovených ZoKB či prováděcí vyhláškou (např. doplnění nedostatečně vedené bezpečnostní dokumentace, aktualizace kontaktních údajů).

Obsahem nápravných opatření, v závislosti na charakteru zjištěných nedostatků a jejich možných následků, mohou být i jiné povinnosti stanovené NÚKIB.

Pokud kontrolovaný orgán nebo osoba nesplní povinnosti definované v nápravném opatření, dopustí se přestupku dle § 25 odst. 1 písm. b) ZoKB (v případě, že se jedná o poskytovatele služby elektronických komunikací a subjekt zajišťující síť elektronických komunikací nebo orgán nebo osobu zajišťující významnou síť), § 25 odst. 2 písm. j) ZoKB (v případě, že se jedná o správce nebo provozovatele informačního nebo komunikačního systému kritické informační infrastruktury nebo správce nebo provozovatele významného informačního systému), § 25

odst. 7 písm. f) ZoKB (v případě, že se jedná o správce a provozovatele informačního systému základní služby). Sankce za přestupek dle § 25 odst. 1 písm. b), § 25 odst. 7 písm. f) ZoKB je dle ustanovení § 25 odst. 12 písm. b) ZoKB 1 000 000 Kč.

Zřejmě díky legislativní chybě není ve výčtu sankcí uvedených v § 25 odst. 12 písm. b) ZoKB uvedeno ustanovení § 25 odst. 2 písm. j) ZoKB.

**K odst. 2)**
**V případě, že je** pro nedostatky zjištěné během kontrolní činnosti dle § 23 ZoKB **bezprostředně ohrožen kybernetickým bezpečnostním incidentem**, který jej může významně poškodit nebo zničit, **informační systém kritické informační infrastruktury, komunikační systém kritické informační infrastruktury, informační systém základní služby nebo významný informační systém**, **je NÚKIB oprávněn zakázat** kontrolovanému orgánu nebo osobě **používání tohoto systému anebo jeho části. Zákaz používání tohoto sytému platí do doby, než bude zjištěný nedostatek odstraněn.**

Ustanovení § 24 odst. 2 ZoKB představuje krajní prostředek, který bude NÚKIB zpravidla využíván pouze tehdy, kdy jsou zjištěné nedostatky v oblasti kybernetické bezpečnosti natolik vážné, že může dojít k ohrožení či zničení významných informačních a komunikačních systémů, na nichž je stát přímo závislý.

**§ 24a**
**Kontrola činnosti Úřadu**

**(1) Kontrolu činnosti Úřadu vykonává Poslanecká sněmovna, která k tomuto účelu zřizuje zvláštní kontrolní orgán (dále jen „kontrolní orgán").**
**(2) Kontrolní orgán se skládá nejméně ze 7 členů. Poslanecká sněmovna stanoví počet členů tak, aby byl zastoupen každý poslanecký klub ustavený podle příslušnosti k politické straně nebo politickému hnutí, za něž poslanci kandidovali ve volbách; počet členů je vždy lichý. Členem kontrolního orgánu může být pouze poslanec Poslanecké sněmovny.**
**(3) Pokud tento zákon nestanoví jinak, vztahuje se na jednání kontrolního orgánu a na práva a povinnosti jeho členů přiměřeně jiný právní předpis.**[437]
**(4) Členové kontrolního orgánu mohou vstupovat v doprovodu ředitele Úřadu nebo jím pověřeného zaměstnance do objektů Úřadu.**
**(5) Ředitel Úřadu předkládá kontrolnímu orgánu**
- **a) zprávu o činnosti Úřadu,**
- **b) návrh rozpočtu Úřadu,**
- **c) podklady potřebné ke kontrole plnění rozpočtu Úřadu,**

437: Zákon č. 90/1995 Sb., o jednacím řádu Poslanecké sněmovny, ve znění pozdějších předpisů.

**d) vnitřní předpisy Úřadu,**
**e) na vyžádání zprávu o jednotlivých kybernetických bezpečnostních incidentech z kritické informační infrastruktury, významných informačních systémů a informačních systémů základní služby.**

Z důvodové zprávy:

Činnost NBÚ vymezená zákonem č. 412/2005 Sb., podléhá kontrole, kterou je oprávněna *vykonávat Poslanecká sněmovna Parlamentu České republiky. Protože se podle návrhu zákona kompetence NBÚ rozšíří o oblast kybernetické bezpečnosti, je třeba upravit příslušná ustanovení zákona č. 412/2005 Sb. tak, aby Poslanecká sněmovna, respektive jí zřízený zvláštní kontrolní orgán, mohl vykonávat kontrolu činnosti NBÚ rovněž v oblasti kybernetické bezpečnosti.*

**K odst. 1)**
Kontrolu činnosti NÚKIB (tj. zejména plnění povinností dle ZoKB a dle jiných právních předpisů) vykonává Poslanecká sněmovna, která k tomuto účelu zřizuje zvláštní kontrolní orgán.

Tímto kontrolním orgánem je **Stálá komise pro kontrolu činnosti Národního úřadu pro kybernetickou a informační bezpečnost**[438]**,** která vznikla na základě zákona č. 205/2017 Sb., kterým se novelizoval ZoKB. Stálá komise pro kontrolu NÚKIB je zvláštním kontrolním orgánem Poslanecké sněmovny pro kontrolu činnosti NÚKIB.

**K odst. 2) až 4)**
Stálá komise pro kontrolu NÚKIB se skládá nejméně ze 7 členů.[439] Poslanecká sněmovna stanoví počet členů tak, aby byl zastoupen každý poslanecký klub ustavený podle příslušnosti k politické straně nebo politickému hnutí, za něž poslanci kandidovali ve volbách.

Počet členů Stálé komise pro kontrolu NÚKIB je vždy lichý, přičemž členem této komise může být pouze poslanec Poslanecké sněmovny.

Pokud ZoKB nestanoví jinak, vztahuje se na jednání Stálé komise pro kontrolu NÚKIB zákon č. 90/1995 Sb., o jednacím řádu Poslanecké sněmovny, ve znění pozdějších předpisů.

Členové Stálé komise pro kontrolu NÚKIB mohou vstupovat v doprovodu ředitele NÚKIB nebo jím pověřeného zaměstnance do objektů NÚKIB.

438: Dále jen Stálá komise pro kontrolu NÚKIB

439: Seznam členů Stálé komise pro kontrolu NÚKIB je možné nalézt [online]. [cit. 21. 8. 2018]. Dostupné z: https://www.psp.cz/sqw/hp.sqw?k=7801

**K odst. 5)**
Ředitel NÚKIB předkládá Stálé komisi pro kontrolu NÚKIB:

- zprávu o činnosti NÚKIB,
- návrh rozpočtu a podklady potřebné ke kontrole plnění rozpočtu NÚKIB,
- vnitřní předpisy NÚKIB,
- na vyžádání zprávu o jednotlivých kybernetických bezpečnostních incidentech z kritické informační infrastruktury, významných informačních systémů a informačních systémů základní služby.

**§ 24b**

**(1) Má-li kontrolní orgán za to, že činnost Úřadu nezákonně omezuje nebo poškozuje práva a svobody občanů nebo že rozhodovací činnost Úřadu v rámci správního řízení je stižena vadami, je oprávněn požadovat od ředitele Úřadu potřebné vysvětlení.**
**(2) Každé porušení zákona zaměstnancem Úřadu při plnění povinností podle tohoto zákona a ve vybraných oblastech podle zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti, které kontrolní orgán zjistí při své činnosti, je povinen oznámit řediteli Úřadu a předsedovi vlády.**

**K odst. 1)**
Stálá komise pro kontrolu NÚKIB je oprávněna požadovat od ředitele NÚKIB potřebné vysvětlení, pokud má za to, že:

- činnost NÚKIB nezákonně omezuje nebo poškozuje práva a svobody občanů,
- rozhodovací činnost Úřadu v rámci správního řízení je stižena vadami.

**K odst. 2)**
Stálá komise pro kontrolu NÚKIB oznámí řediteli NÚKIB a předsedovi vlády, následující skutečnosti zjištěné v rámci své činnosti:

- porušení zákona o kybernetické bezpečnosti zaměstnancem NÚKIB při plnění povinností podle tohoto zákona,
- porušení zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti (ve vybraných oblastech) zaměstnancem NÚKIB při plnění povinností podle tohoto zákona.

**§ 24c**

**Povinnost zachovávat mlčenlivost uložená členům kontrolního orgánu podle zákona se nevztahuje na případy, kdy kontrolní orgán podává oznámení podle § 24b odst. 2.**

Členové Stálé komise pro kontrolu NÚKIB mají uloženu povinnost zachovávat mlčenlivost na základě zákona o kybernetické bezpečnosti.

Povinnost mlčenlivosti se však nevztahuje na případy uvedené v § 24b ZoKB, tj. že se Stálá komise pro kontrolu NÚKIB dozví o porušení zákona zaměstnancem NÚKIB při plnění jeho povinností.

**§ 25**
**Přestupky**

**(1) Poskytovatel služby elektronických komunikací a subjekt zajišťující síť elektronických komunikací nebo orgán nebo osoba zajišťující významnou síť se dopustí přestupku tím, že**

**a) nesplní za stavu kybernetického nebezpečí povinnost uloženou Úřadem v rozhodnutí nebo v opatření obecné povahy podle § 13, nebo**
**b) nesplní některou z povinností uloženou nápravným opatřením podle § 24.**

**(2) Správce nebo provozovatel informačního nebo komunikačního systému kritické informační infrastruktury nebo správce nebo provozovatel významného informačního systému se dopustí přestupku tím, že**

**a) v rozporu s § 4 odst. 2 nezavede nebo neprovádí bezpečnostní opatření anebo nevede bezpečnostní dokumentaci,**
**b) neohlásí kybernetický bezpečnostní incident podle § 8 odst. 1 a 4,**
**c) nesplní povinnost uloženou Úřadem v rozhodnutí nebo v opatření obecné povahy podle § 13 nebo 14,**
**d) nesplní povinnost uloženou Úřadem v rozhodnutí podle § 15a odst. 1,**
**e) nepředá data, provozní údaje a informace podle § 6a odst. 2,**
**f) nepředá data, provozní údaje a informace podle § 6a odst. 3,**
**g) nezničí kopie dat, provozních údajů a informací podle § 6a odst. 3,**
**h) neumožní správci dohled nad průběhem zničení dat, provozních údajů a informací podle § 6a odst. 3,**
**i) neoznámí kontaktní údaje nebo jejich změnu Úřadu podle § 16 odst. 2 písm. b) nebo**
**j) nesplní některou z povinností uloženou nápravným opatřením podle § 24.**

**(3) Správce informačního nebo komunikačního systému kritické informační infrastruktury nebo významného informačního systému se dopustí přestupku tím, že neinformuje provozovatele systému podle § 4a odst. 1.**

**(4) Správce nebo provozovatel informačního nebo komunikačního systému kritické informační infrastruktury se dopustí přestupku tím, že neinformuje subjekt zajišťující síť elektronických komunikací podle § 4a odst. 2.**

**(5) Provozovatel informačního nebo komunikačního systému kritické informační infrastruktury se dopustí přestupku tím, že**

**a) nesplní povinnost uloženou Úřadem v rozhodnutí podle § 15a odst. 1,**
**b) nepředá data, provozní údaje a informace podle § 6a odst. 2,**

**c) nepředá data, provozní údaje a informace podle § 6a odst. 3,**
**d) nezničí kopie dat, provozních údajů a informací podle § 6a odst. 3, nebo**
**e) neumožní správci dohled nad průběhem zničení dat, provozních údajů a informací podle § 6a odst. 3.**

**(6) Orgán nebo osoba zajišťující významnou síť se dopustí přestupku tím, že neohlásí kybernetický bezpečnostní incident podle § 8 odst. 1 a 3.**

**(7) Správce a provozovatel informačního systému základní služby se dopustí přestupku tím, že**
**a) v rozporu s § 4 odst. 2 nezavede nebo neprovádí bezpečnostní opatření nebo nevede bezpečnostní dokumentaci,**
**b) neohlásí kybernetický bezpečnostní incident podle § 8 odst. 1 a 4,**
**c) nesplní povinnost informovat veřejnost uloženou Úřadem podle § 12 odst. 3,**
**d) nesplní povinnost uloženou Úřadem podle § 13 nebo 14,**
**e) neoznámí kontaktní údaje nebo jejich změnu Úřadu podle § 16 odst. 2 písm. b), nebo**
**f) nesplní některou z povinností uloženou nápravným opatřením podle § 24.**

**(8) Správce nebo provozovatel informačního nebo komunikačního systému kritické informační infrastruktury, správce nebo provozovatel významného informačního systému, správce nebo provozovatel informačního systému základní služby a provozovatel základní služby, kteří jsou orgánem veřejné moci, se dopustí přestupku tím, že uzavřou smlouvu s poskytovatelem služeb cloud computingu v rozporu s § 4 odst. 5.**

**(9) Správce nebo provozovatel informačního nebo komunikačního systému kritické informační infrastruktury se dopustí přestupku tím, že nesplní povinnost informovat veřejnost uloženou Úřadem podle § 12 odst. 3.**

**(10) Provozovatel základní služby se dopustí přestupku tím, že**
**a) neinformuje správce nebo provozovatele informačního systému základní služby podle § 4a odst. 3,**
**b) nenahlásí významný dopad na kontinuitu poskytování základní služby podle § 8 odst. 1 a 4,**
**c) nenahlásí významný dopad na kontinuitu poskytování základní služby způsobený kybernetickým bezpečnostním incidentem podle § 8 odst. 8,**
**d) nesplní povinnost informovat veřejnost uloženou Úřadem podle § 12 odst. 3, nebo**
**e) neoznámí kontaktní údaje nebo jejich změnu Úřadu podle § 16 odst. 2 písm. b).**

**(11) Poskytovatel digitální služby se dopustí přestupku tím, že**
**a) neustaví svého zástupce podle § 3a odst. 1,**
**b) v rozporu s § 4 odst. 3 nezavede nebo neprovádí bezpečnostní opatření,**
**c) neohlásí kybernetický bezpečnostní incident podle § 8 odst. 2 a 3,**
**d) nesplní povinnost informovat veřejnost uloženou Úřadem podle § 12 odst. 3, nebo**
**e) neoznámí kontaktní údaje nebo jejich změnu podle § 16 odst. 2 písm. a).**

**(12) Za přestupek lze uložit pokutu do**
**a) 5000000 Kč, jde-li o přestupek podle odstavce 2 písm. a), odstavce 7 písm. a) nebo odstavce 11 písm. b),**

**b) 1000000 Kč, jde-li o přestupek podle odstavce 1 písm. a) nebo b), odstavce 2 písm. b), c) nebo e), odstavce 3, odstavce 4, odstavce 5 písm. a), c) nebo d), odstavce 6, odstavce 7 písm. b) až d) nebo f), odstavce 8, odstavce 9, odstavce 10 písm. a) až d) nebo odstavce 11 písm. a), c) nebo d),**
**c) 200000 Kč, jde-li o přestupek podle odstavce 5 písm. b) nebo e),**
**d) 10000 Kč, jde-li o přestupek podle odstavce 2 písm. d), odstavce 7 písm. e), odstavce 10 písm. e) nebo odstavce 11 písm. e).**

Z důvodové zprávy:

*Toto ustanovení formuluje jednotlivé skutkové podstaty správních deliktů právnických a podnikajících fyzických osob v oblasti kybernetické bezpečnosti. Obecně platí, že povinná osoba se správního deliktu podle tohoto zákona dopustí, neplní-li některé povinnosti stanovené tímto zákonem anebo na jeho základě. Rozsah skutkových podstat správních deliktů poskytovatelů služeb elektronických komunikací, subjektů zajišťujících sítě elektronických komunikací a subjektů zajišťující významné sítě je přitom užší, než u ostatních povinných osob, neboť tato skupina povinných osob je právní regulací zatížena nejméně. Poměrně nízká výše pokuty za správní delikty byla stanovena zejména z toho důvodu, že zákon o kybernetické bezpečnosti je založen na principu prevence a principu autonomie vůle regulovaných subjektů. Vychází se přitom z předpokladu, že zájmem povinných osob je bezpečnost informací v jejich informačních systémech a dostupnost a spolehlivost služeb a sítí elektronických komunikací. Zákon si proto neklade za cíl působit represivně na povinné osoby s cílem nutit je plnit povinnosti stanovené tímto zákonem pod hrozbou vysokých finančních pokut.*

*V závislosti na charakteru a závažnosti správních deliktů je dále výše pokuty diferenciovaná tak, že nesplnění povinnosti oznámit kontaktní údaje nebo jejich změnu NBÚ je sankcionováno pokutou výrazně nižší, než jakou lze uložit za jiné správní delikty.*

Z důvodové zprávy k novele ZoKB:

K § 25 odst.
*Legislativně technická úprava, která sjednocuje označování povinných subjektů v celém ustanovení.*

K § 25 odst. 2 písm. b)
*Legislativně technická úprava vyplývající z doplnění nového odstavce v § 8.*

K § 25 odst. 3 až 11
*Do tohoto ustanovení upravujícího přestupky se nově doplňují přestupky, které vyplývají z nesplnění nově upravených transpozičních i jiných povinností v zákoně. Toto ustanovení implementuje do českého právního řádu čl. 21 směrnice.*

*Předkladatel návrhu zákona si uvědomuje probíhající legislativní proces schvalování návrhu zákona, kterým se mění některé zákony v souvislosti s přijetím zákona o odpovědnosti za přestupky a řízení o nich a zákona o některých přestupcích, a na schválený zákon č. 250/2016 Sb., a reaguje na tyto předpisy v předloženém návrhu zákona.*

K § 25 odst. 12
*Z důvodu vysoké nebezpečnosti nesplnění povinnosti zavést a provádět bezpečnostní opatření a vést bezpečnostní dokumentaci podle § 4 odst. 2 a 3 zákona se přiměřeně zvyšuje maximální výše pokuty u tohoto správního deliktu uvedeného v odst. 2 písm. a), odst. 6 písm. a) a odst. 10 písm. b) tohoto ustanovení až na 5 mil. Kč, což je částka, která je oproti sankci za nesplnění obdobné povinnosti podnikatelů zajišťujících veřejné sítě elektronických komunikací podle § 98 odst. 1 zákona o elektronických komunikacích čtvrtinová (srov. § 118 odst. 14 písm. h) a odst. 22 zákona o elektronických komunikacích). I při stanovování konkrétní výše pokuty za tento správní delikt platí, že NBÚ přihlédne k závažnosti deliktu, zejména ke způsobu spáchání, následkům a okolnostem spáchání. Není tedy důvod obávat se bezbřehého správního uvážení NBÚ a automatického ukládání pokuty v blízkosti maximální hranice.*

*Dále se rozčleňují výše pokut za spáchané přestupky tak, aby přesněji reflektovaly závažnost jednotlivých přestupků.*

**K odst. 1) až 11)**
Zákon o kybernetické bezpečnosti vymezuje v § 25 a 26 ZoKB skutkové podstaty jednotlivých přestupků.

Jednotlivé skutkové podstaty jsou členěny dle toho, jaká osoba se jich dopustí. Obecně platí, že povinná osoba se správního deliktu podle tohoto zákona dopustí, neplní-li některé povinnosti stanovené tímto zákonem anebo na jeho základě.

V § 25 ZoKB jsou uvedeny přestupky právnických osob, podnikajících fyzických osoba a orgánů veřejné moci. Přestupky fyzických osob jsou uvedeny v § 26 ZoKB.

**Výčet jednotlivých přestupků**, kterých se může dopustit konkrétní orgán a osoba, **je uveden v rámci charakteristiky aktiv, práv a povinností** u daného subjektu. Blíže viz § 3 ZoKB.

**K odst. 12)**
Ustanovení § 25 odst. 12 ZoKB obsahuje **výčet jednotlivých sankcí**, které je možné uložit za přestupky uvedené v § 25 odst. 1 až 11 ZoKB.

Zákon o kybernetické bezpečnosti upravuje **sankce pouze ve formě peněžitých pokut** v rozmezí od 5 000 000 Kč za nejzávažnější porušení povinností dle ZoKB až po 10 000 Kč za porušení nejméně závažné.

Při určení druhu správního trestu a jeho výměry přihlédne NÚKIB zejména k povaze a závažnosti přestupku, způsobu spáchání, následkům a okolnostem spáchání.

Zřejmě díky legislativní chybě není ve výčtu sankcí uvedených v § 25 odst. 12 ZoKB uvedena sankce za přestupky dle § 25 odst. 2 písm. f) až j) ZoKB.

**Byť jsou sankce za stejně definované skutkové podstaty, jichž se dopustí provozovatel** informačního nebo komunikačního systému kritické informační infrastruktury (viz § 25 odst. 5 ZoKB) **ve výčtu sankcí** (§ 25 odst. 12 ZoKB) **uvedeny, nelze v případě § 25 odst. 2 písm. f) až j) ZoKB užít analogie.**

**V tomto případě by se jednalo o užití analogie *in malam partem*** (k tíži pachatele), neboť by byly rozšířeny podmínky trestní odpovědnosti a trestnosti. Sankcionován by totiž mohl být nejen provozovatel informačního nebo komunikačního systému kritické informační infrastruktury, ale i správce takovéhoto systému či správce nebo provozovatel významného informačního systému.

**§ 26**

**(1) Fyzická osoba se dopustí přestupku tím, že poruší povinnost uvedenou v § 10 odst. 1.**
**(2) Za přestupek podle odstavce 1 lze uložit pokutu do 50 000 Kč.**

Přestupku se dle § 26 ZoKB mohou dopustit zaměstnanci České republiky zařazení k výkonu práce v NÚKIB, kteří se podílejí na řešení kybernetického bezpečnostního incidentu.

Tito zaměstnanci jsou vázáni povinností mlčenlivosti o údajích z evidence incidentů, přičemž povinnost mlčenlivosti trvá i po skončení pracovněprávního vztahu k NÚKIB.

Přestupku se tak zaměstnanec typicky dopustí tím, že poruší povinnost mlčenlivosti a zveřejní informace z evidence.

K pojmu **evidence** viz § 9 a násl. ZoKB.

Za přestupek dle § 26 odst. 1 ZoKB lze uložit pokutu do 50 000 Kč.

Při určení druhu správního trestu a jeho výměry přihlédne NÚKIB zejména k povaze a závažnosti přestupku, způsobu spáchání, následkům a okolnostem spáchání.

**§ 27**
**Společné ustanovení k přestupkům**

**Přestupky podle tohoto zákona projednává a pokuty vybírá Úřad.**

Přestupky projednává NÚKIB. Uložené pokuty jsou příjmem státního rozpočtu.

HLAVA VI
ZÁVĚREČNÁ USTANOVENÍ

**§ 28**
**Zmocňovací ustanovení**

**(1) Úřad a Ministerstvo vnitra stanoví vyhláškou významné informační systémy a jejich určující kritéria podle § 6 písm. d).**
**(2) Úřad stanoví vyhláškou**
- **a) obsah a strukturu bezpečnostní dokumentace, obsah bezpečnostních opatření a rozsah bezpečnostních opatření podle § 6 písm. a) až c) a obsah a rozsah bezpečnostních pravidel podle § 6 písm. e),**
- **b) typy, kategorie a hodnocení významnosti kybernetických bezpečnostních incidentů a náležitosti a způsob hlášení kybernetického bezpečnostního incidentu podle § 8 odst. 7,**
- **c) náležitosti oznámení o provedení reaktivního opatření a jeho výsledku podle § 13 odst. 4,**
- **d) vzor oznámení kontaktních údajů a jeho formu podle § 16 odst. 7,**
- **e) dopadová a odvětvová kritéria pro určení provozovatele základní služby a vymezení významnosti dopadu narušení základní služby na zabezpečení společenských nebo ekonomických činností podle § 22a odst. 1,**
- **f) způsob likvidace dat, provozních údajů, informací a jejich kopií.**

Z důvodové zprávy:

*Toto ustanovení upravuje zmocnění NBÚ a Ministerstva vnitra k vydání prováděcích právních předpisů ve formě vyhlášky k provedení příslušných ustanovení návrhu zákona.*

Z důvodové zprávy k novele ZoKB:

K § 28 odst. 2 písm. b)
*Legislativně technická úprava vnitřního odkazu v rámci zákona vyplývající z vložení nového odstavce do § 8.*

K § 28 odst. 2 písm. c)
*Jedná se o legislativně technickou úpravu vyvolanou potřebou doplnit do ustanovení nová písmena e).*

K § 28 odst. 2 písm. e)
*Legislativně technicky se upravuje a doplňuje zmocňovací ustanovení, které nově ukládá NBÚ vydat vyhlášku k provedení § 22a odst. 1.*

Národní úřad pro kybernetickou a informační bezpečnost a Ministerstvo vnitra stanoví vyhláškou významné informační systémy a jejich určující kritéria.

**Na základě tohoto zmocňovacího ustanovení byla přijata vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích a** vyhláška č. 316/2014, o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (**vyhláška o kybernetické bezpečnosti**).

Druhá jmenovaná vyhláška byla následně rekodifikována a současné době jde o **vyhlášku č. 82/2018 Sb.**, o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (**vyhláška o kybernetické bezpečnosti**).

**Přechodná ustanovení**
**§ 29**
(lhůty k plnění povinností)

**(1) Orgány a osoby uvedené v § 3 písm. a) a b) oznámí kontaktní údaje podle § 16 nejpozději do 30 dnů ode dne nabytí účinnosti tohoto zákona.**
**(2) Orgány a osoby uvedené v § 3 písm. b) začnou plnit povinnost stanovenou v § 8 odst. 1 a 2 nejpozději do 1 roku ode dne nabytí účinnosti tohoto zákona.**

Z důvodové zprávy:

*Lhůta ke splnění povinnosti hlásit kontaktní údaje je navázána na počátek účinnosti zákona. Vzhledem k tomu, že k předání kontaktních údajů bude formou prováděcího předpisu stanoven formulář a jednoduchý technický postup, nemělo by její dodržení činit povinným subjektům žádné obtíže.*

*Lhůta ke splnění povinnosti subjektů zajišťujících významné sítě hlásit kybernetické bezpečnostní incidenty je stanovena tak, aby měly tyto subjekty dostatečnou časovou rezervu k organizačním opatřením umožňující kontakt s národním dohledovým pracovištěm.*

Ustanovení § 29 ZoKB definuje lhůty ke splnění povinností vyplývajících z tohoto zákona pro orgány a osoby, které jsou poskytovatelem služby elektronických komunikací a subjektem zajišťujícím síť elektronických komunikací či orgánem nebo osobou zajišťující významnou síť.

**Výčet jednotlivých lhůt a povinností je uveden v rámci charakteristiky aktiv, práv a povinností** u daného subjektu. Blíže viz § 3 a) a b) ZoKB.

**§ 30**

(splnění povinností správců informačních a komunikačních systémů kritické informační infrastruktury)

**Orgány a osoby uvedené v § 3 písm. c) a d)**

**a) oznámí kontaktní údaje podle § 16 nejpozději do 30 dnů ode dne určení jejich informačního systému nebo komunikačního systému kritickou informační infrastrukturou,**

**b) začnou plnit povinnost stanovenou v § 8 odst. 1 a 4 nejpozději do 1 roku ode dne určení jejich informačního systému nebo komunikačního systému kritickou informační infrastrukturou a**

**c) zavedou bezpečnostní opatření podle § 4 odst. 2 nejpozději do 1 roku ode dne určení jejich informačního systému nebo komunikačního systému kritickou informační infrastrukturou.**

Z důvodové zprávy:

*Lhůty ke splnění povinností správců informačních a komunikačních systémů kritické informační infrastruktury oznámit kontaktní údaje a hlásit kybernetické bezpečnostní incidenty jsou stanoveny analogicky se lhůtami ve výše uvedeném ustanovení s tím rozdílem, že rozhodným dnem pro počátek běhu lhůty je den, kdy byl příslušní informační nebo komunikační systém povinné osoby určen kritickou informační infrastrukturou, respektive jejím prvkem. Dalším rozdílem oproti předchozímu ustanovení je stanovení přechodného období pro implementaci a dokumentaci bezpečnostních opatření. U obou typů povinných osob, jichž se týká toto ustanovení, lze očekávat, že již bezpečnostními opatřeními na úrovni zákonného standardu, respektive technického standardu stanoveného prováděcím předpisem vzhledem k důležitosti příslušné informační a komunikační infrastruktury disponují, a proto je v jejich případě roční lhůta stanovena s dostatečnou časovou rezervou.*

Z důvodové zprávy k novele ZoKB:

K § 30 písm. b)
*Legislativně technická úprava vnitřního odkazu v rámci zákona vyplývající z vložení nového odstavce do § 4.*

Ustanovení § 30 ZoKB definuje lhůty ke splnění povinností vyplývajících z tohoto zákona pro orgány a osoby, které jsou správcem a provozovatelem informačního systému kritické informační infrastruktury či správcem a provozovatelem komunikačního systému kritické informační infrastruktury.

**Výčet jednotlivých lhůt a povinností je uveden v rámci charakteristiky aktiv, práv a povinností** u daného subjektu. Blíže viz § 3 c) a d) ZoKB.

**§ 31**
(splnění povinností správců významných informačních systémů)

**Orgány a osoby uvedené v § 3 písm. e)**

**a) oznámí kontaktní údaje podle § 16 nejpozději do 30 dnů ode dne naplnění určujících kritérií významného informačního systému jejich informačních systémů,**
**b) začnou plnit povinnost stanovenou v § 8 odst. 1 a 4 nejpozději do 1 roku ode dne naplnění určujících kritérií významného informačního systému a**
**c) zavedou bezpečnostní opatření podle § 4 odst. 2 nejpozději do 1 roku ode dne naplnění určujících kritérií významného informačního systému.**

Z důvodové zprávy:

*Lhůty k přizpůsobení se novým zákonným povinnostem jsou u správců významných informačních systémů stanoveny analogicky s předchozím ustanovením s tím, že počátek jejich běhu je stanoven ke dni, kdy příslušný informační systém nabyl parametry významného informačního systému stanovené prováděcím právním předpisem.*

Z důvodové zprávy k novele ZoKB:

K § 31 písm. b)
*Legislativně technická úprava vnitřního odkazu v rámci zákona vyplývající z vložení nového odstavce do § 4.*

Ustanovení § 31 ZoKB definuje lhůty ke splnění povinností vyplývajících z tohoto zákona pro orgány a osoby, které jsou správcem a provozovatelem významného informačního systému.

**Výčet jednotlivých lhůt a povinností je uveden v rámci charakteristiky aktiv, práv a povinností** u daného subjektu. Blíže viz § 3 písm. e) ZoKB.

**§ 32**
(výkon činnosti národního CERT)

**Činnost národního CERT vykonává do doby, než nabude účinnosti veřejnoprávní smlouva uzavřená podle § 19, ten, kdo přede dnem nabytí účinnosti tohoto zákona vykonával činnost, kterou podle tohoto zákona vykonává národní CERT, nejdéle však do 2 let ode dne nabytí účinnosti tohoto zákona.**

Z důvodové zprávy:

*V současnosti je potřeba národního soukromoprávního „single point of contact" řešena při absenci zákonného právního rámce, tj. bez založení kompetencí nebo stanovení povinností třetím stranám, spoluprací se soukromoprávním subjektem provizorně provozujícím dohledové pracoviště, a to na základě neformálního inominátního memoranda o spolupráci uzavřeného s NBÚ. Teprve po nabytí účinnosti tohoto zákona bude moci být vypsáno řízení o výběru žádosti podle správního řádu, v jehož rámci bude vybrána právnická osoba, která bude vykonávat činnost provozovatele národního CERT a s níž NBÚ uzavře příslušnou veřejnoprávní smlouvu. Mohlo by zde tak dojít k určité časové prodlevě mezi nabytím účinnosti návrhu zákona a uzavřením veřejnoprávní smlouvy, kdy by činnost národního CERT do vybrání jeho provozovatele měl podle dikce zákona vykonávat NBÚ, avšak současně by zde byl subjekt, který tuto činnost dlouhodobě vykonával a má k ní vytvořeny odpovídající podmínky. Z hlediska zachování kontinuity činnosti, jakož i efektivnosti se jeví jako vhodnější řešení, podle kterého by tento subjekt po dobu účinnosti shora uvedeného memoranda vykonával činnost provozovatele národního CERT podle návrhu zákona, avšak s časovým omezením. Maximální lhůta dvou let pro toto provizorní řešení umožní provést adekvátní výběrové řízení a bez technických nebo organizačních obtíží předat provoz národního CERT řádně vybranému subjektu.*

Ustanovení § 32 ZoKB mělo zajistit kontinuitu činnosti národního CERT týmu do doby, než bude vybrán provozovatel národního CERT týmu.

Dne 19. prosince 2012 podepsali zástupci sdružení CZ.NIC a Národního bezpečnostního úřadu memorandum[440] (navazující na předchozí memoranda) týkající se provozu agendy Národního bezpečnostního týmu CSIRT.CZ sdružením CZ.NIC. Toto memorandum vstoupilo v platnost 1. ledna 2013 a platilo po dobu tří let.

V srpnu 2015 byl na základě požadavků stanovených v ZoKB vybrán provozovatel Národního CERT týmu. Tímto provozovatelem se stalo sdružení CZ.NIC.[441] Dne 18. prosince 2015 pak

440: *Memorandum o Computer Emergency Response Team/Computer Security Incident Response Team České republiky.* [online]. Dostupné z: https://www.nic.cz/files/nic/NBU_Memorandum_12-12.pdf

441: Viz https://www.nic.cz/page/351/

došlo k podpisu Veřejnoprávní smlouvy o zajištění činnosti Národního CERT a o spolupráci v oblasti kybernetické bezpečnosti.[442] Tato smlouva byla uzavřena na dobu neurčitou.

**§ 33**
**Společná ustanovení**

**(1) Tento zákon se vztahuje pouze na takové informační nebo komunikační systémy zpravodajských služeb, které splňují podmínky pro určení kritické informační infrastruktury, a to v rozsahu § 12 a 16; ustanovení § 4 se na tyto systémy použije přiměřeně a Úřad je jako prvky kritické infrastruktury podle § 22 odst. 2 písm. m) nenavrhuje.**
**(2) Na informační systém Policie České republiky a Generální inspekce bezpečnostních sborů pro analytickou činnost v trestním řízení se tento zákon vztahuje pouze v rozsahu § 12 a 16; ustanovení § 4 se na tento systém použije přiměřeně. To neplatí, pokud je tento systém kritickou informační infrastrukturou.**
**(3) Tento zákon se vztahuje pouze na poskytovatele digitální služby, který je právnickou osobou a není mikropodnikem nebo malým podnikem.**[443]
**(4) Tento zákon se nevztahuje na poskytovatele digitální služby, který má sídlo v jiném členském státě.**

Z důvodové zprávy:

*Účelem tohoto ustanovení je partikulární vynětí informačních a komunikačních systémů používaných zpravodajskými službami z působnosti tohoto zákona. Vzhledem k charakteru těchto systémů není žádoucí ani technicky možné, aby byly informace o jejich bezpečnostní situaci zpracovávány národním nebo vládním dohledovým pracovištěm, neboť by to vyžadovalo technické i personální oddělení veškerých evidencí a postupů, a to by indukovalo neúměrné personální, organizační i transakční náklady. Zabezpečení těchto systémů je přitom dostatečně řešeno na úrovni jednotlivých zpravodajských služeb, takže tyto systémy nepředstavují pro národní kybernetickou bezpečnost žádné podstatné riziko. Z těchto důvodů zákon předpokládá pouze základní vzájemnou komunikaci mezi správci těchto systémů, vládním dohledovým pracovištěm. Zpravodajské služby tak budou povinny oznámit NBÚ kontaktní údaje systémů, které splňují formální požadavky pro zařazení do kritické informační infrastruktury a prostřednictvím těchto kontaktních údajů jim budou zasílána varování před hrozbami v oblasti kybernetické bezpečnosti s případnými doporučeními, jak těmto hrozbám čelit. V těchto informačních nebo komunikačních systémech by rovněž měla být zavedena bezpečnostní opatření, nikoliv však v plném rozsahu, ale přiměřeně s ohledem na jejich technické vlastnosti a účel jejich provozu. Z důvodů uvedených výše nebudou rovněž tyto systémy navrhovány do příslušného seznamu prvků kritické infrastruktury.*

442: Blíže viz [online]. Dostupné z: https://www.nic.cz/files/nic/doc/NBU-Smlouva-narodni-cert-201512.pdf

443: Příloha doporučení Komise 2003/361/ES ze dne 6. května 2003 o definici mikropodniků a malých a středních podniků.

Z důvodové zprávy k novele ZoKB:

K § 33 odst. 3 a 4
*Povinnosti poskytovatelů digitálních služeb, které se do zákona zavádějí touto novelou, se v souladu s čl. 16 odst. 11 směrnice nevztahují na mikropodniky a malé podniky, jak jsou definovány doporučením Komise o definici mikropodniků, malých a středních podniků. Toto negativní vymezení povinností, jež nově dopadají na poskytovatele digitálních služeb, zajišťuje proporcionalitu směrnice. Ve smyslu přílohy doporučení, na kterou je v poznámce pod čarou odkazováno, je mikropodnikem (někdy je označován jako drobný podnik) podnik, který zaměstnává méně než 10 zaměstnanců a jeho roční obrat nebo bilanční suma roční rozvahy nepřesahuje ročně 2 mil. EUR. Malým podnikem je pak podnik, jenž zaměstnává méně než 50 zaměstnanců a roční obrat nebo bilanční suma roční rozvahy nepřesahuje ročně 10 mil. EUR. Vždy platí, že obě podmínky, jak personální, tak i finanční, musí být splněny kumulativně.*

**K odst. 1)**
Zákon o kybernetické bezpečnosti se nevztahuje na informační nebo komunikační systémy zpravodajských služeb.

V případě, že tyto systémy splňují podmínky pro určení kritické informační infrastruktury, má na ně být přiměřeně aplikována povinnost:

- přijímat varování (§ 12 ZoKB) před hrozbami v oblasti kybernetické bezpečnosti s případnými doporučeními, jak těmto hrozbám čelit,
- zavést bezpečnostní opatření, přiměřeně s ohledem na jejich technické vlastnosti a účel jejich provozu,
- poskytovat NÚKIB kontaktní údaje (§ 16 ZoKB).

Národní úřad pro kybernetickou a informační bezpečnost nenavrhuje Ministerstvu vnitra informační nebo komunikační systémy zpravodajských služeb jako prvky kritické infrastruktury.

**K odst. 2)**
Zákon o kybernetické bezpečnosti se vztahuje na informační systémy Policie České republiky a Generální inspekce bezpečnostních sborů pro analytickou činnost v trestním řízení pouze v tom rozsahu, že na ně má být přiměřeně aplikována povinnost:

- přijímat varování (§ 12 ZoKB) před hrozbami v oblasti kybernetické bezpečnosti s případnými doporučeními, jak těmto hrozbám čelit,
- zavést bezpečnostní opatření, přiměřeně s ohledem na jejich technické vlastnosti a účel jejich provozu,
- poskytovat NÚKIB kontaktní údaje (§ 16 ZoKB).

To neplatí, pokud je tento systém kritickou informační infrastrukturou.

**K odst. 3)**
Zákon o kybernetické bezpečnosti vymezuje poskytovatele digitálních služeb. Vedle tohoto pozitivního vymezení uvádí shodně NIS[444] i ZoKB[445] negativní vymezení, které stanoví, že se tyto předpisy aplikují pouze v případě, že právnická osoba, která digitální službu poskytuje, zároveň není mikropodnikem ani malým podnikem ve smyslu doporučení Komise 2003/361/ES.[446]

**Mikropodnikem** se dle tohoto doporučení rozumí podnik **s méně než 10 zaměstnanci** a ročním obratem (finanční částka získaná za určité období) nebo rozvahou (výkaz aktiv a pasiv společnosti) **do 2 milionů EUR.**

**Malým podnikem** se dle tohoto doporučení rozumí podnik **s méně než 50 zaměstnanci** a ročním obratem nebo rozvahou **do 10 milionů EUR.**

Vždy platí, že obě podmínky, jak personální, tak i finanční, musí být splněny kumulativně.

**K odst. 4)**
V případě, že má poskytovatel digitální služby již existující sídlo v jiném členském státě unie, zákon o kybernetické bezpečnosti se na něj nevztahuje.

## ČÁST TŘETÍ

### Změna zákona o elektronických komunikacích
### § 35

Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění zákona č. 290/2005 Sb., zákona č. 361/2005 Sb., zákona č. 186/2006 Sb., zákona č. 235/2006 Sb., zákona č. 310/2006 Sb., zákona č. 110/2007 Sb., zákona č. 261/2007 Sb., zákona č. 304/2007 Sb., zákona č. 124/2008 Sb., zákona č. 177/2008 Sb., zákona č. 189/2008 Sb., zákona č. 247/2008 Sb., zákona č. 384/2008 Sb., zákona č. 227/2009 Sb., zákona č. 281/2009 Sb., zákona č. 153/2010 Sb., nálezu Ústavního soudu, vyhlášeného pod č. 94/2011 Sb., zákona č. 137/2011 Sb., zákona č. 341/2011 Sb., zákona č. 375/2011 Sb., zákona č. 420/2011 Sb., zákona č. 457/2011 Sb., zákona č. 458/2011 Sb., zákona č. 468/2011 Sb., zákona č. 18/2012 Sb., zákona č. 19/2012 Sb., zákona č. 142/2012 Sb., zákona č. 167/2012 Sb., zákona č. 273/2012 Sb., zákona č. 214/2013 Sb. a zákona č. 303/2013 Sb., se mění takto:

444: Čl. 4 odst. 6 a 16 odst. 11 NIS

445: § 33 odst. 3 ZoKB

446: Příloha doporučení Komise 2003/361/ES ze dne 6. května 2003 o definici mikropodniků a malých a středních podniků.

1. V § 89 se doplňuje odstavec 4, který včetně poznámky pod čarou č. 62 zní:
„(4) Podnikatel zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací je povinen na žádost účastníka bezplatně a ve formě umožňující další elektronické zpracování dat poskytnout mu provozní a lokalizační údaje, které má k dispozici na základě tohoto zákona, pokud je nemohl účastník pro poruchu na jeho zařízení v důsledku kybernetického bezpečnostního incidentu[62]) zachytit nebo uložit. Údaje podnikatel předá, je-li to technicky možné, bezodkladně, nejpozději však do 3 dnů ode dne doručení žádosti nebo v případě probíhající komunikace ode dne jejího uskutečnění.[62]) § 7 odst. 2 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).“.

2. V § 118 odst. 14 písm. y) se slovo „nebo“ zrušuje.

3. V § 118 se na konci odstavce 14 tečka nahrazuje slovem „ , nebo“ a doplňuje se písmeno ad), které zní:
„*ad*) v rozporu s § 89 odst. 4 neposkytne údaje, nebo je poskytne opožděně.“.

4. V § 118 odst. 22 písm. a) se slovo „nebo“ nahrazuje čárkou a na konci textu písmene a) se doplňují slova „nebo odstavce 14 písm. ad)“.

## ČÁST PÁTÁ

### Změna zákona o provozování rozhlasového a televizního vysílání
### § 37

V § 32 odst. 1 písm. k) zákona č. 231/2001 Sb., o provozování rozhlasového a televizního vysílání a o změně dalších zákonů, ve znění zákona č. 274/2003 Sb., se za slova „válečného stavu,“ vkládají slova „stavu kybernetického nebezpečí,“.

## ČÁST ŠESTÁ
## ÚČINNOST

### § 38
### Tento zákon nabývá účinnosti dnem 1. ledna 2015.

**Přechodné ustanovení zavedeno zákonem č. 104/2017 Sb. Čl. IV**

Provozovatel informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému určeného podle zákona č. 181/2014 Sb., ve znění účinném přede dnem nabytí účinnosti tohoto zákona,

a) oznámí kontaktní údaje podle § 16 zákona č. 181/2014 Sb. nejpozději do 30 dnů ode dne nabytí účinnosti tohoto zákona,

b) začne plnit povinnost stanovenou v § 8 odst. 1 a 3 zákona č. 181/2014 Sb. nejpozději do 6 měsíců ode dne nabytí účinnosti tohoto zákona a

c) zavede bezpečnostní opatření podle § 4 odst. 2 zákona č. 181/2014 Sb. nejpozději do 6 měsíců ode dne nabytí účinnosti tohoto zákona. V případě zavedení bezpečnostních opatření má provozovatel nárok na úhradu nákladů spojených s přijetím bezpečnostního opatření; náklady provozovateli uhradí správce daného systému.

**Přechodná ustanovení zavedena zákonem č. 205/2017 Sb. Čl. II**

1. Úřad určí provozovatele základní služby a informační systém základní služby podle § 22a odst. 1 zákona č. 181/2014 Sb., ve znění účinném ode dne nabytí účinnosti tohoto zákona, do 9. listopadu 2018.

2. Orgány a osoby uvedené v § 3 písm. f) zákona č. 181/2014 Sb., ve znění účinném ode dne nabytí účinnosti tohoto zákona,

   a) oznámí Úřadu do 30 dnů ode dne, kdy byly informovány podle § 4a odst. 3 zákona č. 181/2014 Sb., ve znění účinném ode dne nabytí účinnosti tohoto zákona, kontaktní údaje podle § 16 odst. 1 zákona č. 181/2014 Sb., ve znění účinném ke dni nabytí účinnosti tohoto zákona, a

   b) začnou nejpozději do 1 roku ode dne, kdy byly informovány podle § 4a odst. 3 zákona č. 181/2014 Sb., ve znění účinném ode dne nabytí účinnosti tohoto zákona, plnit ostatní povinnosti podle zákona č. 181/2014 Sb., ve znění účinném ode dne nabytí účinnosti tohoto zákona.

3. Poskytovatel digitální služby

   a) oznámí Úřadu nejpozději do 30 dnů ode dne nabytí účinnosti tohoto zákona kontaktní údaje podle § 16 odst. 1 zákona č. 181/2014 Sb., ve znění účinném ke dni nabytí účinnosti tohoto zákona, a

   b) začne nejpozději do 1 roku ode dne nabytí účinnosti tohoto zákona plnit ostatní povinnosti podle zákona č. 181/2014 Sb., ve znění účinném ode dne nabytí účinnosti tohoto zákona.

4. Orgány a osoby uvedené v § 3 písm. c) až f) jsou povinny, v případě, že podmínky jejich smluvního vztahu uzavřeného s dodavatelem pro jejich informační nebo komunikační

systém nesplňují požadavky podle zákona č. 181/2014 Sb., ve znění účinném ode dne nabytí účinnosti tohoto zákona, a jeho prováděcích právních předpisů, uvést smluvní vztah do souladu s těmito požadavky do 1 roku ode dne nabytí účinnosti tohoto zákona.

5. Řízení o správních deliktech a přestupcích podle zákona č. 181/2014 Sb., zahájená a nedokončená přede dnem nabytí účinnosti tohoto zákona dokončí Národní úřad pro kybernetickou a informační bezpečnost. Národní bezpečnostní úřad předá Národnímu úřadu pro kybernetickou a informační bezpečnost ke dni nabytí účinnosti tohoto zákona veškeré doklady a údaje týkající se nedokončených řízení a o předání sepíše s Národním úřadem pro kybernetickou a informační bezpečnost protokol.

6. Výkon práv a povinností ze smlouvy uzavřené podle § 19 odst. 1 zákona č. 181/2014 Sb., přechází ke dni nabytí účinnosti tohoto zákona z Národního bezpečnostního úřadu na Národní úřad pro kybernetickou a informační bezpečnost.

7. Národní bezpečnostní úřad předá Národnímu úřadu pro kybernetickou a informační bezpečnost do 6 měsíců ode dne nabytí účinnosti tohoto zákona veškeré doklady a údaje týkající se výkonu působnosti, která ke dni nabytí účinnosti tohoto zákona přechází na Národní úřad pro kybernetickou a informační bezpečnost.

8. Výkon práv a povinností vyplývajících z pracovněprávních vztahů zaměstnanců Národního bezpečnostního úřadu, kteří zajišťovali činnost Národního bezpečnostního úřadu podle zákona č. 181/2014 Sb., ve znění účinném přede dnem nabytí účinnosti tohoto zákona, která dnem nabytí účinnosti tohoto zákona přechází na Národní úřad pro kybernetickou a informační bezpečnost, přechází dnem nabytí účinnosti tohoto zákona na Národní úřad pro kybernetickou a informační bezpečnost.

9. Příslušnost k hospodaření s majetkem státu užívaným Národním bezpečnostním úřadem přechází ke dni nabytí účinnosti tohoto zákona na Národní úřad pro kybernetickou a informační bezpečnost, pokud byl tento majetek využíván k zajišťování činnosti Národního bezpečnostního úřadu podle zákona č. 181/2014 Sb., ve znění účinném přede dnem nabytí účinnosti tohoto zákona, která přechází ke dni nabytí účinnosti tohoto zákona na Národní úřad pro kybernetickou a informační bezpečnost.

10. Rozpočtované prostředky kapitoly 308 - Národní bezpečnostní úřad podle zákona č. 457/2016 Sb., o státním rozpočtu České republiky na rok 2017, včetně nároků nespotřebovaných výdajů za předcházející léta, které souvisí s výkonem působnosti Národního bezpečnostního úřadu, která ke dni nabytí účinnosti tohoto zákona přechází na Národní úřad pro kybernetickou a informační bezpečnost, se přesouvají ke dni nabytí účinnosti tohoto zákona na Národní úřad pro kybernetickou a informační bezpečnost.

# 3 Kyberbezpečnost prakticky

## III Kyberbezpečnost prakticky

*„Pravidelně jsem dotazován na to, co může průměrný uživatel Internetu udělat, aby si zajistil svoji bezpečnost. Moje první odpověď je obvykle ‚nic; jsi v háji'."*

Bruce Schneier[447]

Bruce Schneier byl v této knize již několikrát citován a bohužel tento jeho citát je z našeho pohledu zřejmě nejpravdivější. Důvodem není ta skutečnost, že by kyberprostor či počítačové systémy, které běžně používáme, byly samy o sobě nebezpečné či nezabezpečené.

Ona potencionální nebezpečnost jak tohoto virtuálního prostředí, tak počítačových systémů a aplikací tkví primárně v nás… uživatelích. Spoléháme se, že naše bezpečnost bude zajištěna někým jiným. Nějakou vyšší mocí, nebo jinou autoritou, ať již v podobě státu, nebo nadnárodní soukromé organizace.

Paradoxem je, že například těmto soukromým organizacím věříme bez toho, že bychom se o ně podrobněji zajímali, či si alespoň přečetli smluvní podmínky smlouvy, kterou s jakoukoliv z těchto organizací uzavíráme on-line. Prostě těmto gigantům věříme…nebo chceme věřit.

Věříme jim proto, že jsou „velcí"? Věříme jim i přes to, že jsme si vědomi, že některé z těchto organizací měly obrovské problémy s úniky dat, analýzou našich dat, profilováním a následným cíleným oslovováním „šitým na míru" tomu kterému uživateli?

**Ano, stále věříme…**
Velmi častou odpovědí uživatelů na výše uvedené však je: *„Vždyť už o nás stejně všechno ví, tak co, případně proč bych s tím něco dělal."* Už jsme jim stejně povolili kompletní sběr a analýzu našich dat či jsme jim je rovnou dobrovolně odevzdali.

Velikost organizace, její vliv, objem uchovávaných dat o uživatelích aj. však asi nejsou oněmi určujícími kritérii, kvůli kterým se řada uživatelů v kyberprostoru chová ne zcela racionálně.

Domníváme se, že problém je možná v tom, že chceme věřit, že někde existuje prostor, který je úžasný, otevřený, vstřícný, bezpečný a přitom všeprostupující. Technicky tímto prostorem skutečně může být kyberprostor, avšak kyberprostor bez nás, uživatelů.

**Chceme věřit…**
Nicméně jsme to my uživatelé, kdo porušuje pravidla a základní principy fungování kyberprostoru. Jsme to my, kdo zasahuje do práv jiného, ať už s jakýmkoliv motivem či cílem.

447: SCHNEIER, Bruce. [online]. [cit. 18. 7. 2018]. Dostupné z: https://www.azquotes.com/quote/699390 Překlad autora.

Uživatelé jsou ti, kdo zcizují data, vylákávají intimní fotografie od jiných, jen aby je následně mohli vydírat, zahlcují systémy DDoS útoky, instalují malware do počítačů atd.

**Poškozujeme a ničíme…**
Pokud budeme schopni přijmout premisu, že se kyberprostor na sociální úrovni[448] nijak neliší od světa reálného, pak by nám nemělo činit problém začít řešit i problematiku kybernetické bezpečnosti (ať už jako jedinec, či organizace).

V případě, že Vám ve světě reálném někdo zcizí věc (např. peníze, počítač, data aj.), protože jste si ji dobře nezabezpečili (např. nechali je bez dozoru na stole v restauraci), reakcí na tuto skutečnost bude mimo jiné i to, že se do budoucna budete snažit tyto hodnoty více chránit, aby k podobné události již nedošlo.

V kyberprostoru, stejně jako ve světě reálném neexistuje jedna bezpečnost a jedno zabezpečení, které by bylo možné univerzálně aplikovat na každého. Pokud chceme řešit bezpečnost, je třeba ji řešit komplexně a je třeba individualizovat.

**Věřme, ale buďme připraveni na nejhorší…**
„*Historie nás učí: nikdy nepodceňujte množství peněz, čas a úsilí, které někdo vynaloží, aby napadl (poškodil) bezpečnostní systém. Vždy je lepší předpokládat to nejhorší. Předpokládejte, že vaši protivníci jsou lepší, než ve skutečnosti jsou. Předpokládejte, že věda a technologie budou brzy schopny dělat věci, které zatím nemohou. Počítejte s chybou. Zajistěte si větší bezpečnost, než jakou potřebujete dnes. Když nastane neočekávané, budete rádi, že jste to udělali.*"

Bruce Schneier[449]

Předchozí kapitoly knihy, kterou čtete, se věnovaly základní terminologii, principům a vývoji legislativy související s problematikou kybernetické bezpečnosti. Samostatná pozornost byla věnována zákonu o kybernetické bezpečnosti a prováděcím vyhláškám k tomuto zákonu.

Při řešení jakéhokoliv problému je rozhodně dobré mít teoretický základ a znát limity definované právem, které se s danou problematikou souvisí.

„*Teorie bez praxe je prázdná (mrtvá), praxe bez teorie je slepá.*"

Immanuel Kant

Zejména díky skutečnosti, že Pavel Bašta dlouhodobě působí jako bezpečnostní analytik (v současné době v rámci národního CSIRT týmu, provozovaného sdružením CZ.NIC), bylo

448: Viz kap. 1 Kyberprostor (Cyberspace)
449: SCHNEIER, Bruce. [online]. [cit. 18. 7. 2018]. Dostupné z: https://www.azquotes.com/quote/570053 Překlad autora.

možné do následujících kapitol přenést praktické zkušenosti autorů z oblasti bezpečné správy ICT, zabezpečení těchto systémů proti kybernetickým hrozbám, útokům či incidentům aj.

Pozornost je zaměřena na zabezpečení proti vnitřním (např. ze strany nespokojených zaměstnanců) i vnějším hrozbám[450], neboť z pohledu běžných organizací právě ony jsou nejčastějšími důvody narušení důvěrnosti, integrity či dostupnosti dat.

Informace obsažené v následujících kapitolách, by při jejich důsledném dodržování, měly čtenáři pomoci snížit či eliminovat rizika pramenící z běžných kybernetických útoků.

Specifickým útokům (např. state-sponsored útokům, APT útoků[451], či útokům organizovaných zločineckých skupin aj.), které obvykle cílí na kritickou infrastrukturu, významné informační systémy a jiné pro stát důležité instituce a služby nebude věnována pozornost.

Pokud čtenář spravuje infrastrukturu, jež by se mohla stát cílem takovýchto specifických útoků, byl s nevětší pravděpodobností určen jako některý ze subjektů uvedených v § 3 ZoKB a problematiku kybernetické bezpečnosti již aktivně řeší.

Přesto lze dle našeho názoru informace obsažené v následujících kapitolách využít i v rámci správy výše uvedených systémů a služeb, neboť jsou paradoxně známy případy[452], kdy útočník pro proniknutí k „citlivým datům" nepotřeboval žádné sofistikované prostředky, stačilo mu pouhé nedodržování základních bezpečnostních principů ze strany napadené organizace.

Není v možnostech jedné knihy obsáhnout všechny aspekty a detaily kybernetické bezpečnosti v celém jejím širokém pojetí. Nelze také předložit konkrétní návody pro každý existující systém či každou myslitelnou situaci.

Jsme si zcela vědomi skutečnosti, že právě v kyberprostoru informace, rady a návody zastarávají či jsou modifikovány mnohem rychleji, než v jiném prostředí a oblasti lidské činnosti.

I z tohoto důvodu jsme se rozhodli knihu interaktivně provázat s portálem https://kyberbezpecnost.csirt.cz/, v rámci kterého Vám můžeme efektivně a rychle poskytovat nové a aktuální informace vztahující se k problematice kybernetické bezpečnosti, hrozeb, útoků aj.

Čtenář by k následujícím kapitolám měl přistupovat jako k určitému vodítku, po jehož přečtení by měl vědět, na které věci se má zaměřit, co hledat v manuálech k používaným produktům, na

450: Blíže viz kap. 2.4.1 Kybernetická hrozba

451: KOLOUCH, Jan. *CyberCrime.* Praha: CZ.NIC, 2016, s. 320–322

452: Viz *Postřehy z bezpečnosti: středoškolský student vs. ředitel CIA 1:0.* [online]. [cit. 4. 7. 2017]. Dostupné z: https://www.root.cz/clanky/postrehy-z-bezpecnosti-stredoskolsky-student-reditel-cia-1-0/

co se zeptat svého dodavatele, či na co se zaměřit z hlediska bezpečnosti při výběrovém řízení na nové ICT řešení.

*„Buďte samouci, nečekejte, až vás naučí život.“*

Stanisław Jerzy Lec

## 5 Fyzická bezpečnost

Fyzická bezpečnost je nedílnou, důležitou a bohužel mnohdy podceňovanou součástí kybernetické bezpečnosti.

K čemu jsou drahé firewally, antiviry nebo SIEM řešení, když může útočník fyzicky dojít až k serveru, připojit k němu USB disk a zkopírovat z něj malware přímo do serveru, či si naopak ze serveru odnést důležitá data.

Fyzická bezpečnost v sobě zahrnuje řadu opatření, mezi které patří:

- **zajištění perimetru**,
- **kontrola přístupu**,
- **vnitřní bezpečnost**,
- **ochrana počítačových systémů** před rozebráním, úpravou, nebo připojením periférií k vstupně výstupním portům.

Krom uvedeného lze do fyzické bezpečnosti zařadit i některé další prvky, jako je například:

- ochrana před nepříznivými přírodními vlivy,
- splnění elektrotechnických a požárních předpisů,
- zajištění vhodného prostředí pro provoz techniky,
- zajištění redundance aj.

### 5.1 Zajištění perimetru

V pojetí fyzické bezpečnosti se obvykle za perimetr považuje oblast, která bezprostředně obklopuje prostor, ve kterém jsou chráněná aktiva[453] (data, informace ale i prvky ICT aj.).

**Příklad:** *Pokud se vaše aktiva nacházejí například v rodinném domě, lze zpravidla za perimetr považovat zdi domu, přilehlý pozemek, plot apod. Pokud organizace sídlí v pronajaté budově, můžeme za perimetr považovat zdi námi pronajatých kanceláří, nebo společné prostory (např. chodba nebo recepce).*

Přesné vymezení toho, jaké části perimetru je potřeba mít pod kontrolou je otázkou provedení analýzy rizik[454], na základě které je také následně možné posoudit, zda, případně jaká opatření v rámci jednotlivých prostor a aktiv je třeba zvolit k jejich účinné ochraně.

453: Viz kap. 2.3.2 Aktivum

454: Blíže viz kap. 2.3.1 Riziko a § 5 písm. b) a násl. ZoKB

Perimetr je možné zajistit například elektronickými systémy detekce pohybu, kamerovými systémy, či například společnou recepcí, která je schopna identifikovat návštěvu a monitorovat její pohyb v rámci chráněného prostoru.

V případě využívání kamerových systémů je však třeba respektovat podmínky (zejména v rovině práva na ochranu osobních údajů) stanovené právními předpisy pro využívání těchto systémů.[455]

## 5.2 Kontrola přístupu

Kontrola přístupu zajišťuje, aby se přes perimetr dostaly pouze osoby k tomu oprávněné. Cílem kontroly přístupu je chránit aktiva (ICT systémy, data aj.) před neoprávněnými zásahy do nich.

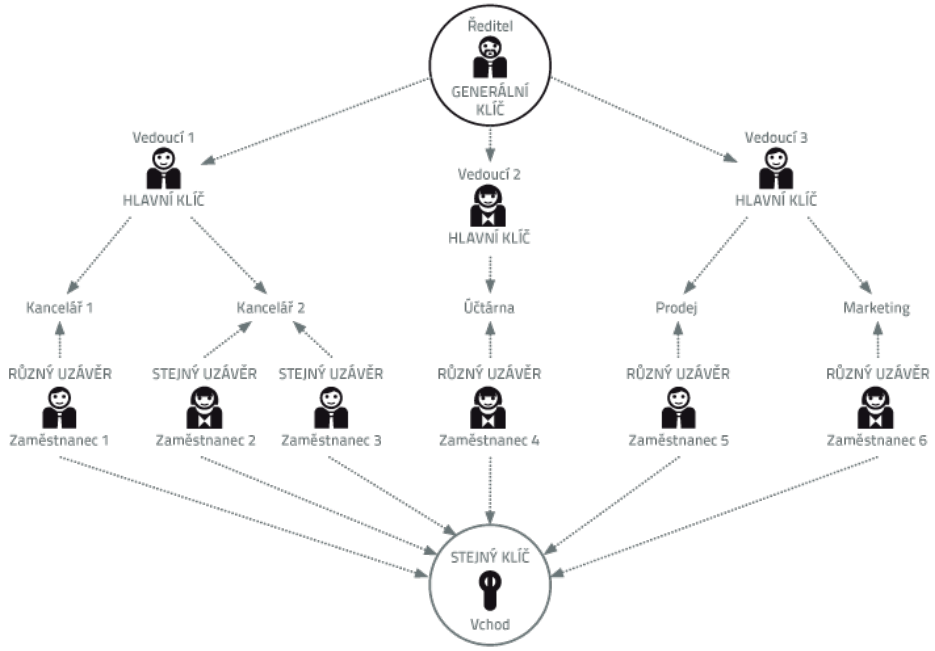
Mechanismů pro kontrolu přístupu a jejich kombinací existuje celá řada. Počínaje klasickými zámky, přes elektronické systémy schopné registrovat docházku zaměstnanců, až po kontrolu lidskou ostrahou. Výše **uvedená řešení je možné kombinovat**, avšak při implementaci je třeba vždy zohlednit výhody a nevýhody toho kterého řešení kontroly přístupu.

**Příklad:** *Malá organizace s jednou kanceláří o pěti lidech si vystačí s bezpečnostním zámkem a sadou klíčů, naopak větší společnost nejspíš uvítá výhody elektronického systému, případně jeho kombinaci s lidskou ostrahou.*

V případě **výběr**u **zámku** je třeba pamatovat na to, že existuje šest bezpečnostních tříd (třídy 5 a 6 se však běžně nevyužívají), které jsou definovány časem, který je potřeba k jejich překonání za použití určité síly, zkušenosti a nástrojů. Důležité je také neopomenout, že bezpečnostní třída zámku by měla být v souladu s bezpečnostní třídou dveří, kováním, vložkami či mříží a pokud je organizace pojištěna, měla by současně naplňovat požadavky pojišťovny tak, jak jsou definovány v pojistné smlouvě.

V určitých případech je vhodné využívat **systém generálního klíče**, kdy zaměstnanec disponuje klíčem, který odemyká pouze jeho kancelář, ředitel daného úseku pak může mít klíč, který mu umožní přístup do všech kanceláří jeho podřízených a ostraha objektu či ředitel firmy může mít k dispozici generální klíč, kterým v případě nouze odemkne jakékoliv dveře ve firmě.

455: Blíže viz GDPR – kap. 3.3.1 a násl. či kap. 3.3.3 Občanský zákoník



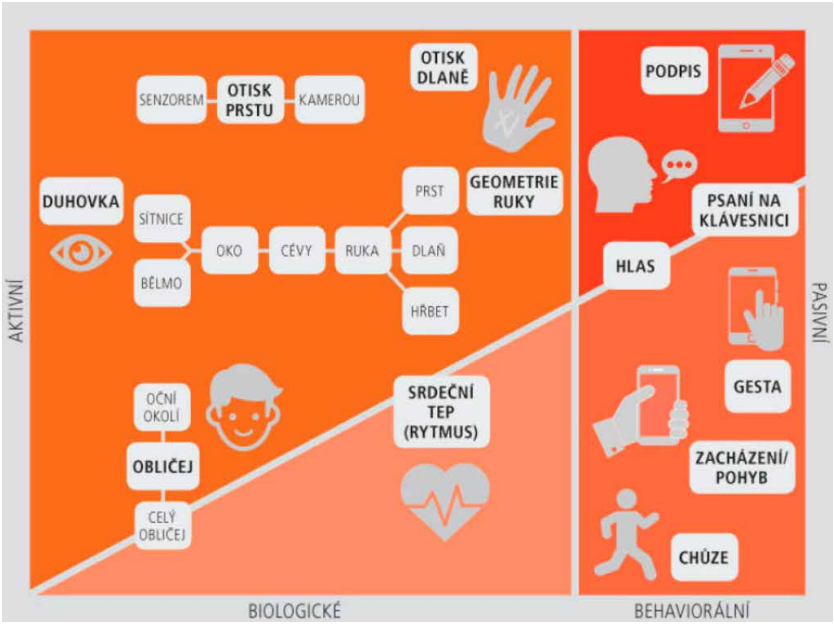

Obrázek 42: Systém generálního klíče[456]

V případě kontroly přístupu pomocí elektronických systémů je třeba zvážit, jaký účel je primárně sledován. Zda jde pouze o kontrolu přístupu osoby vlastnící nějaký **token** (např. čip, kartu aj.), či zda je smyslem tohoto elektronického systému současně i ověřit, že s tímto vstupním tokenem manipuluje její oprávněný držitel.

V praxi je možné nalézt systémy, které využívají pouze přístupový kód, token, snímají biometrické údaje[457] či kombinují uvedené varianty. Dále se lze setkat i se systémy využívajícími turnikety a branky, které by měly zajistit, že do budovy nemůže na jeden token vstoupit více než jedna osoba.

456: *Systémy klíčů.* [online]. [cit. 4. 7. 2018]. Dostupné z: http://www.tokoz.cz/systemy-klicu

457: Jedná se např. o snímače otisků prstů, sken očních duhovek, identifikace na základě obrazu krevního řečiště dlaně aj.




Obrázek 43: Možnosti biometrické identifikace osoby[458]

**Z hlediska zajištění bezpečnosti aktiv je vhodné využívat kombinované systémy umožňující kontrolu přístupu za pomoci tokenu a druhotné autentizace (např. zadáním kódu, využitím biometrických údajů oprávněné osoby aj.).** Kombinovaný systém může zabránit zneužití tokenu například při jeho ztrátě či krádeži a zároveň eliminuje případy, kdy oprávněný uživatel například půjčí token jiné osobě.

Uvedené systémy je dále možné propojit například se systémy pro kontrolu docházky a systémy elektronických zabezpečovacích systémů[459], což ještě dále zvyšuje možné kombinace jejich využití (např. k omezení povolení vstupu do budovy jen v určité době, nebo pouze pokud je EZS bezpečně odkódována).

458: *Biometrie je více než otisk prstu.* [online]. [cit. 4. 7. 2018]. Dostupné z: https://ictrevue.ihned.cz/c3-65967870-0ICT00_d-65967870-biometrie-je-vice-nez-otisk-prstu

459: Dále jen **EZS**

## 5.3 Vnitřní bezpečnost

V rámci vnitřní bezpečnosti je pozornost věnována samotné ochraně prostor, ve kterých se nacházejí aktiva (tj. data, ICT aj.). Jde tedy o řízení přístupů do jednotlivých místností, zajištění prostoru v době, kdy je budova prázdná, či třeba zajištění vhodných podmínek pro provoz ICT zařízení.

I když se tato kniha primárně zabývá bezpečností ICT, je třeba připomenout, že ochranou ICT se také sleduje ochrana dat v těchto systémech uložených. Z tohoto důvodu je třeba při návrhu přístupů do jednotlivých prostor (např. kanceláří, serveroven aj.) vždy zvažovat nejen, zda se v daném prostoru nachází systémy zpracovávající data významná pro organizaci, ale i zda se tam taková data nemohou dostat na jiném nosiči. Pokud ano, je třeba přijmout vhodná opatření, aby měly osoby, které s těmito daty pracují, možnost nosiče s daty bezpečně uložit.

V tomto kontextu jistě stojí za připomenutí, že část bezpečnosti je třeba řešit prostřednictvím interních politik. Jedna z politik, které by neměly v organizaci chybět, je **politika čistého stolu a prázdné obrazovky**, která uvádí, že by zaměstnanec neměl v době své nepřítomnosti v kanceláři nechávat na stole žádné pracovní dokumenty a měl by mít vždy uzamčený počítačový systém tak, aby z něj nebylo možné nic přečíst či jej jinak zneužít.

Při řešení kybernetické bezpečnosti je třeba se zamyslet nad vhodným rozdělením jednotlivých místností (využívaných prostor) a definovat, kdo, kdy a kam by měl mít přístup. Dále je třeba řešit, zda budou v budově umístěny i vlastní servery a klíčové komunikační prvky, nebo jen jejich část. S ohledem na výše uvedené je možné navrhnout vlastní fyzické zabezpečení.

V případě místností určených pro provoz serverů a klíčových komunikačních prvků je třeba myslet na jejich fyzickou bezpečnost, stejně jako na to, že by vybraná místnost neměla sousedit například s rozvody vody, které by v případě havárie způsobily škody na prvcích ICT.

**Prostory určené pro provoz serverů a dalších významných prvků ICT je vhodné vybavit:**

- **kombinovaným systémem přístupu**, který současně zaznamenává na jiný počítačový systém (umístěný mimo serverovnu) jednotlivé přístupy,
- **kamerovým systémem** s automatickým zaznamenáváním při detekci pohybu
- **EZS** napojeným na pult centrální ochrany (PCO),
- **klimatizací a zdrojem nepřerušovaného napájení** (UPS),
- **redundantním připojením na jiný záložní zdroj energie** v případě déletrvajícího výpadku proudu (např. diesel agregát aj.),
- **vhodným hasícím systémem** (např. inertní hasivo IG-541 aj.).

V případě řešení vnitřní bezpečnosti celého objektu je vhodné zvážit instalaci elektronického zabezpečovacího systému a jeho napojení na pult centrální ochrany. V rámci EZS se obvykle používají magnetické kontakty, čidla prostorové ochrany (PIR čidla), MW[460] čidla, ultrazvuková čidla (US), případně kombinace PIR+MW, PIR+US (duální čidla), senzory tříštění skla aj.

Systémy EZS lze dále doplňovat o různá **čidla kouře či některých plynů, infrazávory** apod. Dále jsou pak součástí EZS samotné ústředny a hlásiče poplachu, jako jsou sirény či GSM hlásiče. Při výběru EZS je také potřeba pamatovat na případnou možnost vytváření jednotlivých zón a práv uživatelů, aby například mohla být EZS deaktivována v pracovní době v celé budově s výjimkou serverovny.

Samotnou **ochranu pomocí technických opatření je vhodné doplnit vhodnými opatřeními organizačními**. Ta mohou spočívat například v politice, která vyžaduje, aby zaměstnanci nenechávali návštěvy volně se pohybovat po budově, nebo v politice, která vyžaduje při uzavření smlouvy s novým dodavatelem uzavřít také NDA[461] smlouvu.

Ve větších organizacích, kde se zaměstnanci navzájem neznají, se také vyplatí zavést **identifikační průkazy** s fotografií, které pak u sebe musí zaměstnanci při pohybu po budově viditelně nosit. V případě zavedení identifikačních průkazů je vhodné zavést i kategorii průkazů, které budou jasně (např. díky jinému barevnému provedení) na první pohled odlišovat návštěvy od zaměstnanců. Povinnost nosit viditelně identifikační průkaz se samozřejmě vztahuje i na návštěvy.

## 5.4 Ochrana počítačových systémů

Fyzickou bezpečnost počítačových systémů[462] lze rozdělit na ochranu před krádeží, rozebráním, úpravou, nebo připojením periférií. I když by dodržování opatření zmiňovaných v předchozích částech této kapitoly mělo zabránit nepozorovanému průniku cizích osob až k počítačovým systémům v rámci vaší správy, je třeba mít na paměti, že **bezpečnost je třeba vnímat jako celek složený z jednotlivých vrstev**, přičemž není vhodné spoléhat se pouze na jednu vrstvu ochrany. Případným útočníkem navíc může být interní zaměstnanec, nebo zaměstnanec dodavatele, který řadu bezpečnostních opatření legálně obejde.

460: **PIR** (**P**assive **I**nfrared **S**ensor), **MW** (**M**icro **W**ave). Blíže viz např. *Prostorová ochrana* [online]. [cit. 6. 7. 2017]. Dostupné z:
https://www.alarmsecurity.cz/www-alarmsecurity-cz/5-TECHNICKA-PODPORA/38-Typy-pohybovych-senzoru

461: **Non-Disclousure Agreement**. Tato smlouva zpravidla specifikuje pravidla sdílení důvěrných materiálů, informací a znalostí mezi subjekty, které smlouvu uzavřely.

462: Blíže viz § 1 odst. 2 ZoKB

Jednou z vrstev zajišťujících vyšší úroveň zabezpečení systému jako takového je i **bezpečnost samotných počítačových systémů** (ICT technologií).

### 5.4.1 Opatření proti krádeži počítačových systémů

**Ochrana serverů a klíčových prvků ICT**
Servery by vždy měly být umístěny ve zvlášť k tomu určené, uzamykatelné části organizace (serverovně), nebo přímo ve střeženém hostingovém centru.

Servery se umísťují do standardizovaného systému, tzv. racků, které jsou obvykle uzamykatelné.

**Příklad:** *Je však potřeba upozornit na jednu zkušenost nejen z autorovy praxe. Někteří výrobci dávají do svých racků zámky, které mají pouze několik málo vzorů. Může se tak, obzvlášť ve velkém hostingovém sále stát, že do vašeho racku bude mít někdo přístup díky stejnému klíči. Je proto vhodné se u svého dodavatele na tuto skutečnost informovat a případně vyměnit zámek za jiný.*

Krom klasických zámků je možné dveře k rackům opatřit i jinými bezpečnostními opatřeními (např. přístupem na čip, na základě znalosti číselného kódu, čtečkou biometriky aj.). Zámek umístěný na racku může on-line odesílat do dohledového centra organizace informace o tom, kdo rack otevřel, případně může obsluha dohledového centra o otevření dveří rozhodnout na dálku, například až po telefonické kontrole oprávněného uživatele.

Různých možných kombinací vlastního fyzického zabezpečení serverů existuje celá řada a záleží na konkrétním využití a hodnotě aktiv (dat a zařízení), která jsou chráněna.

**Ochrana ostatních počítačových systémů**
Proti krádeži lze zabezpečit i většinu notebooků, monitorů a desktopů pomocí zámků využívajících např. Kensington Security Slot.[463] Kensington Security Slot je malá, kovem zesílená zdířka, která se používá spolu s příslušným kabelem a zámkem.

Je však třeba zdůraznit, že Kensington lock není nepřekonatelný a ani tak nebyl zamýšlen. Jedná se o systém, jehož primárním cílem je odradit příležitostné zloděje, a ty, jež by chtěli počítačový systém i přes toto zabezpečení ukrást, by měl zdržet co nejdelší dobu.

**Příklad:** *Autor má praktickou zkušenost z velké společnosti, kde se prakticky volně pohybovali jak zaměstnanci, tak i různí dodavatelé. V této společnosti nasazení výše uvedených zámků prokazatelně*

463: Viz *Kensington Security Slot.* [online]. [cit. 6. 7. 2017]. Dostupné z: https://cs.wikipedia.org/wiki/Kensington_Security_Slot

*zredukovalo krádeže notebooků. Nasazení těchto systémů je však individuální záležitostí a dává smysl v určitých konkrétních případech.*

### 5.4.2 Ochrana před rozebráním a úpravou počítačových systémů

**Ochrana serverů**
V případě serverů je ochrana před jejich rozebráním a úpravou relativně jednoduchá, neboť vlastní servery jsou obvykle schopné detekovat a případně i oznámit (automaticky či s pomocí nástroje pro správu), že došlo k otevření serveru. Umístění serverů v místnosti s řízeným přístupem (ideálně vybavené kamerovým systémem) a v zamčeném racku je také možné efektivněji zajistit jejich ochranu před neoprávněnou manipulací s nimi.

**Ochrana ostatních počítačových systémů**
Výrazně složitější je situace v případě ochrany před rozebráním a úpravou u „běžných" počítačových systémů, jako jsou notebooky, desktopy a tiskárny. Tato zařízení se zpravidla nenachází v permanentně zabezpečeném prostoru.

V případě desktopů je možné zakoupit počítačovou skříň s možností uzamčení bočnice či je dnes možné využít možnosti uzamčení pevného disku v BIOSu.[464] Útočník tak sice může pevný disk vymontovat a odnést, ale bez znalosti hesla se k datům nedostane. Další možností je používat šifrování disků.[465]

Z hlediska zajištění kybernetické bezpečnosti jednotlivých počítačových systémů koncových uživatelů a zejména ochrany dat v nich uložených je vhodné nastavit uzamčení pevného disku či jeho šifrování.

Samozřejmostí je, že i samotný přístup do BIOSu (resp. nastavení BIOS) bude chráněn heslem. V případě tiskáren jsou si jejich výrobci vědomi, že tiskové úlohy uložené na pevném disku v tiskárně mohou obsahovat citlivá data, a proto nabízejí tiskárny umožňující šifrování těchto dat. Avšak aby toto opatření splnilo očekávání, je třeba v nastavení tiskárny také změnit výchozí heslo pro šifrování dat.

Z pohledu fyzické bezpečnosti je ještě vhodné explicitně zmínit zařízení, která umožňují odposlech všech dat, která uživatel předává počítačovému systému prostřednictvím klávesnice. Existují různé varianty těchto zařízení využívající vstupy PS2 a USB. Zařízení se zapojí do počítačového systému jako mezikus a v případě, že uživatel fyzicky nekontroluje počítačový

464: Basic Input-Output System. Blíže viz např. *BIOS*. [online]. [cit. 6. 7. 2017]. Dostupné z: https://cs.wikipedia.org/wiki/BIOS

465: Blíže viz kap. 6.5 Paměťová média

systém, je toto zařízení běžnými prostředky neidentifikovatelné. Tato zařízení mohou data ukládat lokálně či je mohou odesílat skrze počítačovou síť. Kromě toho existují také zařízení umožňující sledovat provoz na RS-232, DVI, HDMI, VGA, thunderbolt aj. kabelech.

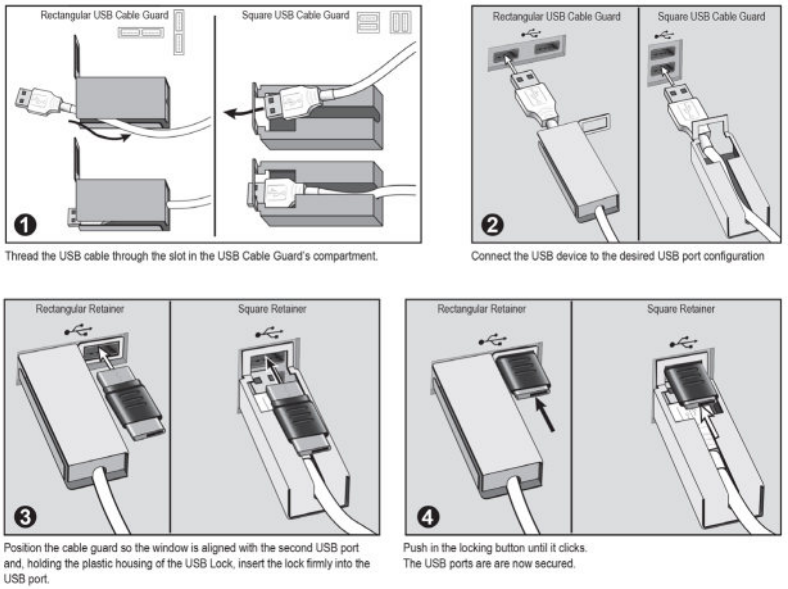

Obrázek 44: Key Grabber[466]

Možnosti ochrany proti tomuto druhu zařízení jsou dnes poměrně malé.

U serverů a dalších významných počítačových systémů je to další z důvodů pro jejich umístění do míst k tomu určených.

U běžných desktopů a notebooků je však na uživateli, aby provedl fyzickou kontrolu, zda mezi jeho klávesnicí a počítačovým systémem není přidáno nové zařízení. Další možností je využívat USB Port Lock with Rectangular Cable Guard od společnosti Kensington. Toto zařízení umožňuje mechanickou cestou připevnit USB kabel do portu. Kabel pak není možné vyjmout bez speciálního klíče. Nevýhodou tohoto řešení je využití USB portů pouze k zamčení USB kabelů (na jeden připojený USB kabel jsou využity dva USB sloty).

466: *KeyGrabber Wi-Fi Premium*. [online]. [cit. 6. 7. 2017]. Dostupné z: https://www.keelog.com/wifi_hardware_keylogger.html




Obrázek 45: Princip fungování USB Cable Guard[467]

Útočníci však využívají i hardwarové keyloggery[468], které lze zabudovat přímo do klávesnice. Takováto zařízení pak už není možné objevit ani zběžnou vizuální kontrolou počítačového systému. V tomto případě může pomoci především dobré rozčlenění jednotlivých zón uvnitř firmy tak, aby se k počítačovým systémům nemohla bez dozoru přiblížit nepovolaná osoba.

### 5.4.3 Ochrana před připojením cizích periferií k počítačovým systémům

Pokud v současnosti hovoříme o připojení cizích periférií, obvykle máme na mysli různá USB zařízení. Dnes lze již pořídit celou řadu zařízení umožňujících útok na počítačový systém, která jsou přímo za tímto účelem vyráběna. **Útok tak může provést i průměrně schopný uživatel.**

Část těchto zařízení zneužívá protokol HID (Human Interface Device), který byl vytvořen kvůli usnadnění vývoje zařízení fungujících jako vstupně výstupní zařízení pro počítačový systém

467: *USB Port Lock with Rectangular Cable Guard.* [cit. 7. 7. 2017]. Dostupné z: https://accoblobstorageus.blob.core.windows.net/literature/1378.pdf

468: Blíže viz KOLOUCH, Jan. *CyberCrime.* Praha: CZ.NIC, 2016, s. 210

a také k usnadnění procesu instalace těchto zařízení. Typickými představiteli těchto zařízení jsou periferní zařízení (např. myši a klávesnice).

Po připojení zařízení k hostitelskému počítačovému systému je z ROM paměti zařízení načten HID descriptor, který obsahuje informace reprezentované daty přenášenými ze zařízení. Díky tomu všechny běžné moderní operační systémy dokáží pracovat s USB HID zařízeními bez nutnosti instalovat speciální ovladače.

Tato vlastnost protokolu HID však může být také snadno zneužita. Představme si situaci, kdy do USB portu připojíte jednoduchý jednočipový počítač, který odešle svůj vlastní HID deskriptor, díky němuž bude toto zařízení považováno hostitelským PC za klávesnici.

Jednočipový počítač pak může být naprogramován tak, aby do hostitelského počítačového systému odeslal po připojení sérii příkazů, které například vypnou firewall v OS Windows. Protože HID je podporován všemi moderními operačními systémy, je tento útok multiplatformní a jeho následky závisí na možnostech ovládání daného operačního systému pomocí příkazů (od nástupu power shellu se tedy tento útok významně dotýká i systému Windows) a na oprávněních aktuálně přihlášeného uživatele.

Pro představu, jak uvedené cizí periferie fungují, uvádíme následující příklady možných útoků.

Prvním z nich je **USB Rubber Ducky**, který lze pořídit za cenu kolem 45 USD. Jeho výhodou je především jednoduchý skriptovací jazyk, se kterým lze vytvářet vlastní payloady, dále pak možnost rozšířit paměť pomocí micro SD karty a podpora komunity. Toto zařízení je přímo určené k penetračnímu testování a hackingu.

Obrázek 46: USB Rubber Ducky[469]

469: *USB Rubber Ducky.* [online]. [cit. 9. 7. 2017]. Dostupné z: https://hakshop.com/products/usb-rubber-ducky-deluxe

Dalším zařízením, které je pro tyto účely používáno, je **jednočipový počítač Teensy**. Pro programování Teensy je dostupné Teensyduino IDE, které je rozšířením pro klasické Arduino IDE. Teensy je také kompatibilní s většinou knihoven pro Arduino.

Pro nováčky, kteří by si chtěli Teensy vyzkoušet pro penetrační testování, vytvořil známý hacker a penetrační tester Nikhil Mittal software Kautylia. S jeho pomocí lze generovat celou řadu kódů, které dokáží například získat uložená hesla k bezdrátovým sítím, kopírovat databázi SAM, stáhnout a spustit kód, změnit v systému nastavení DNS serveru, v OS Linux pak lze například otevřít reverzní shell.

Nikhil Mittal používá Teensy při penetračním testování dvěma způsoby. Pokud se mu podaří narušit fyzickou bezpečnost a dostat se nějakým způsobem dovnitř testované společnosti, vloží Teensy do některé periferie, typicky myši, a tu u některého PC ve firmě vymění. Ráno po přihlášení zaměstnance se kód spustí a provede požadovanou akci. Zaměstnanec zjistí, že má nefunkční myš, nicméně ta je mu prostě vyměněna a nikdo ji více nezkoumá.


Obrázek 47: Ukázka kódu otevírajícího reverzní shell vloženého Teensy - zde je vše záměrně dobře viditelné

Druhým způsobem je pak vložení Teensy do nějakého lákavého zařízení, které je následně zanecháno na místě, kde je předpoklad, že bude nalezeno někým ze zaměstnanců společnosti. Útočník tak spoléhá na lidský faktor a „touhu vyzkoušet nově nalezenou hračku“. Aby nic nevzbudilo podezření uživatelů, otevřené okno, do kterého Teensy odesílá příkazy, může být velmi malé a nadepsané slovy *„installing drivers“*.

Jiným příkladem útoku využívajícího USB portu je **emulace Ethernetu přes USB**. Pokud je zařízení s „USB-to-Ethernet“ adaptérem připojeno, dokonce i do počítačového systému, který je uživatelem uzamčen, počítačový systém odešle DHCP request. Zařízení pak může vrátit

DHCP odpověď upravenou tak, aby napadený počítačový systém věděl, že na LAN[470] síti zařízení připojeného do USB se nachází celý IPv4 rozsah, tedy 0.0.0.0 – 255.255.255.0.

To by za normálních okolností nevadilo, protože nové LAN připojení má menší prioritu, než primární LAN. Nicméně provoz na lokální síti má prioritu před internetovým provozem. A protože napadený počítačový systém byl právě „přesvědčen", že nová LAN obsahuje všechny známé IPv4 adresy, bude další komunikace směrovat k zařízení útočníka.

Výše popsaný útok je v současnosti již zcela automatizovaný a využívá Raspberry Pi Zero (lze využít i Raspberry Pi - verze 1,2 i 3). Samotný software nazvaný PoisonTap, který tato zařízení promění v nebezpečný nástroj, lze stáhnout na githubu. S jeho pomocí lze pak provést několik útoků.

Obrázek 48: Poison Tap[471]

Z napadeného počítače je možné například získat cookies. Pokud totiž v počítači běží prohlížeč s otevřenými stránkami, stačí, pokud tyto stránky odešlou jakýkoliv požadavek. Ten je následně pomocí manipulace s DNS nasměrován na zařízení s PoisonTap a na něm běžící HTTP server získá cookies uživatele. Připojené zařízení lze zneužít i k dalším útokům.

470: **LAN** (**L**ocal **A**rea **N**etwork – lokální počítačová síť. Dále jen **LAN**). Pojem LAN je využíván pro označení lokální či místní sítě, což je síť, v rámci které dochází k propojení uzlů v rámci jedné či více budov. Nezáleží na způsobu propojení jednotlivých uzlů. Toto propojení může být realizováno metalickými, optickými či bezdrátovými sítěmi. Tato síť mívá typicky vyšší přenosovou rychlost a menší vzdálenost mezi jednotlivými uzly. Lokální sítí může být např. kompletní síť (subsítě) univerzity, organizace, ale zároveň se může jednat o malou síť, která je vybudována v rámci domácnosti (například jde o propojení více počítačových systémů: počítače, tiskárny, Smart TV, datové úložiště aj. přes switch či router).

471: *PoisonTap.* [online]. [cit. 11. 7. 2017]. Dostupné z: https://samy.pl/poisontap/

Volné USB porty mohou být také neoprávněně využity samotným uživatelem počítačového systému. Jedním z rizik může být zavlečení malware[472] do počítačové sítě přes přenosné paměťové médium, či krádež dat, která si zaměstnanec zkopíruje na toto médium.

Výše popsané způsoby útoků na počítačové systémy prostřednictvím USB portů nelze podceňovat a je třeba je v rámci kybernetické bezpečnosti řešit. Existuje celá řada více či méně praktických řešení ochrany USB portů. Jejich výběr záleží na situaci a potřebách organizace. Přístup k USB portům lze blokovat fyzicky, například s již zmiňovaným zařízením USB Port Lock. Další, ne zcela praktickou možností, je vypnout USB porty na úrovni BIOSu, případně pracovat s USB porty na úrovni operačního systému.

V prostředí MS Windows lze řídit přístup k USB portům pomocí skupinových politik. Ty umožňují zakázat uživatelům selektivně instalaci určitých zařízení do USB, jako jsou právě třeba přenosná paměťová média. Obráceně lze také využít tyto politiky k whitelistování seznamu určitých konkrétních zařízení, která lze k počítačovému systému připojit, a všechna ostatní zařízení lze zakázat.

V OS Linux lze k blacklistování[473] a whitelistování využít UDEV rules.[474] K jejich použití je třeba znát identifikátor výrobce (idVendor) a identifikátor produktu (idProduct). Následně je možné za pomoci skriptů tato zařízení povolit či zakázat.

Blacklistování či whitelistování podle identifikátorů zařízení však nezaručuje stoprocentní ochranu počítačového systému.

Pokud by se útočníkovi podařilo zjistit identifikátor whitelistovaného zařízení, může například u zařízení Teensy tento identifikátor zapsat do souboru `usb_desc.h`.

472: KOLOUCH, Jan. *CyberCrime.* Praha: CZ.NIC, 2016, s. 204–221

473: Blacklisting představuje seznam využívaný počítačovým systémem definující zakázané prvky (např. síťovou komunikaci, e-mailové adresy aj.)

474: UDEV nahrazuje Device File System v OS Linux. Umožňuje identifikovat počítačové systémy, paměťová média aj. na základě jejich vlastností.

## 6 Bezpečnost sítí a služeb

Následující kapitola se věnuje mnoha různým aspektům kybernetické bezpečnosti, počínaje rozdělením sítí, přes ochranu proti nejčastějším útokům na síťové vrstvě, ochranu na rozhraní sítí, až po doporučení, jak se vypořádat s nastalým incidentem.

V jednotlivých subkapitolách budou popsány jak některé známé útoky a zranitelnosti, tak i doporučení, jak se lze proti nim bránit. Na tomto místě je vhodné připomenout, že bezpečnost je otázkou více vrstev a jednotlivá opatření je nutno zvažovat v kontextu celého chráněného systému i v kontextu ostatních bezpečnostních opatření.

Ve vztahu k bezpečnosti je také důležité si uvědomit vlastní díl odpovědnosti za bezpečnost sítí a počítačových systémů připojených do Internetu. V praxi se bohužel lze setkat se správci ICT či organizacemi dbajícími pouze o zabezpečení systémů, které jsou pro ně z jejich pohledu důležité (klíčové), přičemž opomíjí další ICT systémy, které mají ve své správě.

**Příklad:** *Organizace provozuje CCTV kamery bez jejich dostatečného zabezpečení. Vlastní kamery nejsou po instalaci spravovány, jsou volně dostupné přes Internet atd. Tyto kamery se pak podílely na DDoS útocích na jinou síť v Internetu. Vlastní zneužití kamer k DDoS útokům organizaci, která je provozuje, nezajímá.*

Při implementaci bezpečnostních prvků vlastní sítě či počítačových systémů bychom neměli myslet pouze na bezpečnost našich systémů a dat, ale také na bezpečnost systémů a dat jiných osob, jakož i na bezpečnost celého Internetu.

**Příklad:** *Provozovat lokální rekurzivní DNS server pro vlastní zaměstnance dává smysl; nechat jej dostupný pro všechny, tak aby mohl být zneužíván k amplifikačním útokům, je naopak zcela zbytečné.*

### 6.1 Ochrana sítí

Zajištění bezpečnosti počítačových sítí je jedním ze základních prvků, na kterých je vybudována kybernetická bezpečnost. Bez účinné ochrany počítačových sítí není možné efektivně zajistit ochranu počítačových systémů a dat v nich uložených.

Výjimku z tohoto tvrzení samozřejmě představují zcela izolované počítačové systémy, jež nejsou úmyslně zapojeny do počítačové sítě.

### 6.1.1 Rozdělení sítě jako základní prvek zajištění bezpečnosti

Správné rozdělení počítačové sítě je z pohledu kybernetické bezpečnosti velmi důležité a jedná se o základní prvek bezpečnosti v případě jejich správy.

Při rozdělování počítačové sítě je vhodné zaměřit se na:

- **oddělení systémů se zvýšeným rizikem kompromitace od zbytku sítě**,
  V tomto případě využíváme **demilitarizované zóny (DMZ)**.[475]
- **potřebu rozdělení provozu v síti.**
  Je vhodné oddělit provoz např. jednotlivých oddělení, informačních systémů aj. Dále je vhodné oddělit provoz přicházející z veřejné Wi-Fi sítě určené např. pro návštěvy od ostatního síťového provozu.
  V případě rozdělování provozu sítě si obvykle vystačíme s logickým rozdělením sítě pomocí **Virtuální LAN (VLAN)**.[476]

#### 6.1.1.1 DMZ

Demilitarizovaná zóna tvoří většinou samostatnou fyzickou síť, která je oddělena od ostatních počítačových systémů.

Obvykle jsou v DMZ umístěny servery, na kterých jsou provozované služby, které mají být dostupné uživatelům z jiných sítí. Může se jednat například o webový server, mail server, ftp server a další. Smyslem DMZ je ochránit lokální síť v případě, kdy se útočníkovi podaří kompromitovat některý z veřejně dostupných serverů. Demilitarizovaná zóna se zpravidla implementuje pomocí firewallu, který oddělí jednotlivé sítě WAN[477], DMZ a LAN.

Pro vytvoření DMZ lze také využít i virtuální sítě. Na tento přístup však neexistuje v bezpečnostní komunitě jednoznačný názor. To, zda preferovat dražší, fyzicky realizovanou DMZ, nebo ji „emulovat" s pomocí VLAN, je otázkou dostupných finančních prostředků i zkušeností administrátorů.

475: Dále jen **DMZ**

476: Dále jen **VLAN**.

477: **WAN** (**W**ide **A**rea **N**etwork – vzdálená počítačová síť). Pojem WAN označuje počítačovou síť propojující geograficky vzdálené oblasti. Typicky jsou do sítě WAN propojovány jednotlivé LAN a MAN (**M**etropolitan **A**rea **N**etwork – metropolitní síť) sítě. Z geografického hlediska je možné definovat WAN sítě jako sítě s rozsahem například v teritoriu státu, kontinentu, i jako sítě celosvětové.

Pravdou je, že i pokud útočník nedokáže opustit VLAN vyhrazenou pro server, na který se mu podařilo proniknout, může se stále pokusit provést například DoS útok a vyřazením switche vyřadit celou lokální síť. Ti, kdo se bezpečnosti věnují, se proto spíše přiklánějí k realizaci DMZ s pomocí fyzicky odděleného hardware, než k využití VLAN.

V případě, že není možné DMZ realizovat na fyzické úrovni (např. z důvodu finančních úspor, nedostatku lidských zdrojů aj.), ale s pomocí VLAN, je třeba při jejich konfiguraci pamatovat na všechny potenciální vektory případného útoku.

#### 6.1.1.2 VLAN

**Virtuální LAN umožňuje provést logické rozdělení sítě nezávisle na jejím fyzickém uspořádání.**

**Příklad:** *VLAN může být využita pro IP telefonii v rámci menší organizace. V této organizaci není potřeba oddělovat jednotlivá oddělení do podsítí, nicméně každý zaměstnanec má vlastní IP telefon.*

*Z bezpečnostních i praktických důvodů se doporučuje vytvořit pro IP telefonii vlastní síť. Bylo by však poměrně komplikované po celé budově a na každém patře budovat separátní fyzickou síť.*

*Pomocí VLAN lze tento problém snadno vyřešit a na stejném switchi tak mohou být připojeny jak telefony, tak ostatní zařízení v rámci například jednoho patra budovy. Všechna tato zařízení budou ve dvou samostatných sítích a vzájemně se nebudou schopny detekovat.*

Implementace VLAN má několik výhod spočívajících například v:

- snížení počtu potřebného hardware,
- omezení počtu broadcastů,
- oddělení speciálního provozu,
- zvýšení bezpečnosti,
- jednodušším přesouvání počítačových systémů mezi sítěmi (místo fyzického přepojování datového kabelu stačí překonfigurovat zapojení do jednotlivých VLAN).

Z výše uvedeného vyplývá, že počítačové systémy mohou přímo komunikovat pouze s jinými počítačovými systémy, které jsou ve stejné VLAN. Pro komunikaci počítačových systémů je využíváno klasického routování (provoz z VLAN je vyveden do routeru, který se stará o správné předávání, nebo naopak zahození paketů).

**Příklad:** *Pokud jsou v organizaci dvě oddělení a nechceme, aby tato oddělení měla přístup k počítačovým systémům umístěným v síti druhého oddělení, a zároveň je v organizaci DMZ, ve které jsou umístěny*

*servery, se kterými tato dvě oddělení potřebují komunikovat, je vhodným řešením oddělit tato dvě oddělení pomocí VLAN, přivést provoz do routeru a v něm povolit pouze komunikaci jednotlivých VLAN s DMZ, ve které jsou umístěny společné servery.*

Krom oddělení provozu z veřejné Wi-Fi, oddělení sítě pro IP telefonii či správu serverů, existují i další důvody pro implementaci VLAN v organizaci.

**Příklad:** *Praktickým důvodem může být omezení přístupu k internetovým službám na základě oddělení. Řekněme, že v organizaci existuje oddělení technické podpory, které řeší širokou škálu technických dotazů. U tohoto oddělení nelze předem definovat, na jaké porty serverů v Internetu se bude potřebovat připojit. Pro toto oddělení je vhodné vytvořit separátní VLAN, ze které bude povolena jakákoliv odchozí komunikace, zatímco zbytku organizace je možné omezit odchozí komunikaci pouze na porty, které pro svou práci běžní uživatelé potřebují.*

Samotné zařazení počítačového systému do VLAN může být provedeno podle portu switche, podle MAC adresy počítačového systému, podle protokolu a podle autentizace za pomoci 802.1x. Poslední variantu lze považovat za velice bezpečnou, pokud nedojde ke kompromitaci uživatelského přihlášení.

V souvislosti s VLAN je potřeba také zmínit **trunk port**. Pokud je VLAN používána pouze v rámci jednoho switche, bude si switch udržovat přehled o tom, na kterém portu je která VLAN vytvořena. Jiná situace nastane, pokud je v rámci počítačové sítě propojeno více switchů a má mezi nimi dojít k přenosu dat patřících do určité VLAN.

Jako trunk port je označován právě port sloužící k předávání dat jinému switchi či jinému zařízení. Trunk port k rámcům opouštějícím switch přidává tag, podle kterého následující zařízení pozná, do které VLAN data patří.

Pro úplnost dodejme, že existuje ještě jeden typ portu, kterým je port hybridní. Ten může mít přiřazeno více taggovaných i netaggovaných VLAN a typicky se používá pro IP telefonii, nebo obecně k připojení počítačových systémů, které po startu neznají konfiguraci VLAN a potřebné informace získají až z počítačové sítě z jiného počítačového systému.

**Útoky na VLAN**
Existuje několik útoků, ve kterých se útočník může snažit o proniknutí z jedné VLAN do druhé. Může se jednat například o:

- **VLAN hopping**,
- **Double tagging**,
- **Spanning Tree attack**,
- **VLAN Trunking Protocol attack**,

- **VMPS/VQP attack** aj.

**Bližší informace o jednotlivých útocích, obraně a nápravných krocích je možné nalézt na: https://kyberbezpecnost.csirt.cz/**

### 6.1.2 Ochrana sítě LAN

Koncept lokálních sítí je závislý na řadě mechanismů, které jsou zranitelné již samy o sobě. Především mechanismy pro získání MAC adres ostatních počítačových systémů v síti (ARP protokol), pro získání IP adresy a dalších důležitých síťových nastavení (DHCP protokol), nebo pro získání informací o IP adrese určitého hostitele (DNS protokol), dokázaly v minulosti potrápit nejednoho administrátora. V této části publikace se proto primárně zaměříme na možné útoky na tyto protokoly a na ochranu proti nim, jakož i na některé bezpečnostní mechanismy. Opomenuta nebude ani problematika bezpečnosti IPv6 a bezdrátových sítí.

#### 6.1.2.1 DHCP protokol

**Příklad:** *Traduje se historka o ISP* [478]*, který byl de facto ihned po vybudování své první sítě v Praze nucen řešit „kybernetický útok". Na hotline tohoto ISP se začalo obracet velké množství jeho zákazníků s tím, že jim jde Internet tak pomalu, že v podstatě nejde vůbec.*

*K vlastnímu incidentu došlo v době, kdy SOHO routery* [479]*, jak je známe dnes, v podstatě neexistovaly a kdo chtěl mít doma připojen více než jeden počítač, musel si sám postavit na nějakém starém počítači router a přes něj pak připojit svou privátní síť k Internetu.*

*Právě to, jak se později ukázalo, bylo příčinou výpadku u jmenovaného ISP. Jeden z jeho zákazníků si postavil takovýto router na OS Linux, ale popletl konfiguraci DHCP a začal všem zákazníkům onoho ISP přidělovat svou veřejnou IP adresu jako výchozí bránu. Všechny počítače v dané síti pak následně začaly posílat svá data přes jeho router.*

478: V tomto případě se jednalo o poskytovatele služby, jež spočívá v přenosu informací poskytnutých uživatelem prostřednictvím sítí elektronických komunikací nebo ve zprostředkování přístupu k sítím elektronických komunikací za účelem přenosu informací (viz § 3 odst. 1 ZSIS).
K vlastnímu pojmu ISP, právům a povinnostem jednotlivých ISP viz blíže např. KOLOUCH, Jan. *CyberCrime.* Praha: CZ.NIC, 2016, s. 78 a násl. a s. 109 a násl.

479: **SOHO router** představuje počítačový systém (router) schopný routovat provoz v domácnostech a menších organizacích.

Je možné samozřejmě polemizovat nad tím, do jaké míry je tato historka pravdivá, avšak výše popsaný děj odpovídá útoku známému jako **Rogue DHCP**.

V rámci tohoto útoku si útočník v síti LAN, která je pod správou napadené osoby, spustí vlastní DHCP server a přiděluje počítačovým systémům v této síti vlastní gateway pro přístup do Internetu. Tím docílí toho, že jsou všechna data posílána přes jím ovládaný počítačový systém a útočník tak může tato data a informace získat a zneužít (samozřejmě za předpokladu, že tyto nejsou spolehlivým způsobem šifrovány).

Rogue DHCP je možné rozpoznat pomocí signatur v IDS (Intrusion Detection System), ale i pokud IDS není v počítačové síti provozováno, lze tomuto útoku obvykle předejít i správnou konfigurací síťového prostředí.

Například u switchů Cisco či Juniper je možné zapnout funkci DHCP snooping. Jako správce si určíme takzvané důvěryhodné (trusted) porty, těmi budou porty, do kterých je připojen DHCP server, a porty, kterými jsou propojeny switche. Výhodou je, že při zapnutí této funkce je zároveň vytvářena databáze DHCP Snooping Binding Database, která obsahuje informace o přidělených IP adresách zároveň s MAC, VLAN, dobou pronájmu a informací o portu.

```
RACCSW01#sh ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
90:18:7C:9A:A4:3E   192.168.2.51     674237      dhcp-snooping   20    FastEthernet0/19
F0:25:B7:14:90:B9   192.168.2.39     599277      dhcp-snooping   20    FastEthernet0/19
EC:1F:72:09:E8:6C   192.168.2.63     685604      dhcp-snooping   20    FastEthernet0/19
B0:D0:9C:38:0B:A3   192.168.2.37     683249      dhcp-snooping   20    FastEthernet0/19
24:0A:64:CE:AB:1B   192.168.2.5      689285      dhcp-snooping   20    FastEthernet0/11
30:CD:A7:20:A6:D9   192.168.2.20     520484      dhcp-snooping   20    FastEthernet0/19
34:E6:AD:5A:36:74   192.168.2.21     457304      dhcp-snooping   20    FastEthernet0/11
F0:25:B7:EE:70:26   192.168.2.58     686082      dhcp-snooping   20    FastEthernet0/19
00:13:20:6C:50:E2   192.168.2.47     655844      dhcp-snooping   20    FastEthernet0/4
Total number of bindings: 9

RACCSW01#
```

Obrázek 49: DHCP Snooping Binding Database[480]

Dalším z možných útoků na DHCP je útok **DHCP Starvation**, který spočívá ve vyčerpání dostupných IP adres. Útočník pouze vhodným nástrojem generuje do sítě velké množství DHCP požadavků z podvržených MAC adres a tak vyčerpá administrátorem definovaný rozsah IP adres.

S útokem DHCP starvation se mohla setkat většina z čtenářů, pokud se někdy připojila do nevhodně nakonfigurované sítě.

480: *DHCP Snooping Binding Database.* [online]. [cit. 14. 7. 2017]. Dostupné z: http://www.write-mem.net/?q=dhcp-snoop-dai-ip-src-grd

**Příklad:** *Autorovi této publikace se například na dovolené stalo to, že pravidelně přestávala fungovat veřejně přístupná bezdrátová síť určená pro hosty hotelu. Síť byla viditelná, došlo k inicializaci spojení, avšak nedošlo k přidělení IP adresy koncovému počítači. Po restartu routeru bylo vše zase na krátký čas v pořádku a připojení fungovalo bezchybně. Jak se později ukázalo, problém byl v tom, že technik společnosti, která router pro hotel spravovala, nastavil omylem příliš malý rozsah IP adres a zařízení hostů je vždy velmi rychle vyčerpala. I když se v tomto případě nejednalo ze strany hotelových hostů o úmysl, důsledky byly stejné, jako v případě útoku DHCP Starvation.*

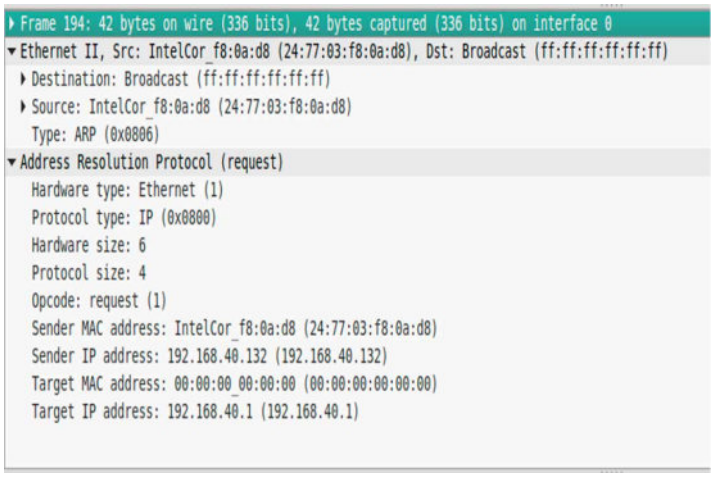
Proti DHCP Starvation útoku se je možné například bránit tak, že bude omezeno množství MAC adres, které se mohou nacházet za jedním portem switche. Pokud zapnete funkci Port Security, můžete buď pouze omezit počet možných MAC adres na portu a jejich definování nechat na automatice, nebo lze dokonce vymezit konkrétní MAC adresy, které jediné mohou být k portu připojené. Rámce s jinou než definovanou MAC adresou pak budou switchem automaticky zahozeny, nebo dojde k úplnému vypnutí portu až do zásahu administrátora.

#### 6.1.2.2 ARP protokol

Protokol ARP slouží v TCP/IP k získání linkové (ethernet) adresy síťového rozhraní cílového počítačového systému ve stejné podsíti pomocí známé IP adresy.

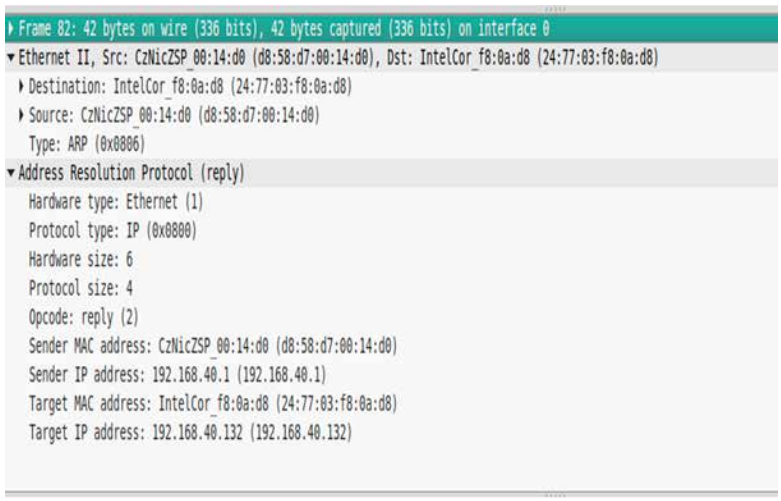
V případě, že chce počítačový systém odeslat jinému systému ve stejné počítačové síti data, musí krom cílové IP adresy znát i cílovou ethernetovou adresu. Z tohoto důvodu je odeslán ARP dotaz, který obsahuje hledanou IP adresu a údaje o odesílajícím počítačovém systému, tedy vlastní IP adresu a MAC adresu.

Protože však odesílající počítačový systém zatím nezná MAC adresu cílového počítačového systému, pošle dotaz linkovým broadcastem na MAC adresu, která je společná všem účastníkům dané lokální sítě (u Ethernetu se jedná o adresu ff:ff:ff:ff:ff:ff).




Obrázek 50: Paket ARP protokolu zachycený programem Wireshark

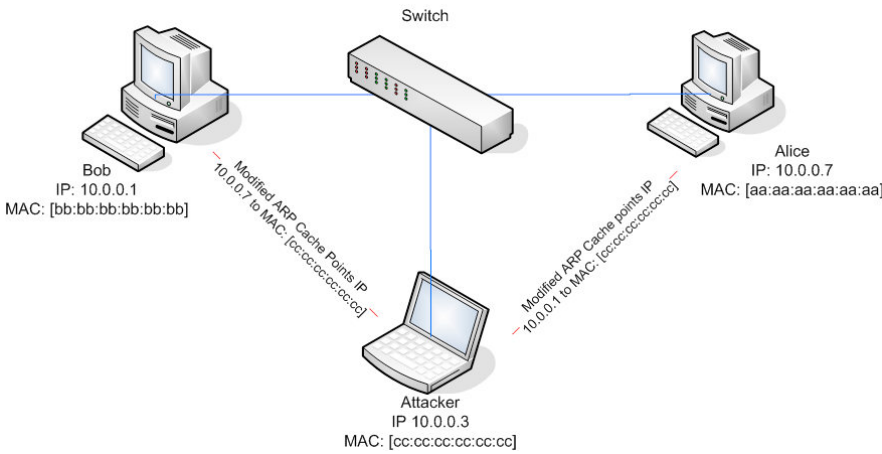
Na obrázku 50 je třeba věnovat pozornost položce **Destination** a **Target MAC address**. Protože byl paket odeslán na adresu Broadcastu, vyzvednou si jej síťová rozhraní všech zařízení v dané lokální síti. Avšak pouze držitel hledané IP adresy odpoví původnímu tazateli zprávou, ve které bude informace o jeho IP adrese a MAC adrese. Tuto informaci si dotazující se počítačový systém zanese do své ARP Cache.




Obrázek 51: Standardní odpověď na ARP request

Problém s ARP protokolem je ten, že se nijak nehlídá, zda byl požadavek opravdu odeslán, jinými slovy, je akceptována a do ARP Cache zapsána i odpověď, na kterou se nikdo neptal. Útočník tak může snadno generovat vlastní ARP odpovědi, ve kterých bude cílovému počítačovému systému tvrdit, že určitá IP adresa v síti, typicky gateway, má jeho, tedy útočníkovu MAC adresu.

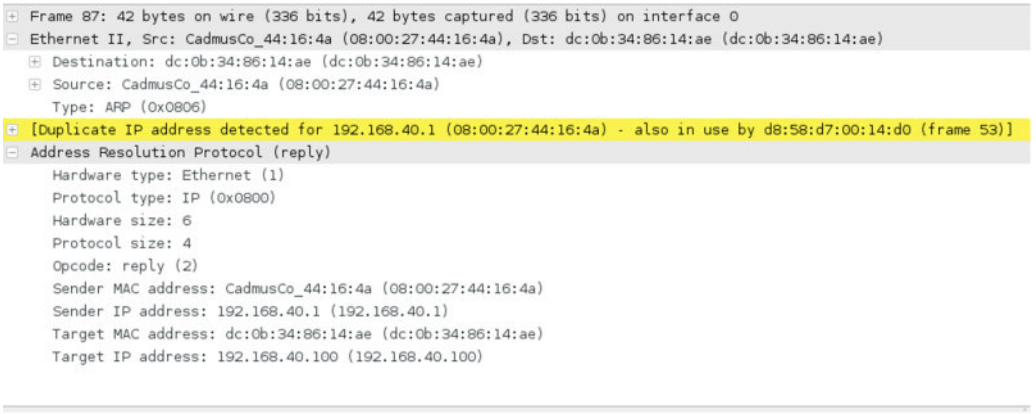
Na obrázku 52 je demonstrován útok **ARP Cache Poisoning**, v rámci kterého útočník posílá Bobovi podvržené ARP odpovědi, ve kterých tvrdí, že počítačový systém Alice, tedy IP 10.0.0.7 má MAC adresu útočníka cc:cc:cc:cc:cc:cc. Zároveň posílá počítačovému systému Alice ARP odpovědi, ve kterých tvrdí, že IP adresa Boba (10.0.0.1) má MAC adresu útočníka cc:cc:cc:cc:cc:cc. Pokud tedy chce Bob komunikovat s Alicí, jeho počítač převezme data, přidá k nim správnou cílovou IP adresu 10.0.0.7, avšak špatnou MAC adresu cc:cc:cc:cc:cc:cc. Když rámec dorazí na switch, ten zkontroluje, pro koho jsou data určena a na základě MAC adresy cc:cc:cc:cc:cc:cc, pošle data na port, kde je připojen počítačový systém útočníka. Útočník data přijme a následně je opatří již správnou MAC adresou a pošle je dál. K Alici tak data skutečně dorazí, jen si je cestou může prohlédnout útočník. Pokud Alice pošle nějaká data Bobovi, situace se opakuje a data jsou opět nejprve odeslána útočníkovi. Z pohledu většiny útočníků bude asi nejzajímavější situace, pokud na místě Alice bude gateway, nebo server s pro útočníka zajímavými daty.




Obrázek 52: ARP Cache Poisoning[481]

481: *ARP Cache Poisoning*. [online]. [cit. 15. 7. 2017]. Dostupné z: https://tournasdimitrios1.wordpress.com/2011/02/08/4426/

Existuje celá řada programů, které lze pro provedení útoku ARP Cache Poisoning využít, namátkou jmenujme programy ***Cain&Abel***, ***Ettercap*** nebo ***arpspoof.*** Některé z těchto programů se i automaticky postarají o předávání paketů do správné destinace, u některých je třeba zapnout předávání paketů v operačním systému (pokud by to útočník neudělal, vyvolal by pouze DoS, kdy by oba počítačové systémy nebyly schopny spolu komunikovat, protože by jejich pakety končily u útočníka, jehož počítačový systém by je ale již dále neodesílal).




Obrázek 53: ARP Cache poisoning zachycený programem Wireshark. Ten umí na případnou duplikaci MAC adres upozornit.

ARP Cache poisoning představuje útok man-in-the-middle (MITM), neboť útočník stojí uprostřed mezi oběma počítačovými systémy. V rámci tohoto útoku se však útočník nemusí omezovat pouze na čtení dat, ale může do nich i aktivně zasahovat, například vkládat do webových stránek vlastní skripty a v případě šifrované komunikace se může pokusit o její narušení.

Ochranu proti ARP Cache poisoning útoku lze rozdělit do dvou částí:

- **ochranu koncových počítačových systémů,**
- **ochranu na úrovni sítě.**

Pokud tedy uživatelé používají přenosné počítačové systémy a organizace chce mít jistotu, že se tito uživatelé nestanou cílem ARP Cache poisoning útoku mimo počítačovou síť organizace, je možné využít některého ze softwarů, který dokáže detekovat ARP spoofing. Jedním z takovýchto nástrojů, který lze nasadit přímo do počítačového systému, je ***XArp***. Detekovat ARP spoofing na úrovni koncového počítačového systému umí ale i některá antivirová řešení.

Pokud jde o ochranu na úrovni počítačové sítě, lze pro detekci pokusů o ARP Cache poisoning využít program ***ARPWatch***, či ochranu na úrovni síťových prvků. ***Dynamic ARP Inspection*** je bezpečnostní funkce síťových prvků, která využívá databázi DHCP Snooping Binding Database.[482]

Dynamic ARP Inspection porovnává informace z hlaviček rámců, které přicházejí na určitém portu vůči informacím z této databáze. Pokud se kombinace zdrojová IP adresa a zdrojová MAC adresa shodují, bude rámec propuštěn, v opačném případě bude zahozen.

Switch, na kterém je spuštěno Dynamic ARP Inspection, provádí také zároveň rate limiting ARP paketů kvůli ochraně před DoS útoky. V případě, že po zapnutí funkce Dynamic ARP Inspection dochází k zahazování ARP paketů, je potřeba změnit výchozí hodnotu tohoto limitu. Vedle ARP Chache Poisoningu se lze setkat s dalším útokem, při kterém útočník získá přístup k datům počítačových systémů připojených do jiného portu switche. Vlastní útok spočívá v přepnutí switche do stavu, ve kterém se bude chovat jako hub. Po tomto přepnutí nebudou posílána data pouze na port, za kterým se nachází cílová MAC adresa, ale budou poslána na všechny porty, s výjimkou toho, ze kterého rámec přišel. Toho může útočník dosáhnout útokem známým jako **MAC flooding**.

Cílem tohoto útoku je zaplnit vnitřní tabulku switche, do které si switch ukládá právě informaci o tom, za kterým portem switche se nachází konkrétní MAC adresy. Cílem útočníka je dosáhnout, aby switch začal pro MAC adresy, které se již nevejdou do jeho paměti, fungovat jako HUB, tedy aby příchozí rámce přeposílal na všechny porty. Existuje více způsobů, jak se s tímto rizikem vypořádat, z těch již dříve zmiňovaných připomeňme funkci port security, která omezí množství MAC adres, které mohou být za jedním portem. Útočník tak nemůže zaplnit paměť switche záplavou nesmyslných záznamů.

### 6.1.2.3 DNS

Při napadení DNS[483] je obvykle cílem útočníka přesměrovat oběti na jeho vlastní verzi webových stránek. Pro tyto útoky se používá souhrnné označení pharming.

V případě útoků na systém DNS se lze typicky setkat s:

1) **DNS Cache Poisoning**
   V podstatě se jedná o útok, při kterém útočník do dočasné paměti DNS serveru umístí falešnou informaci o doméně. Může tak například pozměnit IP adresu, kterou server vrací

482: Blíže viz kap. 6.1.2.1 DHCP protokol

483: Domain Name System - hierarchický systém doménových jmen.

pro stránku internetového bankovnictví, a přesměrovat tak všechny uživatele, kteří DNS server používají, na svou vlastní webovou stránku. Díky zlepšení bezpečnosti v implementaci DNS serverů a zavedení technologie DNSSEC[484] se dnes už s tímto útokem na systém DNS nepotkáváme.

Je však vhodné tento útok zmínit, neboť k němu může dojít například na úrovni lokálního počítačového systému, případně může být napaden SOHO router menších organizací či poboček organizací.

2) **Útoky malware**
Na úrovni lokálního počítačového systému stanice je příčinou napadení DNS zpravidla škodlivý kód (malware[485]). Malware může buď pozměnit nastavení DNS serverů, kterých se bude koncový počítačový systém dotazovat, nebo zasáhnout do souboru hosts. Změnou nastavení DNS serverů proslul malware **DNSChanger**. Ten existoval jak ve variantě pro OS Windows, tak i Mac OS X. Po infikování počítačového systému změnil nastavení DNS na vlastní servery ovládané útočníkem.

Příkladem malware, který mění obsah souboru hosts, byl **Trojan.Qhost**, který do uvedeného souboru vkládal falešné informace pro domény patřící antivirovým společnostem. Cílem útoku bylo neumožnit antivirovým programům provést update.

Ještě dále zašel malware známý jako **Shopperz**. Některé varianty tohoto malware měnily přímo knihovnu `dnsapi.dll` za vlastní verzi. V původní knihovně byla změněna pouze cesta k souboru `hosts`. Díky tomu zůstal originální soubor hosts nedotčen a při jeho případné kontrole tak nebyly změny identifikovány. Tento malware byl svými tvůrci využíván především k injektování vlastní reklamy do webových stránek, proto do souboru `hosts` přidával vlastní záznamy pro domény jako google-analytics.com.

3) **Útoky na SOHO routery**
Útoky na SOHO routery mají podobu komplexního útoku, při němž musí útočník nejprve proniknout do vlastního routeru.

484: **DNSSEC** je rozšíření systému DNS, které zvyšuje bezpečnost služby doménových jmen. Principem DNS je překlad jmenných internetových adres, jako například www.nic.cz nebo www.dobradomena.cz, na adresy číselné, kterým počítače rozumějí a jejichž pomocí dokážou zajistit zobrazování webových stránek, odesílání e-mailů, telefonování po Internetu a další běžné internetové služby. DNSSEC zvyšuje bezpečnost při používání DNS tím, že brání podvržení falešných, pozměněných či neúplných údajů o doménových jménech. Více informací na internetové adrese www.dnssec.cz.

485: Blíže viz KOLOUCH, Jan. *CyberCrime.* Praha: CZ.NIC, 2016, s. 204 a násl.

Útočníci přitom využívají jak špatně zabezpečené routery, které mají dostupné přihlašovací rozhraní a jednoduché či výchozí heslo pro přihlášení, tak také různé zranitelnosti SOHO routerů.

V dalším kroku pak útočník na napadeném routeru změní nastavení DNS tak, aby router navázal komunikaci s útočníkovými DNS servery. S těmi pak může útočník přesměrovat všechny počítačové systémy za napadeným routerem například na vlastní verzi on-line bankovnictví[486], či na falešné verze populárních vyhledávačů.

V jednom ze známých případů byl na těchto útočníkových stránkách nabízen update pro Flashplayer s tvrzením, že bez updatu nebudou stránky správně fungovat. Stažený soubor však místo update Flashplayeru obsahoval bankovního trojského koně.

Při tomto útoku na SOHO routery v České republice byla zneužívána zranitelnost ROM-0[487], která byla řešena i národním bezpečnostním týmem CSIRT.CZ.

Útok na SOHO routery nemusí být nutně veden pouze přes WAN port. Skript známý jako **JS_JITON** umožňuje tento útok provést zevnitř sítě. Stačí, aby uživatel otevřel webovou stránku, která má v sobě tento skript zakomponovaný. Skript se následně zkouší přihlásit k routeru přes LAN rozhraní předdefinovaným seznamem uživatelských jmen a hesel. Pokud dojde k přihlášení k routeru, dojde k upravení nastavení DNS, stejně jako tomu bylo u předchozích útoků.

486: Viz např. *Large-scale DNS redirection on home routers for financial thef*. [online]. [cit. 16. 7. 2017]. Dostupné z: https://www.cert.pl/en/news/single/large-scale-dns-redirection-on-home-routers-for-financial-theft/

487: Viz *Kritická zranitelnost mnoha domácích routerů.* [online]. [cit. 16. 7. 2017]. Dostupné z: https://blog.nic.cz/2014/05/21/kriticka-zranitelnost-mnoha-domacich-routeru/

```
function dns(){
        try{
                var bot = [
                        ["admin","admin"]
//                      ["ADSL","ADSL1234"],
//                      ["SL","SL"],
//                      ["SZIM","SZIM"],
//                      ["admin","0000"],
//                      ["admin","1234"],
//                      ["admin","12345"],
//                      ["admin","123456"],
//                      ["admin","admin"],
//                      ["admin","admin888"],
//                      ["admin","conexant"],
//                      ["admin","dare"],
//                      ["admin","epicrouter"],
//                      ["admin","greennet"],
//                      ["admin","private"],
//                      ["admin","qxcomm1680"],
//                      ["admin","starnetadsl"],
//                      ["admin","utstar"],
//                      ["adsl","adsl1234"],
//                      ["adsl","adsl831"],
//                      ["anonymous","1234"],
//                      ["anonymous","12345"],
//                      ["broadmax","broadmax"],
//                      ["dsl","dsl"],
//                      ["password","password"],
//                      ["putian","123456"],
```

Obrázek 54: Ukázka ze seznamu uživatelských jmen a hesel předdefinovaných ve skritpu JS_JITON[488]

**Bližší informace o útocích na SOHO routery a možnostech jejich nastavení je možné nalézt na: https://kyberbezpecnost.csirt.cz/**

### 6.1.2.4 IEEE 802.1X

V případě lokálních sítí a jejich zabezpečení není možné vynechat protokol IEEE 802.1X, který v sítích typu ethernet umožňuje realizovat řízení přístupu. Pokud se uživatel připojí na síťový port, může komunikovat pouze prostřednictvím EAP protokolu[489], který se stará o autentizaci. Poté koncový počítačový systém odešle pomocí EAP protokolu přihlašovací informace. Každý koncový počítačový systém má za tímto účelem speciální kus softwaru, známý jako suplikant. Počítačový systém, do kterého se uživatel připojil, přepošle přihlašovací údaje na RADIUS server, který uživatele ověří. V případě, že je autentizace úspěšná, je uživatel vpuštěn do počítačové sítě.

488: *The list of log-in IDs and passwords*. [cit. 16.7.2017]. Dostupné z: https://blog.trendmicro.com/trendlabs-security-intelligence/mobile-devices-used-to-execute-dns-malware-against-home-routers/

489: Extensible Authentication Protocol je autentizační protokol zprostředkovávající přenos klíčů.

Na základě přihlašování (autentizace a autorizace) mohou být také uživatelé přidáváni do různých VLAN. Díky tomu je možné mít defaultní VLAN, do které je zařazen neautentizovaný uživatel. V rámci této VLAN získá uživatel přístup pouze k předem nadefinovaným službám, bez možnosti přístupu do vnitřní sítě.

#### 6.1.2.5 Bezdrátové sítě

Bezdrátové sítě přinesly řadu výhod spočívajících například ve snížení nákladů na budování počítačových sítí, větší mobilitu uživatelů, snadnější a rychlejší připojování nových uživatelů aj. Na druhou stranu je využívání bezdrátových sítí spojeno s novými bezpečnostními riziky.

Základní problém bezdrátových sítí představuje relativně nízká schopnost ovlivnit či kontrolovat šíření signálu.[490] To, že není signál Wi-Fi detekovatelný na koncovém počítačovém systému uživatele, ještě nutně nemusí znamenat, že jej ze stejného místa nemůže detekovat útočník vybavený směrovou anténou s velkým ziskem.

Dalším ze základních problémů, který bezprostředně souvisí s provozem bezdrátových sítí Wi-Fi (krom výše uvedené omezené možnosti regulace signálu), je absence ochrany důležité síťové komunikace.

V rámci Wi-Fi sítí nejsou nijak chráněny následující rámce:

- **Control**
  Control rámec se stará například o rezervaci časového pásma RTS (Request-To-Send), potvrzení přijetí rámce ACK (Acknowledgement), nebo o povolení vysílání CTS (Clear-To-Send).

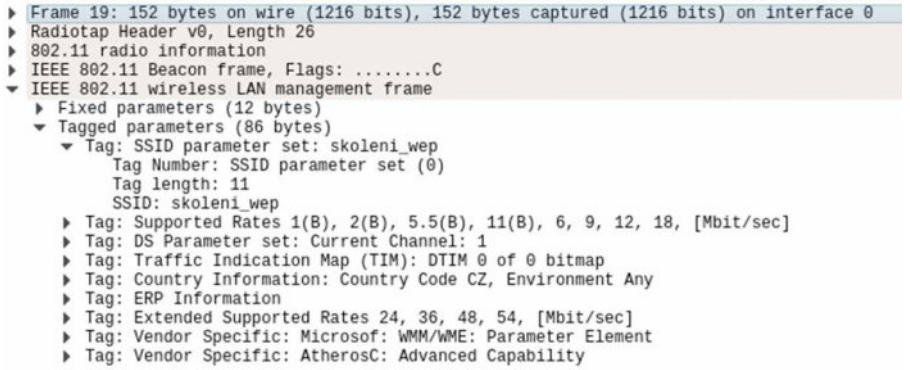
- **Management**
  Management rámce řídí připojování k AP,[491] autentizaci, asociaci, ale také deautentizaci a deasociaci.

  Příkladem managementu rámce je Probe request (počítačový systém zjišťuje, jaká AP jsou v dosahu) a Probe response (což je odpověď na request a beacon rámce).

490: Jednou z možností, jak regulovat šíření signálu, je například využití speciálních nátěrových hmot, které dokáží bránit šíření signálu skrz zdi. Na okna je pak vhodné použít speciální fólie. Blíže viz *New paint protects wireless devices.* [online]. [cit. 16. 7. 2017]. Dostupné z:
http://www.techrepublic.com/blog/it-security/new-paint-protects-wireless-devices/

491: **A**ccess **P**oint – přístupový bod bezdrátové počítačové sítě.

Významným management rámcem je Beacon rámec, kterými dává přístupový bod vědět ostatním počítačovým systémům či prvkům sítě o své existenci. Tyto beacon rámce obsahují mimo jiné informaci o SSID sítě (pokud nebylo zvoleno nastavení: „skrýt SSID“).




Obrázek 55: Beacon rámec zachycený programem Wireshark[492]

Pro úplnost je třeba uvést, že existuje rozšíření pro standard IEEE 802.11, známý jako IEEE802.11w[493], který řeší zabezpečení vybraných management rámců. V případě budování či rekonstrukce Wi-Fi sítě je vhodné vybírat prvky sítě podporující tento standard.

Zabezpečení Wi-Fi sítí není mnohdy věnována taková pozornost, jaká by měla. Mnohdy se lze setkat se „zakořeněnými pravdami“, které demagogicky opakují, že pro zabezpečení Wi-Fi sítě je dostačující filtrování MAC adres, skrytí SSID sítě aj. I z tohoto důvodu jsme se rozhodli v této subkapitole řešit problematiku „neprolomitelnosti“ některých zabezpečení Wi-Fi sítí.

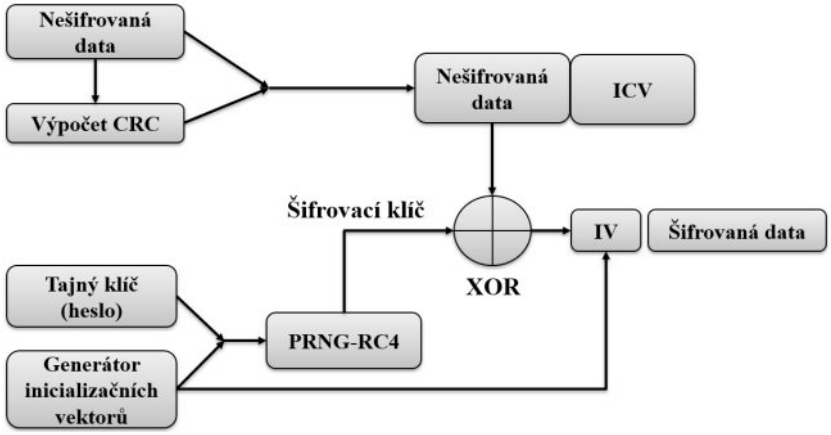
**Filtrace přístupu podle MAC adres**

Filtrace přístupu podle MAC adres není vhodným způsobem zabezpečení Wi-Fi sítí, neboť při tomto zabezpečení dochází k přenosu nezašifrovaných dat (data jsou čitelná) a průměrně schopný útočník si může zjistit MAC adresy počítačových systémů, které mají přístup k počítačové síti. Díky tomu si útočník může nastavit stejnou MAC adresu a vydávat se tak za legitimního uživatele (resp. počítačový systém).

492: Tento rámec nese kromě SSID i další důležité informace, jako podporované rychlosti, číslo vysílacího kanálu a další.

493: Viz *Protected Management Frames (802.11w)*. [online]. [cit. 17. 7. 2017]. Dostupné z: https://wlan1nde.wordpress.com/2014/10/21/protected-management-frames-802-11w/

**Wired Equivalent Privacy (WEP)**
Wired Equivalent Privacy (WEP) představuje v současnosti již naprosto nedostatečný způsob zabezpečení. Toto zabezpečení bylo prolomeno již v roce 2001. Problém WEP spočívá v použití stream šifry RC4. V případě této šifry by neměl být nikdy použit stejný klíč dvakrát, jinak se šifra stává prolomitelnou. Klíč pro šifrování dat se však u WEP vytváří ze společného klíče, který může být buď 40 bitový, nebo 104 bitový. K tomuto společnému klíči se vždy připojí náhodně generovaný inicializační vektor (IV). Tento vektor má ovšem ve všech případech stejnou velikost 24 bit. Kombinací sdíleného klíče a inicializačního vektoru získáme buď 64 bitový, nebo 128 bitový klíč.




Obrázek 56: Princip šifrování dat WEP

Jak je znázorněno na obrázku 56, klíč vzniklý z tajného (sdíleného) klíče a inicializačního vektoru je využit algoritmem PRNG-RC4 pro generování šifrovacího klíče, který následně XORuje (logická operace exkluzivní disjunkce) s původními nešifrovanými daty, ke kterým je připojen kontrolní součet. K šifrovaným datům je nakonec připojen inicializační vektor (IV), který byl použit pro vytvoření aktuálně použitého klíče.

Počítačový systém, který paket přijme, následně provede obrácený postup, tedy na základě sdíleného klíče a iniciačního vektoru získá šifrovací klíč, kterým pak opět s pomocí logické operace XOR získá zpět původní nezašifrovaná data.

Účelem inicializačního vektoru, který je přenášen nešifrovaně spolu s daty, bylo zabránit opakování šifrovacího klíče. Klíč, který měl 24-bitů, se ovšem ukázal jako nedostatečně dlouhý. V tomto případě existuje 50% šance, že stejný inicializační vektor bude použit znovu po

zašifrování 5000 paketů. Pokud na počítačové síti není dostatečný provoz, může útočník celý útok urychlit například odchycením vhodného datového paketu (například ARP dotaz[494]).

Útočník sice v této chvíli ještě není schopen zjistit obsah paketů, protože nezná šifrovací klíč, ale obsah paketu může odhadovat podle jeho délky. Pokud tedy zachytí paket, který by mohl být ARP dotazem, pošle jej zpět do počítačové sítě. Pokud to skutečně byl ARP paket, pak druhá strana bude na každý znovu odeslaný paket odpovídat zašifrovanou odpovědí ARP replay. Na její zašifrování ale použije vždy jiný inicializační vektor. Takto může útočník během několika minut vygenerovat potřebné množství 5000 paketů.

Za účelem provádění nejen těchto útoků byla vytvořena řada nástrojů. Jedním z nejznámějších nástrojů je skupina programů známá jako **aircrack-ng**.

K využití tohoto programu je třeba disponovat Wi-Fi kartou, jejíž chipset a driver podporují přepnutí z běžného managed módu do módu monitor, ideálně i do módu injection. Monitor mód umožňuje zachytit všechny rámce v dané Wi-Fi síti, a to bez potřeby asociace s přístupovým bodem. Útočník tedy může zcela pasivně naslouchat, a pokud zná heslo k Wi-Fi síti, může v případě WEPu automaticky dešifrovat veškerý přenášený provoz. Takovéto on-line dešifrování umí provádět například program **Wireshark**, pokud do něj útočník vloží heslo k Wi-Fi síti.

Většina karet, které lze přepnout do výše zmiňovaných módů, jsou provozovány v rámci OS Linux. Seznamy vyzkoušených karet je možné nalézt na Internetu a jejich ceny se pohybují v řádech stokorun. I v tomto případě platí, že výše popsaného útoku (resp. využití zranitelnosti) se může relativně jednoduše dopustit i zkušenější uživatel.

Balíček programů „aircrack“ se skládá z následujících programů:

- **airmon-ng** (umožňuje přepnutí karty do monitor a injection módu),
- **airodump-ng** (umožňuje monitoring bezdrátových sítí),
- **aireplay-ng** (injektuje pakety do počítačové sítě),
- **airbase-ng** (vytváří vlastní přístupový bodu),
- **aircrack-ng** (je schopen ze zachycených dat získat hesla jak pro WEP, tak i pro WPA PSK).

Dalším problémem WEP, který je specifický pro Českou republiku je skutečnost, že se zde vyskytuje řada Wi-Fi sítí s SSID: „***VOIP***“. Důvod pro řadu shodných označení Wi-Fi sítí spočívá ve faktu, že před několika lety jedna ze společností, které v ČR poskytují DSL služby, poskytovala svým zákazníkům routery, které měly možnost konfigurace až čtyř Wi-Fi sítí.

494: Blíže viz kap. 6.1.2.2 ARP protokol

V routeru byly zobrazeny čtyři záložky pro nastavení Wi-Fi sítě, přičemž první, třetí a čtvrtá záložka byla nevyplněná, aby si uživatel mohl nastavit vlastní síť dle svých požadavků.

Na druhé záložce však byla nakonfigurována síť VOIP, která právě používá WEP. Samotná síť VOIP obvykle nedisponuje žádnými počítačovými systémy, není tedy možné se do ní dostat výše popsaným útokem. Síť VOIP ovšem používá něco jako universální heslo, které sice není všude stejné, ale lze ho jednoduše odhalit jen s pomocí mobilního telefonu s OS Android a aplikací schopnou zobrazit BSSID (MAC adresu) přístupových bodů v okolí.

Na výše zmíněný problém upozorňujeme především proto, že řada těchto routerů a sítí je stále aktivních, ačkoliv již nejsou nová zařízení distribuována. V případě, že využíváte starší router k DSL, doporučujeme zkontrolovat, zda nejste nedobrovolnými provozovateli tohoto v podstatě bezplatného připojení.

**Příklad:** *Autor se s tímto problémem setkal na pobočce banky. Samotná pobočka nesloužila veřejnosti, ale pouze administrativní činnosti. Z tohoto důvodu na pobočce stačilo DSL připojení s obyčejným routerem od poskytovatele, který ovšem byl nakonfigurován i s VOIP sítí chráněnou WEP.*

**WPA (Wi-Fi Protected Access)**
Další možností zabezpečení Wi-Fi sítě je použití protokolu WPA, který vznikl v reakci na prolomení WEP. Protokol WPA představoval řešení, které mělo být rychle nasaditelné bez nutnosti měnit stávající hardware. Díky tomuto požadavku WPA používá stejnou šifru RC4 jako WEP, avšak pro WPA byl vyvinut Temporal Key Integrity Protocol (TKIP) protokol, který řeší nedostatky, které vedly k prolomení WEP. Díky TKIP je v rámci WPA každý paket šifrován skutečně jedinečným klíčem.

I přes výše uvedené se objevily dva útoky (**Beck-Tews** a **Ohigashi-Morii**), které umožňují prolomit určitou část dat zabezpečených WPA. Z tohoto důvodu není doporučeno protokol WPA používat.

**WPA2 (Wi-Fi Protected Access2)**
V současnosti je nejvyužívanějším standardem pro zajištění bezpečnosti bezdrátových sítí protokol WPA2, který má podporu de facto ve všech počítačových systémech. Protokol WPA2 používá k šifrování protokol CCMP, který je odvozen od standardu AES[495], nicméně z důvodu zpětné kompatibility je i WPA2 možné provozovat s protokolem TKIP.[496]

495: **A**dvanced **E**ncryption **S**tandard – pokročilé šifrování.

496: Byť je takováto funkcionalita umožněna, není ji doporučeno využívat vzhledem k útokům **Beck-Tews** a **Ohigashi-Morii.**

U protokolů WPA i WPA2 je vhodné zmínit rizika a útoky vztahující se k využívání těchto protokolů:

1) **Možnost získání hesla slovníkovým útokem**
   V případě, že je používán protokol WPA-PSK, je za určitých okolností možné získat heslo k Wi-Fi síti slovníkovým útokem.

   PSK je zkratkou slov Pre-shared key, což znamená, že všechny počítačové systémy používají pro přístup k počítačové bezdrátové (Wi-Fi) síti stejné heslo. Ve skutečnosti má každý počítačový systém stejný 256 bitů dlouhý PMK (Pairwise Master Key).

   Spojení řetězce z hesla (PSK) a SSID je 4096krát hashováno, čímž je získán 256 bitový PMK klíč, kterým se zařízení přihlašuje k přístupovému bodu. Hash opakovaný 4096krát chrání WPA-PSK proti útokům hrubou silou, neboť útočník je nucen vypočítat a prověřit značné množství možných kombinací, což je dostatečně zpomalující.

   Použití unikátní SSID brání útokům, které by spoléhaly na přepočítání nebo rainbow tables.[497] Díky skutečnosti, že řada uživatelů nemění defaultně nastavené SSID názvy, byly vytvořeny rainbow tables.[498] Na Internetu lze nalézt rainbow tables například pro SSID linksys[499] nebo default. Odkazy na rainbow tables je možné nalézt i na stránkách, které se věnují penetračnímu testování, neboť cílem bezpečnostní komunity je sdílet informace o možných hrozbách.[500]

497: Toto tvrzení neplatí v případech, kdy je použit typicky výrobcem předdefinovaný název sítě.

498: Viz např. *List of Rainbow Tables.* [online]. [cit. 11. 8. 2018]. Dostupné z: https://project-rainbowcrack.com/table.htm

499: Blíže viz Obrázek 57: Rainbow tables nejčastějších SSID

500: Blíže viz např. *[Download] WPA-PSK Rainbow Tables.* [online]. [cit. 11. 8. 2018]. Dostupné z: https://securityonline.info/wpa-psk-tables/

The most common SSIDs

```
linksys
<no ssid>
default
NETGEAR
Wireless
WLAN
Belkin54g
MSHOME
home
hpsetup
smc
tsunami
ACTIONTEC
orange
USR8054
101
tmobile
<hidden ssid>
SpeedStream
linksys-g
3Com
WaveLAN Network
Wayport_Access
hhonors
```

Obrázek 57: Rainbow tables nejčastějších SSID[501]

Pokud útočník odchytí při přihlašování do sítě klíč PMK, může se pokusit o slovníkový útok, neboť zná SSID počítačové sítě a ví, jakým způsobem postupovat při výpočtu. Tak jako při jiných off-line útocích bude útočník brát hesla ze slovníku, z těch vygeneruje PMK klíč a výsledek porovná se zachyceným PMK klíčem.

2) **Bezpečnost šifrování komunikace koncových počítačových systémů s přístupovým bodem na WPA-PSK**
Krom klíče PMK má také každý koncový počítačový systém v počítačové síti svůj jedinečný PTK (Pairwise Transient Key) klíč, který je vygenerován během Four-way handshake[502] při

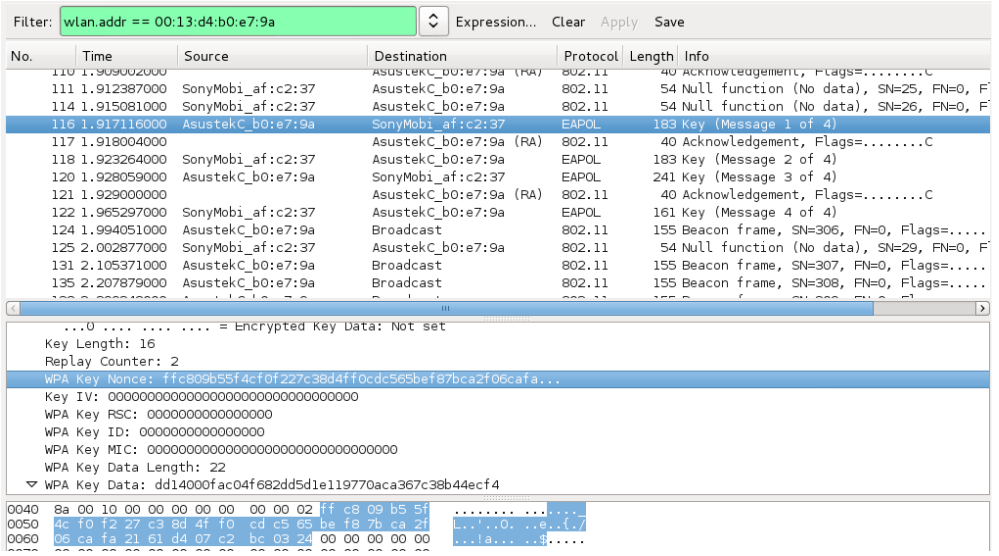
501: *Rainbow tables/hash tables versus WPA/WPA2.* [online]. [cit. 11. 8. 2018]. Dostupné z: https://security.stackexchange.com/questions/92903/rainbow-tables-hash-tables-versus-wpa-wpa2

502: Blíže viz např. *Four-Way Handshake.* [online]. [cit. 11. 8. 2018]. Dostupné z: https://www.techopedia.com/definition/27188/four-way-handshake

přihlašování počítačového systému do počítačové sítě. Z PTK se odvozují klíče pro šifrování. Každý počítačový systém v počítačové síti tedy šifruje komunikaci s přístupovým bodem svou vlastní sadou klíčů.

Samotný PTK se generuje z PMK, MAC adresy počítačového systému, přístupového bodu sítě a z výzvy počítačového systému a přístupového bodu. Všechna tato data jsou při přihlašování přenášena v čitelné podobě.

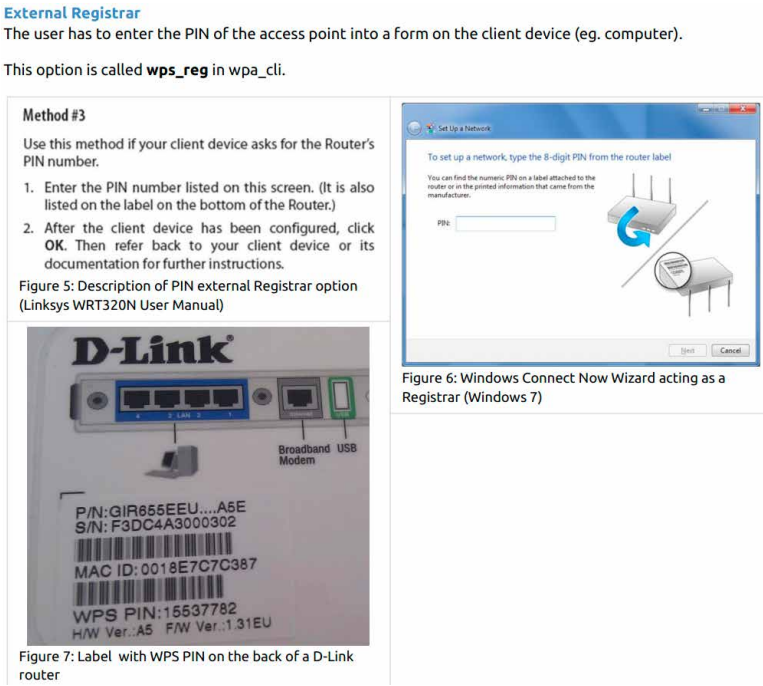
Byť má každý uživatel své vlastní klíče pro šifrování, útočník je schopen tyto klíče dovodit, pokud se mu podaří zachytit Four-way handshake. V případě, že je již koncový počítačový systém připojený k bezdrátové počítačové síti (Wi-Fi), může útočník zaslat tomuto koncovému počítačovému systému žádost o deautentizaci, která bude vypadat, jako kdyby byla odeslána přístupovým bodem. Na základě této žádosti se koncový počítačový systém odpojí od počítačové sítě a znovu se k ní připojí. Díky novému přihlášení může útočník Four-way handshake odchytit.




Obrázek 58: Four-way handshake (EAPOL rámce) zachycený v programu Wireshark

V případě, že je Four-way handshake součástí dat zachycených ve Wi-Fi síti a pokud zná útočník heslo, dokáží mu programy, jako je například Wireshark, automaticky dešifrovat komunikaci koncového počítačového systému. Mimo jiné i z tohoto důvodu je vhodné využívat dodatečné šifrování.

3) **Chyba WPS**
Wi-Fi Protected Setup (WPS) měl uživatelům usnadnit připojování nových počítačových systémů k jejich Wi-Fi sítím. Pro připojení nového počítačového systému k síti je v rámci WPS třeba zadat speciální osmimístný PIN, který je možné nalézt na routeru.




Obrázek 59: WPS PIN[503]

Problém WPS je, že ačkoliv WPS používá unikátní 8 místný PIN, samotný systém WPS část tohoto PINu prozrazuje.

V případě, kdy router posílá zamítavou odpověď, totiž přidá do této odpovědi informaci, zda náhodou nebyla první či druhá část PINu správně.[504] Zároveň poslední číslo v PINu představuje kontrolní součet. Útočníkovi pro prolomení WPS stačí uhodnout první 4 a pak

503: *WPS PIN*. [online]. [cit. 16. 7. 2017]. Dostupné z: https://krebsonsecurity.com/2011/12/new-tools-bypass-wireless-router-security/

504: Blíže viz *Brute forcing Wi-Fi Protected Setup (802.11w)*. [online]. [cit. 20. 7. 2017]. Dostupné z: https://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf

další 3 číslice. Tato skutečnost významně zmenšuje množství kombinací a pokusů nutných pro prolomení zabezpečení, ze zhruba 100 000 000 na 20 000.

Jako protiopatření se doporučuje uživatelům deaktivovat WPS a výrobcům zavést nějakou formu blokace po více nepodařených pokusech.

4) **Technický útok spojený se sociálním inženýrstvím**
V případě tohoto útoku se jedná o modifikaci útoku známého jako Evil Twin.[505]

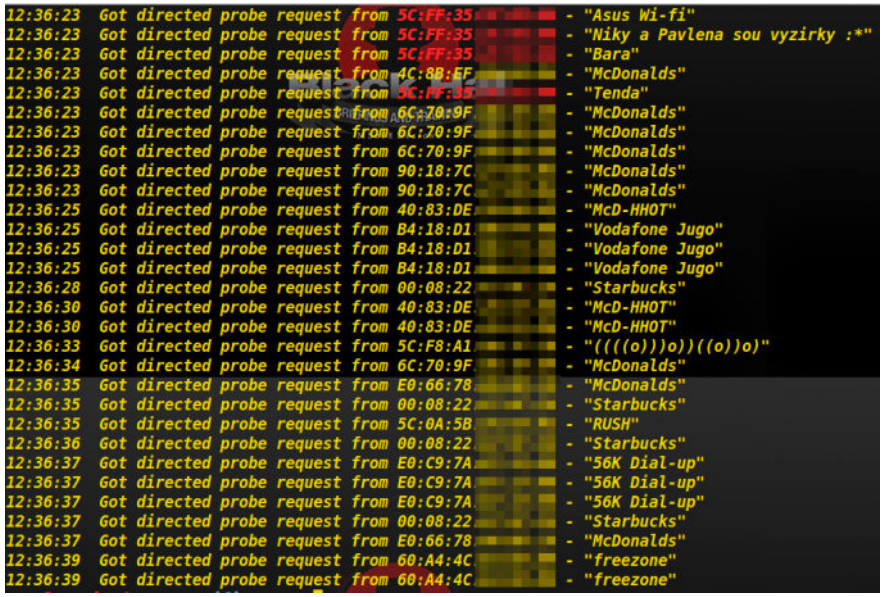
Vlastní útok je proveden tak, že si útočník vytvoří vlastní Wi-Fi síť se stejným SSID již existující sítě a vytvoří webovou stránku, která bude vzhledem napodobovat web počítačového systému (routeru), který organizace používá. Útočníkem vytvořená webová stránka bude požadovat zadání hesla k Wi-Fi síti s tím, že po jeho zadání bude mít uživatel opět přístupnou celou počítačovou síť.

Následně začne útočník z nepodvržené (originální) Wi-Fi sítě odpojovat jednotlivé počítačové systémy a vyčká, zda se některý z uživatelů nebude snažit zkontrolovat seznam dostupných Wi-Fi sítí. Uživateli se v seznamu dostupných Wi-Fi sítí zobrazí útočníkem vytvořená síť se stejným SSID jako síť původní. V případě, že si uživatel vybere útočníkovu Wi-Fi síť bude přesměrován na podvrženou webovou stránku s výzvou k zadání hesla.

5) **Permanentně zapnuté Wi-Fi rozhraní**
V případech, kdy uživatel nechává na svém počítačovém systému (např. mobilním telefonu, tabletu aj.) stále zapnuté Wi-Fi rozhraní, vystavuje se riziku, že se jeho počítačový systém bude pokoušet připojit přímo na konkrétní Wi-Fi sítě, které v minulosti navštívil (za předpokladu, že zůstaly přístupové údaje k těmto sítím v telefonu uloženy).

Koncový počítačový systém se na dostupné Wi-Fi sítě ptá pomocí broadcastového dotazu, na který pak jednotlivé přístupové body odpoví ohlášením svého SSID a dalšími údaji o bezdrátové počítačové síti. Řada koncových počítačových systémů se na Wi-Fi sítě dotazuje přímo, a to tak, jak je možné vidět na následujícím obrázku.

505: Blíže viz např. *Evil twin (wireless networks).* [online]. [cit. 11. 8. 2018]. Dostupné z: https://en.wikipedia.org/wiki/Evil_twin_(wireless_networks)
či *BackTrack, Kali Linux a Evil (Twin) Access Point.* [online]. [cit. 11. 8. 2018]. Dostupné z: https://www.root.cz/clanky/backtrack-kali-linux-a-evil-twin-access-point/




Obrázek 60: Zobrazení SSID sítí v rámci zaslaného requestu[506]

Takovéto přímé dotazování koncového počítačového systému může v některých případech znamenat narušení soukromí a bezpečnosti uživatele, neboť z názvů Wi-Fi sítí je v některých případech možné odvodit, kde se daný uživatel pohyboval.[507]

Z bezpečnostního hlediska je rizikem skutečnost, že se v uvedeném seznamu hledaných sítí bude nacházet otevřená Wi-Fi síť (což lze často odhadnout), nebo Wi-Fi síť, která sice vyžaduje heslo, ale toto heslo lze snadno zjistit (například heslo k Wi-Fi ve vaší oblíbené restauraci).

Díky tomu může útočník připravit falešnou síť se stejným SSID a tak docílit automatického připojení koncového počítačového systému k jeho síti, zcela bez vědomí uživatele. Následně může útočník odposlouchávat veškerou nešifrovanou komunikaci připojeného koncového počítačového systému.

506: *787, 618, 302, 67, 18, Aneb statistiky jednoho „bláznivého oběda“.* [online]. [cit. 20. 7. 2017]. Dostupné z: https://blog.nic.cz/2014/10/20/787-618-302-67-18-aneb-statistiky-jednoho-blazniveho-obeda/

507: Blíže viz Tamtéž.

Díky skutečnosti, že:

- zejména ve svých mobilních počítačových systémech máme nainstalovánu řadu různých aplikací, které vyžadují neustálé připojení k Internetu (např. z důvodu synchronizace dat aj.),
- implementace šifrované komunikace je na těchto zařízeních značně chybová[508],
- uživatelé používají stejné či obdobné heslo do více aplikací,

představuje tento útok pro uživatele značné riziko.

Pro úplnost ještě dodejme, že v minulosti bylo nalezeno také několik zranitelností v různých Wi-Fi kartách a jejich ovladačích. Z pohledu útočníka je velkou výhodou, že nemusí být připojen do žádné sítě, stačí mu, pokud je v dosahu počítačový systém (router), na který chce útočit.

Pro malé počítačové sítě, kde není vysoká pravděpodobnost útoku sofistikovaného útočníka nebo útoku zevnitř této sítě, lze za dostatečně bezpečné považovat WPA2 s šifrováním CCMP. V případě, že je cílem zajistit vyšší možnou míru zabezpečení, je vhodné pro řízení přístupu do sítě použít 802.1x.[509] Tento standard zajistí při správné implementaci vzájemné ověření jak uživatele, tak i přístupového bodu.

V roce 2017 byla odhalena řada nových bezpečnostních chyb týkajících se protokolu WPA2. Prezentován byl také **KRACK** (**K**ey **R**einstallation **A**tta**ck**s), který manipuluje s úvodním Four-way handshake. KRACK zneužívá chyby ve třetím kroku, kdy je možné šifrovací klíč poslat několikrát. Pokud je útok proveden správným způsobem, může být úvodní nonce použit tak, že to kompletně boří bezpečnost šifrování.[510]

**WPA3 (Wi-Fi Protected Access3)**
Ačkoliv je v současnosti protokol WPA2 při správné konfiguraci stále považován za dostatečně bezpečný, stejně se v jeho implementacích v minulosti objevily chyby[511], kterým se snaží předejít

508: Blíže viz *SSL Vulnerabilities: Who listens when Android applications talk?* [online]. [cit. 20. 7. 2017]. Dostupné z: https://www.fireeye.com/blog/threat-research/2014/08/ssl-vulnerabilities-who-listens-when-android-applications-talk.html

509: Blíže viz kap. 6.1.2.4 IEEE 802.1X

510: Blíže viz *Šifrování WPA2 prolomeno, Wi-Fi sítě je možné odposlouchávat (aktualizováno).* [online]. [cit. 1. 2. 2018]. Dostupné z: https://www.root.cz/clanky/sifrovani-wpa2-bylo-prolomeno-wi-fi-site-je-mozne-odposlouchavat/

511: Více viz *An overview of the Wi-Fi WPA2 vulnerability*. [online]. [cit. 11. 9. 2018]. Dostupné z: https://www.enisa.europa.eu/publications/info-notes/an-overview-of-the-wi-fi-wpa2-vulnerability

nový protokol WPA3.[512] Ten byl uvolněn v červnu 2018 a odstraňuje některé problémy svého předchůdce.

**WPA3-Personal** přináší autentizaci, která je odolná i pokud uživatel zvolí jednoduché heslo. Součástí WPA3 je také protokol Simultaneous Authentication of Equals (SAE), který poskytuje vyšší odolnost vůči slovníkovým útokům a útokům hrubou silou. Tyto útoky nebude nadále možné provádět ani on-line, ani offline. WPA3 přináší také dopřednou bezpečnost, která zajišťuje, že prozrazení soukromého hesla neohrozí bezpečí dříve vyměňovaných dat. I přes zvýšení bezpečnosti by samotné používání protokolu mělo být pro uživatele velmi snadné.

**WPA3-Enterprise** nabízí 192 bitové šifrování, silnější šifrování při přihlašování, pro odvození a potvrzení klíče používá 384-bit Hashed Message Authentication Mode (HMAC) se Secure Hash Algorithm (HMAC-SHA384) a přináší robustní ochranu management rámců.

Očekává se, že první počítačové systémy s podporou WPA3 by se mohly na trhu objevit koncem roku 2018 nebo začátkem roku 2019.

#### 6.1.2.6 IPv6

S postupným vyčerpáváním rozsahu IPv4 adres[513] dochází ke stále většímu rozmachu protokolu IPv6, ačkoliv jeho nasazování neprobíhá tak rychle, jak by bylo vhodné.

Jedním z důvodů, které mohou stát za pomalejším nástupem IPv6 sítí, jsou obavy o bezpečnost sítě a o to, zda nebude při nasazení IPv6 opomenut některý důležitý bezpečnostní aspekt. Na druhou stranu je třeba uvést, že protokol IPv6 je na většině operačních systémů ve výchozím stavu podporován a některé z útoků je tak možné provést bez ohledu na to, zda je v síti IPv6 nasazeno či nikoliv.

V následující části subkapitoly se zaměříme na nejčastější problémy v sítích s IPv6 z pohledu bezpečnosti.

Jedním z nejznámějších útoků v rámci počítačových sítí, které využívají IPv6, je útok **Router Advertisement** (**RA**) – útok na oznámení směrovače. Oznámení směrovače hraje důležitou roli při autokonfiguraci koncových počítačových systémů v IPv6 sítích. Pokud se počítačový systém připojuje do počítačové sítě, probíhá celý proces tak, že si nejdříve s pomocí vybrané procedury vytvoří ID rozhraní. Následně si vytvoří linkovou lokální adresu, a to tak, že k prefixu

512: Více viz *Discover Wi-Fi Security.* [online]. [cit. 11. 9. 2018]. Dostupné z: https://www.wi-fi.org/discover-wi-fi/security

513: Blíže viz KOLOUCH, Jan. *CyberCrime.* Praha: CZ.NIC, 2016, s. 74 a násl.

FE80::/10 přidá ID rozhraní, které si vytvořil v prvním kroku. Počítačový systém následně pošle do počítačové sítě dotaz Router Solicitation, a pokud je v síti router, tuto zprávu přijme a odpoví zprávou Router Advertisement, ve které je oznamovaný prefix, router lifetime (tedy čas, po který bude daný router figurovat jako výchozí brána) a další parametry, jako je MTU.[514]

Koncový počítačový systém si na základě zaslaného prefixu a ID rozhraní vytvoří unikátní globální IPv6 adresu a pokud je lifetime routeru větší než nula, zařadí si jeho IPv6 adresu do seznamu výchozích bran. Oznámení směrovače je posíláno všem počítačovým systémům v síti (ale může být posláno i cíleně jen jednomu zařízení), což představuje oproti klasickému DHCP výhodu v tom, že je možné rychle informovat všechny koncové počítačové systémy v síti například o změně směrovače.

Problém z pohledu bezpečnosti představuje skutečnost, že za směrovač se může vydávat kterýkoliv počítačový systém. Tento může do počítačové sítě poslat vlastní oznámení směrovače, a tím tak koncovým počítačovým systémům v síti vnutit například útočníkovu „výchozí bránu". Uvedený útok umožňuje útočníkovi sledovat provoz, případně do něj zasahovat, jak tomu bylo i v případě ARP Cache Poisoning [515]u IPv4.

V praxi je možné se setkat s různými variantami tohoto útoku, přičemž útočník se může v lokální síti vydávat například za servery Google, což uskuteční tak, že v RA paketu oznámí počítačovým systémům v síti prefix, který je ve skutečnosti prefixem používaným skutečnou sítí Google pro servery. Následně svému počítačovému systému nastaví IPv6 adresy, které používá například gmail.com. Protože se počítačové systémy v síti domnívají, že jsou ve stejné počítačové síti jako servery Google, budou posílat své požadavky na gmail.com po lokální síti a ty tak skončí na serveru útočníka. Jiná varianta tohoto útoku může způsobit DoS (nedostupnost připojení k Internetu), a to v případě, že útočník donutí počítačové systémy odstranit ze seznamu výchozích bran všechny dostupné routery.

Dalším útokem, v rámci něhož je zneužit RA paket, se nazývá **Router Advertisement flooding**, v rámci něhož útočník opakovaně generuje pakety s oznámením směrovače s novými náhodně zvolenými prefixy. Současné operační systémy jsou proti tomuto útoku většinou chráněny, nicméně problém se může týkat i různých starších síťových počítačových systémů.

**Příklad:** *Autor tímto způsobem odpojil od připojení k Internetu celou organizaci, byť byl tento útok demonstrován jako ukázka v oddělené části sítě. Bohužel se následně ukázalo, že v organizaci jsou dočasně všechny počítačové sítě routovány přes jeden starší router, který tento útok nebyl schopen zvládnout.*

514: Maximum transmission unit - maximální přenosová jednotka

515: Blíže viz kap. 6.1.2.2 ARP protokol

Další variantou výše popsaného útoku je zahlcení směrovací tabulky s pomocí volby Route Information Option, která rozšiřuje možnosti RA paketů. Dopady těchto útoků jsou u různých systémů různě závažné.[516]

Možnou ochranou proti manipulaci s Router Advertisiment pakety představuje nasazení technologií **RA-Guard** a **ND-Snooping**.

**RA-Guard** funguje na podobném principu, jako DHCP Snooping v IPv4. Switch je správcem nakonfigurován tak, aby pakety obsahující oznámení směrovače akceptoval pouze na portu, na kterém je připojen směrovač. Útočník tak ze svého počítačového systému může i nadále zasílat falešné RA pakety, ty však neprojdou přes port switche a nedostanou se tak k ostatním počítačovým systémům v síti.

**ND-Snooping** brání tomu, aby útočník nepodvrhl záznamy v CAM tabulce na switchi. Switch přitom sleduje dotazy jednotlivých zařízení připojujících se do sítě, kterými tato zařízení ověřují unikátnost zvolené IPv6 adresy. Problémem nasazení této techniky je možný útok typu DoS, kdy si útočník dopředu zjistí, jakou IPv6 adresu používá konkrétní zařízení v síti, a když se odpojí, zaregistruje si jeho IPv6 adresu.

Pokud se v počítačové síti využívá DHCPv6, je doporučeno implementovat funkci DHCPv6 Snooping, která odposlouchává DHCPv6 komunikaci a na základě zjištěných informací vytváří tabulku, ze které switch pozná, zda jsou informace v odesílaném paketu validní kombinací.

V souvislosti s bezpečným provozováním IPv6 sítě je vhodné upozornit také na problematiku cache sousedů (*neighbor cache*). Ta je obdobou ARP cache z IPv4 a obsahuje vždy IPv6 adresu a k ní relevantní MAC adresu. Samotné naplnění této cache se provádí pomocí dvojice zpráv *výzva sousedovi* a *ohlášení souseda*.[517]

V případě IPv6 cache sousedů se může útočník pokusit o útok tak, že využije tohoto mechanismu k tomu, aby na routeru v síti (nejlépe routeru starajícímu se o připojení celé sítě) zaplnil tuto tabulku. K vlastnímu útoku stačí generování paketů s různými zdrojovými IPv6 adresami. V okamžiku, kdy router obdrží tento dotaz, musí zjistit MAC adresu daného souseda. Proto odešle do sítě *výzvu sousedovi*, na kterou útočník odpoví zprávou *ohlášení souseda*. Tímto způsobem postupně zaplní cache sousedů na cílovém počítačovém systému. Pokud je cílem útoku router, může útok vést k různým následkům v závislosti na konkrétní implementaci (např. nepřipojení dalších počítačových systémů, či přetížení počítačového systému aj.).

516: Více viz *New RA Flood Attack.* [online]. [cit. 20. 7. 2017]. Dostupné z: https://samsclass.info/ipv6/proj/RA_flood2.htm

517: Blíže viz SATRAPA, Pavel. *IPv6.* Praha: CZ.NIC. ISBN 978-80-904248-4-5 [online]. [cit. 9. 8. 2017]. Dostupné z: https://knihy.nic.cz/files/edice/ipv6_2012.pdf

Možnou ochranu proti tomuto útoku představuje například funkce IPv6 Destination Guard[518], SEND (Secure Neighbor Discovery), omezení počtu IPv6 adres v cache sousedů na síťovém rozhraní, použití statických položek v cache sousedů nebo omezení času, po který je záznam v cache sousedů platný. Každé z těchto řešení však má své limity či požadavky, jejichž popis je mimo rozsah této knihy.

Existuje i vzdálená varianta útoku na cache sousedů. Při tomto útoku zasílá útočník pakety do cílové počítačové sítě a současně náhodně mění cílové IP adresy. Pokud hraniční router obdrží paket pro IP adresu ve „své" počítačové síti, vygeneruje pro ni *výzvu sousedovi*. Rozdíl oproti předchozímu útoku spočívá v tom, že útočník již nemůže zaslat odpověď v podobě *ohlášení souseda*. V takovém případě si router do cache sousedů uloží pouze dočasnou informaci, která je obvykle ve velmi krátkém čase odstraněna, pokud nedošlo k obdržení odpovědi *ohlášení souseda*. Tímto způsobem nedojde k vyčerpání cache sousedů, ale útok způsobí větší vytížení procesoru zařízení.

Kromě již výše popsaných způsobů ochrany lze v případě vzdálené varianty útoku na cache sousedů využít i možnosti filtrace podle IP adresy. Díky znalosti IPv6 adres ve spravované počítačové síti je možné pakety na vstupu filtrovat a ty, které směřují na neexistující adresy, rovnou zahodit.

Další problém, se kterým se mohou správci počítačových sítí setkat, je zneužití protokolu MLD (Multicast Listener Discovery) k přetížení síťových počítačových systémů, ke zjištění, které IP adresy jsou v síti aktivní, případně k DoS útoku na multicast provoz.

V případě využívání IPv6 je vhodné nezanedbat konfiguraci pravidel na lokálních i síťových firewallech. Uživatel může nedostatečné konfigurace využít například k obcházení pravidel provozu v síti.

**Příklad:** *Jako příklad uvedeme blokaci přístupu k IPv4 adresám Facebooku. Ten je však dostupný i po IPv6. Uživatel tak může zkusit jednoduchý trik a donutit počítačový systém, aby pro přístup k Facebooku primárně využil IPv6 tunel. Stejně pak omezení přístupu k serveru v síti jen pro určité IP adresy může být neúčinné, pokud si server automaticky nakonfiguroval link local adresu a správce přístupy k serveru omezil pouze na úrovni protokolu IPv4.*

518: Blíže viz *IPv6 First-Hop Security Configuration GuideIPv6 Destination Guard.* [online]. [cit. 12. 8. 2017]. Dostupné z: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_fhsec/configuration/xe-16/ip6f-xe-16-book/ipv-6-dest-guard.html

K otestování odolnosti počítačové sítě a síťových počítačových systémů vůči známým útokům na IPv6 lze využít nástroj pro penetrační testování Metasploit, nebo přímo balíky nástrojů THC-IPV6[519] a SI6 Networks IPv6 Toolkit.[520]

### 6.1.3 Ochrana na rozhraní sítí

Následující subkapitola se věnuje ochraně na úrovni řízení síťové komunikace a ochraně na základě kontroly přenášených dat.

#### 6.1.3.1 Access Control List (ACL)

Access Control List představuje základní možnost omezení prostupů z a dovnitř počítačové sítě. V této kapitole se zabýváme ACL z pohledu síťové bezpečnosti, nicméně ACL je také termín, který se týká řízení přístupů ke složkám a souborům jednotlivými uživateli a jejich skupinami. Access Control List v pojetí počítačových sítí představuje pravidla, která řídí přístup k portům či síťovým službám.

Jednotlivé implementace ACL se mohou v závislosti na počítačovém systému (např. server, router aj.) lišit.

#### 6.1.3.2 Firewall

Smyslem firewallu je zabránit nechtěné síťové komunikaci mezi dvěma různými zónami, kterými mohou být dvě či více různých počítačových sítí, nebo rozhraní sítě a koncového počítačového systému.

Rozhodnutí, jaká komunikace bude povolena či zakázána se řídí bezpečnostní politikou, jejíž pravidla jsou aplikována na každý paket, procházející firewallem. Firewally lze rozdělit **podle způsobu jejich fungování a síťové vrstvy**, kterou sledují, na:

- **paketové filtry,**
- **stavové paketové filtry.**

Někdy se dále rozlišují stavové paketové filtry s deep packet inspection, či s kontrolou protokolů.

519: Blíže viz *THC-IPV6.* [online]. [cit. 12. 8. 2017]. Dostupné z: https://www.thc.org/thc-ipv6/

520: Blíže viz *SI6 Networks' IPv6 Toolkit.* [online]. [cit. 12. 8. 2017]. Dostupné z: https://www.si6networks.com/tools/ipv6toolkit/

Firewally lze také rozdělit **dle jejich určení** na:

- osobní firewally,
- SOHO firewally,
- Enterprise firewally,
- specializované firewally,
- aplikační firewally.

**Dle způsobu nasazení** jsou rozeznávány:

- firewally softwarové,
- firewally hardwarové.

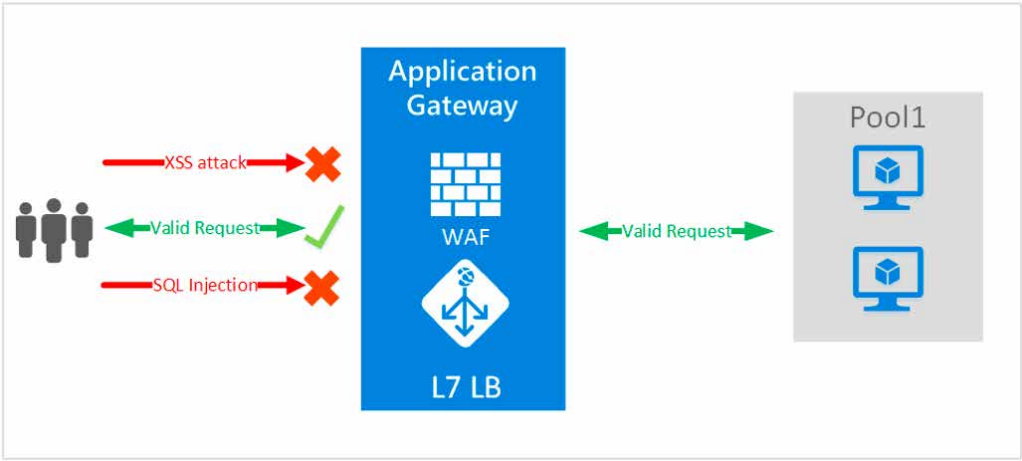
**Paketové filtry** pracují na síťové vrstvě a umožňují pouze povrchní filtrování na základě informací z 3 a 4 síťové vrstvy.[521] Tyto filtry představují velmi rychlou a levnou variantu firewallu. Příkladem mohou být starší implementace Access Control List na zařízeních Cisco, nebo starší implementace firewallu v jádru OS Linux.

**Stavové paketové filtry** fungují podobně jako paketové filtry, avšak navíc umožňují ukládání informací o povolených spojeních. Firewall tak nemusí vždy znovu odesílat všechny pakety do rozhodovacího procesu, ale může využít informace o již povolených spojeních a pakety rovnou propustit. Ke zvýšení bezpečnosti přispívá možnost nastavit, z které strany může být spojení zahájeno. Pakety odcházející z druhé strany jako odpovědi firewall povolí až po zahájení komunikace první stranou.

Současné stavové paketové filtry se obvykle neomezují pouze na výše popsané funkce, ale přidávají možnosti kontroly obsahu paketů nebo analýzu dat konkrétního aplikačního protokolu. Díky tomu tak například dokáží rozpoznat pokus o tunelování nějakého protokolu skrz HTTP protokol. Moderní firewally dokáží také rozpoznat některé pokusy o útok podle známých signatur nebo na základě vlastní heuristiky.

Speciálním druhem firewallu jsou pak *aplikační brány*, někdy také nazývané proxy firewally nebo aplikační proxy. Tyto firewally oddělují komunikaci mezi sítěmi. Aplikační brána přijme požadavek počítačového systému, zpracuje jej a předá serveru, který vrátí odpověď aplikační bráně a ta ji následně vrátí počítačovému systému. Aplikační brána rozumí protokolu, pro který byla postavena, a dokáže v tomto protokolu detekovat nejrůznější chyby i útoky. V případě HTTP serveru tak může rozpoznat pokusy o SQL injection, XSS, nebo rozpoznat pokusy o útoky hrubou silou na uživatelské účty a takovéto dotazy rovnou zahodit.

521: K šíťovým vrstvám viz např. KOLOUCH, Jan. *CyberCrime.* Praha: CZ.NIC, 2016, s. 70 a násl.




Obrázek 61: Aplikační gateway[522]

Při výběru vhodného firewallu je vhodné předem definovat účel, k jakému bude firewall využíván. Bezpečnostní politika vztahující se k počítačové síti a službám by měla definovat:

- povolené služby a aplikace,
- rozsah filtrovaného provozu,
- rozsah údajů, jež budou logovány[523] aj.

Krom příchozího provozu je také třeba nastavit pravidla i pro provoz odchozí. Kontrola odchozího provozu může správce sítě včas upozornit na nevhodné chování uživatele (např. rozesílání spamu, stahování torrentů aj.), ale také může pomoci s ochranou v případě napadení počítačové sítě škodlivým softwarem (malware).[524]

Při výběru firewallu s pokročilými funkcemi je vhodné se předem seznámit s jejich možnostmi i případnými limity.

522: *Aplikační gateway*. [online]. [cit. 15. 8. 2017]. Dostupné z: https://docs.microsoft.com/en-us/azure/application-gateway/application-gateway-web-application-firewall-portal

523: Blíže viz kap. 6.2.4 Logy a logování

524: Může být například odhalena komunikace malware s jeho řídícím serverem. Blíže viz *Detecting and Preventing Unauthorized Outbound Traffic.* [online]. [cit. 16. 8. 2017]. Dostupné z: https://www.sans.org/reading-room/whitepapers/detection/detecting-preventing-unauthorized-outbound-traffic-1951

### 6.1.3.3 Proxy server

S kontrolou síťové komunikace úzce souvisí proxy server, který umožňuje kontrolovat obsah, k němuž budou uživatelé přistupovat, stejně jako kontrolovat obsah přenášených dat, nebo cachovat přenášená data a tím šetřit síťový provoz. V dnešní době, pokud hovoříme o proxy, máme zpravidla na mysli web proxy, nicméně princip použití proxy je univerzálnější.

Rozlišovány jsou tři základní typy proxy serverů:

- **Reverzní proxy server**
  Reverzní proxy server je nasazován na stejné místo, jako výše popsaná aplikační gateway, a některé poskytované funkce jsou obdobné. Reverzní proxy server bývá nasazován například před webovými servery a jednotlivé požadavky od klientů buď zpracuje sám (pokud má požadovaný obsah v cache a je tak nastaven, typicky se jedná o statický obsah), nebo jej předá dalším serverům. Předávání na jednotlivé servery lze řídit dle pravidel, například dle klientem požadované URL. Reverzní proxy server také umožňuje balancování zátěže jednotlivých serverů, akceleraci šifrování, provádění komprese dat aj.

- **Forward proxy server**
  Forward proxy server umožňuje velmi přesně řídit přístup jednotlivých uživatelů k cílovému serveru (např. webovým stránkám). Pokud se uživatelé k proxy serveru autentizují, může mít každý uživatel povolen přístup k jinému rozsahu webových stránek. Stránky lze také filtrovat podle obsahu určitých slov, podle obsahu URL a dle dalších parametrů. Z pohledu bezpečnosti je vhodné uvést, že funkci proxy serveru lze spojit s dalšími bezpečnostními prvky a lze tak například s pomocí antiviru kontrolovat přenášená data a v případě nebezpečí tato data zablokovat.

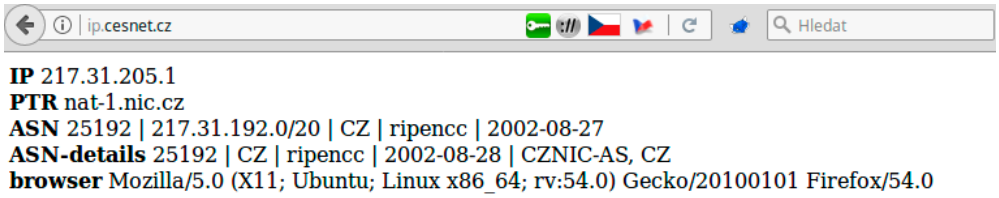
- **Open proxy server**
  Open proxy server je forward proxy server, který je dostupný kterémukoliv uživateli na Internetu. Některé open proxy servery je třeba nakonfigurovat v rozhraní prohlížeče, jiné umožňují použití prostým přistoupením na jejich stránky.

  Existují seznamy open proxy[525], na kterých si může uživatel vybrat proxy server podle jeho fyzického umístění, například pokud potřebuje přistupovat k obsahu, který je dostupný pouze uživatelům daného státu.

  Následující dva obrázky byly pořízeny ve stejné době na stejném počítačovém systému. První byl pořízen při přímém navštívení adresy ip.cesnet.cz, což je jedna z webových stránek, na

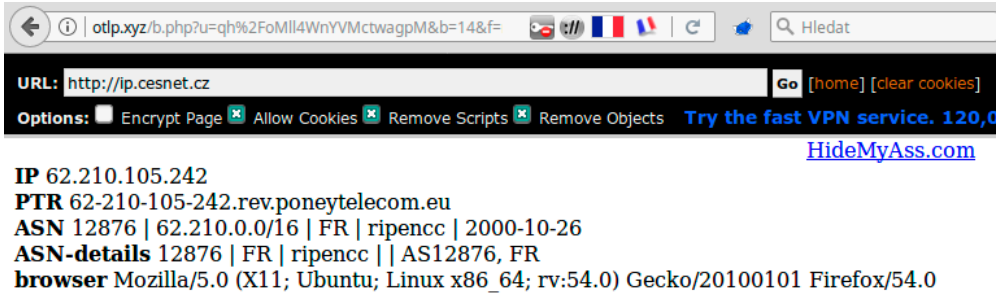
525: Například http://www.proxy4free.com/list/webproxy1.html nebo http://proxy.org/web_proxies.shtml

nichž si může uživatel snadno zjistit, pod jakou IP adresou vystupuje na Internetu, tedy jak jej vidí servery, které navštíví.




Obrázek 62: Přístup na web ip.cesnet.cz

Druhý obrázek pak zobrazuje stejnou stránku, ovšem navštívenou s využitím open proxy umístěné ve Francii.




Obrázek 63: Přístup na web ip.cesnet.cz za využití proxy serveru

V druhém případě má z pohledu serveru uživatel IP adresu 62.210.105.242, která je dle údajů z RIPE alokována do Francie. Za zmínku také stojí skutečnost, že ne každý proxy server pozměňuje i informace o prohlížeči uživatele. Například v tomto případě jsou tyto informace zachovány.

**Příklad:** *Někteří útočníci v případě, že se jim podaří napadnout webový server a inicializují na něm například phishingovou stránku, překonfigurují server tak, aby k dané phishingové stránce měli přístup pouze uživatelé z IP adres, které jsou alokovány do země, na jejíž uživatele útok cílí. Touto změnou útočníci oddálí objevení podvodné stránky administrátorem serveru*[526] *a může se také prodloužit proces řešení incidentu.*

V CSIRT.CZ je využíván open proxy server právě k ověření, zda nedošlo k výše popsanému zablokování přístupu. Používání open proxy serveru může na druhou stranu představovat i bezpečnostní riziko, neboť nemusí být známo, kdo má daný open proxy server pod kontrolou, a správce proxy serveru může do webových stránek přidat vlastní obsah, od falešné zprávy do zpravodajského portálu až po odkaz na stažení malware.

#### 6.1.3.4 Intrusion Detection System (IDS) a Intrusion Prevention System (IPS)

Intrusion detection system představuje systém, který se na základě sledování síťového provozu, nebo na základě chování procesů a operačního systému na konkrétním počítačovém systému, snaží identifikovat případné pokusy o útok a další podezřelé jevy. IDS dokáže zjistit pokusy o skenování portů, exfiltraci dat, exploitaci zranitelností aj.

Existují dva základní typy IDS:

- **HIDS (Host-based Intrusion Detection System)**
  HIDS je obvykle nainstalován přímo v koncovém počítačovém systému, kde kontroluje obsah logů, chování aplikací, monitoruje různé změny v systému, integritu souborů, sledují se některá systémová volání a další parametry, které by mohly poukázat na probíhající, či již provedený útok.

- **NIDS (Network Intrusion Detection System)**
  NIDS bývá umístěn na síťových prvcích, nebo je v síti umístěn v podobě specializované sondy. Tento systém monitoruje síťový provoz, ve kterém hledá známé signatury útoků, anomálie v provozu a z nich detekuje případný útok. NIDS také dokáže upozornit i na nežádoucí odchozí provoz, odesílání definovaných dokumentů a další podezřelé aktivity.

526: Za předpokladu, že administrátor nezkontroluje faktický stav na serveru, ale otevře URL, jež mu byla nahlášena jako phishingová, může mu být zobrazena chyba 404 - stránka neexistuje a celá věc je následně vyhodnocena jako falešný poplach.

Dle architektury se IDS systémy dělí na:

- **monolitické** (všechny části IDS jsou provozovány v jednom počítačovém systému),
- **hierarchické**.
  Výhodou hierarchické architektury IDS je spojení informací z více počítačových systémů do jednoho místa, které může korelací a dalším zpracováním získaných dat odhalit útok.

Intrusion Prevention System (IPS) představuje systém, který na rozdíl od IDS sám aktivně zasáhne proti rozpoznanému útoku, například resetováním síťového spojení, zablokováním provozu z podezřelé IP adresy, nebo zahozením závadných paketů.

Výstupy ze systémů IDS/IPS nemusí sloužit pouze jako prvky upozorňující na útok, či anomálie v počítačové sítí a počítačových systémech, ale mohou být také použity jako jeden ze vstupů pro systémy SIEM.

#### 6.1.3.5 Security Information and Event Management (SIEM)

SIEM umožňuje monitorování, ukládání, agregaci, korelaci bezpečnostních informací a z nich plynoucích incidentů a jejich zobrazování, reportování a vydávání varování. SIEM technologie sbírá v reálném čase informace ze síťových počítačových systémů, aplikací, systémových logů, jejichž vyhodnocení umožňuje identifikovat potenciální bezpečnostní hrozby.

Data mohou být sbírána z webových serverů, routerů, firewallů, Active Directory serverů, databázových serverů a tyto informace mohou být dále doplněny o informace dávající těmto datům kontext, jako jsou informace o uživatelích, výsledcích bezpečnostních skenů, informace z externích zdrojů a informace o běžných návycích uživatelů. Získané informace jsou následně agregovány, korelovány a je nad nimi prováděna analýza, která má ukázat na možné bezpečnostní problémy.

Je však třeba říci, že SIEM řešení není vhodné pro každou situaci. Zatímco firewall nebo antispam mají smysl v podstatě v každé organizaci, SIEM představuje robustní řešení, které vyžaduje poměrně dost zdrojů.

Kromě samotné implementace je třeba počítat také v podstatě s každodenní údržbou, přičemž čím složitější je prostředí, tím větší jsou nároky na údržbu. Stačí totiž poměrně malá změna v části počítačové sítě či počítačovém systému a již nakonfigurovaný SIEM může začít generovat řadu false positive hlášení. Rozhodnutí, zda SIEM využít, záleží na velikosti organizace, hodnotě chráněných aktiv i na náročnosti implementace a údržbě SIEM řešení.

#### 6.1.3.6 Antivir, Antispam

Možnosti ochrany na rozhraní sítí doplňme ještě informací o vhodnosti provozovat na mail serveru antivirové a antispamové řešení.

Antivirové řešení v rámci mail serveru prohledává přílohy e-mailových zpráv a hledá v nich škodlivý kód. Antispamové řešení pak chrání koncové uživatele před nevyžádanou poštou. Nevyžádaná pošta nemusí znamenat pouze nevyžádaná obchodní sdělení, ale také phishingové[527] e-maily, nebo e-maily obsahující odkaz ke stažení malware. Z tohoto důvodu je třeba také dobře zvážit, jaké typy souborů v příloze e-mailu budou na mail serveru zakázány.

**Bližší informace o phishingových, pharmingových aj. útocích, obraně a nápravných krocích je možné nalézt na: https://kyberbezpecnost.csirt.cz/**

### 6.2 Aplikační bezpečnost

Aplikační bezpečnost v sobě zahrnuje řízení přístupů, ověřování uživatelů, hesla, logování, zranitelnosti, šifrovanou komunikaci aj. V této subkapitole se zaměříme na některá nastíněná témata z pohledu jejich zranitelnosti a zvýšení kybernetické bezpečnosti.

### 6.2.1 Řízení přístupů

Při řízení přístupu je ověřována úroveň oprávnění a práv uživatele k určitému zdroji nebo objektu. **Zdrojem** může být připojení k síti, využití kapacity paměťového média, přístup k počítačovým systémům (serverům, síťovým prvkům, tiskárnám aj.) atd., zatímco **objektem** jsou například data uložená v určitém adresáři, nebo samostatný soubor. Ověřovaným objektem může být oprávnění uživatele, skupiny, ale i samotných počítačových systémů. Uživatel může mít stejná práva jako ostatní členové skupiny a zároveň i nějaká oprávnění, která má pouze dotyčný uživatel.

Rozdělení uživatelů do skupin je velmi praktické, obvykle se v organizaci vyskytují určité skupiny uživatelů, kteří využívají stejné zdroje.

**Příklad:** *Je možné vytvořit například skupinu Marketing, jejíž členové budou po přihlášení k síti zařazeni do společné VLAN, případně budou mít všichni přístup do společného adresáře na sdíleném síťovém úložišti.*

527: KOLOUCH, Jan. *CyberCrime.* Praha: CZ.NIC, 2016, s. 246–263

**Granularita nastavení práv** závisí na používaném systému. Obvykle je možné pro soubory a adresáře určit minimálně oprávnění pro čtení, zápis, odstranění, spuštění a změnu vlastníka souboru či adresáře.

### 6.2.2 Ověřování uživatelů

Aby vůbec mohlo dojít k řízení uživatelských přístupů, musí být nejprve systémem ověřena identita uživatele. **Nejčastěji lze ověřit identitu uživatele na základě toho:**

- **co zná,**
- **co vlastní,**
- **čím je.**

Nejběžnějším je **ověření uživatele na základě toho, co zná** v podobě hesla (určitého řetězce znaků), který uživatel obvykle na základě výzvy systému zadá. Zadané heslo je následně porovnáno s heslem již dříve uloženým uživatelem do systému. Pokud se hesla shodují, je uživatel přihlášen a jsou mu přidělena oprávnění.

**Výhodou hesel je jejich snadné použití a snadná implementace do systému**. Čím je však heslo kvalitnější, tím je obvykle pro uživatele hůře zapamatovatelné. Nevýhodou hesla je, že je lze odpozorovat či předat. K problematice hesel blíže viz kap. 6.2.3.

**Ověření uživatele na základě vlastnictví předmětu** bývá realizováno díky držení určitého tokenu uživatelem (např. čipové karty, klíče, aj.). Tuto funkci dnes může převzít například i mobilní telefon. Nevýhodou ověření na základě vlastnictví předmětu je skutečnost, že i tato zařízení je možné předat, zcizit, ztratit. Navíc jsou s jejich použitím často spojeny výrazně vyšší náklady než při ověření na základě toho, co uživatel zná.

**Ověřením uživatele na základě toho čím je** se zabývá biometrie, která rozpoznává jedinečné biologické charakteristiky daného uživatele. Existuje několik charakteristik, u nichž se předpokládá nebo je matematicky prokázáno, že jsou pro každého člověka unikátní. Uvedené charakteristiky jsou často využívány jinými vědními obory (např. kriminalistika) k jedinečné identifikaci člověka.

Uživatele je možné ověřovat podle otisku prstu, podle obličeje, dynamiky při psaní, hlasu, mozkových vln, oční duhovky, krevního řečiště atd.[528] Nicméně ne všechny tyto možnosti najdou v současné době běžné využití v praxi. Nevýhodu ověření uživatele na základě toho,

528: Blíže viz kap. 5.3 Vnitřní bezpečnost

čím je, představuje nutnost pořízení speciálního hardwaru, nemožnost změnit „heslo" v případě prozrazení používaných charakteristik a možnost napodobení některých biometrických údajů.

„*Pokud někdo ukradne vaše heslo, můžete jej změnit.*
*Ale pokud někdo ukradne vaše otisky, nemůžete získat nový palec.*
*Režimy selhání jsou velmi odlišné.*"

Bruce Schneier[529]

Za vhodnou a pro většinu běžných aplikací a systémů dostatečnou, lze označit autentizaci, která využívá dva z výše uvedených způsobů a kombinuje tak například znalost hesla s vlastnictvím zařízení, nebo s biometrickými údaji. V takovém případě mluvíme o dvoufaktorové autentizaci.

**Příklad:** *Nejběžnějším příkladem dvoufaktorové autenzizace je výběr peněz z bankomatu, kdy uživatel vlastní platební kartu, ale zároveň musí znát i příslušný PIN kód.*

### 6.2.3 Hesla

Hesla stále představují nejrozšířenější způsob autentizace uživatelů, a proto je vhodné jim věnovat větší pozornost. Jak již bylo uvedeno, heslo je po zadání uživatelem porovnáno s heslem, které uživatel zadal do systému již dříve.

Tím vzniká první problém, který spočívá v **procesu uložení hesla do systému** tak, aby se k němu nedostal útočník, pokud se mu podaří do systému proniknout. Další potencionální riziko představuje i oprávněný správce systému, který má z principu přístup do celého systému a mohl by si tak přečíst heslo uživatele a následně je zneužít.

Dříve se hesla v systémech někdy ukládala i v původní čitelné podobě, některé systémy se snažily řešit uvedený problém šifrováním hesel. V případě, že však útočník dokázal proniknout do systému, získal přístup nejenom k zašifrovaným heslům, ale obvykle i k šifrovacímu klíči. Díky této zjevné zranitelnosti se ve velkém prosadily hashovací funkce.

**Hashovací funkce** mají následující vlastnosti, které je činí vhodnými pro vytváření otisků (hashů) hesel:

- jedná se o funkce jednocestné (z hashe není matematickými metodami možné získat zpět původní text),

529: SCHNEIER, Bruce. [online]. [cit. 18. 7. 2018]. Dostupné z: https://www.azquotes.com/quote/570046 Překlad autora.

- jakákoliv drobná změna textu na vstupu funkce vyvolá dramatickou změnu na výstupu (dva otisky stejného textu, na kterém došlo jen k drobné úpravě, budou vypadat zcela odlišně),
- je prakticky nemožné nalézt dva vstupy, pro které bude stejný výstup,
- výstup funkce je vždy stejně dlouhý bez ohledu na velikost vstupních dat.

Pří výběru vhodné hashovací funkce je možné využít jako vodítko například minimální požadavky na kryptografické algoritmy, které jsou definovány ve vyhlášce o kybernetické bezpečnosti.

Pokud se uživatel přihlašuje do systému, je z jeho hesla nejdříve vytvořen hash, který je následně porovnán s uloženou hodnotou. Pokud se hashe shodují, je ověřeno, že uživatel „něco zná“, a na základě této znalosti je ověřen.

**V současnosti rozeznáváme řadu útoků na hesla. Heslo může být:**

1) odchyceno z provozu na počítačové síti,
2) z uživatele vylákáno sociálním inženýrstvím (např. phishingovým útokem aj.),
3) získáno z počítačového systému za použití malware (např. pomocí keylogeru aj.),
4) uhádnuto,
5) „lámáno“.

Lámání on-line představuje situaci, kdy útočník zasílá různá hesla a čeká na jejich ověření v počítačovém systému. Obecně je tento způsob útoku relativně pomalý a útočníkovi hrozí, že si jeho počínání někdo všimne a v logu se objeví příliš mnoho pokusů o přihlášení z jedné IP adresy, případně na více účtů.

V následujícím výpisu z logu routeru lze pozorovat pokus útočníka o uhodnutí jména uživatele. Výpis představuje minutovou sekvenci pokusů.

Nov/18/2017 11:40:30 system,error,critical login failure for **user dev** from **111.230.195.101** via ssh
Nov/18/2017 11:40:32 system,error,critical login failure for **user tech** from **111.230.195.101** via ssh
Nov/18/2017 11:40:34 system,error,critical login failure for **user nexus** from **111.230.195.101** via ssh
Nov/18/2017 11:40:36 system,error,critical login failure for **user susan** from **111.230.195.101** via ssh
Nov/18/2017 11:40:38 system,error,critical login failure for **user http** from **111.230.195.101** via ssh
Nov/18/2017 11:40:41 system,error,critical login failure for **user samp** from **111.230.195.101** via ssh
Nov/18/2017 11:40:43 system,error,critical login failure for **user elasticsearch** from **111.230.195.101** via ssh
Nov/18/2017 11:40:46 system,error,critical login failure for **user glassfish** from **111.230.195.101** via ssh
Nov/18/2017 11:40:48 system,error,critical login failure for **user csgo** from **111.230.195.101** via ssh
Nov/18/2017 11:40:50 system,error,critical login failure for **user bot** from **111.230.195.101** via ssh
Nov/18/2017 11:40:53 system,error,critical login failure for **user daemon** from **111.230.195.101** via ssh
Nov/18/2017 11:40:55 system,error,critical login failure for **user ts3bot** from **111.230.195.101** via ssh

```
Nov/18/2017 11:40:57 system,error,critical login failure for user dropbox from 111.230.195.101 via ssh
Nov/18/2017 11:41:00 system,error,critical login failure for user from 111.230.195.101 via ssh
Nov/18/2017 11:41:02 system,error,critical login failure for user shoutchast from 111.230.195.101 via ssh
Nov/18/2017 11:41:04 system,error,critical login failure for user jenkins from 111.230.195.101 via ssh
Nov/18/2017 11:41:06 system,error,critical login failure for user testuser from 111.230.195.101 via ssh
Nov/18/2017 11:41:09 system,error,critical login failure for user tester from 111.230.195.101 via ssh
Nov/18/2017 11:41:11 system,error,critical login failure for user test from 111.230.195.101 via ssh
Nov/18/2017 11:41:14 system,error,critical login failure for user test1 from 111.230.195.101 via ssh
Nov/18/2017 11:41:16 system,error,critical login failure for user xbmc from 111.230.195.101 via ssh
Nov/18/2017 11:41:19 system,error,critical login failure for user ansible from 111.230.195.101 via ssh
Nov/18/2017 11:41:21 system,error,critical login failure for user a from 111.230.195.101 via ssh
Nov/18/2017 11:41:23 system,error,critical login failure for user ansible from 111.230.195.101 via ssh
Nov/18/2017 11:41:25 system,error,critical login failure for user z from 111.230.195.101 via ssh
Nov/18/2017 11:41:28 system,error,critical login failure for user user1 from 111.230.195.101 via ssh
Nov/18/2017 11:41:30 system,error,critical login failure for user znc from 111.230.195.101 via ssh
```

Obranou proti on-line lámání hesel může být zamčení účtu po několika neúspěšných pokusech nebo zpomalení vyhodnocování hesel v systému.

Protože je on-line lámání hesel pomalé a relativně snadno zjistitelné, je pro útočníka lepší variantou, pokud se dokáže dostat přímo k heslům uživatelů. Ta by však měla být ukládána ve formě, která neumožní jejich snadné přečtení, tedy v podobě hashe hesla. Pokud útočník hashe získá, má několik možností, jak na ně zaútočit.

Než se pustíme do popisu jednotlivých možností útočníka, je potřeba připomenout, že hash je jednocestná funkce. Útočník tedy vždy postupuje tak, že nejdříve vytvoří z hesla hash a ten pak porovná s hashem získaným útokem. Liší se tedy hlavně způsoby, kterými útočník vybírá vhodné kandidáty na heslo, jehož hash bude porovnáván.

Důležitým pojmem, který souvisí s útoky na hesla, je pojem **keyspace**, který v kryptografii **označuje množinu všech možných klíčů, které konkrétní šifrovací algoritmus může využít**. V případě hesel pak jako keyspace označujeme množství znaků, ze kterých je možné heslo vytvořit. Na české klávesnici máme pro jejich vytvoření k dispozici celkem deset číslic, dvacet šest malých a velkých písmen abecedy a třiatřicet speciálních symbolů.

**Počet možných variací je dán: V (počet variací) = Keyspace^délka hesla**.

Pokud správce po uživatelích vyžaduje pouze hesla složená z malých písmen a maximální možná délka hesla je 7 znaků, pak je počet variací roven $26^7$, což je 8031810176 možných variací.

**V praxi je však po uživatelích vyžadováno použití malých, velkých písmen, čísel a speciálních znaků**[530] **s tím, že je stanovena také nejmenší možná délka hesla**.

Útočník spoléhá na to, že člověk je tvor pohodlný, a proto se bude většina uživatelů snažit naplnit pouze minimální požadavky na heslo, aby si nemuseli pamatovat složitá a dlouhá hesla.

Mezi nejčastější útoky na hashe se řadí:

1) **Útok hrubou silou (Brute force)**
   Při tomto útoku útočník generuje postupně všechna možná hesla, která právě splňují požadavky daného systému na tvorbu hesel. Tento způsob útoku se vyplatí pouze u systémů, které nemají nijak definovanou délku hesla nebo mají na heslo příliš malé nároky. Při dostatečně dlouhém hesle a velkém keyspace může prolomení hesla trvat i řadu let.

   K výběru požadavků na délku hesla a množství znaků nelze přistupovat pouze jako k jednoduché matematické rovnici, kde na jedné straně vstupuje rychlost současných procesorů při generování konkrétního typu hashe a na druhé straně množství variací, které bude muset útočník vyzkoušet. Při útoku se využívají některé další možnosti. Útočníci například při hádání hesel mohou vynechat znaky, o kterých vědí, že jsou mezi uživateli nepopulární (pro české uživatele to jsou znaky z/y a Z/Y, kterým se někteří uživatelé snaží vyhnout kvůli možnému prohození těchto dvou znaků na klávesnicích na různých systémech.). Útočníci také berou v potaz skutečnost, že **mnohdy se uživatelé snaží pouze vyhovět určité politice**, a proto lze očekávat, že číslice a další speciální znaky budou až na konci hesla.

2) **Distribuce útoku na více počítačových systémů v počítačové síti**
   Další možnost útoku představuje distribuce útoku na více počítačových systémů v počítačové síti, v rámci nějž jeden z počítačových systémů řídí práci a rozděluje hesla, která je ještě potřeba vyzkoušet. K tomuto útoku lze využít různé specializované čipové sady. Útočníci zjistili, že pro prolamování hesel jsou velmi dobře využitelné GPU (Graphic Processing Unit) čipy[531], které najdeme v grafických kartách NVIDIA nebo AMD. Pokud se výkon karet zřetězí, může útočník lámat hashe rychlostmi dosahujícími stovek miliard pokusů za sekundu.[532]

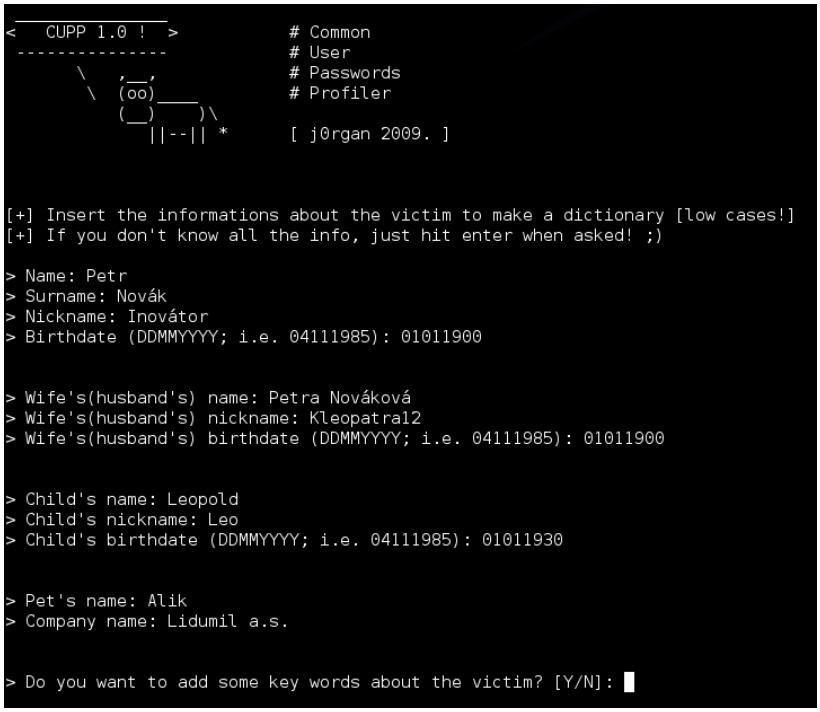
530: Blíže viz § 19 odst. 5 písm. a), b), c) VoKB

531: Viz *Password Cracking with 8x NVIDIA GTX 1080 Ti GPUs*. [online]. [cit. 20. 8. 2017]. Dostupné z: https://www.servethehome.com/password-cracking-with-8x-nvidia-gtx-1080-ti-gpus/

532: Viz *25-GPU cluster cracks every standard Windows password in <6 hours.* [online]. [cit. 20. 8. 2017]. Dostupné z: https://arstechnica.com/information-technology/2012/12/25-gpu-cluster-cracks-every-standard-windows-password-in-6-hours/

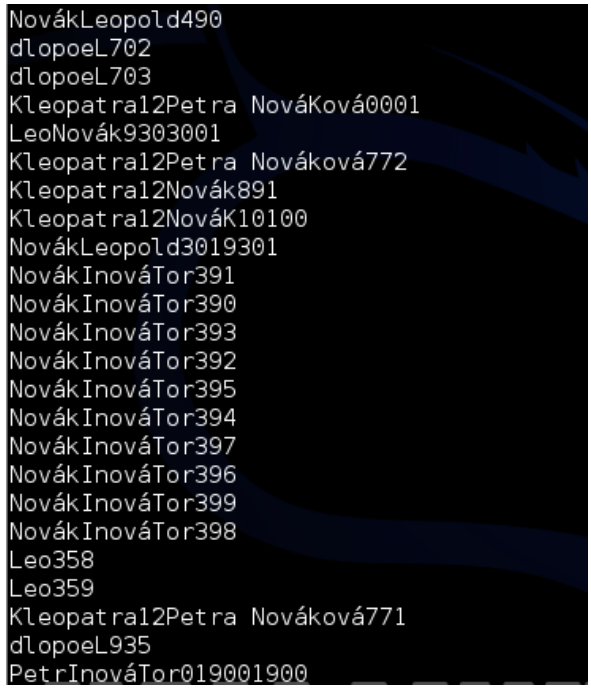
3) **Slovníkový útok**
Algoritmy pro slovníkové útoky počítají s tím, že je potřeba vyzkoušet různé kombinace daného slova. Běžné je zkoušet různé kombinace malých a velkých písmen, přidávat do zkoumaného slova čísla a speciální znaky. Heslo *„PaSSword1."* není tedy z tohoto pohledu o nic bezpečnější než *„password"*. Jeden z velmi známých slovníků, Rockyou[533], je postupně vytvářen s využitím hesel, která unikla z nejrůznějších systémů. Obsahuje tak veliké množství hesel reálně používaných uživateli.

Vedle již existujících slovníků jsou dostupné nástroje, které umožňují vytvořit slovník na míru dle informací, jež má útočník o své oběti. Nástrojem umožňujícím vytvořit specifický slovník dle obsahu webových stránek je například program *cewl*. Jiným nástrojem, který lze využít pro generování slovníku na míru, je program *cupp*. Tento program umí vygenerovat slovník na míru konkrétní osobě, jak můžete vidět na následujícím obrázku.




Obrázek 64: Cupp - zadání informací o osobě

533: Viz *Password dictionary.* [online]. [cit. 21. 8. 2017]. Dostupné z: http://www.kalitut.com/2015/12/best-password-dictionary.html




Obrázek 65: Cupp - ukázka výstupu v podobě slovníku

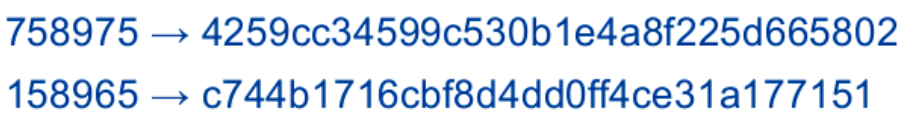
4) **Použití rainbow tables**
Dalším způsobem, který je útočníky používán k získání hesla, je využití rainbow tables.[534]

**Rainbow tables představují pro útočníka vhodný kompromis mezi možností mít hashe předpočítané a být schopen tato data někam uložit.** V případě rainbow tables se kromě hashovacího algoritmu uplatní ještě takzvané redukční funkce. Jejich úkolem je ze získaného hashe opět získat heslo, na které opět použijeme hashovací funkci, na výsledek opět redukční a tak stále dokola. Jako velmi zjednodušený příklad, který však názorně demonstruje celý proces vzniku rainbow tables, si můžeme uvést příklad generování rainbow table pro 6místná hesla a MD5 hash, složená pouze z čísel.

Na začátku je vygenerováno první náhodné heslo 493823, na něj se aplikuje hashovací funkce MD5, čímž získáme hash „*222f00dc4b7f9131c89cff641d1a8c50*“. Redukční funkce pak vybere prvních šest čísel a získáme heslo 222004. Na toto číslo opět aplikujeme hashovací funkci

534: Blíže viz také kap. 6.1.2.5 Bezdrátové sítě

a na výsledek opět funkci redukční. Kolikrát tento cyklus proběhne, je možné programu pro generování rainbow tables určit. Čím více cyklů bude mít jeden průběh, tím méně řádků bude tabulka obsahovat, ale o to déle bude trvat její prohledávání. Takto se postupně vytváří v tabulce záznamy, které vypadají tak, jako na následujícím obrázku.

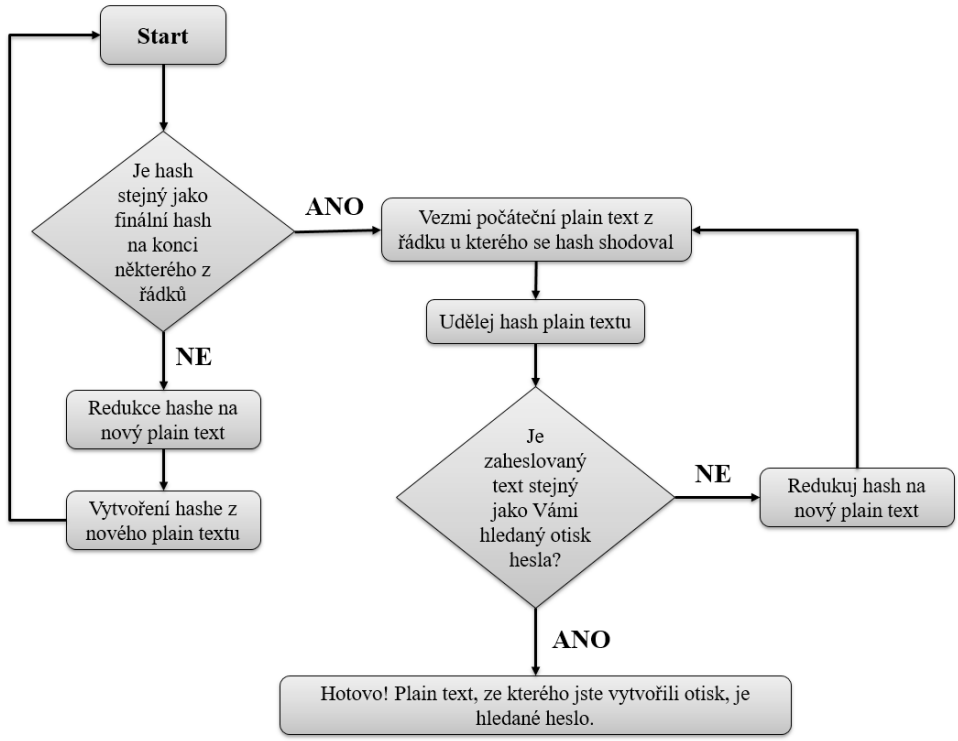



Obrázek 66: Ukázka výsledných řádků v rainbow tables

První sloupec obsahuje vždy výchozí heslo, druhý sloupec pak konečný hash, ke kterému se došlo po proběhnutí přednastaveného počtu cyklů hashování hesel a redukování výsledných hashů. Na dalším řádku je pak opět výsledek stejného procesu.

Snadno by se mohlo stát, že v průběhu hashování a redukování hesla bychom se dostali zpět k číslu 758975 z prvního řádku a došlo by tak ke kolizi, která by vedla k tomu, že bychom zbytečně znovu počítali to, co již bylo v prvním řádku spočítáno. Aby se tomu předešlo, střídá se při generování více redukčních funkcí, což zajistí, že i pokud bychom v dalších řádcích narazili na heslo, které je na našem obrázku jako první, redukční funkce by z něj vytvořila jiné heslo, než tomu bylo v prvním řádku.

Vyhledávací algoritmus pak funguje tak, že vezme hash, pro který chceme získat původní heslo a tento hash porovná s hashi v tabulce. Pokud nic nenalezne, redukuje hash na jiný plaintext a udělá hash tohoto plaintextu. Tento hash opět porovná s hashi v tabulce. Takto celý proces pokračuje, dokud není nalezena shoda. Po té program vezme počáteční heslo z řádku, na kterém nalezl shodný hash a provede tolik hash a redukčních funkcí, až se dostane k heslu, které představoval původně vyhledávaný hash.




Obrázek 67: Algoritmus vyhledávání v rainbow tables

Nejčastěji je jako obrana proti lámání hesel pomocí rainbow tables doporučována technika zvaná variabilní salt. Při ní se před vytvořením hashe přidá k heslu ještě řetězec vygenerovaný systémem. Výsledný hash tedy vznikne například takto SHA2 (salt+heslo). Algoritmus však může být i složitější a salt může do hesla zapracovat i jinak, než jejím pouhým přidáním na začátek či konec. Salt pak můžete uložit do databáze hned vedle výsledného hashe.

Až uživatel zadá heslo, algoritmus k němu přidá salt tak jak má, vytvoří se hash a ten se porovná s tím, který je uložený v databázi. Pokud má každý uživatel odlišný salt, znemožní to útočníkovi smysluplné použití rainbow tables. I z triviálního hesla zadaného uživatelem vznikne při použití dlouhého řetězce salt heslo, které bude mimo běžné možnosti rainbow tables. V kapitole o zabezpečení Wi-Fi sítí bylo upozorňováno na rizika, spojená s použitím defaultního SSID výrobce. Důvodem je, že SSID působí při tvorbě přihlašovacího řetězce jako salt, kvůli které se nevyplatí vytvářet dopředu rainbow tables. Ovšem pouze pokud nemá stejné SSID větší množství sítí.

Ještě je třeba upozornit, že pokud získá útočník databázi a zná i způsob, jakým je kombinován salt a heslo (což obvykle není pro útočníka tak obtížné zjistit), může stále pro lámání hesel použít další zmiňované způsoby, tedy brute force a slovníkový útok. Pouze vždy k heslu, které aktuálně vygeneroval, přidá ještě salt uložený v databázi.

I toto bude ale pro útočníka pomalejší, protože bez položky salt by mu stačilo vygenerovat hash pro aktuálně testované heslo a porovnat jej se všemi otisky napříč databází. To může útočníkovi značně dost urychlit práci, protože například heslo ***12345678*** je mezi uživateli bohužel poměrně populární a v databázi bude nejspíše více uživatelů s otiskem:

***ef797c8118f02dfb649607dd5d3f8c7623048c9c063d532cc95c5ed7a898a64f***

což je SHA – 256 pro zmiňované heslo. Pokud je ale ke každému z těchto hesel přidán originální salt, bude je útočník muset hledat uživatel po uživateli.

Jak již bylo zmíněno, můžete salt uložit do databáze, ale zrovna tak lze generovat například z uživatelského jména a nějakého dalšího parametru, třeba názvu vaší domény. V takovém případě není salt potřeba do databáze ukládat a útočník bude muset přijít na to, jakým způsobem variabilní salt vytváříte.

Pro zabezpečení hesel nejen proti rainbow tables se dnes doporučuje použití funkce *bcrypt*, jejíž použití je momentálně považováno za vysoce bezpečný způsob ukládání hesel a jejíž implementace existují v řadě jazyků, jako jsou C, C#, JavaScript, Perl, Python, PHP a další.

Funkce bcrypt nabízí zajímavý koncept, který spočívá v možnosti tento algoritmus zpomalit. Můžeme totiž nastavit proměnnou, které se v konceptu bcryptu říká *cost*, tedy cena. To v podstatě znamená nastavení náročnosti výpočtu hashe a tedy i doby, po kterou se bude počítat. Uživatel při přihlašování do systému nepozná, že se jeho přihlašování protáhlo o 100 ms, ale útočníkovi to v podstatě znemožní provedení brute force útoku.

S navyšováním výpočetního výkonu budoucích počítačů lze navíc zvyšovat i cost v bcryptu. Bcrypt navíc zvládá i variabilní sůl, chrání tedy i před útoky s pomocí rainbow tables. Výsledný formát hashe, který se bude ukládat, vypadá následovně:

$2a$10$wovOdyW7AxH1mJ/ndSuxIectUDfAvblBIkSqS0oQ862IBz.uABlEm

| | |
|---|---|
| Červená část: | $2a znamená verzi bcryptu. |
| Zelená část: | $10 představuje cost, se kterým byl hash vytvořen. |
| Modrá část: | $wovOdyW7AxH1mJ/ndSuxIe představuje salt. |
| Šedá část: | ctUDfAvblBIkSqS0oQ862IBz.uABlEm je samotný hash hesla. |

Kromě samotného způsobu zabezpečení uložených hesel je třeba se zabývat i otázkou vynucování kvality hesel a stanovení politik pro nakládání s hesly.

Je vhodné mít v organizaci zavedenu politiku tvorby a uchovávání hesel, neboť může uživatelům pomoci zjistit, že při tvorbě a péči o heslo chybují. Zajištění vyšší úrovně bezpečnosti u koncových uživatelů může pomoci zvýšit úroveň bezpečnosti organizace jako takové. Druhým faktorem pro implementaci uvedených politik je i možnost, že v případě prokazatelného seznámení se s politikou ze strany uživatele je vůči němu možné vyvodit odpovědnost v případě, že bude při vyšetřování incidentu zjištěno, že k němu došlo z důvodu nedodržení této politiky.

Politika by měla uživatelům připomenout, že nesmí své heslo nikomu sdělit, že jej musí zadávat vždy tak, aby jej jiná osoba nemohla v dané chvíli odpozorovat, že by neměli používat stejná hesla pro pracovní a soukromé účely, případně jaké jsou akceptované nástroje pro ukládání hesel. Pokud uživatel využívá velké množství aplikací a systémů vyžadujících ověření pomocí hesla je vhodné využít některého správce přihlašovacích údajů, jako je například program KeePass.[535]

Pokud jde o kvalitu hesel, ukazuje se, že klasický přístup, uživateli, vyber si dvě velká, dvě malá písmena, číslo a speciální znak a heslo musí být aspoň x znaků dlouhé, vede k používání hesel, která jsou pro útočníky snadno prolomitelná. Stačí si projít text výše a je jasné, že heslo typu pepa1256 při slovníkovém útoku dlouho neobstojí.

Rejthar se věnoval analýze hesel[536], která unikla z jednoho českého e-shopu, a dospěl k následujícím výsledkům:

- ¼ uživatelů měla **heslo 8 znaků dlouhé**,
- ¼ uživatelů měla **heslo kratší než 8 znaků**,
- většina hesel, která obsahují číslice, je mají **na konci**,

535: Blíže viz: https://keepass.info/

536: Viz *Jak se Češi s hesly potýkají: analýza 16 tisíc ukradených hesel.* [online]. [cit. 4. 9. 2017]. Dostupné z: https://www.root.cz/clanky/jak-se-cesi-s-hesly-potykaji-analyza-16-tisic-ukradenych-hesel/

- nezanedbatelná část uživatelů použije **v heslu několik písmen z uživatelského jména,**
- **nejoblíbenější speciální znak** uživatelů **je tečka a** čtvrtina z těch, kteří si ji oblíbili, ji umístí **na konec hesla**.

Právě kvůli jisté schematičnosti při tvorbě hesel, ale i kvůli obtížnosti jejich zapamatování, například v případě nucení uživatelů k jejich časté změně, dochází postupně k revidování zažitých pravidel. Mnoho významných služeb dnes především spoléhá na dvoufaktorovou autentizaci. Díky rozšířenosti mobilních telefonů, které lze pro toto zabezpečení využít, totiž nevyžaduje od uživatelů pořízení dalšího dodatečného hardwaru.

Pokud jde o samotná pravidla pro tvorbu hesel a jejich obměnu, například americká organizace NIST (National Institute of Standards and Technology) připravila nová doporučení[537] pro správu digitální identity, ve které se této problematice obšírně věnuje.

Tato organizace například nedoporučuje vynucování změny hesla, pokud k tomu není důvod, nebo si ji nepřeje sám uživatel. Místo kontroly složitosti hesla doporučuje spíše kontrolovat hesla podle slovníků, databází uniklých hesel, nebo zda neobsahují signifikantní části uživatelského jména, název služby a podobně. Tento dokument může být vhodným vodítkem při definování požadavků na uživatelská hesla i politiku práce s nimi. Jako u všech pravidel, i zde je potřeba zvážit jednotlivé požadavky a smysluplnou realizovatelnost jejich nasazení v kontextu dané služby, aplikace či organizace.

Pro webové aplikace lze také využít unikátní českou službu mojeID.[538] Ta umožňuje správci propojení webové aplikace se službou, která dovoluje uživatelům zřídit si a centrálně spravovat svoji Internetovou identitu. Využití služby moje ID webové aplikaci přináší větší úroveň zabezpečení, neboť uživatelé této služby mají k dispozici kromě klasické možnosti jména a hesla také možnost používat jednorázové heslo, nebo se přihlašovat pomocí digitálního certifikátu.

537: Viz *Digital Identity Guidelines.* [online]. [cit. 4. 9. 2017]. Dostupné z: https://pages.nist.gov/800-63-3/sp800-63b.html#sec5

538: **mojeID** je služba, díky níž mají uživatelé českého Internetu možnost používat pro přihlašování na různé internetové stránky a k různým webovým službám jednotné identifikační údaje (uživatelské jméno a heslo). S využitím mojeID není potřeba zakládat vždy nový účet a procházet opakovaně procesem registrace. mojeID umožňuje udržovat údaje o jeho držiteli na jednom bezpečném místě a stále aktuální. mojeID je možné využívat u všech služeb, jejichž provozovatelé podporují přímo službu mojeID či alespoň technologii OpenID. Více informací o této službě je k dispozici na internetové adrese www.mojeid.cz. Služba je pro koncové uživatele poskytována zdarma.
Více též na: https://www.mojeid.cz/page/1860/vyhody-pro-vas-web/

### 6.2.4 Logy a logování

Důležitou součástí bezpečného provozu systémů, služeb a aplikací je zaznamenávání informací o jejich činnosti a běhu, tzv. logování. Záznamy mohou být ukládány ve formě prostého textového souboru, ale mohou být také ukládány do databázového souboru. Existuje řada různých formátů, ve kterých jsou data ukládána, nejčastěji ve formátu syslog, textovém formátu (XML, CSV, W3C), ale můžeme se setkat i s logováním v binární podobě.

Úroveň detailu logování je dána možnostmi dané aplikace či systému. Často je možné nastavit několik různých úrovní logování, podle aktuální potřeby administrátora. Je potřeba si uvědomit, že ačkoliv by se mohlo zdát nejvýhodnější logovat veškeré události, které je aplikace schopna zaznamenat, není to obvykle v reálném provozu žádoucí. Příliš detailní logování znamená zvýšenou zátěž výpočetního systému a zároveň generuje více dat, která je potřeba uložit. Nastavení úrovně logování je proto potřeba pečlivě zvážit.

Z pohledu bezpečnosti musí vlastní implementaci logování předcházet rozvaha, ze které bychom měli zjistit, jaké bezpečnostní události či bezpečnostní incidenty poskytované služby, počítačové systémy či sítě ohrožují. Z této analýzy je následně možné vydefinovat, které data a informace je potřeba logovat, aby bylo možné zjistit, že k bezpečnostní události či incidentu došlo, jakož i zjistit zdroj škodlivé aktivity (např. úmyslná lidská činnost, incident způsobený selháním jiného počítačového systému v síti aj.).

**Příklad:** *Pokud se bude jednat o jednoduché webové stránky, které nerozeznávají jednotlivé uživatele, bude nás minimálně zajímat IP adresa, ze které uživatel přistupoval, prováděná akce a přesný čas a datum. V případě lokální aplikace využívané více uživateli nás bude zajímat identifikace aktuálně přihlášeného uživatele, provedená akce a opět přesný čas a datum.*

Důležitou podmínkou pro správné vyhodnocení logů a pro jejich další využití při odhalování sledu událostí je správně nastavený systémový čas. Pro správné nastavení systémového času na všech spravovaných serverech nelze než doporučit využití protokolu NTP [539], který zajistí, že čas bude správně synchronizovaný na všech systémech v síti.

Logy aplikací i systémů mohou být ukládány lokálně, nebo na centrální *log server*. Výhodou centrálního ukládání logů je především možnost jejich snadnější analýzy, především pomocí různých nástrojů, které umožňují automatizaci těchto analýz. Nástroje typu SIEM umí z logů odhalit nejen pokus o útok na jeden ze serverů, ale díky korelaci dat z logů více systémů a aplikací mohou odhalit i sofistikovanější útok, útočící na více různých počítačových systémů.

539: Network Time Protocol – Protokol pro synchronizaci času

Centrální log server také snižuje některá rizika, spojená s logováním. V případě prohledávání logů nezatěžujete server, který je používán k obsluze uživatelů, logy jsou chráněny proti ztrátě, v případě úplného pádu serveru máte možnost zjistit, co tomuto pádu předcházelo, a také nehrozí, že by došlo k zaplnění pevného disku na produkčním serveru.

V případě potřeby je také možné informace zasílané na centrální log server šifrovat a vzniklé soubory s logy podepisovat.

### 6.2.5 Zabezpečení důvěrnosti a integrity přenášených dat

Pokud jsou data mezi uživatelem a počítačovými systémy či službami přenášena po počítačové síti, je potřeba věnovat pozornost i otázce zabezpečení důvěrnosti a integrity dat. K vlastnímu zabezpečení dat jsou používány různé kryptografické protokoly. Mezi nejznámější patří protokol Transport Layer Security (TLS) využívající asymetrickou kryptografii.

Protokol TLS umožňuje provést autentizaci obou koncových bodů, tedy uživatele (resp. jeho počítačového systému) i serveru a zároveň šifrováním přenášených dat zajišťuje jejich důvěrnost a integritu. Nutno říci, že ve většině případů je prováděna pouze autentizace serveru, díky které uživatel ví, že komunikuje se správným serverem. Pokud to však situace vyžaduje, je možné provést i ověření uživatele vůči serveru. TLS je postaveno na využití certifikátů, které jsou podepisovány certifikačními autoritami. Jedná se v podstatě o přenesení důvěry, kdy klient spoléhá, že certifikační autorita, které důvěřuje, ověřila informace, které jsou v certifikátu uvedeny, tedy například jméno serveru, instituce, která službu provozuje, nebo v případě e-mailové komunikace totožnost uživatele, který podepsaným certifikátem disponuje.

Postup při navazování komunikace mezi koncovým počítačovým systémem a serverem probíhá v několika krocích. Nejprve se koncový počítačový systém a server dohodnou na používaných algoritmech. Následně server zašle tomuto počítačovému systému svůj certifikát, který obsahuje veřejný klíč serveru, jméno serveru a informace o certifikační autoritě, která certifikát podepsala.

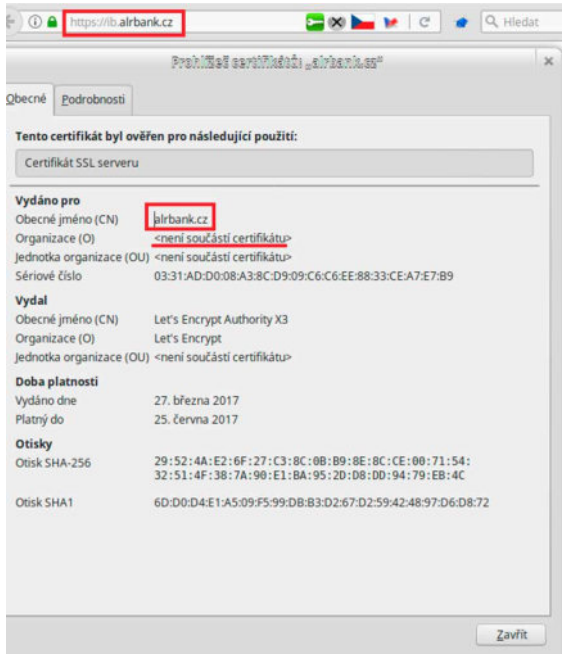
Pokud koncový počítačový systém považuje certifikační autoritu za důvěryhodnou, zkontroluje správnost podpisu certifikátu zaslaného serverem, a tím dojde k ověření identity serveru. Následně koncový počítačový systém zašle serveru náhodná data, která jsou šifrována pomocí veřejného klíče, který byl součástí zaslaného certifikátu. Důležité je, že tato data dokáže dešifrovat pouze server s pomocí příslušného privátního klíče.

Server odpoví také náhodnými daty. Server a koncový počítačový systém předem dohodnutým algoritmem zkombinují náhodná data a použijí na ně dohodnutou funkci pro odvození klíče. Tímto způsobem dojde k vytvoření klíče, který znají jen koncový počítačový systém a server a ten pak již dále používají pro výměnu dat s pomocí symetrické kryptografie.

Do nedávné doby bylo získání certifikátu relativně finančně náročné a doprovázené složitou procedurou ověřování oprávněnosti daného požadavku. Od konce roku 2015 je možné získat certifikát pro doménu zcela zdarma a bez složitých procedur. Jedná se o certifikáty vystavené na základě takzvaného doménového ověření certifikační autoritou *Let's Encrypt*.

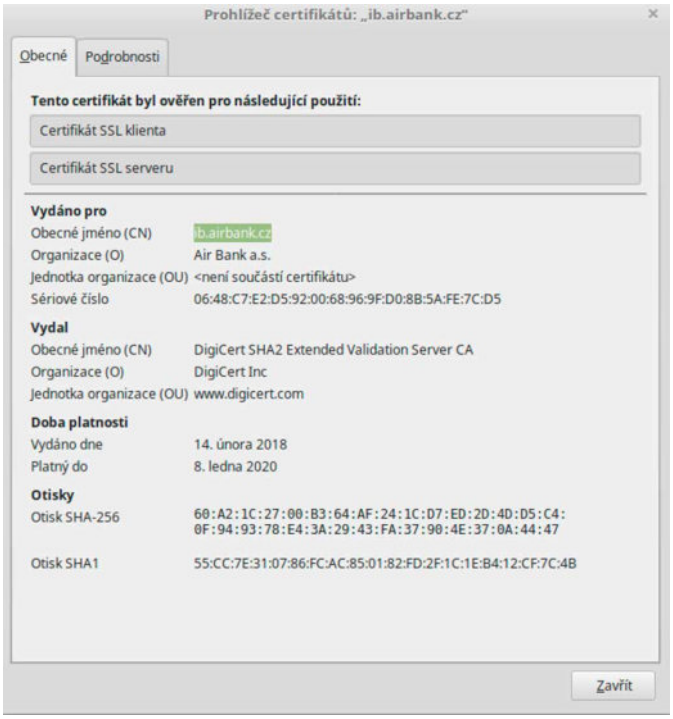
V případě certifikátů od Let's Encrypt se neověřuje název organizace, která doménu drží, ale pouze to, že subjekt, který o doménu požádal, je schopen spravovat server, na který je doménové jméno směrováno. Certifikáty jsou na rozdíl od placených certifikátů, které bývají obvykle vystavovány na více let, platné pouze po dobu tří měsíců, avšak celý proces vystavení certifikátu je možné automatizovat.

Certifikát od Let's Encrypt zajistí, že komunikace s uživateli systému či služby bude šifrována a uživatel zároveň ví, že komunikuje se serverem, pro který byl certifikát vystaven. Pro systémy či služby, u kterých hrozí pokusy o phishingový útok, může být vhodnější využití certifikátů, u kterých je prováděno i ověření organizace, která je držitelem domény. V takovém případě se název organizace zobrazí v informacích o certifikátu a uživatel tak má možnost zjistit, pro koho byla doména vydána. Příkladem může být následující webová stránka, která byla před časem nahlášena národnímu CSIRT týmu jako podezřelá.




Obrázek 68: Falešný certifikát

V certifikátu, který je vystaven pro doménu *ib.alrbank.cz*, zcela chybí informace o organizaci, která by měla být držitelem tohoto doménového jména. Oproti tomu certifikát legitimní stránky společnosti vypadá následovně.




Obrázek 69: Pravý certifikát

### 6.2.6 Zranitelnosti

Zranitelností se rozumí chyba v programu či systému, jejímž důsledkem je snížení úrovně zabezpečení daného systému. Zranitelnosti se vyskytují v operačních systémech, uživatelských programech, serverových aplikacích, ale i ve firmware a operačních systémech nejrůznějších routerů, switchů, IoT aj.

V širším pojetí se také hovoří o zranitelnostech i v případě hardwaru, sítí, organizačních opatření, fyzického zabezpečení, nebo personální bezpečnosti.

Z praktického pohledu lze zranitelnosti rozdělit do dvou zásadních skupin:

1) **Zranitelnosti, pro něž ještě nebyly vydány opravné záplaty.**
   Těmto zranitelnostem se říká zranitelnosti nultého dne (**Zero-Day Vulnerabilities**) a z pohledu potenciálních útočníků jsou nejvíce cenné. Tím, že pro tyto zranitelnosti neexistují v dané chvíli záplaty, získává útočník značnou výhodu. Pokud se informace o takovéto zranitelnosti stanou veřejně dostupnými, je vždy potřeba hledat řešení, které zabrání potenciálnímu útoku. Rozsah opatření závisí na konkrétní zranitelnosti. Může se jednat například o změnu konkrétní konfigurace, o které se ví, že umožňuje úspěšný útok, až po úplné zakázání používání zranitelné aplikace v organizaci až do vydání opravných záplat.

2) **Zranitelnosti, pro které již byly vydány záplaty.**
   I přes dostupnost záplat vždy zůstává určité množství systémů či aplikací, na kterých nebyly záplaty implementovány. Důvodů může být celá řada, od celkem racionálních, až po obyčejnou lidskou lenost a pohodlnost. Odhaduje se, že útoky s využitím zranitelností nultého dne tvoří maximálně několik procent z celkového množství útoků na Internetu.

   Z tohoto důvodu je zajištění pravidelné aplikace dostupných záplat na veškeré systémy jednou z vašich priorit kybernetické bezpečnosti v organizaci. V případě implementace záplat na důležité služby a systémy se doporučuje otestovat nové záplaty v rámci testovacího prostředí a teprve po otestování je aplikovat do produkčního prostředí.

**Příklad:** *Podstatu jednoho typu zranitelností představíme na tzv. Persistentním XSS. Představme si, že máme webové fórum, kam mohou uživatelé psát své názory. Pokud programátor neošetří, aby nebylo možné do diskuzního fóra vkládat HTML tagy, pak může útočník vložit například následující příspěvek.*

*Ahoj, co si myslíte* `<script>nebezpecnykod</script>` *o tom novém automobilu?*

*Nebezpečný kód pak může například získávat z prohlížeče návštěvníků uložené cookies a odesílat je na server útočníka, nebo může za přihlášeného uživatele provádět změny v nastavení aplikace, manipulovat s obsahem stránky, nebo přesměrovat uživatele na jiný web. Omezení zde plynou z možností samotného javascriptu.*

*Celý příspěvek útočníka se uloží do databáze aplikace a server jej při každé návštěvě příslušné stránky diskuzního fóra odešle prohlížeči uživatele, který si obsah stránky vyžádal. Protože však tag* `<script>` *z pohledu prohlížeče obsahuje kód, který se má vykonat, uživateli se v prohlížeči zobrazí vše následovně:*

***Ahoj, co si myslíte o tom novém automobilu?***

*Prohlížeč uživatele však zároveň vykoná instrukce obsažené ve vloženém skriptu.*

## 6.3 Ochrana koncových počítačových systémů

Velká část bezpečnostních prvků majících vliv na bezpečnost koncových počítačových systémů byla rozebrána v rámci předchozích kapitol. V této kapitole budou tyto prvky připomenuty a doplněny o nové dosud nepopsané aspekty.

Tak, jak je doporučováno nasazení firewallu na rozhraní sítě a nasazení antiviru a antispamu v místech, kde dochází k přenosu dat, je třeba myslet na tato opatření také na koncových počítačových systémech. Byť by se mohlo zdát, že se jedná o nadbytečné opatření, není tomu tak hned z několika důvodů.

První z nich je, že bezpečnost je otázkou více vrstev a jednotlivá opatření je nutno zvažovat v kontextu celého chráněného systému i v kontextu ostatních bezpečnostních opatření. V případě, kdy by z nějakého důvodu došlo k selhání některého z opatření, mohou tuto funkci přebrat opatření další (např. i na koncovém počítačovém systému).

Dalším důvodem je značná mobilita počítačových systémů, které jsou v dnešní době standardně používány (např. mobilní telefony, tablety, notebooky aj.). Tyto počítačové systémy jsou zpravidla ve výlučné dispozici uživatelů a jsou využívány v různých počítačových sítích.

Dalším argumentem, a to především v případě antivirů, může být skutečnost, že každý výrobce používá svou databázi škodlivých vzorků, přičemž se mohou lišit i způsoby plnění této databáze (s čímž souvisí rychlost přidávání nových vzorků) a také algoritmy používané pro heuristickou analýzu (schopnost rozpoznat i škodlivý kód, který zatím nebyl identifikován). Podobně to platí i pro lokální antispamová řešení, ta jsou ale často součástí používaných poštovních klientů.

Vzhledem k prudkému nárůstu ransomware, ke kterému došlo v posledních letech, stojí kromě klasických antivirů za zmínku také specializované nástroje, které se zabývají ochranou proti tomuto druhu malware. Tyto nástroje kombinují různé přístupy, od detekce podezřelého chování spuštěných procesů, přes omezení přístupu k určeným adresářům pouze na známé, povolené programy.

Další důležitou součástí ochrany koncových počítačových systémů je ochrana dat, která jsou na nich uložena. Typicky se jedná o šifrování obsahu disků.

Existuje celá řada komerčních i bezplatných a open-source řešení, umožňujících šifrování disků. Je možné jak šifrovat celý obsah disku, tedy včetně dat operačního systému, tak jen domovský adresář uživatele nebo konkrétní adresáře a soubory. Šifrování celého disku je náročnější na systémové prostředky, na druhou stranu chrání systém i proti pozměnění systémových souborů, pokud není dostatečně zajištěna fyzická bezpečnost zařízení. Pokud by tedy útočník získal

přístup k počítačovému systému a nabootoval z jiného média, nedokázal by například vyměnit spustitelný systémový soubor za soubor s připojeným malware.

Další z možností ochrany dat na paměťových médiích je nastavení hesla pro toto médium v BIOSu nebo UEFI. Takto vytvořené heslo brání v přístupu k obsahu paměťového média, a dokud není zadáno, není možné se k datům dostat. Samotné heslo je uložené ve firmware paměťového média. Pokud je toto médium zapojeno do jiného počítačového systému, ochrana dat zůstává a heslo je pro přístup k těmto datům stále vyžadováno. Je však třeba uvést, že v tomto případě nejsou samotná data na paměťovém médiu šifrována, pouze se k nim bez znalosti hesla nelze dostat.

Tento způsob ochrany není tak spolehlivý jako šifrování, neboť různé forenzní nástroje či výrobci paměťových médií nabízejí možnost odstranit toto heslo a získat tak přístup k datům.

Další součástí ochrany koncových stanic tvoří ochrana proti neautorizovanému připojování externích zařízení[540] a kontrola obsahu přenášeného po počítačové síti.[541]

## 6.4 Vzdálený přístup k počítačovým systémům

V dnešní době patří vzdálený přístup k neodmyslitelné součásti využívání informačních a komunikačních technologií. Vzdálený přístup v sobě zahrnuje řízení a konfiguraci vzdálených počítačových systémů, řešení požadavku uživatele bez nutnosti osobně být u uživatelova počítačového systému aj. Využívání vzdálených přístupů k počítačovým systémům umožňuje efektivněji využívat finanční i lidské zdroje. Na druhou stranu nesprávně řešený vzdálený přístup může znamenat značné bezpečnostní riziko.

Z historického hlediska se dosud lze setkat s protokolem **Telnet.** Tento nešifrovaný protokol slouží k přístupu na textové rozhraní ovládaného počítačového systému (koncový počítač, server, router aj.). Použití tohoto protokolu není v současné době vhodné, neboť veškerá komunikace, v rámci které je odesláno jméno a heslo pro přihlášení, je nešifrovaná.

Protokol Telnet je stále častěji nahrazován novějším protokolem **SSH**, který posílá hesla šifrovanou cestou. Tento protokol také umožňuje přihlašování i SSH klíčem, tedy bez nutnosti zadávat heslo. K přihlašování je také možné použít i jednorázové heslo (One Time Password -OTP), čipovou kartu, tzv. yubikey či libovolnou kombinaci výše jmenovaného. Protokol SSH také obsahuje mechanizmy proti útokům typu man-in-the-middle a důrazně upozorní, že se

540: Blíže viz kap. 5.4.3 Ochrana před připojením cizích periferií k počítačovým systémům

541: Blíže viz kap. 6.1 Ochrana sítí

místo očekávaného počítačového systému připojil systém jiný. Protokol SSH též umožňuje přenos souborů, vytváření síťových tunelů či spouštění a ovládání grafických aplikací.

Pro správu počítačových systémů s OS Windows je často využíván protokol **RDP** (Remote Desktop Protocol – vzdálená plocha). Jelikož byl RDP během své historie častým terčem kybernetických útoků, nelze zcela jeho použití na Internetu doporučit. Nicméně pro konfigurace na úrovni lokální sítě má zásadní význam.

Dalším užívaným nástrojem je aplikace **TeamViewer**, která je pro osobní použití poskytována zdarma. TeamViewer je považován za relativně bezpečný, zvláště díky faktu, že nepotřebuje mít na lokálním počítači otevřený síťový port. Ke zvážení zůstává riziko představované třetí stranou, a sice výrobcem programu TeamViewer. To vychází z úvahy, že všechna data tečou (mohou téci) přes něj.

Zejména z bezpečnostních důvodů se stále častěji v organizacích dochází k závěrům, že řada služeb by neměla být veřejně dostupná v prostředí Internetu. Na druhou stranu naopak vyvstává potřeba pracovat i mimo organizaci. Obdobně tomu je i v případě dislokovaných poboček, které potřebují přístup k síťovým službám, které jsou zvenku organizace nedostupné. Pro výše uvedené situace jsou využívány služby **VPN** (Virtual Private Network – virtuální privátní síť).

Virtuální privátní síť umožňuje vytvoření virtuální počítačové sítě nad sítí klasickou. Tím dovoluje zpravidla zajistit autenticitu a důvěrnost dat. Uživatelé tak mají možnost se připojit do počítačové sítě organizace či může dojít k propojení jednotlivých poboček, a to velmi bezpečným způsobem. Veškerá data jsou v rámci VPN přenášena šifrovaným tunelem.

Ještě donedávna se pro VPN používal protokol MS-CHAP-v2. Z dnešního pohledu je však považován za zastaralý a obsahující několik slabin. Tento protokol je založený na Challenge Handshake Authentication Protocol (CHAP), což znamená, že VPN server musí mít uložená hesla svých uživatelů v čitelné podobě. Z dnešního hlediska se takovýto přístup k heslům považuje za bezpečnostní riziko.

Aktuálně nad ostatní komerční řešení výrazně vystupuje **OpenVPN server**, což je open source řešení nabízející širokou škálu autentizačních protokolů. Běžně se však používají RSA certifikáty s dostatečnou délkou klíče (dnes již alespoň 4 096 bitů) pro autentizaci a 256 bit AES-CBC pro šifrování dat. Největší nevýhodou OpenVPN je potřeba bezpečně a kvalitně vygenerovat privátní a veřejný klíč, následně požádat o vydání certifikátu, který je nutné doručit na certifikační autoritu. Tam je třeba certifikát podepsat a dodat zpět uživateli.

Praxe posledních let, kdy bylo zaznamenáno několik závažných incidentů[542] v souvislosti se vzdálenou správou, ukazuje, že se nelze spoléhat pouze na jednu vrstvu zabezpečení, tedy například nakonfigurovat na serveru RDP a nechat příslušný port dostupný z Internetu.

Za vhodné řešení nelze považovat ani přesunutí portu služby pro vzdálený přístup na jiný port, jako se to někdy dělá například v případě SSH. Takovýmto přesunem je sice možné se bránit plošným skenům hledajícím dostupné porty konkrétní služby, ale při důkladnějším skenování daného počítačového systému útočník rychle odhalí, že se jedná o službu pro vzdálený přístup, pouze na jiném portu. Kromě chyby uživatele či administrátora může dojít k útoku například i díky nalezené zranitelnosti daného systému.

Z tohoto důvodu je vhodné skrýt rozhraní umožňující vzdálený přístup k počítačovému systému za další bezpečnostní prvek. Nejčastěji se k tomuto účelu využívá VPN.

Pokud z nějakého důvodu nemáte možnost využívat VPN, stále existují způsoby, jak potenciálnímu útočníkovi jeho postup ztížit až znemožnit. Pokud víte, že pro vzdálený přístup využíváte jen připojení z konkrétních IP adres, můžete omezit přístup k dané službě pouze na tyto IP adresy. Další variantou je pak využití metody port knocking (klepání na porty).

Port knocking umožňuje nastavit na firewallu taková pravidla, díky nimž dojde k otevření konkrétního portu až po odeslání „PINu". Tímto PINem či heslem je speciální, předem nastavená sekvence zaslaných dat odeslaných na konkrétní porty. Může se skládat z libovolného počtu paketů různých protokolů (TCP, UDP a další) zaslaných na konkrétní čísla portů takto chráněného systému. Díky port knockingu tak může být daný systém při skenování portů útočníkem zcela netečný a útočník vůbec netuší, že na daném počítačovém systému je provozována například služba SSH. Pouze pokud administrátor odešle předem definovaná data, dojde k otevření potřebného portu a administrátor se může na službu SSH připojit.

Je třeba říci, že port knocking je náchylný na možné odchycení zasílané sekvence a její opakování útočníkem, pokud bude mít útočník vhodnou pozici pro její zachycení. Opět proto platí, že se nelze spoléhat pouze na tuto vrstvu a SSH skryté za tímto mechanismem musí být správně a bezpečně nakonfigurováno.

542: Viz např. *Statement on Ransomware Infections via TeamViewer.* [online]. [cit. 7. 8. 2018]. Dostupné z: https://www.teamviewer.com/en/company/press/statement-on-ransomware-infections-via-teamviewer/ nebo *Analýza napadení ransomware: stačí otevřený port RDP a slabé heslo.* [online]. [cit. 7. 8. 2018]. Dostupné z: https://www.root.cz/clanky/analyza-napadeni-ransomware-staci-otevreny-port-rdp-a-slabe-heslo/

## 6.5 Paměťová média

Otázku nakládání s paměťovými médii lze rozdělit do dvou primárních oblastí:

- **bezpečné mazání dat a likvidace starých paměťových médií,**
- **bezpečnost uložených dat.**

Problematika bezpečného smazání souborů začíná již u interakce mezi uživatelem a operačním systémem. Běžný uživatel považuje soubor za smazaný ve chvíli, kdy ho „vyhodí do koše". Pokročilejší uživatel má za to, že soubor je smazaný v momentě, kdy „vysype koš". Ještě pokročilejší uživatel žije v domnění, že soubory jsou skutečně smazány při formátování disku. Avšak soustředíme-li se na magnetické disky, je skutečnost taková, že po vysypání souboru z koše dojde pouze ke smazání záznamu o existenci souboru a jiných metadat. V tu chvíli tedy systém přestane mít k dispozici informaci o názvu souboru, datu vytvoření (změny, přístupu apod.) a jeho fyzickém umístění na disku. V tomto momentě lze soubor zachránit například nalezením starší/záložní tabulky souborů (MFT), kde tato informace smazána nebyla. Kdyby tato možnost selhala, je možné soubor najít podle jeho hlavičky.

Každý typ souboru má na svém začátku hlavičku, podle které lze rozpoznat typ souboru. Například soubor typu .docx má na svém začátku řetězec bajtů „*50 4B 03 04*". Pokud se tedy při prohledávání disku narazí na sektor začínající touto sekvencí, je velmi pravděpodobné, že následující data dávají dohromady textový dokument. Právě na tomto principu funguje software sloužící k záchraně smazaných dat. Nutno podotknout, že takto smazaný soubor je možné obnovit pouze do chvíle, než dojde k jeho přepsání jiným souborem. Tím se dostáváme k problematice **bezpečné**ho **smazání dat**.

Pevný disk určený k likvidaci, který obsahuje či obsahoval citlivá data, je zapotřebí kompletně celý přepsat, aby byla data skutečně bezpečně smazána. Již prvním přepsáním se zajistí, že data nepůjdou zachránit pomocí běžně dostupného softwaru. Existuje však podezření, že data je možno částečně obnovit na základě zbytkového magnetismu. Proto se v případě obzvlášť citlivých dat doporučuje přepsat celý disk několikrát, a to pomocí jak nul a jedniček, tak i náhodných dat.

Odlišně je třeba přistupovat k nemagnetickým paměťovým médiím jako flash disky a SSD disky. Vzhledem k faktu, že SSD disky mají omezený počet zápisů do jednotlivých paměťových buněk, byl za účelem prodloužení životnosti zařízení pozměněn způsob ukládání dat. Pro zlepšení spolupráce s operačním systémem byl do těchto disků přidán příkaz TRIM, kterým může operační systém SSD disku oznámit, které sektory považuje za volné. Díky dostatku volných sektorů pak může vnitřní logika SSD disku rozkládat zátěž tak, aby k opotřebení jednotlivých buněk docházelo rovnoměrně. Důsledkem je to, že „smazaný" soubor může být nevratně ztracen podstatně dříve než u disků magnetických.

Avšak i přes všechnu moderní techniku zůstává jako prostředek pro nejbezpečnější a definitivní smazání dat fyzická nevratná destrukce paměťového média. Existují také společnosti, které garantují, že provedou spolehlivou a bezpečnou likvidaci paměťových médií za vás. Tyto společnosti používají různé formy mechanické a chemické likvidace, případně takzvané magnetické pece, které trvale zlikvidují všechna data pomocí elektromagnetického pulzu.

Pro potlačení či snížení rizika úniku dat při ztracení, ukradení či infekci paměťových médií je vhodné používat **šifrování dat**. To je možné provádět na několika úrovních včetně jejich případné kombinace. Mezi možnosti patří šifrování souboru, šifrování oddílu na disku a šifrování celého disku.

Byť může šifrování výrazně snížit pravděpodobnost zásahu do dat, je třeba si uvědomit, že ochrana zašifrovaných dat bezprostředně závisí na složitosti použitého hesla. Útočník při získání zašifrovaných dat totiž může zkoušet libovolné kombinace tak rychle, jak mu to počítačový systém dovolí. Pro tyto účely je tedy nutné mít silné heslo.

Krom hesla také závisí ochrana zašifrovaných dat na algoritmu použitém k šifrování. V dnešní době se nejčastěji doporučuje AES s délkou bloku 256 bitů. Například DES i 3DES jsou z dnešního pohledu pro tyto účely již zastaralé algoritmy. K použitému algoritmu je ovšem třeba definovat i způsob použití. Mezi ty patří například CTR (Counter), ECB (Electronic Code Book), CBC (Cipher Block Chaining) a XTS.

Každý z těchto režimů má své výhody, nevýhody či slabiny v případě špatného použití. Zatímco ještě před pár lety se pro šifrování používal mód CBC, dnes již moderní nástroje přešly na užívání bezpečnějšího XTS. Ten se používá například pro šifrování disků v systémech založených na OS Linux používajícím nástroj cryptsetup.

Zapotřebí je také bezpečná implementace použitého algoritmu. Špatnou implementací mohou být průběh algoritmu nebo i některé informace (ať už o obsahu šifrovaných dokumentů nebo dokonce o klíči) vyzrazeny.

Šifrování bude pravděpodobně v budoucnu ovlivněno i kvantovými počítači, které dokáží některé úlohy řešit výrazně rychleji. Často se například hovoří o možném prolomení RSA, avšak podle současných znalostí by u AES mělo dojít pouze k jeho oslabení.

## 6.6 Správa a dohled nad počítačovou sítí

Každý správce by měl mít přehled o tom, co se v jeho počítačové síti odehrává, jaký je stav služeb a počítačových systémů a zda nehrozí situace, která by mohla ohrozit bezpečný provoz sítě,

koncových počítačových systémů a serverů. Jedním z nástrojů, které k výkonu správy a dohledu nad počítačovou sítí slouží, je logování.[543]

Kromě logování je však možné využít nástroje, které budou monitorovat jednotlivé systémy a předávat informace o jejich aktuálním stavu. V závislosti na konkrétním nástroji lze monitorovat dostupnost systémů a služeb na nich běžících, běh procesů přímo na serveru, či je možné nastavit varování pokud load serveru dosáhne určité hodnoty atd.

Velcí výrobci hardwaru také často nabízejí vlastní nástroje pro monitoring svých produktů s využitím SNMP protokolu. Díky těmto nástrojům se správce může včas dozvědět například o problémech disku v diskovém poli, nebo například o docházejícím toneru v tiskárně.

Velmi důležitou součástí moderních serverových řešení jsou nástroje pro vzdálenou správu serveru, které umožňují spravovat server na dálku. S jejich pomocí lze například restartovat server, pokud samotný operační systém přestane reagovat, lze se připojit na vzdálenou obrazovku i v případě, že není možné se vzdáleně přihlásit k operačnímu systému a s pomocí těchto nástrojů je také možné instalovat operační systém na dálku. Možnosti vzdáleného přístupu se u jednotlivých výrobců liší.

Z pohledu bezpečnosti stojí za zmínku, že tato zařízení dnes umožňují jak použití dvoufaktorové autentizace, tak je některé možné propojit na Active Directory či LDAP. Pro zvýšení bezpečnosti se také doporučuje umístit tato zařízení do dedikované VLANy, kam nemají přístup běžní uživatelé a která je určena pouze pro vzdálený management serverů.

V kapitole o správě počítačových sítí je také třeba zmínit koncept Infrastructure as code (IaC), což je v podstatě způsob provádění konfigurace systémů s pomocí automatizace. Kódem je v tomto případě myšlena specifikace postupu při konfiguraci konkrétního zařízení. Nástrojů, které toto umožňují, najdeme celou řadu (např. Ansible, Puppet nebo Chef). Tyto nástroje značně usnadňují správu především větších sítí.

Některé z uvedených nástrojů požadují pro své fungování instalaci klientů na koncových serverech, některé nikoliv. Za bezpečnější řešení je považována druhá varianta, kdy se k serverům připojuje server starající se o konfiguraci pomocí SSH. V obecné rovině lze říci, že tyto nástroje umožňují nejen provádět automatickou konfiguraci, ale lze s jejich pomocí snadno získat informace o určitém konkrétním nastavení všech serverů, a to jediným příkazem a bez nutnosti připojovat se na každý server zvlášť. Například tak lze získat informace o verzi jádra na jednotlivých serverech. Je to tedy nástroj, který lze využít i k rychlé kontrole určitých parametrů vašich systémů, spojených s bezpečností.

543: Blíže viz kap. 6.2.4 Logy a logování

Samozřejmě je možné vytvářet skupiny serverů dle jejich rolí a je tak možné například provést instalaci serveru Knot DNS na skupinu DNS serverů a provést potřebnou konfiguraci. Výhodou těchto řešení je také obvykle to, že případná změna provedená individuálně na některém serveru, která je v rozporu s požadavky nastavenými na centrálním konfiguračním serveru, bude při další synchronizaci vrácena zpět. Tyto nástroje lze také využít k rychlé instalaci záplat a oprav nalezených chyb.

Na druhou stranu představují tyto nástroje single point of failure a jejich selhání nebo napadení může za určitých okolností mít vážný dopad. Proto je potřeba věnovat dohledu a zabezpečení těchto systémů velkou pozornost.

Velmi dobré možnosti pokud jde o konfiguraci a vynucování nejrůznějších bezpečnostních nastavení na serverech a koncových stanicích nabízí také Active Directory od společnosti Microsoft. S tímto nástrojem lze snadno vytvářet skupiny zařízení (např. web servery, koncové stanice v konkrétní lokalitě) a uživatelů (např. marketing, finanční oddělení) a těmto skupinám přiřazovat nejen různá oprávnění pro přístup k prostředkům v síti, ale také automaticky nastavovat různá oprávnění, například omezit používání USB na konkrétní typy zařízení, nebo automaticky vynutit používání určitého proxy serveru pro konkrétní uživatele či systémy.

Rozhodnutí, zda nasadit Active Directory, nebo jinou kombinaci nástrojů umožňujících získat požadované možnosti pro automatickou konfiguraci, závisí na konkrétních okolnostech, převládajících systémech (Active Directory je úzce spjato s prostředím produktů společnosti Microsoft) a na schopnostech a znalostech správců.

## 6.7 Přenosné počítačové systémy

Problematiku přenosných počítačových systémů lze rozdělit do dvou skupin:

- **počítačové systémy organizace** (odnášená mimo organizaci),
- **počítačové systémy patřící uživatelům** (připojovaná do počítačové sítě organizace).

U první skupiny počítačových systémů je třeba primárně dbát na bezpečnost dat, tak jak již bylo popsáno v předchozích kapitolách. V případě kompromitace těchto počítačových systémů může dojít ke zcizení, ztrátě systému jako celku či k vyzrazení dat. Uživatelé zpravidla také mohou do těchto systémů instalovat potencionálně závadný software, počítačový systém může být napaden malwarem, nebo kompromitován útokem po počítačové síti, pokud se nachází v sítích mimo kontrolu organizace.

V případě počítačových systémů organizace je třeba zajistit zálohování a šifrování dat, komplexní ochranu proti malware, firewall, omezení instalace softwaru aj. Tam, kde to zařízení umožňuje,

je také možné využít software umožňující počítačový systém v případě ztráty či zcizení nalézt, nebo aspoň vymazat citlivá firemní data.

Komplexní přístup k zabezpečení přenosných zařízení připojujících se do sítě organizace se nazývá Endpoint security.

Druhou skupinu představují počítačové systémy, které jsou připojovány do počítačové sítě organizace uživateli samotnými, případně návštěvami. Pokud chce organizace pouze umožnit uživatelům využívat počítačovou síť k přístupu na Internet, je vhodné pro tyto účely vytvořit separátní síť, která bude striktně oddělena od zbytku počítačové sítě.

I v tomto případě je třeba zvážit všechny možné souvislosti, neboť i když je tato síť izolována, může být některý počítačový systém například součástí botnetu atd.

Takto přístupná počítačová síť také může být zneužita například ke stahování nelegálního obsahu.[544]

Speciální podskupinou počítačových systémů přinášených do počítačové sítě organizace mohou být zařízení spadající do kategorie známé jako **BYOD** (Bring Your Own Device). Jedná se o vlastní počítačové systémy uživatelů, které jim typicky zaměstnavatel dovolí využívat pro plnění pracovních činností. Nejčastějším projevem fenoménu BYOD je příjem a odesílání firemní e-mailové pošty na soukromých mobilních telefonech, nicméně jsou i zaměstnavatelé, kteří dovolují zaměstnancům používat pro práci soukromé tablety nebo laptopy.

BYOD představuje pro zajištění bezpečnosti služeb a sítě významný problém pramenící z faktu, že uživatelé přinášejí do organizace počítačové systémy, které jsou zcela v jejich správě, zpracovávají na nich data organizace a získávají přístup k souborům a službám organizace.

544: Směrnice však nebrání tomu, aby se nositel práv u vnitrostátního soudního nebo správního orgánu domáhal toho, aby bylo takovému poskytovateli nařízeno ukončit veškeré porušování autorských práv, jehož se dopouští jeho zákazníci, nebo takovému porušení předcházet. Více viz Rozsudek ve věci C-484/14 Tobias Mc Fadden v. Sony Music Entertainment Germany GmbH. [online]. [cit. 10. 1. 2018]. Dostupné z:
https://curia.europa.eu/jcms/upload/docs/application/pdf/2016-09/cp160099cs.pdf
Dle názoru Soudního dvora EU je pak možným řešením poskytovat heslo na základě ověření totožnosti uživatele, kterému je toto heslo zpřístupněno, neboť dle názoru Soudního dvora EU by vědomí, že je přístup k síti řízen, mělo uživatele od stahování odradit. Praktická implementace však bude narážet na jisté limity. Pokud bude přístup k síti zabezpečen sdíleným heslem, je velmi pravděpodobné, že v průběhu času se toto heslo dostane i k uživatelům, kteří žádným ověřením totožnosti neprošli. Implementace WPA Enterprise zase přináší značnou režii jak na straně administrátorů, kteří musí zřizovat jednotlivé účty, tak na straně uživatelů, kteří musí poměrně složitě konfigurovat jejich zařízení.

Pokud politika organizace umožňuje používání soukromých počítačových systémů pro pracovní účely, je potřeba přesně vymezit povinnosti uživatele, včetně takových detailů, jako je například povinnost smazat veškerá data organizace při ukončení pracovního poměru. Politiky týkající se BYOD by měly dále zahrnovat minimální požadavky stanovené na bezpečnost (například požadavek na zámek obrazovky, používání a aktualizace antiviru) a definovat způsob jejich kontroly, dále seznam aplikací a dat, ke kterým uživatelé mohou ze soukromých počítačových systémů přistupovat, nebo právo organizace mít na tomto systému software umožňující vynucení některých politik a pravidel. Organizace by také měla mít právo vymazat obsah uživatelova počítačového systému (nebo to požadovat po uživateli), pokud jej uživatel ztratí či je mu zcizeno.

Z dostupných technických opatření, která zde ještě nebyla zmíněna a mají vztah k problematice BYOD, lze zmínit kontejnerizaci, umožňující dle konkrétní implementace izolovat jednotlivé aplikace a procesy, případně provést určité rozdělení už na úrovni systému. Dalším nástrojem využitelným v kontrole BYOD je Mobile Device Management (MDM). Tyto nástroje umožňují centrálně spravovat „chytré" telefony, tablety i laptopy. MDM obvykle zahrnuje možnost vzdálené instalace programů, vynucení konkrétní politiky, zabezpečení e-mailů a dokumentů organizace, nebo oddělení a zabezpečení dat organizace.

## 6.8 Bezpečnost lidských zdrojů

Člověk je všeobecně považován za nejslabší článek zabezpečení. Nemusí se vždy jednat jen o chybu koncového uživatele, chybují i správci či bezpečáci. Chybovat je lidské. Je však třeba pokud možno lidským chybám předcházet. K tomu slouží řetězec opatření, která dokáží riziko, že dojde k selhání lidského faktoru, zmenšit.

Důležitý je již samotný proces přijímání nových zaměstnanců. Tato problematika spadá spíše do oblasti řízení lidských zdrojů, ovšem i zde už mohou být uplatněny některé prvotní filtry. Pokud to povaha jeho práce vyžaduje, je možné u budoucího zaměstnance provádět kontrolu informací uváděných v profesním životopisu, včetně ověření informací o dosaženém vzdělání, kontrolovat trestní bezúhonnost, případně si zjistit doplňkové informace o uchazeči z veřejných zdrojů. Vždy je však potřeba postupovat v souladu s platnými zákony. Zaměstnanci by také, například v rámci pracovní smlouvy, měli být seznámeni s povinností ochrany informací a povinností mlčenlivosti v patřičném rozsahu.

V rámci již probíhajícího pracovně právního vztahu by zaměstnanci měli mít k dispozici všechny směrnice týkající se bezpečnosti a měli by se s nimi prokazatelnou formou seznámit. Důležité je také pravidelné školení zaměstnanců. To může být realizováno fyzicky, ale i formou e-learningu. Praxe ukazuje, že je třeba uživatelům nejen vštípit určitá pravidla, ale také vysvětlit, proč je jejich dodržování důležité. Pokud si totiž uživatelé nevezmou pravidla týkající se bezpečnosti za svá, pravděpodobně je dříve či později začnou ignorovat, či dokonce záměrně obcházet.

Z hlediska bezpečnosti lidských zdrojů je důležité zavést systém klasifikace dat organizace tak, aby uživatelé věděli, jak s kterým druhem informací mohou nakládat a s kým jej mohou sdílet. Mezi známé principy patří **princip Need to Know**, který v podstatě říká, že zaměstnanec by měl mít přístup pouze k informacím, které potřebuje pro svou práci, tedy ne na základě například své pozice ve firmě. Tento princip je uplatňován především ve specializovaných organizacích. V běžné praxi závisí jeho smysluplné uplatnění na mnoha faktorech. Některé informace zaměstnanec běžně ke své práci nepotřebuje, nicméně ve specifických případech mu může informace, která mu nepřísluší, pomoci udělat správné rozhodnutí.

Kde však je princip Need to Know zásadní, je oblast aplikací, ve kterých zaměstnanci pracují. Zde je potřeba již při návrhu aplikace přemýšlet o možných rolích tak, aby například v databázi klientů neviděl každý zaměstnanec veškeré informace a aby přístup k potenciálně citlivým informacím byl podmíněn speciální akcí, která bude zvlášť logována.

S výše uvedeným pak souvisí i disciplinární řízení. Zaměstnanci by měli být informováni o tom, jaké jsou možné důsledky porušení pravidel bezpečnosti a pravidla pro toto řízení by měla být formalizována.

Další důležitou oblastí bezpečnosti lidských zdrojů je ukončení pracovního poměru. Je třeba jasně určit odpovědnosti za správný průběh tohoto procesu, především za vrácení předmětů přidělených zaměstnanci za účelem plnění pracovních povinností a také za zrušení přístupových práv. Podobně by měl být ošetřen i proces změny pracovního zařazení, kdy je potřeba revidovat existující přístupová práva tak, aby zůstal zachován princip Need to Know a zaměstnanec tak neměl například přístup do databáze, kterou už nepotřebuje.

## 6.9 Reakce na incident

Otázkou není, zda v nějaké organizaci či u jedince dojde k bezpečnostnímu incidentu, ale kdy se tak stane a hlavně, jak na tuto situaci budete připraveni. Z tohoto důvodu je potřeba mít připraveny plány pro případ bezpečnostního incidentu nebo přímo úmyslného útoku a dále mít plány pro zotavení po kybernetickém incidentu, pokud by tento měl skutečně závažný dopad.

Prvním krokem v organizaci by mělo být vytvoření týmu, který se bude řešením bezpečnostních incidentů zabývat. Vlastní rozsah a složení týmu se bude lišit dle dané organizace a její hlavní činnosti.

**Příklad:** *V bance může být členem někdo z oddělení správy serverů, odborník na bankovní aplikace a někdo z oddělení sítí. U ISP bude v tomto týmu minimálně zástupce oddělení zodpovědného za správu sítě, ale také zástupce oddělení odpovědného za správu důležitých serverů a služeb, jako DNS, DHCP, NTP nebo SMTP. Společnost podnikající v oblasti energetiky, vodohospodářství a obecně*

*v průmyslu zase nejspíš k výše uvedeným zástupcům nominuje také odborníka na správu průmyslových řídicích systémů, jako jsou různé SCADA či PLC systémy.*

Kromě technických odborníků, kteří budou pravděpodobně řešit většinu incidentů, by v širším smyslu měli v bezpečnostním týmu být také zástupci právního oddělení a oddělení zodpovědného za komunikaci. Je také nutné ihned na začátku určit člověka, který bude lídrem bezpečnostního týmu. Dalším krokem by mělo být nastavení reakčních dob pro jednotlivé typy incidentů a definování eskalačních procedur.

Dalším krokem by mělo být definování plánu, podle kterého se bude postupovat při řešení incidentů. V této chvíli je vhodné definovat si určité spouštěče, které bezpečnostnímu týmu pomohou při určení priority daného incidentu, a zároveň podle nich tým pozná, kdy je načase aktivovat kterou z nastavených eskalačních procedur. Těmito spouštěči může být výše finanční ztráty hrozící firmě, počet zákazníků ohrožených incidentem či dokonce výše hrozících ztrát na majetku, počet ohrožených životů aj.

Bezpečnostní tým při počáteční analýze odhadne možné následky incidentu a ve většině případů jej pravděpodobně bude řešit v rámci standardních časů a procedur. Ovšem pokud vyhodnotí například dopad incidentu na velké množství zákazníků, aktivuje příslušnou eskalační proceduru a bude informovat management společnosti, public relation oddělení a oddělení pro péči o zákazníky. Počet stran, které je nutné informovat, může být vyšší. Může se jednat například o úřad pro ochranu osobních údajů, pokud incident spadá do příslušné kategorie, nebo jiný dohledový orgán či mateřskou společnost. Při tvorbě plánu na zvládání incidentů je třeba od počátku konzultovat návrhy na řešení incidentu s právním oddělením, aby nebyla opomenuta některá ze zákonných povinností.

V plánu na řešení incidentů by mělo být aspoň rámcově vymezeno, jaké pravomoci mají členové týmu při řešení incidentů, především s přihlédnutím k omezení potenciálních škod na minimum. Dále by mělo být definováno, jaké důkazní materiály má tým zabezpečit a jakým způsobem by měl případně dokumentovat svou činnost, a to pro případné pozdější vyšetřování (v případě, že se bude jednat o rozsáhlé incidenty, u kterých lze nějaké další vyšetřování a analýzy očekávat).

Na plány a eskalační procedury bezpečnostního týmu by pak měly rámcově navazovat krizové plány dalších oddělení. Například public relation oddělení by mělo mít představu, jakými kanály bude v konkrétních případech informace předávat dál a v jakém rozsahu.

Na zvládání bezpečnostních incidentů navazuje ještě jedna důležitá oblast a tou je **plán kontinuity činnosti organizace**, ve kterém by měly být opět aspoň rámcově popsány nejdůležitější kroky vedoucí k obnově normálního fungování organizace, a měla by být vymezena důležitost jednotlivých služeb tak, aby bylo jasné, které části infrastruktury je potřeba opravit nejdříve.

Plán kontinuity by měl pamatovat na obnovení infrastruktury, obnovu dat a obnovu služeb. Také by v tomto plánu mělo být definováno, jakým způsobem bude probíhat například komunikace směrem k zákazníkům, pokud se jich bude výpadek služeb také týkat.

Plán kontinuity by měl být také v určitých časových intervalech revidován, neboť může docházet jak ke změně informačních a komunikačních technologií a postupů potřebných pro obnovu, tak i ke změně důležitosti jednotlivých služeb. Oddělení IT by také mělo pravidelně testovat schopnost obnovit podle nastavených postupů činnost serverů, včetně obnovy dat. Není nutné testovat celou infrastrukturu, obvykle postačí otestovat cvičnou obnovou jednoho systému funkčnost nastavených postupů.

### 6.9.1 Hlášení bezpečnostních incidentů

Hlášení bezpečnostních incidentů je nedílnou součástí celého procesu udržování požadované úrovně bezpečnosti organizace. Z praktických důvodů v této kapitole popíšeme, jak by mělo probíhat hlášení interních bezpečnostních incidentů a jak lze případně využít pomoc národního bezpečnostního týmu CSIRT.CZ. Hlášení prováděná v souladu se Zákonem o kybernetické bezpečnosti již byla rozebírána v § 8 ZoKB.

### 6.9.2 Interní hlášení bezpečnostních incidentů

Je potřeba si uvědomit, že kromě samotného řešení aktuálně probíhajícího incidentu má hlášení incidentů i další význam, a tím je možnost sledování dlouhodobých trendů. Aby bylo možné tohoto cíle dosáhnout je potřeba bezpečnostní incidenty vhodně třídit a zpracovávat v systému, který nám umožní provést jejich periodické vyhodnocení. K tomuto účelu je možné využít různé tiketovací systémy.

V tiketovacím systému lze došlá hlášení automaticky i ručně rozřazovat do front, nastavovat jim různé vlastnosti (např. typ incidentu, stav incidentu, přijaté prostředky aj.) a především je zpracovávat a vyhledávat v nich. Tiketovací systém má obvykle řadu různých funkcí, je proto potřeba vybrat takový, který bude vyhovovat potřebám organizace.

Povinnost hlásit interní bezpečnostní incidenty by měla být zakotvena v interních směrnicích a politikách a uživatelé by měli být školeni, aby dokázali bezpečnostní incident rozpoznat. Dále musí být popsán způsob, jakým mají hlášení bezpečnostního incidentu podávat. Pokud to tiketovací systém umožňuje, můžete vytvořit šablonu, která uživatelům podání hlášení usnadní. Její položky mohou být následující:

- jméno, příjmení a oddělení/úsek osoby hlásící incident,

- stručný popis incidentu,
- dosud provedené akce,
- opatření k nápravě aktuálně vzniklé škody,
- preventivní opatření,
- plánovaná kontrola účinnosti zavedených opatření,
- výsledek kontroly.

Poslední tři body (dle konkrétní situace) jsou primárně určeny pro bezpečnostní tým, který se bude řešením incidentu zabývat. Po nahlášení incidentu uživatelem proběhne fáze samotného řešení incidentu. Na konci procesu řešení by měl tým zvážit, zda incident, který proběhl, vyžaduje nasazení nějakého preventivního opatření, které by vzniku incidentu předcházelo. Pokud ano, je potřeba také naplánovat příslušný audit, který zkontroluje účinnost zavedených opatření. Po té je možno incident uzavřít, nebo pokud zavedená opatření selhávají, navrhnout nová a poslední část cyklu opakovat.

V rámci systému řízení bezpečnosti informací (ISMS) se také v pravidelných intervalech provádí analýza všech bezpečnostních aspektů, zaznamenaných v období od předchozí analýzy (obvykle jeden rok). V rámci této analýzy jsou vyhodnocovány také bezpečnostní incidenty. Praxe ukazuje, že i pokud není v organizaci zaveden systém řízení bezpečnosti informací, je pravidelné vyhodnocování bezpečnostních incidentů dobrou cestou, jak odhalit případné nedostatky v oblasti bezpečnosti.

### 6.9.3 Řešení bezpečnostních incidentů

Řešení bezpečnostního incidentu má obvykle 4 hlavní fáze:

1) **Detekce**
   V této fázi je incident odhalen a nahlášen. Detekce incidentů nemusí probíhat pouze prostřednictvím zaměstnanců firmy, ale mohou být detekovány automatickými či poloautomatickými nástroji. Jedním z možných nástrojů pro detekci je SIEM. Informace o incidentech je možné přijímat i z externích zdrojů. V praxi se stává poměrně často, že je malware na počítači odhalen až díky stížnosti či oznámení z jiné sítě, ve které se škodlivý kód pokoušel například skenovat porty nebo prováděl jiné útoky.

   Všechny relevantní informace z různých zdrojů, ať už interních hlášení, detekčních mechanismů, nebo od externích subjektů, je možné sbírat v tiketovacím systému.

2) **Analýza skutečného stavu**
   Na detekci incidentu navazuje analýza skutečného stavu, při které je zjišťován (na místě, z logů, nebo jiným vhodným způsobem) skutečný stav věci. Pokud si to komplexnost či

rozsah incidentu vyžadují, dojde pravděpodobně v průběhu této fáze k aktivaci dalších členů bezpečnostního týmu. Výsledkem analýzy by měla být informace o rozsahu incidentu, jeho dopadech a také o jeho příčinách. Právě tyto informace mohou vést k přechodu do další fáze.

3) **Reakce na incident**
Ve fázi reakce na incident je potřeba navrhnout možná řešení aktuálního problému. Primárním cílem je snížení dopadů bezpečnostního incidentu či jeho úplná eliminace. Znamená to tedy navrhnout a realizovat opatření, která ukončí probíhající incident.

Pokud je zdrojem incidentu provoz přicházející z IP adresy mimo spravovanou počítačovou síť (např. skenování portů aj.), nebo je taková IP adresa využívána k útoku na organizaci (např. phishingová stránka napodobující interní aplikaci organizace), neobejde se řešení incidentu bez komunikace se správcem sítě, ve které má incident svůj původ. K hlášení incidentu se obvykle používají k tomu speciálně určené abuse adresy, často ve formátu *abuse@doména*. Abuse adresy pro jednotlivé IP rozsahy lze obvykle snadno dohledat v databázi WHOIS.[545]

```
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf

% Note: this output has been filtered.
%       To receive output for a database update, use the "-B" flag.

% Information related to '217.31.205.0 - 217.31.206.255'

% Abuse contact for '217.31.205.0 - 217.31.206.255' is 'abuse@nic.cz'

inetnum:        217.31.205.0 - 217.31.206.255
netname:        CZ-NIC-I
descr:          CZ.NIC, z.s.p.o.
descr:          Infrastructure
country:        CZ
admin-c:        CZ-RIPE
tech-c:         CZ-RIPE
status:         ASSIGNED PA
mnt-by:         CZ-NIC-MNT
```

Obrázek 70: Ukázka abuse adresy pro IP rozsah sdružení CZ.NIC

Problém může nastat, pokud v databázi WHOIS držitel IP adres tento rozsah uveden nemá, nebo pokud u něj nemá uvedenou abuse adresu. V takovém případě je potřeba improvizovat

545: WHOIS představuje označení pro databázi, která slouží k evidenci údajů o držitelích internetových domén a IP adres. Provozovatelem WHOIS s informací o držitelích české národní domény .CZ sdružení CZ.NIC. Databázi s informacemi o alokaci IP adresních bloků v regionu Evropy pak spravuje organizace RIPE NCC (www.ripe.net).

a pokusit se vhodný kontakt získat jinou cestou. Dalším bohužel častým problémem je pak ta skutečnost, že abuse adresu nikdo v dané organizaci ve skutečnosti nesleduje.

Teprve pokud se v rámci řešení incidentu nedočkáte nápravy, druhá strana věc odmítá řešit nebo nereaguje, je možné kontaktovat národní bezpečnostní tým CSIRT.CZ, který se pak pokusí s druhou stranou dospět ke zdárnému řešení. Primárně by se vždy měli správci zainteresovaných sítí snažit vyřešit situaci nejprve bez využití služeb národního CSIRT. Národní CSIRT by také měl být informován, pokud během vyšetřování incidentu dojdete k názoru, že by se mohlo jednat o plošný problém zasahující více sítí či více různých uživatelů. Národní CSIRT pak využije své kontakty a bude potenciální možné oběti informovat, případně může v roli koordinátora zprostředkovat výměnu informací mezi více napadenými subjekty.

4) **Vyhodnocení incidentu**
V poslední, velmi důležité fázi dochází k vyhodnocení příčiny incidentu, je vyšetřován primární spouštěcí mechanismus incidentu a jsou navrhována opatření, která sníží pravděpodobnost opakování incidentu v budoucnosti.

Celý proces řešení incidentu demonstrujeme na následujícím příkladu.

**Příklad:** *Naše detekční nástroje nás informují o nebývale vysokém provozu v síti. Při bližší analýze zjistíme, že nezvyklý provoz je generován naším mailovým serverem. Další analýza přímo na serveru pak ukáže, že zvýšený provoz je odchozí pošta, odesílaná z jednoho konkrétního účtu. Následně zjistíte, že se k účtu připojila IP adresa ze zahraničí, která zprávy, pravděpodobně nevyžádané, rozesílá. Další logický krok bude zablokování účtu, aby se předešlo dalším škodám. Následně můžete s oprávněným uživatelem dohodnout, že si změní heslo ke svému mailovému účtu.*

*Tím jsme v podstatě zabránili vzniku dalších škod. Nyní je možné spustit poslední fázi, během níž zjišťujeme, co bylo příčinou samotného úniku hesla a zároveň navrhneme opatření, která předejdou dalšímu opakování incidentu. To může zahrnovat kontrolu politiky hesel a jejího vynucování, kontrolu stanic, ze kterých se uživatel, jehož účet byl napaden, pokoušel připojovat, na přítomnost malware, osobní pohovor s uživatelem, který by například odhalil, že se uživatel stal obětí phishingového útoku, a další kroky. Podle zjištění pak můžeme jako opatření navrhnout lepší vynucování politiky hesel nebo častější školení zaměstnanců na rizika spojená s používáním informačních technologií.*

## 6.10 Možnosti využití dalších informačních zdrojů o incidentech

Jak bylo řečeno v předchozí kapitole, existuje celá řada veřejných zdrojů informací vztahujících se k incidentům. Některé společnosti toho využívají a aktivně se snaží data z těchto zdrojů získávat. Bohužel tyto zdroje nejsou sjednocené a informace v nich bývají mnohdy kusé.

Z tohoto důvodu provozuje národní bezpečnostní tým CSIRT.CZ dvě služby, které administrátorům získávání těchto informací značně usnadňují. Jednou z nich je služba **Malicious Domain Manager** (MDM), zaměřená na obsah webových stránek, a druhou pak služba **PROKI**, která sbírá informace o bezpečnostních incidentech ze všech relevantních zdrojů.

### 6.10.1 Malicious Domain Manager

Malicious Domain Manager (MDM) je služba, kterou národní CSIRT spustil již v roce 2011 a od té doby ji stále vyvíjí a přidává do ní nové funkcionality.

Primárním cílem aplikace MDM bylo urychleně informovat držitele domény .CZ, pokud dojde ke kompromitaci webové prezentace umístěné na této doméně. Za tímto účelem sbírá tato aplikace informace z veřejných i poloveřejných zdrojů, spojuje je do logického celku v rámci jedné domény a následně zasílá informaci o napadení webu právě držiteli dané domény.

Typový rozsah incidentů odpovídá profilu incidentů spojených s webovými stránkami. Dominují incidenty spojené s šířením malware, kdy úspěšnou kompromitaci webových stránek využije útočník k šíření malware[546] na počítačové systémy návštěvníků. Dalšími incidenty, které se v aplikaci MDM objevují, jsou phishingové stránky nebo defacement (změna obsahu webových stránek).

Posláním informace držiteli však práce s daty nekončí, jednotlivé útoky jsou poloautomaticky analyzovány a takto získaná data jsou dále využívána v dalších projektech, mimo jiné také ke zvýšení bezpečnosti uživatelů v projektu Turris.

Projekt MDM splnil očekávání, mezi lety 2011 až 2018 v něm bylo řešeno přes sto padesát tisíc URL na více než deseti tisících sedmi stech doménách. Zároveň během prvních tří let od spuštění aplikace[547] docházelo k postupnému snižování počtu phishingových útoků v doméně .CZ a především k postupnému snižování průměrného uptime phishingových stránek.

Zkušenosti z úspěšného provozování aplikace MDM byly jedním z důvodů, proč později vznikl projekt PROKI s mnohem širším dopadem.

546: Blíže viz *Útoky pomocí iframe, jejich maskování útočníky a obrana*. [online]. [cit. 28. 8.2018]. Dostupné z: https://blog.nic.cz/2012/07/18/utoky-pomoci-iframe-jejich-maskovani-utocniky-a-obrana/

547: Více viz *Počet phishingových útoků v doméně .CZ se opět snížil.* [online]. [cit. 28. 8. 2018]. Dostupné z: https://blog.nic.cz/2013/08/22/pocet-phishingovych-utoku-v-domene-cz-se-opet-snizil/

### 6.10.2 Cyber Threat Intelligence Project - PROKI

Tato kapitola vznikla s využitím již dříve publikovaných výstupů[548] z projektu PROKI a byla doplněna o některé aktuální informace.

Výzkumný projekt **PR**edikce a **O**chrana **P**řed **K**ybernetickými **I**ncidenty[549] vznikl v rámci českého národního bezpečnostního týmu CSIRT.CZ[550] jako reakce na rostoucí počet dostupných zdrojů informací o probíhajících i uskutečněných kybernetických incidentech a jejich původcích.

Ve svých východiscích **projekt reaguje na dva hlavní problémy**, které sebou přináší rostoucí tlak na zpracování těchto informačních zdrojů. První z nich je **potřeba distribuce informací o incidentech** do jednotlivých sítí způsobem, který bude pro správce v koncových sítích srozumitelný a přehledný. Druhý problém pak představuje **rostoucí potřeba hlubší analýzy jednotlivých incidentů** a vztahů mezi nimi. Samotný projekt PROKI sestává ze tří článků, které umožňují naplnit hlavní cíle projektu:

- **Sběr informací o incidentech**
  Velká variabilita veřejných zdrojů o incidentech přináší nároky na jejich hromadné zpracování a následné využití. Problém se týká jak variability metod použitých pro doručení (HTTP, SMTP, vlastní API), tak ještě širší variability formátů, ve kterých jsou informace doručovány (csv, xml, json, stix, openioc). Nesené informace jsou také nekonzistentní z pohledu typu útoku (domény a URL hostující malware, IP adresy aktivně útočící na jiné stroje, IP adresy C&C serverů, IP adresy klientů botnetů, či phishingové URL). Shromáždění všech těchto informací do jednoho místa a jejich distribuce a vyhodnocování jsou tedy náplní výzkumného projektu PROKI.

  Po zvážení různých kritérií byl jako základní kámen systému PROKI vybrán společný open source projekt IntelMQ vyvíjený ve spolupráci Evropské agentury pro informační a síťovou bezpečnost (ENISA) a evropských CSIRT týmů.[551] Tento projekt splňuje požadavky na jednoduchost a modularitu, která i v budoucích fázích projektu umožní reagovat na případné změny zdrojů informací o incidentech i jejich snadné rozšiřování. Tým CSIRT.CZ se také aktivně zapojil do vývoje tohoto softwaru. Funkcí IntelMQ v rámci projektu PROKI je

548: BAŠTA, Pavel. Budování a implementace českého národního Cyber Threat Intelligence System. *Bezpečnostní teorie a praxe.* 2016 (4), s. 129–136

549: Projekt „Predikce a ochrana před kybernetickými incidenty (PROKI)" (VI20152020026) je realizován v rámci Programu bezpečnostního výzkumu ČR na léta 2015 – 2020. Dále jen **PROKI**.

550: Provozovatelem národního CERT dle § 17 a § 18 ZoKB je na základě veřejnoprávní smlouvy uzavřené s Národním bezpečnostním úřadem dne 18. prosince 2015 sdružení CZ.NIC, správce národní domény .cz.

551: Více informací viz.
https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/incident-handling-automation

primárně získávání dat týkajících se bezpečnostních incidentů z různých zdrojů.[552] IntelMQ si díky mnoha různým konektorům dokáže poradit s celou řadou informačních zdrojů. Takto získaná data jsou následně sjednocena a obohacena o geolokační informace a společně s daty z IntelMQ předávána dalším dvěma článkům.

- **Notifikace a distribuce**
  První z těchto článků představuje **aplikace, která se stará o inteligentní distribuci informací o incidentech do zdrojových sítí**.

  Pokud mají být informace o incidentech skutečně řešeny, je potřeba je do koncových sítí rozesílat v rozumném intervalu a zároveň je členit tak, aby si správce dané sítě mohl sám určit prioritu jejich řešení, případně rozhodnout, které má zájem řešit a které nikoliv. Ze zkušenosti z provozu národního bezpečnostního týmu CSIRT.CZ vyplývá, že to, co může menší společnost vyhodnotit jako incident vyžadující řešení, může být pro velkého poskytovatele připojení minoritní záležitost.

  Záleží také na zasazení incidentu do reálného prostředí. Z pohledu ISP bude mít zcela jistě jinou prioritu podezření na malware na některém z jeho webových serverů a jinou prioritu podezření na malware na stanici koncového zákazníka. Software určený k rozesílání těchto zpráv do koncových sítí získává potřebné kontaktní informace z veřejně dostupného WHOIS rozhraní. Při rozesílání informací o incidentech jsou preferovány kontakty typu abuse.[553]

  V roce 2018 byla do této části na četné žádosti komunity implementována **možnost získávat data relevantní pro danou síť také prostřednictvím API**, což umožňuje správcům ještě rychlejší reakci při řešení bezpečnostních incidentů. Pro přístup k API rozhraní je potřeba požádat o získání přístupového klíče. Na jeho základě pak lze získávat data pro příslušný rozsah IP adres s využitím automatických nástrojů. Výhodou přístupu přes API je především možnost získávat aktuální data pro požadované období, kterým může být den, týden, měsíc, nebo konkrétní rozsah dnů.

  Výstup z PROKI určený koncovým správcům obsahuje následující informace:

  - **time_detected** - čas, kdy byl incident detekován zdrojovým systémem
  - **ip** - IP adresa vykazující popisované chování
  - **class** - třída incidentu např. Malicious Code, Intrusion Attempts, Information Gather
  - **type** - typ incidentu (jedna třída může obsahovat více typů) např. botnet drone, scanner, malware

552: Seznam zdrojů projektu PROKI je k dispozici na URL https://csirt.cz/page/3587/zdroje-dat/

553: Podrobněji se problematice abuse kontaktů věnuje článek *Kde hledat abuse kontakty?* [online]. [cit. 28. 8. 2018]. Dostupné z: https://blog.nic.cz/2016/04/04/kde-hledat-abuse-kontakty/

- **time_delivered** - čas, kdy byl incident zaregistrován systémem PROKI
- **country_code** - kód země
- **asn** - číslo autonomního systému
- **description** - dodatečný popis incidentu, pokud je dostupný
- **malware** - rodina nebo název malwaru, pokud je dostupný např. Trojan.Backdoor, Office. Word. Downloader
- **feed_name** - název zdrojového feedu, jejich seznam je uveden dále
- **feed_url** - URL zdrojového feedu
- **raw** - původní záznam ze zdrojového feedu

- **Archivace a analýza incidentů**
  Druhým z článků, do kterých systém IntelMQ předává data je analytická část, která je v systému PROKI reprezentována systémy **Elasticsearch a Kibana**. Tyto nástroje se starají o **ukládání, indexaci a zobrazování získaných informací o incidentech**. Tento software je dále rozvíjen tak, aby byla data automaticky, či na vyžádání analytika obohacována o informace z dalších zdrojů.

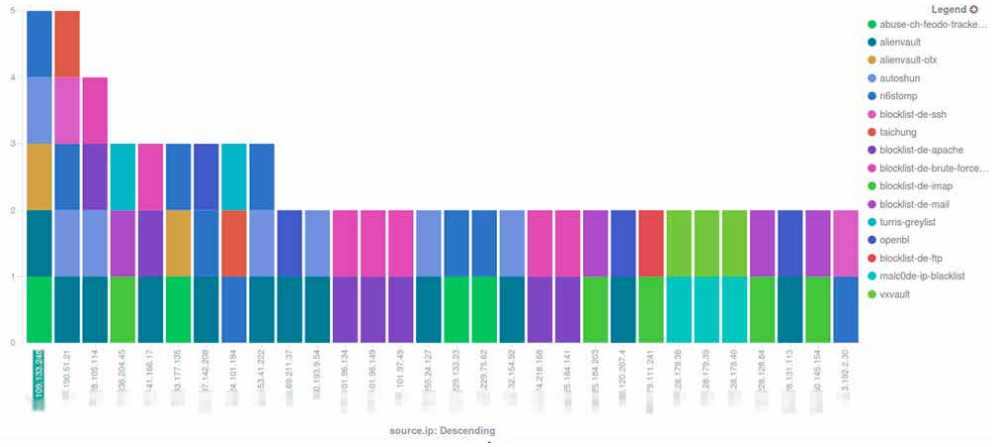
  Analytická část projektu přináší **možnost zjistit historii informací o incidentech spojených s konkrétní IP adresou**, možnost pravidelně vyhodnocovat dění spojené s nejproblematičtějšími IP adresami, nalézt sítě, které jsou největším zdrojem incidentů, což v poměru k jejich velikosti může ukazovat i na zaměření dané společnosti, minimálně na tolerování problematických aktivit. Tato část projektu národnímu CSIRT také umožní sledovat spojitosti mezi incidenty a díky tomu predikovat další možné cíle či zdroje útoků. Jak vypadá práce s analytickou částí projektu, vysvětlíme v následujícím příkladu.

  Na obrázku č. 72 je jeden z výstupů PROKI, který analytikovi Národního bezpečnostního týmu CSIRT.CZ přehledně v grafické podobě zobrazuje 30 IP adres, které vedou v pomyslném celosvětovém žebříčku IP adres reportovaných z největšího množství zdrojů informujících o kybernetických hrozbách za posledních 10 dnů.

  Každá barva reprezentuje jeden zdroj informací o podezřelých IP adresách. Úplně nahoře je možné vidět modrou barvou znázorněná data z projektu Turris, respektive IP adresy, vyhodnocené projektem jako podezřelé a z tohoto důvodu zahrnuté do tzv. greylistu.

  Tato data v podobě podezřelých IP adres se velmi často potkávají s dalšími databázemi zaměřenými na shromažďování informací o problematických IP adresách. Ještě zajímavější

je situace, pokud některou z podezřelých IP adres zkusíme vložit do databází jako je PassiveDNS nebo VirusTotal.[554]




Obrázek 71: Grafické znázornění nejvíce reportovaných závadných IP adres

Jednotlivé IP adresy na ose X jsou řazeny dle četnosti jejich reportování jako zdrojů ohrožení a zároveň podle množství zdrojů, které je reportovaly. Tyto zdroje jsou reprezentovány jednotlivými barvami.

V dalším kroku systém umožňuje analytikovi porovnávat IP adresy s informacemi z externích zdrojů. Služba PassiveDNS následně na jednu z takovýchto IP adres vrátí seznam domén, které na tuto IP adresu ukazují.

554: BAŠTA, Pavel. *Vytěžování informací o incidentech a jejich distribuce Aneb co je to PROKI.* [online]. [cit. 28. 8. 2018]. Dostupné z:
http://blog.nic.cz/2016/02/04/vytezovani-informaci-o-incidentech-a-jejich-distribuce-aneb-co-je-to-proki/

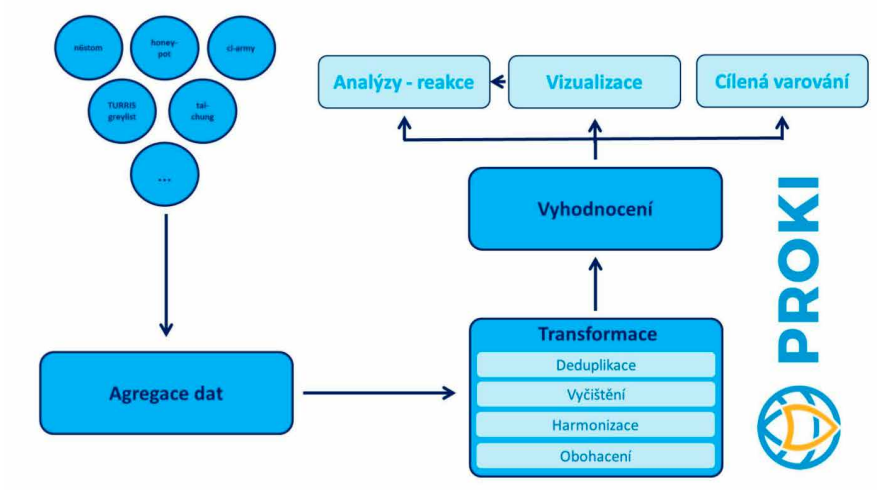
| LEFT | RTYPE | RIGHT |
|---|---|---|
| aaw5zjuu.info | A | 56.64.97 |
| acl4tsgf.info | A | 56.64.97 |
| aebmayn.info | A | 56.64.97 |
| ahwqxmm.info | A | 56.64.97 |
| ajdxzru.info | A | 56.64.97 |
| akfbjke.info | A | 56.64.97 |
| anpvqug.info | A | 56.64.97 |
| antxxit.info | A | 56.64.97 |
| aplrcbp.info | A | 56.64.97 |
| apm3qjyp.info | A | 56.64.97 |
| asbojayg.info | A | 56.64.97 |
| ato2voqt.info | A | 56.64.97 |
| ayfdzrc.info | A | 56.64.97 |
| azo1pinz.info | A | 56.64.97 |
| badnnri.info | A | 56.64.97 |
| bavwehfm.info | A | 56.64.97 |
| bicembyn.info | A | 56.64.97 |
| bjewzvj.us | A | 56.64.97 |
| bjiwchl.us | A | 56.64.97 |
| bndosgs.us | A | 56.64.97 |
| bnizxyi.us | A | 56.64.97 |
| bnxextd.info | A | 56.64.97 |
| boaerbp.info | A | 56.64.97 |
| braftam.us | A | 56.64.97 |

Obrázek 72: Ukázka výstupu historie konkrétní IP adresy v PassiveDNS

*V levém sloupci můžeme vidět jednotlivé domény a jejich A záznamy, které všechny ukazují na IP adresu, vyhodnocenou v rámci PROKI jako problematickou. Neobvyklé názvy domén ukazují na možné zneužívání IP adresy, například jako C&C serveru botnetu.*

Již samotné názvy domén v tomto případě ukazují na možné zneužití IP adresy, například jako C&C serveru. Analytik tak v rámci své činnosti může dále sledovat historii těchto domén a najít tak další potenciální C&C servery.

**Projekt PROKI představuje unikátní nástroj pro detekci, identifikaci a predikci kybernetických hrozeb a vyhodnocování kybernetických bezpečnostních incidentů** (tzv. *Cyber Threat Intelligence*), který umožňuje národnímu bezpečnostnímu týmu CSIRT. CZ nebýt odkázán k roli pouhého řešitele reportovaných incidentů, ale umožňuje mu se proaktivně zapojit do boje proti narůstající kybernetické kriminalitě. Celkový náhled na fungování tohoto systému přináší následující obrázek, který shrnuje vše dříve řečené do jednoho srozumitelného celku.




Obrázek 73: Schéma fungování systému PROKI

**Využití výstupů z PROKI v organizacích**
Existují dvě oblasti, ve kterých jsou data z PROKI v organizacích využívána. Tou první je již od počátku projektu sledovaný záměr umožnit administrátorům reagovat na incidenty, které byly detekovány v jiných počítačových sítích, ale měly svůj původ v jimi spravované počítačové síti. Takovéto incidenty mohou mít jako svého typického původce malware, kompromitovaný systém, napadené webové stránky[555], může za nimi být také špatná konfigurace některého ze systémů, či třeba uživatel.

Informace o incidentech jsou v pravidelných intervalech zasílány do koncových počítačových sítí, nebo je možné je získávat pomocí API rozhraní. Data jsou agregována podle abuse adresy uvedené u konkrétních rozsahů. Pokud vám internetový provider poskytl vlastní rozsah IP adres, je potřeba se s ním domluvit, aby příslušnou informaci zanesl také do databáze WHOIS. Pokud tak nečiní, budou hlášení chodit na abuse adresu daného poskytovatele. Pak samozřejmě záleží na tomto konkrétním poskytovateli, zda data svým zákazníkům dále předává.

Data z projektu PROKI může administrátor využít jako jeden ze zdrojů informací o incidentech ve spravované počítačové síti. Z pohledu administrátora je výhodou, že nemusí data stahovat z různých na Internetu dostupných zdrojů, ale dostává data již agregovaná a připravená pro

555: Více viz *Background: DDoS Attack on Major US banks.* [online]. [cit. 25. 8. 2018]. Dostupné z: https://www.incapsula.com/blog/cyber-attack-us-banks.html

případné strojové zpracování. Další podstatnou výhodu představuje určitý komunitní dohled nad projektem, kdy CSIRT.CZ na podkladě zpětné vazby od komunity administrátorů a bezpečnostních odborníků sám přidává nové zdroje, nebo naopak odstraňuje takové zdroje, které komunita označila za špatné.

Kromě tohoto využití nacházejí výsledky analýz probíhajících v systému PROKI využití i v organizacích, které se bezpečností přímo zabývají, a jsou tak v určité formě využívány k nastavení preventivních opatření u jejich klientů, například v rámci konfigurace firewallů.

## 7 CERT/CSIRT týmy

Internet zaznamenal v 21. století masivní rozvoj a komercionalizaci. Dramaticky se zvýšil počet uživatelů, počet počítačových systémů připojených do globální sítě a také počet provozovaných kritických služeb, ať už ze sféry komerční (např. elektronické bankovnictví, e-shopy, elektronické aukce), tak také ze sféry státní (např. informační servis státní správy a samosprávy, registry). Bezpečnostní incidenty, kybernetické útoky a trestná činnost páchaná prostřednictvím informačních a komunikačních technologií v reálném i virtuálním světě jsou čím dál více závažnější a zhoršují se také jejich dopady a následky.

Výraznou odlišností této kyberkriminality od ostatních druhů kriminality je její vysoká latentnost, vysoká míra tolerance společnosti (včetně lhostejnosti uživatelů), anonymita pachatele a jeho často obtížná identifikace. Vzrůstá tak potřeba zefektivnit obranu proti těmto útokům, především zlepšit prostředí a prostředky umožňující dohledání pachatele, sjednotit a zformalizovat postupy a také vzdělávat uživatele, aby byli schopni rozpoznat hrozby a rizikové situace, vypořádat se s nimi a v ideálním případě jim předcházet. Za tímto účelem je budována infrastruktura bezpečnostních týmů CERT a CSIRT.

### 7.1 Historie

Za první bezpečnostní incident, který negativně ovlivnil provoz tehdejšího Internetu tím, že vyřadil z chodu přibližně 10 % všech připojených zařízení, je označován tzv. Morissův červ *(Morris worm)*. Červ byl do Internetu vypuštěn v roce 1988 Robertem Morrisem, studentem Cornellovy univerzity v USA. Tento incident odstartoval éru vytváření a šíření počítačových virů, červů, trojských koní a další podobné „elektronické havěti", souhrnně označovaných jako *malware*. A právě tato zkušenost nastartovala na konci 80. let minulého století diskuzi o bezpečnosti sítí a služeb, aby následně došlo ke zformulování základních principů obrany, prevence a ochrany přenosu citlivých dat.

V reakci na Morissův červ byl na Carnegie Meelon University (CMU) v USA zformován první CERT tým. Tento první ad-hoc sestavený CERT měl za úkol prozkoumání Morissova červu, nalezení účinné obrany a návrhu řešení problémové situace. Nejcennějším výsledkem práce tohoto týmu nakonec bylo zjištění, že nejdůležitější je být na možnost narušení bezpečnosti předem připraven a v okamžiku problému spustit předem definovaný a vyzkoušený záchranný plán obrany a obnovy, a ne teprve začít zkoumat, co je nutné udělat a v jakých krocích. Výsledek práce tohoto prvního CERTu tak odstartoval éru budování světové infrastruktury týmů tohoto typu.

Carnegie Mellon University si zkratku CERT zaregistrovala jako ochrannou známku, a ač se jejímu užití ostatními organizacemi v tomto kontextu nebrání (organizace, která chce ve jménu

svého týmu tuto zkratku použít, musí požádat o svolení zkratku používat a obvykle jej dostane), právě toto bylo příčinou vzniku a zavedení druhého pojmu CSIRT.

## 7.2 CERT a CSIRT týmy

**CERT** (Computer Emergency Response Team) a **CSIRT** (Computer Security Incident Response Team). Každá z těchto zkratek má sice trochu jiný význam a hlavně trochu jinou historickou genezi, ve skutečnosti je dnes za oběma zkratkami možno chápat stejný typ týmu - **tým, který je ve svém jasně definovaném poli působnosti zodpovědný za řešení bezpečnostních incidentů a (kyber) hrozeb, z pohledu uživatelů nebo jiných týmů tedy místo, na které se mohou obrátit se zjištěným bezpečnostním incidentem, se žádostí o spolupráci, výměnu informací, pomoc apod.**

CERT/CSIRT týmy vznikají na úrovni jednotlivých organizací, přičemž jde jak o organizace, které zprostředkovávají chod Internetu (ISP - poskytovatelé připojení a služeb), tak také o organizace, které prostředí Internetu používají ke své hlavní činnosti (např. IT firmy, poskytovatelé obsahu, banky).

**Základní povinností každého CSIRT týmu je reakce na hrozbu („response") a spolupráce při řešení incidentů.** CSIRT tým obvykle řeší problém, který se vyskytne v jeho poli působnosti (např. vlastní síťové infrastruktuře), tedy tam, kde má reálné možnosti k zásahu.

CERT/CSIRT dané sítě (organizace) obecně představuje záchytný bod, na který se uživatelé mohou obrátit se zjištěným bezpečnostním problémem (nebo jen podezřením na problém), který se týká počítačové sítě nebo některé z provozovaných služeb. Profesionální CERT/CSIRT tým by každé přijaté hlášení (i potenciálního) bezpečnostního incidentu měl prozkoumat a podle svých možností zjednat nápravu.

Nejde o nic převratného a v praxi neexistujícího, každá větší organizace, poskytovatel připojení nebo poskytovatel služeb provozuje bezpečnostní tým. **Rozdíl mezi běžným bezpečnostním týmem a týmem typu CERT/CSIRT je zejména v zapojení do** světové bezpečnostní infrastruktury, sdílení informací v rámci této infrastruktury **a dodržování stanovených formálních postupů**.

Existence alespoň jednoho oficiálního CERT/CSIRT týmu je žádoucí v každé provozované síti, obzvláště pak v těch velkých (tranzitní, regionální, univerzitní), tzn. na úrovni velkých ISP, ale také v bankách nebo u poskytovatelů služeb.

Významnou a **specifickou roli mají** v rámci jednotlivých států zastřešující **vrcholové týmy** - tzv. **národní** a **vládní**, kterým bude věnována samostatná subkapitola.

Globálně lze pak na existující CERT/CSIRT týmy nahlížet jako na infrastrukturu, která řeší bezpečnostní problémy Internetu. Při práci čerpá CERT/CSIRT tým především ze svých zkušeností, předem připravených a v praxi ověřených postupů a ze spolupráce a výměny informací s ostatními CERT/CSIRT týmy.

***Základním požadavkem*** komunity **je, aby CERT/CSIRT tým veřejně deklaroval své kontaktní informace a pravidla činnosti:**

- kdo je jeho provozovatel,
- kdo jsou jeho členové,
- způsob jak a kdy je možné tým zastihnout,
- jaké **služby** nabízí,
- **pole působnosti** (číslo AS[556], síť, domény, služby), ve kterém je tým způsobilý konat a jakým způsobem, tzn. definování jeho pravomocí a odpovědnosti. Na základě pole působnosti je potom tým kontaktován (např. napadenými) a řeší jemu příslušející problémy (incidenty).

Termín **řešit bezpečnostní incident** přitom může mít různá specifika v závislosti na nastavení týmu a jeho interní politice - může to být prostá eliminace útoku (zneškodnění zdroje problému např. odpojením kompromitovaného počítačového systému od sítě), dohledání útočníka, rychlé obnovení provozu napadené služby/sítě apod.

Právě v závislosti na činnosti týmu při řešení bezpečnostního incidentu je možné týmy označit jako *interní* (institucionální) nebo *koordinační*. Tým interního typu má obvykle možnost přímého zásahu (odpojit zdroj problému, zavést filtraci síťového provozu apod.), tým koordinačního typu možnost přímého zásahu nemá, jeho činnost se soustřeďuje na komunikaci, spolupráci a zprostředkování informací (v této roli jsou obvykle tzv. *národní* týmy, o kterých bude řeč dále).

V případě řešení konkrétního incidentu se jej zúčastnění snaží řešit přímo u zdroje, tzn. s tím, kdo má ke zdroji nebo cíli incidentu nejblíže a může co nejefektivněji zasáhnout (správce koncové sítě nebo služby). Ideální situace nastává, je-li zdroj i cíl v poli působnosti nějakého CSIRT týmu, protože je velmi jednoduché a rychlé najít konkrétního odborníka v místě problému. Ten potom také dokáže problém efektivně řešit a jeho reakce jsou předvídatelné - protože svá pravidla hry sám dobrovolně zveřejnil. Tento postup při komunikaci je velmi pružný díky tomu, že komunikace neprochází přes různé úrovně, je rychlá a přesná a stejná potom může být i reakce. Pokud však napadený nemůže nalézt odpovídající protějšek (ať už proto, že neexistuje, nedává o sobě žádné použitelné informace, odmítá problém řešit nebo prostě nereaguje), hodila

556: **AS** – **A**utonomous **S**ystem (autonomní systém). Autonomní systém je množina IP sítí a routerů pod společnou technickou správou, která reprezentuje vůči Internetu společnou routovací politiku.

by se nějaká „páka“. Tu jsou obvykle do jisté míry schopny poskytnout vrcholové týmy - **národní** a **vládní**.[557]

## 7.3 Jak vzniká CERT/CSIRT tým

Organizace, která se rozhodne zřídit tým typu CERT/CSIRT, si musí na začátku jasně a srozumitelně definovat, čeho chce vytvořením týmu dosáhnout, jakou roli od týmu požaduje (tzn. specifikuje jeho pole působnosti, jeho pravomoci, zodpovědnost a provozované služby) a musí jej také vhodným způsobem ukotvit v organizaci.

**Pole působnosti**
Polem působnosti je obvykle myšlena oblast kyberprostoru, ve které je tým způsobilý konat a nad kterou má příslušné pravomoci a odpovědnosti definované zřizovatelem. Na základě deklarovaného pole působnosti je potom tým kontaktován např. napadenými a řeší problémy ve sféře svého vlivu. Pole působnosti týmu může být definováno jako konkrétní síť/sítě, autonomní systém(y), jmenná doména/domény, objevují se ale také týmy, které jako pole působnosti uvádějí své expertní dovednosti, konkrétní službu apod.

**Služby**
Aby se tým mohl oficiálně nazývat týmem typu CERT/CSIRT, je potřeba, aby nabízel především službu řešení nebo koordinace řešení bezpečnostních incidentů v rámci svého definovaného pole působnosti, a tím naplnil myšlenku „response“ použité ve zkratkách CERT/CSIRT, tzn. je třeba, aby tento tým uměl *reagovat* na bezpečnostní incident. Tým ale může nabízet řadu dalších služeb z mnoha oblastí, např. školení, varování před aktuálními útoky, slabinami OS, bezpečnostní audity, SW konzultace, doporučení základních bezpečnostních pravidel, vývoj a provoz nástrojů pro sledování provozu sítě a služeb a mnoho dalších.

**Členové týmu**
Oblastí, která má rozhodující vliv na kvalitu týmu, je jeho personální obsazení. V každé provozované síti obvykle existuje oddělení, nebo skupina techniků, kteří mají na starosti provoz a rozvoj sítě a služeb a zabývají se také bezpečnostními aspekty (obecně „IT staff“, „bezpečáci“, „správci“ aj.). To jsou obvykle ty správné osoby pro začlenění do CERT/CSIRT týmu, nebo pro pověření jej vybudovat. V týmu je ovšem vhodné mít i další typy odborníků (např. právníka, v případě národních a vládních týmů najde uplatnění odborník přes komunikaci s médii, manažer, sociolog aj.). Záleží na zaměření, prostředí, nabízených službách a roli týmu.

557: Blíže viz kap. 7.8 Národní CSIRT České republiky a 7.9 Vládní CERT České republiky

Z „vnějšího“ pohledu se tým stane CERT/CSIRT týmem tehdy, až jej jako takový akceptují ostatní již existující světové CERT/CSIRT týmy. Cesta k získání statutu CERT/CSIRT tým není složitá, na jejím začátku stačí jasným způsobem deklarovat následující:

1) **Základní kontaktní informace** – jméno týmu, jméno organizace provozující tým, emailová adresa(y) týmu, na kterou je možné hlásit bezpečnostní incidenty nebo tým kontaktovat, telefonní číslo(a) týmu, adresu sídla, jména členů týmu, pracovní dobu po kterou je tým k zastižení apod.

2) **Pole působnosti týmu** – definuje, za co tým zodpovídá a jaká je jeho role. To se samozřejmě odvíjí od toho, o jaký tým jde. Je možné zřídit týmy zhruba těchto typů:

   - ***interní*** – slouží a zodpovídá za konkrétní síť (např. za konkrétní rozsah IP adres, domény), obvykle je zřízen provozovatelem sítě,
   - ***koordinační*** – tým, jehož hlavním úkolem je koordinovat řešení bezpečnostních incidentů, nemusí je cíleně řešit,
   - ***vendor*** – tým zabývající se řešením bezpečnostních incidentů, které se dotýkají konkrétního produktu (SW),
   - ***národní, vládní*** – speciální případy založené na principech prvních dvou zmíněných týmů (interní a koordinační), jejich pole působnosti a role závisí na zřizovateli a často také na legislativě konkrétní země.

3) **Nabízené služby –** tým typu CERT/CSIRT musí provozovat alespoň službu řešení bezpečnostních incidentů.

V okamžiku, kdy se nově zřízený CSIRT/CERT tým vypořádá s výše uvedenými kroky a stanoví si základní týmovou politiku řešení bezpečnostních incidentů, která obnáší klasifikaci vážnosti incidentů, pravidla reakce na incidenty, dosažitelnost členů týmu, pravidla pro komunikaci s autorem hlášení bezpečnostního incidentu apod., je na dobré cestě, aby jej okolní týmy akceptovaly. Samozřejmou a nezbytnou součástí je nutnost seznámit se se základními pravidly, na kterých se CSIRT komunita dohodla, a dodržovat je.

Na úplném počátku vytváření týmu typu CERT/CSIRT stojí také vybudování jeho technického a organizačního zázemí, bez kterého nemůže efektivně fungovat žádný tým.

**Technickým zázemím** se myslí například nástroj pro efektivní správu hlášení bezpečnostních incidentů, který umožní sledovat celý jeho životní cyklus, tj. kdy bylo hlášení zasláno, kým, kdo se v kterých fázích incidentem zabýval, proč, jak postupoval, kdo koho požádal o spolupráci, o jak závažný incident se jednalo a jaké se na něj uplatnily eskalační procedury apod. Pro tuto

oblast týmy obvykle používají různé tzv. ticketovací systémy, např. RTIR[558], OTRS[559]. Dalšími důležitými pomocníky na poli technických nástrojů jsou různé systémy IDS (Intrusion Detection System), systémy pro bezpečnostní audity sítě a zařízení, systémy pro forenzní analýzu, sledování provozu sítě (netflow) apod.

**Organizační zázemí** představuje právě onu zmiňovanou „připravenost" na problém, tzn. definování základních pravidel pro chod týmu tak, aby každý člen týmu znal svou roli, povinnosti a zodpovědnost, politiku postupu řešení bezpečnostních incidentů, pravidla pro komunikaci, sdílení a výměnu informací, spolupráci apod. Základem v této oblasti je obecně dobře zvládnutý tzv. ***incident management.***

V okamžiku, kdy nově vznikající tým zvládne výše uvedené, tzn. dokáže sebe a svou činnost popsat a vykonávat, může se zapojit do spolupráce na národní a mezinárodní úrovni.

## 7.4 Spolupráce CERT/CSIRT infrastruktury

CERT/CSIRT týmy vznikají na dobrovolné bázi a v jejich zájmu je navzájem efektivně komunikovat, vyměňovat si důležité informace a poznatky a spolupracovat. Sdružují se proto v mezinárodních organizacích. V současnosti nejznámější a nejaktivnější organizace, které se touto problematikou zabývají a vytvářejí vhodné prostředí pro výše uvedené záměry, jsou mezinárodní organizace **GÉANT**[560] a organizace **FIRST** (Forum for Incident Response and Security Teams).[561]

Obě výše zmíněné organizace iniciují a umožňují pravidelná setkávání členů bezpečnostních týmů, výměnu zkušeností a podílí se na definování základních pravidel spolupráce a komunikace mezi světovými CERT/CSIRT týmy.

Evropsky působící organizace GÉANT provozuje hned několik aktivit, do kterých se v případě zájmů světové CERT/CSIRT týmy mohou zapojit:

- **TF-CSIRT** (Task Force for CSIRT) je pracovní skupina, která umožňuje spolupráci týmů formou pravidelných dvou-třídenních setkání, která se konají 3x ročně (toto setkání obvykle hostuje některý CERT/CSIRT tým). Více informací je možné nalézt na: https://tf-csirt.org/.

558: **RTIR** - **R**equest **Tracker** for **I**ncident **R**esponse. Blíže viz např.: http://www.bestpractical.com/rtir/.

559: **OTRS** - **O**pen **S**ource **T**icket **R**equest **Systém**. Blíže viz např.: http://www.otrs.org/.

560: Sdružení vzniklo sloučením sdružení TERENA (Trans-European Research and Education Networking Association) a společnosti DANTE.

561: Více informací o organizaci FIRST je možné nalézt na: https://www.first.org

- **CSIRT Training** – slouží pro vyškolení nových členů CSIRT/CERT týmů, nebo pro ty, kdo se chystají CERT/CSIRT tým založit. Koná se obvykle 2x ročně a školiteli jsou zkušení členové renomovaných CERT/CSIRT týmů a další špičkoví odborníci z oblasti bezpečnosti. Více informací je možné nalézt na: https://tf-csirt.org/transits/.

- **Trusted Introducer**[562] – úřad, jehož primárním úkolem je budování důvěry mezi jednotlivými CERT/CSIRT týmy a pomoc při vzniku nových. Více informací je možné nalézt na: https://www.trusted-introducer.org/.

Organizace FIRST kromě každý rok pořádané velké výroční konference pořádá řadu školení, vytváří návody a standardy pro efektivní práci CERT/CSIRT týmů a samozřejmě spolupracuje s aktivitou TF-CSIRT.

Organizace GÉANT a FIRST v rámci světové infrastruktury CERT/CSIRT týmů plní roli jakési „záruky" toho, že tým, který o sobě tvrdí, že je CERT/CSIRT týmem, jím opravdu je, a že jím deklarovaný model chování je pravdivý. Každý nový tým, který se chce zapojit do bezpečnostní infrastruktury, prochází vstupním procesem, který ověří, zda tým odpovídá standardům komunity, je transparentní a neexistují závažné důvody proti jeho přijetí. V případě evropské infrastruktury (platformy TF-CSIRT) tento vstupní proces zajišťuje úřad Trusted Introducer a nový tým jej vlastně žádá o registraci v seznamu týmů a udělení statusu ***listed***.[563]

Mezi existujícími týmy se také musí najít alespoň dva týmy (tzv. sponzoři), které nový tým podpoří a žádný již etablovaný tým nesmí vznést námitku proti jeho přijetí. Pokud se vše podaří, jsou informace o novém týmu uloženy do seznamu, který udržuje úřad TI (a část z nich je zveřejněna), tým získává status ***listed*** a komunita přivítá nového člena.

V případě organizace FIRST je vstupní procedura velmi podobná, jen končí ne udělením statusu, ale získáním ***členství***.

Oba procesy mají jedno společné - jde o zjištění a zpřístupnění maximálního množství informací o daném týmu, popisu jeho chování a vnímání problematiky řešení bezpečnostních incidentů tak, aby to korespondovalo s požadavky komunity.

V případě úřadu Trusted Introducer je možné dosáhnout na další, významnější, statusy, a to statusy ***accredited*** a ***certified***. Rozdíly jsou následující:

- Tým s dosaženým statusem ***listed*** o sobě poskytl základní informace, deklaroval snahu chovat se jako CSIRT tým a komunita jej přijala.

562: Déle také **TI**.

563: ***Listed*** – uvedení nebo doslova „zalistování" týmu v databázi všech registrovaných týmů.

- Tým se statusem ***accredited*** deklaruje komunitou požadovanou úroveň svých postupů a zavázal se dodržovat společné TI politiky.

- Tým se statusem ***certified*** pak prokázal svou „úroveň zralosti“ (maturity) v rámci certifikačního procesu.

Být ***accredited*** nebo ***certified*** týmem vyžaduje kontinuální úsilí o udržení stavu týmu. Součástí tohoto úsilí je také povinnost udržovat v seznamu TI o týmu aktuální informace. Pokud by tak tým dlouhodobě nečinil, může o své statusy přijít a v nejhorším případě být komunitou vyloučen. Tato povinnost se týká také ***listed*** týmů, které v případě, že do tří let od získání statusu listed neprojdou procesem akreditace, musí svůj status listed obnovit prokázáním podpory ze strany ostatních týmů (tzn. re-listed proces). Tento mechanismus zajišťuje vysokou míru aktuálnosti informací v seznamu TI a tím jejich důvěryhodnost.

Další organizací, která působí v oblasti bezpečnosti, je organizace **ENISA** (European Network and Information Security Agency, http://www.enisa.europa.eu/). Ta úzce spolupracuje s členskými státy EU a soukromým sektorem a zastřešuje řadu aktivit zahrnujících celoevropské kybernetické bezpečnostní cvičení, rozvoj národních strategií v oblasti kybernetické bezpečnosti, spolupráci mezi CERT/CSIRT týmy a budování jejich kapacit, zabývá se problematikou ochrany osobních údajů a spolupracuje na vytváření a implementaci práva v záležitostech týkajících se síťové informační bezpečnosti (NIS - Network Information Security).

Všechny tři zmíněné organizace mají společnou ještě jednu funkci – shromažďují know-how z celé komunity a umožňují jeho sdílení (formulováním tzv. best-practices dokumentů, návodů, doporučení).

## 7.5 Hierarchie CERT/CSIRT týmů?

**CERT/CSIRT týmy žádnou oficiální hierarchii**, která by jeden tým činila nadřazeným jinému týmu, **nemají**. **Všechny týmy jsou si** z hlediska fungování, komunikace, spolupráce a výměny informací **rovnocenné** a nejsou v těchto oblastech nijak limitovány. Existence tzv. vrcholových národních a vládních týmů sice trochu evokuje, že nadřazenost mezi týmy existuje, ale není tomu tak. Jedinou „nadřazenost“, ale spíše by bylo na místě říci „větší akceschopnost“, dává vrcholovému týmu legislativa dané země, která upravuje jeho pravomoci (např. v oblasti požadované reakce na bezpečnostní hrozby ze strany provozovatelů sítí a služeb apod.[564]).

Ve světě CERT/CSIRT týmů je klíčová **ochota sdílet důležité informace** o incidentu a hrozbách. K tomu je nezbytné, aby si týmy navzájem důvěřovaly a také aby svým týmům

564: Blíže viz § 18 a § 20 ZoKB

věřili uživatelé. Získat důvěru uživatelů a komunity je dlouhodobý úkol, týmy musí své kvality ukazovat při všech aspektech svého fungování a důvěryhodnost si budovat postupně - nejen schopností pomoci, ale také schopností zajistit důvěrnost sdílených dat a korektní zacházení s nimi, transparentností chování apod.

## 7.6 Národní a vládní CERT/CSIRT týmy

Národní a vládní týmy jsou speciální formou CERT/CSIRT týmů. Jednají s ostatními CERT/CSIRT týmy jako rovný s rovnými, ale jejich role v celém systému je odlišná.

**Národní CERT/CSIRT** plní funkci jakéhosi **last resort – poslední instance**, u které je možné žádat o **zásah, pomoc a intervenci**. Jeho cílem je (v rámci státu, nebo oblasti kde působí) zprostředkovat kontakt mezi napadeným a původcem problému a napomoci úspěšnému řešení problému. Národní týmy (obvykle) nevládnou nad fyzickou infrastrukturou, takže nemají (na rozdíl od týmů interního/institucionálního typu) možnost přímého zásahu. Jejich role spočívá ve zprostředkování kontaktu, případně v koordinaci (odtud typ týmu **koordinační**) postupu jednotlivých řešitelů v případě, že problém je rozsáhlejší a jeho řešení vyžaduje spolupráci více složek.

Z principu fungování celé struktury jsou incidenty, které projdou přes systém národního CSIRTu, zpravidla jen zlomkem celkového počtu. Většina incidentů se vyřeší v rámci přímé komunikace, bez nutnosti eskalací a zprostředkování. K národnímu týmu se tak dostávají převážně incidenty, které nelze vyřešit jinak (zodpovědné osoby je řešit odmítají, není jednoduché identifikovat, kdo je za jejich řešení zodpovědný), velmi závažné nebo opakující se problémy, nebo problémy, které mohou mít plošný dopad apod.

Národní CERT/CSIRT má obvykle ve svém popisu práce také **vzdělávání a spolupráci**. Jedná se jak o osvětu směrem k veřejnosti, tak o působení v rámci internetové infrastruktury. Cílem je podpora vytváření dalších CERT/CSIRT týmů v zemi, jejich uvádění na mezinárodní scénu a podpora při zavádění standardních postupů a procedur. To vše výrazně zvyšuje transparentnost prostředí a dává napadeným šanci efektivně se dobrat nápravy.

Vládní **CERT/CSIRT** se obvykle zaměřuje na oblast státní správy a samosprávy a na řešení incidentů, které ohrožují bezpečnost státu a jeho služeb. Vládní CERT/CSIRT může mít podobu týmu interního s možností přímého zásahu v případě problému. Jeho existence je obvykle podpořena legislativně.

Výše uvedené ale není dogma, situace v jednotlivých zemích se liší. Jsou země, kde funguje pouze národní tým (a plní také funkci vládního), jsou země, kde funguje vládní (a plní roli

národního), jsou země, kde existují oba, jsou země, kde není ani jeden a roli vrcholového týmu supluje jeden z existujících týmů a pod.

## 7.7 Situace v ČR a ve světě

V současné době je ve světě oficiálně konstituováno okolo 380 bezpečnostních týmů typu CERT/CSIRT, které jsou buď členy organizace FIRST, nebo evropské platformy TF-CSIRT (případně obou).

V České republice je aktuálně oficiálně zřízeno a úřadem Trusted Intoducer uznáno 39 bezpečnostních týmů typu CERT/CSIRT, což z České republiky činí takřka světovou „velmoc", kdy co do počtu konkuruje pouze Francie, Německo a Velká Británie. Nejde samozřejmě o kvantitu, ale především o kvalitu.

Prvním bezpečnostním týmem typu CERT/CSIRT, který v České republice vznikl, je bezpečnostní tým **CESNET-CERTS** (https://csirt.cesnet.cz/). Byl oficiálně konstituován v roce 2003, v lednu 2004 jej pak oficiálně uznala mezinárodní infrastruktura a úřad Trusted Introducer. Je provozován sdružením CESNET[565] a je zodpovědný za řešení a koordinaci řešení bezpečnostních incidentů v e-infrastruktuře CESNET. Mimo jiné se zabývá vývojem bezpečnostních nástrojů a pro uživatele ve sféře svého vlivu poskytuje také služby osvětového charakteru.

Další týmy pak byly založeny ve sdružení CZ.NIC (CZ.NIC-CSIRT) v roce 2008, na Masarykově univerzitě v Brně (CSIRT-MU) v roce 2009, ve společnosti Active24 (tým Active24-CSIRT) v roce 2012 a v rámci projektu podporovaného Ministerstvem vnitra ČR tým CSIRT.CZ (od roku 2011 Národní CSIRT ČR).

Velký boom v oblasti budování bezpečnostních CERT/CSIRT týmů můžeme v České republice pozorovat především od roku 2013, kdy Česká republika čelila sérii DDoS útoků na veřejné www služby. Tato událost následně iniciovala vznik projektu Fenix (https://fe.nix.cz/) na půdě českého peeringového centra NIX.CZ.

Smyslem tohoto projektu je umožnit v případě DoS útoku dostupnost internetových služeb v rámci subjektů zapojených do této aktivity. Projekt Fenix definoval řadu technických a organizačních pravidel, které musí zájemci o vstup do projektu splnit a jedním z nich je také oficiálně konstituovaný tým typu CERT/CSIRT. To bylo pro řadu organizací impulsem, aby své

565: Sdružení CESNET, z. s. p. o., je zájmové sdružení právnických osob, založené v roce 1996 vysokými školami a Akademií věd České republiky. Provozuje národní vysokorychlostní počítačovou síť určenou pro vědu, výzkum, vývoj a vzdělávání CESNET2. Více viz http://www.cesnet.cz/.

bezpečnostní týmy formalizovaly do podoby CERT/CSIRT týmu a začlenily je do mezinárodní infrastruktury.

Za další motivační impuls, který vedl ke konstituování nových týmů, lze také označit přijetí a následnou účinnost zákona o kybernetické bezpečnosti. Řada organizací pochopila, že bezpečností se vyplatí zabývat, a že zřízení týmu typu CERT/CSIRT přináší výhody.

Současná infrastruktura CERT/CSIRT týmů v ČR čítající 39 týmů sestává z národního a vládního týmu, jsou zde týmy na úrovni velkých ISP, několik týmů v akademickém sektoru, týmy v bankovním odvětví, v IT firmách, u doménových registrátorů a v neposlední řadě také na půdě českého peeringového centra NIX.CZ, na půdě sdružení CZ.NIC. Dohromady se tak jedná o velice různorodou a ve výsledku robustní a životaschopnou infrastrukturu, které nechybí zkušenosti z různých odvětví.

**Aktuální seznam českých CERT/CSIRT týmů je možné nalézt na:**
https://tiw.trusted-introducer.org/directory/country_LICSA.html

## 7.8 Národní CSIRT České republiky

V prosinci roku 2010 se oficiálního zřízení Národního CSIRTu České republiky dočkala i Česká republika. Sdružení CZ.NIC a Ministerstvo vnitra podepsaly (16. prosince 2010) Memorandum, podle kterého správce české národní domény sdružení CZ.NIC převzal agendu týmu CSIRT.CZ a od ledna 2011 jej z pověření MV ČR[566] provozuje jako Národní CSIRT ČR.

Pracoviště CSIRT.CZ (http://www.csirt.cz/) vzniklo v rámci plnění grantu Ministerstva vnitra České republiky *„Problematika kybernetických hrozeb z hlediska bezpečnostních zájmů České republiky"* (identifikační kód projektu je VD20072010B013) a bylo vybudováno sdružením CESNET. Toto pracoviště bylo označováno jako modelové a bylo vybudováno za účelem ověření stavu bezpečnostní infrastruktury v ČR a ověření realizovatelnosti vybudování distribuované hierarchie pro systematické plošné řešení bezpečnostní problematiky v počítačových sítích ČR prostřednictvím CSIRT týmů. Provoz tohoto týmu byl oficiálně spuštěn 3. dubna 2008, v květnu téhož roku byl na zasedání TF-CSIRT komunity (které proběhlo v Oslu, Norsko) představen ostatním evropským CERT/CSIRT týmům jako pracoviště typu CSIRT s rolí *„last resort"* pro Českou republiku a jako takový byl komunitou přijat.

566: Tato gesce přešla v roce 2011 z MV ČR na NBÚ.
Blíže viz kap. 3.1 Legislativní vývoj kybernetické bezpečnosti v ČR

Pracoviště CSIRT.CZ položilo základy pro další rozvoj vrcholové úrovně CERT/CSIRT infrastruktury v ČR, a to především v oblasti spolupráce. Zároveň ověřil a potvrdil předpoklad, že vrcholové CERT/CSIRT týmy v České republice mají smysl.

Národní CSIRT České republiky plní i další úkoly – blíže viz § 18 ZoKB.

## 7.9 Vládní CERT České republiky

Dne 19. října 2011 přijala vláda České republiky usnesení č. 781 o ustavení Národního bezpečnostního úřadu (NBÚ) gestorem problematiky kybernetické bezpečnosti v České republice a zároveň národní autoritou pro tuto oblast. NBÚ se od počátku svého jmenování soustředilo na tři úkoly – napsání zákona o kybernetické bezpečnosti, vybudování NCKB (Národního centra kybernetické bezpečnosti) a vybudování Vládního CERT ČR.

Vládní CERT ČR, tým GovCERT.CZ, byl do mezinárodní komunity začleněn v roce 2012, a tím se Česká republika zařadila mezi země, které mají Národní i Vládní CERT/CSIRT tým.

Do kompetence GovCERT.CZ spadají sítě státní správy, samosprávy a kritické infrastruktury ČR. Tým se dále soustřeďuje na vývoj a provoz bezpečnostních služeb, osvětu a zapojuje se také do národní a mezinárodní spolupráce.

Vládní CERT České republiky plní i další úkoly – blíže viz § 20 ZoKB.

## 7.10 Na který CERT/CSIRT tým se obrátit?

Název této subkapitoly je zároveň častým postesknutím uživatele Internetu, který se dostal do problému (např. na něj někdo útočí, zcizil mu identitu, naboural facebookový profil nebo e-mailový účet, nebo se stal svědkem šíření dětské pornografie). Co má takový uživatel dělat? Obrátit se na Policii ČR? Nebo na poskytovatele připojení, např. jeho helpdesk? Nebo na Národní úřad pro kybernetickou a informační bezpečnost, když je gestorem pro oblast kyberbezpečnosti? Na horkou linku Národního centra bezpečnějšího internetu? Nebo na nějaký CSIRT tým, když se o nich pořád mluví? Ale na který?

**Na proces hlášení a řešení bezpečnostních incidentů** (neboli opravdu „na koho se mám obrátit, když chci ohlásit nebo řešit zjištěný bezpečnostní incident“) **je možné nahlížet ze dvou úhlů pohledu.** Z pohledu **techniků** (správců sítí a služeb, členů bezpečnostních týmů) a z pohledu **uživatelů**.

Pro techniky (správce sítí a služeb, členy bezpečnostních týmů) je odpověď na otázku „na koho se mám se žádostí o akci vlastně obrátit“ celkem jasná, ale to je dáno drilem, zkušenostmi a především velmi dobrou znalostí prostředí Internetu a jeho základních principů, jakož i znalostí toho, kde jsou k mání kontaktní informace k jednotlivým existujícím sítím, službám, doménám apod.

Pro členy CERT/CSIRT týmů jsou základními zdroji kontaktních informací databáze RIRů, databáze provozovatelů domén nejvyšší úrovně a katalogy CERT/CSIRT týmů.

**RIR** (Regionální Internetový Registr) drží a zpřístupňují informace o tom, komu byl přidělen který blok IP adres. Svět je rozdělen na oblasti a každý RIR (aktuálně RIPE, ARIN, APNIC, LACNIC, AFRINIC) přiděluje IP adresy pro svoji oblast. Oblast Evropy, Blízkého východu a části Asie je pod správou organizace RIPE NCC (https://www.ripe.net/). RIR provozují veřejně přístupné databáze, které obsahují údaje o přidělených internetových sítích a jejich správcích. Tyto databáze tak umožňují vyhledat údaje o tom, která organizace a kteří správci jsou zodpovědní za konkrétní IP adresy.

Dalším zdrojem užitečných informací jsou údaje o doménách, které provozují a zpřístupňují správci domén nejvyšší úrovně, pro TLD doménu .cz je to sdružení CZ.NIC.

A pak je zde oblast CERT/CSIRT týmů, které své pole působnosti obvykle definují pomocí internetových identifikátorů, jmenných domén, nebo klidně jen slovně. Vzhledem k jejich počtu, způsobu definování jejich pole působnosti a zejména rozdílům v jejich úrovni není vždy snadné najít tým, který je schopný pomoci. Pro usnadnění orientace mezi týmy vznikly jakési „katalogy“, o které se starají organizace FIRST a úřad Trusted Introducer. Tyto katalogy obsahují základní informace o CERT/CSIRTech, kontaktech, jejich poli působnosti apod.

Proces hlášení a řešení bezpečnostních incidentů (odborně ***incident handling***) není exaktní proces, právě naopak, a hodně záleží na zkušenostech a občas i kreativitě člověka, který tento proces provádí. Výměna informací mezi týmy obvykle probíhá rychle a efektivně, i když ani to často nezaručuje rychlé vyřešení problému, protože na to je celá infrastruktura ještě stále poměrně „řídká“, a bohužel je nutné konstatovat, že i úroveň týmů je různá.

**Optimální stav infrastruktury by byl ten, kdyby se každá IP adresa vyskytovala v poli působnosti oficiálního CSIRT týmu.** V této situaci ale infrastruktura CERT/CSIRT týmů zdaleka není.

***Z pohledu normálního uživatele*** je situace značně nejasná a popravdě i matoucí. Co by tedy uživatel měl v případě zjištění bezpečnostního incidentu vlastně dělat a na koho by se měl obrátit? Těžko po uživateli chtít, aby se orientoval v problematice CERT/CSIRT týmů, dokázal si najít ten správný, nastudoval jeho politiku hlášení bezpečnostních incidentů a šel konat. Uživatel

by se v první řadě měl **obrátit na administrátora své sítě či služeb** (pokud někoho takového má), případně by měl spolupracovat s poskytovatelem připojení, tzn. **helpdeskem svého ISP nebo jeho uživatelskou podporou**. Na straně poskytovatele připojení či služeb by měl pro jeho uživatele existovat jasně popsaný vstupní bod (kontakt), na který by se uživatelé mohli a měli obracet v případě, kdy se stanou cílem útoku, zjistí bezpečnostní incident, nebo mají pocit, že něco není v pořádku. To je důvod, proč je prostředí poskytovatelů připojení jednou z nejdůležitějších oblastí, kde by měl být konstituován oficiální CERT/CSIRT tým a poskytovat služby z oblasti bezpečnosti uživatelům své sítě.

Samozřejmě může nastat situace, kdy jak technik, tak uživatel udělá všechno správně, a řešení problému stejně není v dohledu. Osoba či tým na hlášený problém nereaguje, nebo jej dokonce odmítá řešit (s tím, že to není jeho problém, nebo to není tak vážné) apod. To je právě moment, kdy ke slovu přichází buď Policie ČR (uživatel se na ni může obrátit s podáním trestního oznámení), nebo vrcholový tým (národní nebo vládní), na nějž se uživatel může obrátit jako na poslední instanci, od které lze očekávat pomoc a reakci.

**Mezi národním a vládním týmem existuje velmi úzká spolupráce** a výměna informací a relevantních dat, a tedy i předání nahlášeného problému k řešení od jednoho týmu k druhému nebo přímo spolupráce na řešení.

Národní i vládní tým by obecně pro provozovatele sítí, služeb (a v případě nutnosti i pro uživatele) měly být místem, kde je v případě problémů, nejasností apod. možné žádat o pomoc a konzultaci, např. dohledání vhodného protějšku ke komunikaci (zahraničního CERT/CSIRT týmu), zprostředkování komunikace (ano, někdy se „páka“ vrcholového týmu hodí, protějšek je pak ochotnější), a zdrojem know-how a informací.

**Obecně by ale bylo žádoucí, aby správci sítí a služeb a členové bezpečnostních týmů zvládali a aplikovali principy procesu *incident handling* a maximum komunikace probíhalo přímo** (ne přes vrcholové týmy). To činí proces incident handlingu rychlým a efektivním, další mezistupně do něj mohou vnášet nepříjemná zdržení a bohužel i zkreslení. Ale jak už bylo řečeno, záleží na závažnosti situace a řešeného problému.

**Týmy typu CERT/CSIRT a jejich infrastruktura obecně nejsou všespasitelné a neznamenají zajištění bezpečnosti „v kostce“.**

Jejich existence je jen jeden z kamínků v oblasti budování bezpečnosti Internetu, ve kterém hrají svou důležitou roli všichni zainteresovaní, tj. správci sítí, služeb, manažeři, kteří rozhodují o zázemí pro efektivní zabezpečení sítí a služeb, ISP, provozovatelé kritických služeb, bezpečnostní složky, stát, a v neposlední řadě také my uživatelé.

# Závěr

## Závěr

*„Svoboda je nerozlučně spojena s odpovědností."*

Benjamin Franklin

Žijeme v době, kdy jsou informační a komunikační technologie již neodmyslitelně propojeny s každým aspektem našeho bytí. Určitým paradoxem je, že de facto nemáme možnost se tomuto prostupu a vzájemné interakci s ICT vyhnout, což nás současně činí více zranitelnými.

Díky informačním a komunikačním technologiím a propojeným službám vytváříme odraz své identity či osobnosti ve světě virtuálním.

Naše digitální „já" má všechny předpoklady pro to být „mnohem trvanlivější" než naše fyzické tělo. Informace o našich aktivitách v kyberprostoru, naše kyberosobnosti, účty a digitální stopy budou díky archivaci dat a informací o nás žít i po naší smrti.

S tím, jak roste objem dat a informací ukládaných v jednotlivých ISP, začínají být stále více řešeny i otázky jejich efektivního zabezpečení, předávání či vymazání, a to ne jen na základě smlouvy uzavřené mezi poskytovatelem dané služby a koncovým uživatelem, ale i na základě nově vznikajících právních předpisů.

Státy, organizace, ale i jednotlivci si čím dál více uvědomují, že informace a data představují významný potenciál, který je ve stále větší míře napadán kybernetickými útoky ať již s cílem zcizení, poškození, znepřístupnění, či vymazání dat.

Pokud chceme v současné společnosti žít a využívat její benefity, není možné se od ICT oprostit a rozhodně nemá smysl tyto technologie přestat využívat. Je třeba se začít učit, jak tyto technologie a služby využívat, jak se vyhnout či alespoň eliminovat následky způsobené kybernetickými útoky.

Řadě negativních událostí se lze vyhnout, pokud budou jedinci i organizace respektovat alespoň základní principy kybernetické bezpečnosti.

V této knize jsme se Vám snažili předat informace o tom, co to kybernetická bezpečnost vůbec je, na jakých principech je postavena a jaké další pojmy s ní bezprostředně souvisejí.

Podstatná část monografie byla věnována legislativě, zejména pak komentáři k zákonu č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), který je stěžejní českou právní normou právě v oblasti kybernetické bezpečnosti. Do vlastního komentáře byly zaimplementovány i požadavky plynoucí ze směrnice Evropského parlamentu a Rady (EU) 2016/1148 o opatřeních k zajištění vysoké společné úrovně

bezpečnosti sítí a informačních systémů v Unii (NIS) a z prováděcích právních předpisů k zákonu o kybernetické bezpečnosti. Komentář k zákonu o kybernetické bezpečnosti by měl poskytnout čtenáři vhled do práv a povinností jednotlivých subjektů, ale i do základních principů kybernetické bezpečnosti, které jsou v tomto zákoně definovány.

**Bezpečnost není stav…**
**Bezpečnost je proces…**
**Bezpečnost může být cíl…**
**Bezpečnost není neměnná konstanta…**

Je na nás, koncových uživatelích, abychom pochopili principy bezpečnosti (zejména té kybernetické), tyto principy si upravili dle svých potřeb a zejména je respektovali.

V kyberprostoru, stejně jako ve světě reálném, neexistuje jedna bezpečnost a jedno zabezpečení, které by bylo možné univerzálně aplikovat na každého. Pokud chceme řešit bezpečnost, je třeba ji řešit komplexně a je třeba individualizovat.

Informační a komunikační technologie jsou oborem, který se nejdynamičtěji a nejmasivněji vyvíjí. Oblasti, kterým bychom v této souvislost měli věnovat extrémní pozornost, jsou bezpečnost a edukace uživatelů.

„*Vědění je dvojího druhu. Buďto známe předmět, anebo víme, kde se o něm poučit.*“

Samuel Johnson

# Seznam použitých pramenů a dalších zdrojů

## Seznam použitých pramenů a dalších zdrojů

*[Download] WPA-PSK Rainbow Tables.* [online]. [cit. 11. 8. 2018]. Dostupné z: https://securityonline.info/wpa-psk-tables/

*2018 Data Breach Investigation Report. 11th Edition.* [online]. [cit. 28. 7. 2018]. Dostupné z: http://www.documentwereld.nl/files/2018/Verizon-DBIR_2018-Main_report.pdf

*25-GPU cluster cracks every standard Windows password in <6 hours.* [online]. [cit. 20. 8. 2017]. Dostupné z: https://arstechnica.com/information-technology/2012/12/25-gpu-cluster-cracks-every-standard-windows-password-in-6-hours/

*787, 618, 302, 67, 18, Aneb statistiky jednoho „bláznivého oběda".* [online]. [cit. 20. 7. 2017]. Dostupné z: https://blog.nic.cz/2014/10/20/787-618-302-67-18-aneb-statistiky-jednoho-blazniveho-obeda/

*Akční plán k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020.* [online]. Dostupné z: https://www.govcert.cz/download/gov-cert/container-nodeid-967/akc48dnc3adplc3a1n-rkb-final-150408.pdf

*An overview of the Wi-Fi WPA2 vulnerability*. [online]. [cit. 11. 9. 2018]. Dostupné z: https://www.enisa.europa.eu/publications/info-notes/an-overview-of-the-wi-fi-wpa2-vulnerability

*Analýza rizik.* [online]. [cit. 1. 7. 2018]. Dostupné z: https://www.vlastnicesta.cz/metody/analyza-rizik-risk/

ANDRESS, Jason. *The Basics of Information Security*. 2nd Edition. Syngress. ISBN: 9780128007440

*Aplikační gateway.* [online]. [cit. 15. 8. 2017]. Dostupné z: https://docs.microsoft.com/en-us/azure/application-gateway/application-gateway-web-application-firewall-portal

*ARP Cache Poisoning.* [online]. [cit. 15. 7. 2017]. Dostupné z: https://tournasdimitrios1.wordpress.com/2011/02/08/4426/

*Attacking IPv6 Implementation Using Fragmentation.* [online]. [cit. 5. 8. 2017]. Dostupné z: https://media.blackhat.com/bh-eu-12/Atlasis/bh-eu-12-Atlasis-Attacking_IPv6-WP.pdf

*Authorization to Use the CERT Mark.* [online]. [cit. 1. 7. 2018]. Dostupné z: https://www.sei.cmu.edu/education-outreach/license-sei-materials/authorization-to-use-cert-mark/index.cfm

*Background: DDoS Attack on Major US banks.* [online]. [cit. 25. 8. 2018]. Dostupné z: https://www.incapsula.com/blog/cyber-attack-us-banks.html

*BackTrack, Kali Linux a Evil (Twin) Access Point.* [online]. [cit. 11. 8. 2018]. Dostupné z: https://www.root.cz/clanky/backtrack-kali-linux-a-evil-twin-access-point/

BARLOW, Perry John. *A Declaration of the Independence of Cyberspace.* [online]. [cit. 23. 9. 2014]. Dostupné z: https://www.eff.org/cyberspace-independence.
Český zdroj: http://www.piratskelisty.cz/clanek-1476-deklarace-nezavislosti-kyberprostoru

BAŠTA, Pavel. Budování a implementace českého národního Cyber Threat Intelligence System. *Bezpečnostní teorie a praxe.* 2016 (4), s. 129–136

BAŠTA, Pavel. *Vytěžování informací o incidentech a jejich distribuce Aneb co je to PROKI.* [online]. [cit. 28. 8. 2018]. Dostupné z: http://blog.nic.cz/2016/02/04/vytezovani-informaci-o-incidentech-a-jejich-distribuce-aneb-co-je-to-proki/

*Bezpečnostní role a jejich začlenění v organizaci.* [online]. [cit. 21. 8. 2018]. Dostupné z: https://nukib.cz/download/kii-vis/container-nodeid-574/bezpecnostnirolev41.pdf

*Biometrie je více než otisk prstu.* [online]. [cit. 4. 7. 2018]. Dostupné z: https://ictrevue.ihned.cz/c3-65967870-0ICT00_d-65967870-biometrie-je-vice-nez-otisk-prstu

*BIOS.* [online]. [cit. 6. 7. 2017]. Dostupné z: https://cs.wikipedia.org/wiki/BIOS

*Brute forcing Wi-Fi Protected Setup (802.11w).* [online]. [cit. 20. 7. 2017]. Dostupné z: https://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf

CASEY, Eoghan. *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, Second Edition.* London: Academic Press, 2004. ISBN 0-12-163104-4.

*CIA triad methodology.* [online]. [cit. 10. 7. 2018]. Dostupné z: https://en.wikipedia.org/wiki/Information_security#/media/File:CIAJMK1209.png

*Cloud Computing Begins to Gain Traction on Wall Street.* [online]. [cit. 15. 4. 2012]. Dostupné z: http://www.wallstreetandtech.com/it-infrastructure/212700913

*Cloudware.* [online]. [cit. 10.4.2012]. Dostupné z: http://www.cloudwareinc.com/

*Computer Security Incident Handling Guide* [online]. [cit. 13. 8. 2018]. Dostupné z: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

*Configuring IP Access Lists.* [online]. [cit. 13. 8. 2017]. Dostupné z: https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html

*Cybersecurity.* [online]. [cit. 6. 7. 2018]. Dostupné z: https://en.oxforddictionaries.com/definition/cybersecurity Překlad autora.

*Cybersecurity.* [online]. [cit. 6. 7. 2018]. Dostupné z: https://www.merriam-webster.com/dictionary/cybersecurity Překlad autora.

*Cyberspace.* [online]. [cit. 6. 7. 2018]. Dostupné z: https://en.oxforddictionaries.com/definition/cyberspace Překlad autora.

*Cyberspace Operations: Concept Capability Plan 2016-2028*. [online]. [cit. 18. 2. 2018], s. 8-9 Dostupné z: www.fas.org/irp/doddir/army/pam525-7-8.pdf?

*Cyberthreat.* [online]. [cit. 6. 7. 2018]. Dostupné z: https://en.oxforddictionaries.com/definition/cyberthreat Překlad autora.

*Definition of Cybersecurity - Gaps and overlaps in standardisation*. [online]. [cit. 10. 12. 2017]. Dostupné z: https://www.enisa.europa.eu/publications/definition-of-cybersecurity

*Detecting and Preventing Unauthorized Outbound Traffic.* [online]. [cit. 16. 8. 2017]. Dostupné z: https://www.sans.org/reading-room/whitepapers/detection/detecting-preventing-unauthorized-outbound-traffic-1951

*DHCP Snooping Binding Database.* [online]. [cit. 14. 7. 2017]. Dostupné z: http://www.write-mem.net/?q=dhcp-snoop-dai-ip-src-grd

*Digital Identity Guidelines.* [online]. [cit. 4. 9. 2017]. Dostupné z: https://pages.nist.gov/800-63-3/sp800-63b.html#sec5

*Discover Wi-Fi Security.* [online]. [cit. 11. 9. 2018]. Dostupné z: https://www.wi-fi.org/discover-wi-fi/security

*Doporučení NÚKIB k ustanovení § 10a zákona o kybernetické bezpečnosti.* [online]. [cit. 1.8.2018]. Dostupné z: https://nukib.cz/download/kii-vis/Ustanoven%C3%AD_para10a_ZKB_a_utajovane_informace_v1-1_web.pdf s. 4

*Důvodová zpráva k návrhu zákona č. 205/2014 Sb.* [online]. [cit. 21. 8. 2018]. Dostupné z: https://apps.odok.cz/veklep-detail?pid=ALBSABVH86O2

*Důvodová zpráva.* [online]. [cit. 21. 8. 2018]. Dostupné z: https://www.govcert.cz/download/legislativa/container-nodeid-708/nbu-zkb-navrh-130415-duvodzprava.pdf s. 70

ELIÁŠ, Karel. *Věc, jako pojem soukromého práva.* [online]. [cit. 6. 6. 2016]. Dostupné z: http://www.pavelpetr.cz/soubory/29/87/Karel_Elias_Vec_jako_pojem_soukromeho_prava.pdf

EVANS, Donald, Philip, BOND a Arden BEMET. *Standards for Security Categorization of Federal Information and Information Systems.* National Institute of Standards and Technology, Computer Security Resource Center. [online]. [cit. 10. 12. 2017]. Dostupné z: https://csrc.nist.gov/csrc/media/publications/fips/199/final/documents/fips-pub-199-final.pdf

*Evidence podnikatelů v elektronických komunikacích podle všeobecného oprávnění.* [online]. [cit. 21. 8. 2018]. Dostupné z: https://www.ctu.cz/vyhledavaci-databaze/evidence-podnikatelu-v-elektronickych-komunikacich-podle-vseobecneho-opravneni

*Evil twin (wireless networks).* [online]. [cit. 11. 8. 2018]. Dostupné z: https://en.wikipedia.org/wiki/Evil_twin_(wireless_networks)

*Four-Way Handshake.* [online]. [cit. 11. 8. 2018]. Dostupné z: https://www.techopedia.com/definition/27188/four-way-handshake

FRANK, Libor. *Bezpečnostní studia.* [online]. [cit. 10. 7. 2018]. Dostupné z: https://moodle.unob.cz/pluginfile.php/20182/mod_resource/content/1/N%C3%A1rodn%C3%AD%20strategie%20informa%C4%8Dn%C3%AD%20bezpe%C4%8Dnosti%20%C4%8CR.pdf

FRUHLINGER, Josh. *What is Stuxnet, who created it and how does it work?* [online]. [cit. 1. 7. 2018]. Dostupné z: https://www.csoonline.com/article/3218104/malware/what-is-stuxnet-who-created-it-and-how-does-it-work.html

*GDPR stručně.* [online]. [cit. 7. 8. 2018]. Dostupné z: https://www.uoou.cz/gdpr%2Dstrucne/ds-4843/archiv=0&p1=3938

GREENFIELD, David. *Integrovaná bezpečnost: Už nastal její čas?* [online]. [cit. 1. 3. 2018]. Dostupné z: http://www.controlengcesko.com/hlavni-menu/artykuly/artykul/article/integrovana-bezpecnost-uz-nastal-jeji-cas/

GUZMAN, Andrew, Joost H. B. PAUWELYN. *International Trade Law*. Aspen Publishers, 2012, s. 37.

HAVELKA, Jiří a kol. *Výkladový slovník výpočetní techniky a komunikací.* 1. Vyd. Praha: Computer Press, 1997. ISBN 80-7226-023-5.

HENDERSON, Anthony. *The CIA Triad: Confidentiality, Integrity, availability.* [online]. [cit. 13. 1. 2018]. Dostupné z: http://panmore.com/the-cia-triad-confidentiality-integrity-availability

*Hrozba.* [online]. [cit. 28. 7. 2018]. Dostupné z: http://www.mvcr.cz/clanek/hrozba.aspx

HSU, D. Frank a D. MARINUCCI (eds.). *Advances in cyber security: technology, operations, and experiences*. New York: Fordham University Press, 2013. 272 s. ISBN 978-0-8232-4456-0.

HUSOVEC, Martin. *Zodpovednosť na Internete podľa českého a slovenského práva*. Praha: CZ.NIC, 2014. ISBN: 978-80-904248-8-3.

*Informace o institutu provozovatele informačního nebo komunikačního systému.* [online]. [cit. 7. 8. 2018]. Dostupné z: https://nukib.cz/download/kii-vis/provozovatel_IS-KS_v1.0-final.pdf s. 4

*Informace o institutu základní služby.* [online]. [cit. 7. 8. 2018]. Dostupné z: https://nukib.cz/download/kii-vis/Informace_o_institutu_z%C3%A1kladn%C3%AD_slu%C5%BEby_v1.2.pdf

*Integrovaná multidisciplinární bezpečnost.* [online]. [cit. 17. 2. 2018]. Dostupné z: https://www2.deloitte.com/cz/cs/pages/risk/solutions/integrovana-multidisciplinarni-bezpecnost.html

*Internet of Things (IoT).* [online]. [cit. 15. 7. 2016]. Dostupné z: http://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT

*IPv6 First-Hop Security Configuration GuideIPv6 Destination Guard.* [online]. [cit. 12. 8. 2017]. Dostupné z: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_fhsec/configuration/xe-16/ip6f-xe-16-book/ipv6-dest-guard.html

*Jak se Češi s hesly potýkají: analýza 16 tisíc ukradených hesel.* [online]. [cit. 4. 9. 2017]. Dostupné z: https://www.root.cz/clanky/jak-se-cesi-s-hesly-potykaji-analyza-16-tisic-ukradenych-hesel/

JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. 3. aktualiz. vyd. Praha: AFCEA, 2015. ISBN 978-80-7251-436-6. Dostupné z: https://www.govcert.cz/download/slovnik/vykladovy_slovnik_KB_3_vydani.pdf

JIROVSKÝ, Václav. *Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada, 2007. ISBN 978-80-247-1561-2.

KADLECOVÁ, Lucie. *Konceptuální a teoretické aspekty kybernetické bezpečnosti.* [online]. [cit. 21. 7. 2018]. Dostupné z: https://is.muni.cz/el/1423/podzim2015/BSS469/um/Prezentace_FSS_Konceptualni_a_teoreticke_aspekty_KB.pdf

*Kde hledat abuse kontakty?* [online]. [cit. 28. 8. 2018]. Dostupné z: https://blog.nic.cz/2016/04/04/kde-hledat-abuse-kontakty/

*Kdy nás kontaktovat.* [online]. [cit. 7. 7. 2018]. Dostupné z: https://www.csirt.cz/page/2632/kdy-nas-kontaktovat/

*Kensington Security Slot.* [online]. [cit. 6. 7. 2017]. Dostupné z: https://cs.wikipedia.org/wiki/Kensington_Security_Slot

*KeyGrabber Wi-Fi Premium*. [online]. [cit. 6. 7. 2017]. Dostupné z: https://www.keelog.com/wifi_hardware_keylogger.html

KODET, Jaroslav. *Kybernetický zákon: Využijte naplno open source nástroje.* [online]. [cit. 25. 4. 2018]. Dostupné z: https://www.nic.cz/files/nic/doc/Securityworld_CSIRTCZ_112015.pdf

KOLOUCH, Jan a Petr VOLEVECKÝ. *Trestněprávní ochrana před kybernetickou kriminalitou.* Praha: Policejní akademie České republiky v Praze, 2013, s. 65

KOLOUCH, Jan. *CyberCrime.* [online]. Praha: CZ.NIC, 2016. [cit. 31.12. 2016]. ISBN 978-80-88168-18-8. Dostupné z: https://knihy.nic.cz/files/edice/cybercrime.pdf

KOLOUCH, Jan. *CyberCrime.* [online]. Praha: CZ.NIC, 2016. [cit. 31.12. 2016]. ISBN 978-80-88168-17-1. Dostupné z: https://knihy.nic.cz/files/edice/cybercrime.mobi

KOLOUCH, Jan. *CyberCrime.* [online]. Praha: CZ.NIC, 2016. [cit. 31.12. 2016]. ISBN 978-80-88168-16-4. Dostupné z: https://knihy.nic.cz/files/edice/cybercrime.epub

KOLOUCH, Jan. *CyberCrime.* Praha: CZ.NIC, 2016. ISBN 978-80-88168-15-7

*Koncepce boje proti organizovanému zločinu (2000).* [online]. Dostupné z: https://www.databaze-strategie.cz/cz/mv/strategie/koncepce-boje-proti-organizovanemu-zlocinu?typ=download

*Koncepce boje proti trestné činnosti v oblasti informačních technologií včetně Harmonogramu opatření.* [online]. [cit. 13. 8. 2018], s. 3. Dostupné z: http://www.mvcr.cz/soubor/koncepce-pdf.aspx

*Kritická zranitelnost mnoha domácích routerů.* [online]. [cit. 16. 7. 2017]. Dostupné z: https://blog.nic.cz/2014/05/21/kriticka-zranitelnost-mnoha-domacich-routeru/

KROPÁČOVÁ, Andrea. *CERT/CSIRT týmy a jejich role.* [online]. [cit. 1. 7. 2018]. Dostupné z: https://www.root.cz/clanky/cert-csirt-tymy-a-jejich-role/

*Kybernetická bezpečnost: Co s tím?* [online]. [cit. 29. 6. 2018]. Dostupné z: http://www.businessinfo.cz/cs/clanky/kyberneticka-bezpecnost-co-s-tim-84467.html

*Large-scale DNS redirection on home routers for financial thef.* [online]. [cit. 16. 7. 2017]. Dostupné z: https://www.cert.pl/en/news/single/large-scale-dns-redirection-on-home-routers-for-financial-theft/

LAVICKÝ, Petr a kol. *Občanský zákoník I. Obecná část (§ 1–654). Komentář*. Praha: C. H. Beck, 2014. ISBN 978-80-7400-529-9.

*Let's Encrypt: How It Works.* [online]. [cit. 11. 10. 2017]. Dostupné z: https://www.root.cz/clanky/jak-se-cesi-s-hesly-potykaji-analyza-16-tisic-ukradenych-hesel/

*Lhůty pro plnění povinností podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti.* [online]. [cit. 21. 8. 2018]. Dostupné z: https://nukib.cz/download/kii-vis/Schema_lhuty.pdf

*List of Rainbow Tables.* [online]. [cit. 11. 8. 2018]. Dostupné z: https://project-rainbowcrack.com/table.htm

*Locky mail.* [online]. [cit. 18. 8. 2017]. Dostupné z: https://csirt.cz/page/3605/presvedcive-podvodne-e-maily-sirici-ransomware-locky/

*Macronův volební štáb napadli hackeři, tvrdí japonská protivirová firma.* [online]. [cit. 29. 6. 2017]. Dostupné z: http://zpravy.idnes.cz/macron-utok-hackeri-trend-micro-d3b-/zahranicni.aspx?c=A170425_071554_zahranicni_san

MAISNER, Martin a Barbora VLACHOVÁ. *Zákon o kybernetické bezpečnosti. Komentář.* Praha: Wolters Kluwer, 2015. 232 s. ISBN 978-80-7478-817-8

MAREŠ, Miroslav. *Bezpečnost.* [online]. [cit. 10. 7. 2018]. Dostupné z: https://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=69511

*Masivní kyberútok zasáhl ve stovce zemí. Ochromil nemocnice i Telefóniku.* [online]. [cit. 27. 6. 2017]. Dostupné z: https://www.cnews.cz/ransomware-wanacryptor-wcry-wannacry

MATUROVÁ, Jana a Miroslav VALTA. *Prevence rizik - provádění kontrol technického stavu technických zařízení.* [online]. [cit. 1. 7. 2018]. Dostupné z: https://www.bozpinfo.cz/prevence-rizik-provadeni-kontrol-technickeho-stavu-technickych-zarizeni

*Memorandum o Computer Emergency Response Team/Computer Security Incident Response Team České republiky.* [online]. Dostupné z: https://www.nic.cz/files/nic/NBU_Memorandum_12-12.pdf

*Národní strategie informační bezpečnosti ČR. NSIB. Verze: 0.8. 4. 10. 2005.* [online]. Dostupné z: http://www.micr.cz/scripts/detail.php?id=2470

*Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020.* [online]. [cit. 1. 7. 2018]. Dostupné z: https://www.govcert.cz/download/gov-cert/container-nodeid-998/nskb-150216-final.pdf s. 5

Nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)

nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury

*Návrh SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY, kterou se stanoví evropský kodex pro elektronické komunikace (přepracované znění).* [online]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:52016PC0590

NEFF, Ondřej. *Tma.* Praha: Plus. ISBN 978-80-259-0279-0

*New paint protects wireless devices.* [online]. [cit. 16. 7. 2017]. Dostupné z: http://www.techrepublic.com/blog/it-security/new-paint-protects-wireless-devices/

*New RA Flood Attack.* [online]. [cit. 20. 7. 2017]. Dostupné z: https://samsclass.info/ipv6/proj/RA_flood2.htm

*PaaS Solution Stacks: WINS And LAMP.* [online]. [cit. 10. 4. 2012]. Dostupné z: http://thecloudguytim.wordpress.com/2010/09/08/paas-solution-stacks-wins-lamp/

*Parkerian Hexad*. [online]. [cit. 20. 8. 2016]. Dostupné z: https://vputhuseeri.wordpress.com/2009/08/16/149/

*Password Cracking with 8x NVIDIA GTX 1080 Ti GPUs*. [online]. [cit. 20. 8. 2017]. Dostupné z: https://www.servethehome.com/password-cracking-with-8x-nvidia-gtx-1080-ti-gpus/

*Password dictionary.* [online]. [cit. 21. 8. 2017]. Dostupné z: http://www.kalitut.com/2015/12/best-password-dictionary.html

*Password space sizes.* [online]. [cit. 29. 8. 2017]. Dostupné z: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.460.2104&rep=rep1&type=pdf

*PDCA cycle.* [online]. [cit. 6. 7. 2018]. Dostupné z: https://www.creativesafetysupply.com/glossary/pdca-cycle/

*Počet phishingových útoků v doméně .CZ se opět snížil.* [online]. [cit. 28. 8. 2018]. Dostupné z: https://blog.nic.cz/2013/08/22/pocet-phishingovych-utoku-v-domene-cz-se-opet-snizil/

*Podpůrný materiál k identifikaci poskytovatelů digitálních služeb.* [online]. [cit. 7. 8. 2018]. Dostupné z: https://nukib.cz/download/kii-vis/Definice_DSP_v1.pdf

POLČÁK, Radim, Jakub HARAŠTA a Vaclav STUPKA. *Právní problémy kybernetické bezpečnosti*. Brno: Masarykova univerzita, 2016. ISBN 978-80-210-8426-1.

POLČÁK, Radim. *Internet a proměny práva*. Praha: AUDITORIUM, 2012. ISBN 978-80-87284-22-3

*Poskytované služby.* [online]. [cit. 1. 8. 2018]. Dostupné z: https://www.govcert.cz/cs/vladni-cert/poskytovane-sluzby/

*Postřehy z bezpečnosti: středoškolský student vs. ředitel CIA 1:0.* [online]. [cit. 4. 7. 2017]. Dostupné z: https://www.root.cz/clanky/postrehy-z-bezpecnosti-stredoskolsky-student-reditel-cia-1-0/

POŽÁR, Josef a Luděk NOVÁK. *Pracovní příručka bezpečnostního manažera.* Praha: AFCEA, 2011. ISBN 978-80-7251-364-2,

POŽÁR, Josef a Luděk NOVÁK. *Systém řízení informační bezpečnosti.* [online]. [cit. 6. 7. 2018]. Dostupné z: https://www.cybersecurity.cz/data/srib.pdf s. 1

POŽÁR, Josef. *Informační bezpečnost*. Plzeň: Aleš Čeněk, 2005. ISBN 80-86898-38-5

POŽÁR, Josef. *Vybrané hrozby informační bezpečnosti organizace.* [online]. [cit. 6. 7. 2018]. Dostupné z: https://www.cybersecurity.cz/data/pozar2.pdf

*Proces určování kritické informační infrastruktury.* [online]. [cit. 7. 8. 2018]. Dostupné z: https://nukib.cz/download/kii-vis/Schema_KII.pdf

*Proces určování provozovatelů základních služeb a informačních systémů základních služeb.* [online]. [cit. 7. 8. 2018]. Dostupné z: https://nukib.cz/download/kii-vis/Schema_rozhodovani_PZS_v2.1.pdf

*Proces určování významných informačních systémů.* [online]. [cit. 7. 8. 2018]. Dostupné z: https://nukib.cz/download/kii-vis/Schema_VIS.pdf

PROSISE, Chris a Kevin MANDIVA. *Incident response & computer forensic, second edition.* Emeryville : McGraw-Hill, 2003. ISBN 0-07-222696-X.

*Prostorová ochrana* [online]. [cit. 6. 7. 2017]. Dostupné z: https://www.alarmsecurity.cz/www-alarmsecurity-cz/5-TECHNICKA-PODPORA/38-Typy-pohybovych-senzoru

*Protected Management Frames (802.11w).* [online]. [cit. 17. 7. 2017]. Dostupné z: https://wlan1nde.wordpress.com/2014/10/21/protected-management-frames-802-11w/

*Před čím chránit? – Bezpečnostní hrozby, události, incidenty.* [online]. [cit. 6. 7. 2018]. Dostupné z: https://www.kybez.cz/bezpecnost/pred-cim-chranit

*Příchod Hackerů: červ Roberta Morrise.* [online]. [cit. 1. 7. 2018]. Dostupné z: https://www.root.cz/clanky/prichod-hackeru-cerv-roberta-morrise/

*Příchod hackerů: příběh Stuxnetu.* [online]. [cit. 1. 7. 2018]. Dostupné z: https://www.root.cz/clanky/prichod-hackeru-pribeh-stuxnetu/

*Příchod hackerů: zrod CERT a CSIRT.* [online]. [cit. 1. 7. 2018]. Dostupné z: https://www.root.cz/clanky/prichod-hackeru-zrod-cert-a-csirt/

*Rainbow tables/hash tables versus WPA/WPA2.* [online]. [cit. 11. 8. 2018]. Dostupné z: https://security.stackexchange.com/questions/92903/rainbow-tables-hash-tables-versus-wpa-wpa2

RAK, Roman. Homo sapiens versus security. ICT fórum/PERSONALIS 2006. [předneseno 27. 9. 2006]. Praha (prezentace na konferenci).

*RANSOMWARE IS ONE OF THE WORLD'S FASTEST GROWING TYPES OF MALWARE.* [online]. [cit. 28. 6. 2017]. Dostupné z: https://go.kaspersky.com/Anti-ransomware-tool.html

REED, Chris. *Internet Law.* Cambridge: Cambridge University Press, 2004. ISBN: 9780521605229.

*Referenční údaj.* [online]. [cit. 30. 8. 2018]. Dostupné z: http://www.szrcr.cz/referencni-udaj

ROSER, Christoph. *The Many Flavors of the PDCA.* [online]. [cit. 6. 7. 2018]. Dostupné z: https://www.allaboutlean.com/pdca-variants/

Rozsudek Nejvyššího soudu 30 Cdo 530/2014, ze dne 30. 7. 2015. [online]. [cit. 8. 7. 2016]. Dostupné z: https://www.mfcr.cz/assets/cs/media/Metodika-Pr-002_2016_Rozsudek-Nejvyssiho-soudu-CR-ze-dne-30-7-2015.pdf

Rozsudek ve věci C-484/14 Tobias Mc Fadden v. Sony Music Entertainment Germany GmbH. [online]. [cit. 10. 1. 2018]. Dostupné z: https://curia.europa.eu/jcms/upload/docs/application/pdf/2016-09/cp160099cs.pdf

SATRAPA, Pavel. *IPv6.* Praha: CZ.NIC. ISBN 978-80-904248-4-5 [online]. [cit. 9.8.2017]. Dostupné z: https://knihy.nic.cz/files/edice/ipv6_2012.pdf

*Security authorization. An Approach for Community Cloud Computing Environments* [online]. [cit. 15. 4. 2012]. Dostupné z: http://www.federalnewsradio.com/wp-content/uploads/pdfs/SecurityAuthorizationandAssessmentSECURITYNov2009.pdf

SHACKELFORD, Scott J., Scott RUSSEL a Andreas KUEHN. *Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors*. Chicago Journal of International Law. 2016, 17(1). ISSN 1529-0816.

SCHNEIER, Bruce. [online]. [cit. 18. 7. 2018]. Dostupné z: https://www.azquotes.com/quote/570039 Překlad autora.

SCHNEIER, Bruce. [online]. [cit. 18. 7. 2018]. Dostupné z: https://www.azquotes.com/quote/570035 Překlad autora.

SCHNEIER, Bruce. [online]. [cit. 18. 7. 2018]. Dostupné z: https://www.azquotes.com/quote/570040 Překlad autora.

SCHNEIER, Bruce. [online]. [cit. 18. 7. 2018]. Dostupné z: https://www.azquotes.com/quote/570047 Překlad autora.

SCHNEIER, Bruce. [online]. [cit. 18. 7. 2018]. Dostupné z: https://www.azquotes.com/quote/699390 Překlad autora.

SCHNEIER, Bruce. [online]. [cit. 18. 7. 2018]. Dostupné z: https://www.azquotes.com/quote/570053 Překlad autora.

SCHNEIER, Bruce. [online]. [cit. 18. 7. 2018]. Dostupné z: https://www.azquotes.com/quote/570046 Překlad autora.

*SI6 Networks' IPv6 Toolkit.* [online]. [cit. 12. 8. 2017]. Dostupné z: https://www.si6networks.com/tools/ipv6toolkit/

*Služby CSIRT.CZ.* [online]. [cit. 7. 7. 2018]. Dostupné z: https://csirt.cz/page/2764/sluzby/

SMEJKAL, Vladimír. *Kybernetická kriminalita.* Plzeň: Aleš Čeněk, 2015. ISBN 978-80-7380-501-2.

Směrnice Evropského parlamentu a Rady (EU) 2016/1148 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii [online]. [cit. 1. 7. 2018]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32016L1148&from=EN

*SSL Vulnerabilities: Who listens when Android applications talk?* [online]. [cit. 20. 7. 2017]. Dostupné z: https://www.fireeye.com/blog/threat-research/2014/08/ssl-vulnerabilities-who-listens-when-android-applications-talk.html

STANČÍK, Petr. *100 miliard neuronů.* [online]. [cit. 16. 8. 2018]. Dostupné z: https://backendstories.skoda-kariera.cz/assets/files/library/b01/100_MILIARD_NEURONU_-_PETR_STANCIK.pdf s. 133

*Státní informační a komunikační politika e-Česko 2006.* [online]. Dostupné z: http://www.culturenet.cz/res/data/002/000269.pdf

*Strategie pro oblast kybernetické bezpečnosti České republiky na období let 2011 až 2015.* [online]. Dostupné z: https://www.databaze-strategie.cz/cz/cr/strategie/strategie-pro-oblast-kyberneticke-bezpecnosti-cr-2011-2015?typ=struktura

*Strategie pro oblast kybernetické bezpečnosti České republiky na období 2012 – 2015.* [online]. Dostupné z: https://www.govcert.cz/download/legislativa/container-nodeid-719/20120209strategieprooblastkbnbu.pdf

*Surface Web, Deep Web, Dark Web – What's the Difference.* [online]. [cit. 20. 7. 2016]. Dostupné z: https://www.cambiaresearch.com/articles/85/surface-web-deep-web-dark-web----whats-the-difference

SVOBODA, Ivan. *Řešení kybernetické bezpečnosti*. Přednáška v rámci CRIF Academy. (23. 9. 2014)

*Systémy klíčů.* [online]. [cit. 4. 7. 2018]. Dostupné z: http://www.tokoz.cz/systemy-klicu

ŠÁMAL, Pavel a kol. *Trestní zákoník II. § 140 až 421. Komentář.* 2. vyd. Praha: C. H. Beck, 2012. ISBN 974-80-7400-4285

*Šifrování WPA2 prolomeno, Wi-Fi sítě je možné odposlouchávat (aktualizováno).* [online]. [cit. 1. 2. 2018]. Dostupné z: https://www.root.cz/clanky/sifrovani-wpa2-bylo-prolomeno-wi-fi-site-je-mozne-odposlouchavat/

*Šíří se staronový vir vyděrač. Výkupné neplaťte, adresa je nefunkční*. [online]. [cit. 28. 6. 2017]. Dostupné z: https://technet.idnes.cz/kyberneticky-hackersky-utok-ve-svete-ransomware-fbq-/sw_internet.aspx?c=A170627_172510_tec-kratke-zpravy_pka

ŠKORNIČKOVÁ, Eva. *Jednoduchý test: Jak jste na tom s přípravou na GDPR?* [online]. [cit. 10. 11. 2017]. Dostupné z: https://www.gdpr.cz/blog/jednoduchy-test-jak-jste-na-tom-s-pripravou-na-gdpr/

ŠULC, Vladimír. *Kybernetická bezpečnost.* Plzeň: Aleš Čeněk, 2018. ISBN 978-80-7380-737-5

*Tajné služby: Kampaň, která měla ovlivnit prezidentské volby v USA, nařídil Putin.* [online]. [cit. 29. 6. 2017]. Dostupné z: http://www.ceskatelevize.cz/ct24/svet/2005207-tajne-sluzby-kampan-ktera-mela-ovlivnit-prezidentske-volby-v-usa-naridil-putin

*THC-IPV6.* [online]. [cit. 12. 8. 2017]. Dostupné z: https://www.thc.org/thc-ipv6/

*The complete breadth of CGI Cyber Security services.* [online]. [cit. 10. 7. 2018]. Dostupné z: https://mss.cgi.com/service-portfolio

*The dark Web explained.* [online]. [cit. 20. 7. 2016]. Dostupné z: https://www.yahoo.com/katiecouric/now-i-get-it-the-dark-web-explained-214431034.html

*The list of log-in IDs and passwords.* [cit. 16.7.2017]. Dostupné z: https://blog.trendmicro.com/trendlabs-security-intelligence/mobile-devices-used-to-execute-dns-malware-against-home-routers/

*The Parkerian Hexad*. [online]. [cit. 20. 8. 2016]. Dostupné z: http://cs.lewisu.edu/mathcs/msisprojects/papers/georgiependerbey.pdf

*Traffic Light Protocol (TLP) Definitions and Usage.* [online]. [cit. 13. 1. 2018]. Dostupné z: https://www.us-cert.gov/tlp

*UK hospitals hit with massive ransomware attack*. [online]. [cit. 27. 6. 2076]. Dostupné z: https://www.theverge.com/2017/5/12/15630354/nhs-hospitals-ransomware-hack-wannacry-bitcoin

*Úmluva o kyberkriminalitě.* [online]. [cit. 20. 8. 2016]. Dostupné z: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804931c0

*USB Port Lock with Rectangular Cable Guard.* [cit. 7. 7. 2017]. Dostupné z: https://accoblobstorageus.blob.core.windows.net/literature/1378.pdf

*USB Rubber Ducky.* [online]. [cit. 9. 7. 2017]. Dostupné z: https://hakshop.com/products/usb-rubber-ducky-deluxe

*USNESENÍ VLÁDY ČESKÉ REPUBLIKY ze dne 15. března 2010 č. 205 o řešení problematiky kybernetické bezpečnosti České republiky.* [online]. Dostupné z: https://apps.odok.cz/attachment/-/down/KORN97BQ9ASZ

*USNESENÍ VLÁDY ČESKÉ REPUBLIKY ze dne 19. října 2011 č. 781 o ustanovení Národního bezpečnostního úřadu gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast.* [online]. Dostupné z: https://apps.odok.cz/attachment/-/down/KORN97BUKZ3E

Ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky, ve znění ústavního zákona č. 300/2000 Sb.

*Utility computing.* [online]. [cit. 10. 4. 2012]. Dostupné z: http://searchdatacenter.techtarget.com/definition/utility-computing.

*Útoky pomocí iframe, jejich maskování útočníky a obrana.* [online]. [cit. 28. 8.2018]. Dostupné z: https://blog.nic.cz/2012/07/18/utoky-pomoci-iframe-jejich-maskovani-utocniky-a-obrana/

VALÁŠEK, Jarmil, František KOVÁŘÍK a kol. *Krizové řízení při nevojenských krizových situacích*. Praha: Ministerstvo vnitra - generální ředitelství Hasičského záchranného sboru ČR, 2008. [online]. [cit. 1. 7. 2018]. Dostupné z: http://www.hzscr.cz/soubor/modul-c-krizove-rizeni-pri-nevojenskych-krizovych-situacich-pdf.aspx ISBN 978-80-86640-93-8

*Věcný záměr zákona o kybernetické bezpečnosti.* [online]. Dostupné z: https://www.govcert.cz/download/legislativa/container-nodeid-926/vecny-zamer-final-vlada.pdf

vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích

vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby

vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)

WAISOVÁ, Šárka. *Bezpečnost: vývoj a proměny konceptu.* Plzeň: Aleš Čeněk, s.r.o., 2005. ISBN 80-86898-21-0

*WannaCry se neměl vůbec rozšířit. Stačilo, abychom používali Windows Update.* [online]. [cit. 27. 6. 2017]. Dostupné z: https://www.zive.cz/clanky/wannacry-se-nemel-vubec-rozsirit-stacilo-abychom-pouzivali-windows-update/sc-3-a-187740/default.aspx

*What is Internet of Things.* [online]. [cit. 15. 7. 2016]. Dostupné z: https://www.microsoft.com/en-us/cloud-platform/internet-of-things

WIENER, Norbert. *Kybernetika: neboli řízení a sdělování v živých organismech a strojích.* Praha: Státní nakladatelství technické literatury, 1960. 148 s s. 32 a násl.

*WPS PIN*. [online]. [cit. 16. 7. 2017]. Dostupné z: https://krebsonsecurity.com/2011/12/new-tools-bypass-wireless-router-security/

*Základní pojmy.* [online]. [cit. 10. 7. 2018]. Dostupné z: https://www.kybez.cz/bezpecnost/pojmoslovi

*Základní příručka k GDPR.* [online]. [cit. 7. 8. 2018]. Dostupné z: https://www.uoou.cz/zakladni%2Dprirucka%2Dk%2Dgdpr/ds-4744/archiv=0&p1=3938

zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů

zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů

zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů

zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim

zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti), ve znění pozdějších předpisů

zákon č. 89/2012 Sb., občanský zákoník

ZEMAN, Petr a kol. *Česká bezpečnostní terminologie: Výklad základních pojmů.* [online]. [cit. 10. 7. 2018]. Dostupné z: http://www.defenceandstrategy.eu/filemanager/files/file.php?file=16048 . s. 13

*Zpráva o stavu kybernetické bezpečnosti za rok 2017.* [online]. [cit. 29. 6. 2018]. Dostupné z: https://nukib.cz/download/Zpravy-KB-vCR/Zprava-stavu-KB-2017-fin.pdf

# Rejstřík

## Rejstřík


### A

abuse
205, 234, 310, 494, 495, 498, 502, 530

aktivum
53, 54, 60, 68, 72, 253, 275, 287, 411

podpůrné
58, 72, 275

primární
53, 54, 58, 72, 275

soubor aktiv
202, 205, 209, 216, 223, 228, 234

garant aktiva
267, 271, 273, 274

analýza rizik
64, 68, 70, 71, 342, 344, 358, 411, 525

antispam
60, 288, 461, 462, 480

antivir
12, 60, 288, 411, 434, 436, 458, 462, 480, 489

aplikace
36, 42, 43, 44, 45, 59, 60, 61, 62, 68, 75, 77, 100, 103, 105, 109, 114, 116, 117, 123, 134, 135, 136, 146, 148, 158, 193, 195, 196, 246, 254, 268, 279, 285, 286, 287, 288, 292, 346, 407, 443, 450, 457, 460, 461, 464, 473, 474, 475, 478, 479, 482, 489, 490, 494, 496, 498

aplikační
brána
456

firewall
60, 292, 456, 457, 525

APT
27, 79, 409

ARP
429, 431, 432, 433, 434, 435, 442, 452, 453, 525

autentizace
60, 61, 278, 279, 286, 414, 428, 438, 439, 451, 464, 474, 476, 482, 486

availability / dostupnost
38, 44, 45, 48, 54, 55, 68, 72, 77, 83, 111, 139, 141, 142, 145, 154, 195, 238, 241, 242, 244, 245, 247, 251, 253, 266, 275, 281, 293, 302, 321, 391, 409, 479, 486, 514

### B

bcrypt
472, 473

bezpečnost
aplikační bezpečnost
251, 253, 292, 462

fyzická bezpečnost
79, 251, 253, 265, 282, 283, 284, 285, 411, 415, 416, 418, 422, 480

informací
46, 74, 80, 81, 82, 142, 145, 150, 154, 155, 241, 242, 245, 250, 252, 253, 254,

255, 256, 257, 258, 259, 264, 265, 266, 267, 268, 270, 273, 274, 275, 299, 300, 321, 322, 323, 361, 362, 364, 366, 391, 493

lidských zdrojů
251, 252, 265, 276, 489, 490

organizační bezpečnost
250, 252, 258, 264, 266

sítí
27, 29, 44, 68, 93, 96, 97, 138, 139, 140, 141, 189, 197, 233, 239, 241, 342, 370, 373, 425, 505, 522, 536

služeb
80, 81, 82, 118, 120, 299, 300, 306, 322, 323, 361, 362, 364, 366, 488

systémů
425

vnitřní bezpečnost
136, 364, 411, 415, 416, 463

bezpečnostní
dokumentace
210, 213, 217, 220, 223, 226, 241, 243, 245, 251, 252, 253, 264, 265, 266, 294, 295, 319, 369, 382, 384, 385, 389, 390, 392, 394

hrozba
74, 78, 119, 258, 323, 461, 512, 534

incident
51, 71, 73, 81, 82, 92, 93, 99, 129, 133, 134, 136, 138, 144, 168, 169, 198, 199, 203, 205, 206, 207, 209, 210, 212, 213, 217, 218, 219, 220, 223, 224, 225, 226, 228, 229, 230, 233, 234, 235, 236, 242, 245, 248, 251, 252, 253, 259, 264, 265, 267, 279, 280, 281, 290, 291, 293, 294, 295, 299, 300, 301, 302, 303, 304, 305, 306, 307, 308, 309, 310, 311, 312, 313, 314, 315, 316, 318, 319, 320, 321, 323, 324, 325, 326, 327, 329, 330, 331, 332, 333, 334, 335, 341, 342, 343, 345, 346, 347, 349, 356, 357, 358, 359, 360, 361, 363, 368, 370, 374, 377, 382, 383, 384, 385, 386, 387, 388, 389, 390, 394, 395, 396, 475, 490, 491, 492, 493, 496, 498, 501, 505, 506, 507, 508, 509, 510, 511, 514, 516, 517, 518, 539

opatření
14, 44, 51, 61, 80, 92, 93, 99, 100, 109, 110, 112, 133, 134, 135, 144, 164, 197, 199, 209, 210, 211, 213, 217, 218, 220, 223, 224, 226, 234, 236, 241, 242, 243, 244, 245, 246, 247, 248, 251, 252, 253, 258, 263, 264, 268, 269, 273, 275, 278, 280, 281, 291, 294, 295, 312, 316, 318, 321, 329, 330, 361, 363, 367, 369, 370, 375, 378, 381, 382, 383, 389, 390, 392, 394, 395, 396, 397, 399, 340, 403, 416, 425, 480, 539

politika
79, 80, 81, 82, 88, 115, 132, 239, 242, 247, 250, 252, 258, 264, 265, 266, 271, 276, 281, 455, 457

riziko
97, 243, 254, 297, 299, 460, 481, 482

role
58, 73, 266, 267, 268, 271, 272, 273, 274, 276, 277, 278, 279, 280, 291, 526

tým
343, 344, 355, 398, 491, 492, 493, 494, 495, 497, 498, 496, 499, 506, 514, 515

událost
29, 71, 73, 80, 81, 134, 198, 199, 206, 210, 212, 217, 219, 224, 225, 229, 243, 251, 253, 265, 277, 279, 280, 290, 291, 299, 300, 303, 304, 356, 357, 359, 475

biometrie
109, 112, 283, 413, 414, 417, 463, 464, 526

botnet
79, 360, 488, 497, 498, 501

C&C
27, 360, 497, 501

BYOD
27, 488, 489

## C

certifikát
293, 474, 476, 477, 478, 482

CESNET
16, 129, 347, 458, 459, 514, 515

CIA
44, 45, 46, 48, 55, 56, 63, 77, 136, 142, 150, 253, 269, 270, 271, 318, 409, 526, 529, 533

Parkerian hexad
45, 56, 533, 538

cloud
12, 36, 66, 67, 123, 143, 147, 148, 189, 192, 195, 196, 197, 214, 221, 226, 230, 233, 234, 240, 242, 244, 245, 247, 248, 255, 293, 294, 390, 526, 527, 533, 535, 539

confidentiality / důvěrnost
41, 44, 45, 48, 51, 52, 68, 77, 83, 110, 111, 114, 139, 141, 142, 145, 154, 242, 247, 253, 266, 275, 285, 286, 302, 318, 319, 409, 476, 482, 513, 529

control
list
455, 456

rámec
439

cookies
105, 423, 479

CSIRT/CERT
14, 15, 16, 27, 43, 49, 50, 88, 90, 91, 92, 94, 99, 129, 134, 137, 140, 198, 199, 202, 203, 205, 206, 207, 209, 210, 212, 216, 217, 218, 219, 223, 224, 225, 228, 229, 234, 235, 240, 268, 282, 284, 285, 287, 289, 290, 291, 292, 293, 301, 302, 303, 304, 305, 306, 307, 308, 309, 310, 311, 312, 313, 314, 324, 325, 332, 335, 336, 337, 338, 339, 340, 341, 342, 343, 344, 345, 346, 347, 348, 350, 352, 353, 354, 355, 356, 357, 358, 359, 360, 363, 368, 370, 371, 372, 398, 399, 408, 409, 429, 437, 438, 460, 462, 477, 492, 495, 496, 497, 498, 499, 501, 503, 505, 506, 507, 508, 509, 510, 511, 512, 513, 514, 515, 516, 517, 518, 525, 526, 530, 531, 535, 535, 536, 538

národní
92, 134, 137, 140, 198, 199, 202, 203, 205, 206, 234, 235, 301, 302, 303, 304, 305, 306, 308, 309, 311, 313, 314, 323, 324, 335, 336, 337, 338, 339, 340, 341, 342, 344, 345, 346, 347, 348, 349, 350, 352, 353, 354, 355, 356, 358, 386, 360, 363, 368, 372, 398, 399, 408, 477, 492,

495, 496, 497, 498, 499, 501, 508, 213, 514, 515, 516

vládní
90, 91, 134, 140, 199, 202, 203, 206, 207, 209, 210, 212, 216, 217, 218, 219, 223, 224, 225, 228, 229, 235, 301, 303, 304, 305, 306, 308, 309, 310, 312, 323, 332, 338, 339, 342, 345, 356, 357, 358, 359, 360, 371, 508, 512, 513, 515, 516

CZ.NIC
7, 11, 13, 15, 36, 43, 48, 75, 76, 92, 103, 106, 125, 190, 191, 309, 310, 339, 342, 345, 346, 347, 348, 350, 355, 398, 408, 409, 420, 424, 429, 436, 451, 453, 456, 462, 494, 497, 514, 515, 517, 529, 530, 531, 535

**D**

data
12, 13, 14, 15, 27, 28, 35, 36, 38, 41, 42, 43, 44, 45, 46, 47, 48, 49, 51, 52, 53, 54, 60, 62, 66, 67, 68, 72, 74, 75, 76, 77, 79, 80, 83, 87, 88, 93, 95, 99, 100, 101, 102, 103, 104, 105, 107, 108, 109, 112, 117, 118, 119, 123, 129, 139, 141, 142, 145, 149, 151, 152, 154, 187, 190, 195, 196, 211, 212, 213, 214, 218, 219, 220, 242, 244, 245, 247, 248, 252, 253, 254, 255, 257, 258, 261, 268, 275, 277, 279, 280, 282, 284, 285, 288, 289, 290, 291, 292, 295, 296, 297, 298, 309, 310, 313, 315, 318, 333, 334, 339, 349, 353, 360, 361, 375, 379, 380, 383, 389, 390, 394, 395, 402, 407, 408, 409, 411, 412, 415, 417, 418, 419, 421, 423, 424, 425, 427, 428, 429, 430, 431, 433, 434, 435, 440, 441, 442, 443, 446, 450, 451, 455, 456, 458, 460, 461, 462, 465, 469, 475, 476, 480, 481, 482, 483, 484, 485, 487, 488, 489, 490, 492, 495, 496, 498, 499, 502, 505, 513, 518, 521, 525, 534, 537, 539

metadata
117, 118, 119, 120, 484

zpracování dat
118, 119, 254, 375, 402, 461

detekce
45, 62, 63, 133, 137, 206, 210, 217, 224, 251, 253, 265, 279, 280, 290, 291, 302, 305, 412, 415, 434, 480, 493, 501

DHCP
422, 423, 429, 430, 431, 435, 452, 453, 490, 527

DMZ
27, 60, 426, 427, 428

DNS
27, 187, 423, 425, 429, 435, 436, 437, 438, 487, 490, 500, 501, 531, 538

DNSSEC
436

doména
27, 36, 122, 147, 152, 187, 238, 240, 346, 435, 436, 472, 477, 478, 494, 496, 497, 500, 501, 507, 508, 509, 515, 517, 533

dvoufaktorová autentizace
464, 474, 486

**E**

e-mail
15, 38, 60, 62, 66, 81, 104, 105, 107, 108, 114, 116, 117, 123, 157, 161, 162, 191, 205, 209, 217, 223, 228, 234, 286, 309, 310, 347, 424, 436, 462, 476, 488, 489, 516, 531

ePrivacy
97, 99, 100, 113, 114, 115, 116, 117, 118, 119, 120

EULA / SLA
27, 29, 103, 282

evidence
80, 109, 157, 158, 159, 160, 161, 201, 203, 206, 235, 265, 274, 284, 311, 312, 313, 314, 315, 316, 318, 323, 324, 331, 332, 333, 335, 336, 337, 338, 340, 345, 348, 351, 352, 356, 360, 367, 369, 371, 379, 380, 381, 393, 399, 494, 526, 528

EZS
27, 414, 415, 416

**F**

firewall
60, 285, 289, 411, 521, 426, 454, 455, 456, 457, 461, 480, 483, 487, 503, 527

FIRST
105, 454, 510, 511, 514, 517, 529

**G**

gateway
430, 433, 457, 458, 525

GDPR
14, 28, 97, 98, 99, 101, 102, 103, 104, 105, 107, 108, 109, 110, 111, 112, 113, 120, 307, 313, 315

GovCERT
91, 92, 94, 139, 140, 209, 216, 217, 223, 228, 268, 309, 328, 337, 339, 355, 357, 359, 360, 361, 374

**H**

hardware
36, 58, 59, 61, 62, 77, 82, 122, 165, 195, 196, 287, 301, 419, 420, 427, 44, 456, 464, 474, 478, 486, 530

hash
444, 445, 451, 464, 465, 466, 467, 469, 470, 471, 472, 473, 535

heslo
15, 49, 67, 286, 287, 418, 422, 436, 437, 438, 442, 443, 444, 445, 446, 448, 449, 450, 451, 462, 463, 464, 465, 466, 467, 468, 469, 470, 471, 472, 473, 474, 481, 482, 483, 485, 488, 495, 530, 531

hlášení
kontaktních údajů
235, 339, 340, 375, 378

o kybernetických bezpečnostních incidentech
134, 206, 212, 219, 225, 229, 235, 301, 308, 309, 312, 340, 342, 345, 346, 356, 357, 358, 359, 363, 382

hodnocení
aktiv
265, 268, 271, 275, 318, 319

rizik
71, 258, 259, 260, 261, 262, 263, 264, 265, 274, 275, 280

honeypot
60, 347, 361

**I**

ICT
11, 12, 13, 14, 15, 28, 39, 40, 43, 44, 45, 46,

48, 57, 59, 60, 61, 62, 67, 68, 76, 77, 78, 101, 102, 108, 123, 129, 135, 196, 246, 266, 268, 269, 270, 284, 285, 292, 325, 331, 409, 410, 411, 412, 414, 415, 417, 425, 521, 526, 535

identifikační údaje
15, 105, 311, 312, 340, 346, 356, 360, 474

IDS
23, 28, 60, 210, 217, 224, 290, 291, 347, 361, 430, 460, 461, 510

informace
11, 12, 13, 14, 15, 16, 27, 28, 29, 31, 35, 36, 37, 39, 40, 41, 42, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 57, 59, 60, 62, 66, 67, 68, 72, 73, 74, 75, 76, 77, 80, 81, 82, 83, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 102, 103, 104, 105, 106, 107, 108, 109, 112, 113, 114, 115, 116, 118, 119, 123, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145, 146, 148, 149, 150, 151, 152, 153, 154, 155, 156, 157, 158, 159, 160, 161, 162, 163, 164, 165, 167, 168, 169, 170, 171, 173, 174, 175, 177, 179, 180, 182, 183, 184, 185, 187, 188, 189, 190, 191, 192, 194, 195, 197, 198, 199, 201, 203, 204, 205, 208, 209, 210, 211, 212, 213, 214, 216, 217, 218, 219, 220, 221, 222, 223, 224, 225, 226, 228, 229, 230, 232, 233, 234, 237, 238, 239, 240, 241, 242, 243, 244, 245, 246, 247, 247, 249, 250, 251, 252, 253, 254, 255, 256, 257, 258, 259, 260, 261, 264, 265, 266, 267, 268, 269, 270, 271, 273, 274, 275, 276, 277, 278, 279, 280, 281, 282, 284, 285, 286, 287, 288, 289, 290, 291, 292, 293, 294, 295, 296, 297, 298, 299, 300, 301, 302, 303, 304, 305, 306, 307, 308, 309, 310, 312, 313, 314, 315, 316, 317, 318, 319, 320, 321, 322, 323, 324, 325, 326, 327, 329, 330, 331, 333, 334, 335, 336, 337, 338, 339, 340, 341, 342, 344, 345, 346, 347, 348, 350, 353, 354, 356, 357, 358, 359, 360, 361, 362, 363, 364, 365, 366, 367, 368, 369, 370, 371, 372, 373, 373, 375, 376, 377, 378, 379, 380, 381, 382, 383, 384, 385, 386, 387, 388, 389, 390, 391, 393, 394, 395, 396, 397, 399, 400, 402, 403, 404, 409, 411, 416, 417, 421, 426, 428, 429, 430, 432, 435, 436, 438, 440, 444, 447, 453, 454, 456, 459, 461, 462, 468, 474, 475, 476, 477, 478, 479, 481, 484, 485, 486, 489, 490, 491, 492, 493, 494, 495, 496, 497, 498, 499, 500, 502, 505, 506, 507, 509, 510, 511, 512, 516, 517, 518, 521, 522, 526, 528, 529, 531, 532, 534, 536, 537, 539, 540

informační sebeurčení
39, 132, 133, 134, 135, 136, 313, 314, 381

integrity / integrita
29, 41, 44, 45, 48, 52, 53, 54, 68, 75, 77, 80, 81, 82, 83, 110, 111, 139, 141, 142, 145, 154, 242, 247, 251, 253, 266, 275, 285, 299, 300, 302, 306, 322, 323, 362, 364, 366, 409, 443, 460, 476, 529

Internet
11, 12, 13, 28, 29, 30, 36, 38, 58, 60, 67, 80, 105, 106, 114, 115, 118, 130, 131, 132, 134, 135, 140, 143, 144, 147, 156, 163, 187, 189, 190, 191, 192, 194, 195, 196, 203, 207, 212, 219, 225, 229, 233, 234, 236, 238, 240, 287, 293, 309, 323, 324, 330, 332, 339, 347, 349, 353, 368, 374, 407, 423, 425, 428, 429, 430, 435, 436, 442, 444, 450, 452, 458, 459, 474, 479, 482, 483, 488, 494, 502, 505, 506, 507, 513, 514, 516, 517, 518, 526, 529, 533, 535, 537, 539

interpersonální komunikační služba
115, 116

IoT
12, 13, 28, 77, 116, 117, 478, 529

IP adresa
15, 38, 105, 106, 107, 108, 196, 347, 360, 361, 429, 430, 431, 432, 433, 435, 454, 459, 460, 461, 465, 475, 483, 494, 495, 497, 498, 499, 500, 501, 502, 509, 517

IPv4
28, 423, 451, 452, 453, 454

IPv6
28, 429, 451, 452, 453, 454, 455, 525, 529, 533, 535, 536, 538

IPS
28, 60, 210, 217, 224, 290, 460, 461

ISMS
28, 46, 97, 163, 253, 254, 255, 256, 257, 258, 260, 261, 266, 271, 274, 276, 493

ISO normy řady 27000
46, 48, 97, 132, 254, 268

ISP
27, 28, 106, 114, 123, 149, 190, 429, 490, 498, 506, 515, 518, 521

**K**

keylogger
419, 420, 530

kontaktní údaj
198, 199, 202, 203, 205, 206, 207, 209, 212, 213, 216, 219, 220, 223, 225, 226, 228, 229, 230, 234, 235, 236, 238, 252, 265, 310, 323, 324, 331, 332, 333, 335, 336, 337, 338, 339, 340, 342, 345, 349, 356, 357, 359, 375, 378, 382, 385, 389, 390, 391, 394, 395, 396, 397, 399, 400, 403

kritéria
průřezová kritéria
150, 155, 375

odvětvová kritéria
144, 150, 151, 168, 169, 170, 171, 173, 174, 175, 177, 179, 180, 182, 183, 184, 185, 187, 188, 373, 374, 377, 394

určující kritéria
92, 99, 154, 155, 216, 217, 294, 295, 301, 383, 394, 395, 397, 539

speciální kritéria
168, 170, 171, 173, 174, 175, 177, 179, 180, 182, 183, 184, 185, 187, 188, 377

kritická infrastruktura
kritická informační infrastruktura
89, 136, 142, 144, 145, 150, 153, 154, 208, 209, 210, 296, 396, 399, 400

informační systém kritické informační infrastruktury
209, 244, 245, 305, 384, 386

komunikační systém kritické informační infrastruktury
204, 209, 244, 245, 248, 249, 250, 305, 384, 385, 386

prvek kritické infrastruktury
92, 99, 142, 144, 150, 151, 155, 169, 170, 171, 173, 174, 176, 177, 179, 180, 182, 183, 184, 186, 187, 188, 295, 367, 372, 373, 377, 399, 532

kryptografie
52, 53, 61, 93, 251, 253, 265, 285, 286, 292,

293, 367, 371, 465, 466, 476

kyberkriminalita / cybercrime
7, 11, 13, 14, 15, 30, 36, 43, 46, 48, 75, 76, 83, 97, 103, 106, 125, 125, 134, 409, 420, 424, 429, 436, 451, 456, 462, 505, 530, 531, 538

kybernetický
útok
15, 35, 40, 43, 49, 62, 64, 67, 79, 82, 83, 87, 94, 123, 125, 132, 133, 136, 139, 243, 409, 429, 482

prostor - viz kyberprostor
14, 35, 36, 37, 38, 39, 40, 42, 43, 44, 45, 46, 48, 59, 60, 67, 68, 77, 78, 82, 83, 87, 95, 103, 120, 123, 127, 131, 132, 138, 139, 142, 144, 145, 148, 149, 167, 200, 239, 245, 311, 314, 320, 321, 330, 361, 407, 408, 409, 508, 521, 522, 526

bezpečnostní incident
71, 81, 82, 133, 134, 168, 169, 198, 199, 205, 206, 207, 209, 210, 212, 213, 217, 220, 223, 224, 225, 226, 228, 229, 230, 234, 235, 236, 264, 279, 280, 281, 293, 294, 299, 300, 301, 302, 303, 304, 305, 306, 307, 308, 309, 310, 311, 312, 313, 316, 318, 319, 320, 321, 323, 324, 325, 326, 327, 329, 330, 331, 332, 333, 334, 340, 341, 343, 345, 346, 356, 358, 359, 360, 363, 368, 374, 377, 384, 385, 386, 389, 390, 395, 396, 506

kybernetická
bezpečnost
13, 14, 15, 31, 35, 36, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62 63, 64, 65, 66, 67, 68, 71, 72, 73, 74, 77, 79, 80, 81, 28, 87, 88, 89, 90, 91, 92, 93, 94, 95, 98, 99, 100, 101, 105, 113, 120, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145, 146, 150, 151, 154, 164, 197, 198, 199, 200, 201, 202, 203, 204, 205, 206, 207, 208, 209, 210, 211, 212, 215, 216, 217, 218, 219, 221, 222, 223, 224, 225, 226, 228, 229, 231, 234, 235, 237, 241, 243, 245, 246, 247, 249, 252, 253, 255, 258, 259, 264, 265, 266, 267, 268, 269, 270, 271, 274, 275, 277, 278, 279, 280, 281, 282, 294, 295, 296, 297, 298, 299, 300, 301, 302, 303, 304, 305, 306, 308, 311, 312, 313, 314, 315, 316, 317, 318, 319, 320, 323, 324, 325, 329, 333, 336, 337, 340, 341, 342, 344, 345, 346, 347, 348, 349, 350, 351, 352, 353, 354, 355, 356, 357, 358, 359, 360, 363, 364, 367, 368, 369, 371, 372, 373, 374, 378, 381, 382, 383, 386, 387, 388, 389, 391, 392, 395, 396, 399, 400, 401, 402, 408, 409, 411, 415, 418, 424, 425, 426, 462, 465, 479, 492, 512, 515, 516, 521, 522, 525, 528, 530, 531, 532, 533, 537, 538, 539, 540,

trestná činnost
83

hrozba
40, 45, 73, 74, 75, 76, 77, 81, 95, 259, 300, 374, 409

bezpečnostní událost
71, 80, 81, 198, 199, 212, 219, 225, 229, 279, 299, 300, 303, 356, 359

kybernetické nebezpečí
322

kyberprostor / cyberspace
14, 35, 36, 37, 38, 39, 40, 43, 44, 45, 46, 48, 59, 60, 67, 68, 77, 78, 82, 83, 87, 95, 103, 120, 123, 127, 139, 148, 149, 245, 321, 361, 407, 408, 409, 508, 521, 522, 526

**L**

lhůty
204, 206, 208, 209, 210, 212, 215, 216, 217, 220, 221, 222, 223, 224, 226, 227, 231, 234, 235, 237, 306, 318, 330, 331, 332, 333, 353, 354, 355, 365, 375, 378, 384, 385, 395, 396, 397, 398, 531

lidé
11, 13, 35, 39, 45, 47, 55, 57, 58, 59, 61, 62, 63, 72, 77, 89, 93, 103, 109, 118, 121, 122, 135, 167, 251, 252, 264, 265, 273, 276, 277, 297, 376, 409, 412, 422, 427, 475, 479, 481, 489, 490

log / logování
60, 106, 210, 217, 224, 290, 291, 292, 419, 420, 457, 460, 461, 462, 465, 466, 475, 476, 486, 490, 493

**M**

MAC adresa
428, 429, 430, 431, 432, 433, 434, 435, 440, 443, 446, 453

Malicious Domain Manager (MDM)
346, 361, 489, 496

malware
11, 43, 60, 66, 76, 77, 79, 81, 343, 346, 361, 408, 411, 424, 436, 438, 457, 460, 462, 465, 480, 481, 487, 493, 495, 496, 497, 498, 499, 502, 505, 528, 538

man-in-the-middle
434, 481

mlčenlivost
267, 314, 315, 316, 388, 389, 393, 489

Morris
343, 505, 534

motiv
66, 73, 78, 82, 407, 515

**N**

NBÚ
28, 30, 91, 92, 93, 130, 144, 146, 148, 239, 294, 295, 303, 304, 305, 311, 312, 314, 315, 320, 321, 323, 324, 326, 327, 331, 332, 336, 337, 341, 342, 349, 350, 351, 354, 355, 357, 358, 353, 364, 367, 369, 370, 375, 381, 382, 385, 387, 391, 392, 394, 395, 398, 399, 515, 516

NIS
93, 96, 139, 140, 141, 146, 147, 148, 149, 189, 192, 193, 194, 195, 197, 198, 200, 233, 235, 239, 240, 241, 245, 246, 252, 307, 327, 331, 340, 343, 344, 346, 356, 360, 365, 368, 373, 378, 401, 512

NÚKIB
29, 30, 67, 93, 130, 140, 152, 164, 165, 169, 195, 202, 203, 206, 207, 210, 211, 212, 217, 218, 219, 224, 225, 228, 229, 234, 235, 247, 293, 307, 309, 313, 315, 316, 318, 319, 322, 323, 324, 325, 327, 328, 329, 331, 332, 333, 334, 338, 339, 345, 346, 350, 352, 353, 354, 355, 356, 358, 364, 365, 366, 367, 370, 371, 372, 374, 376, 378, 381, 382, 383, 384, 385, 386, 387, 388, 389, 393, 394, 400, 528

## O

ohlašovací povinnost
303, 305, 307, 308

on-line tržiště
143, 147, 148, 189, 192, 193, 194, 233, 134, 240

opatření
reaktivní opatření
51, 92, 93, 99, 202, 206, 210, 217, 218, 224, 252, 295, 317, 318, 319, 320, 321, 322, 325, 326, 327, 329, 336, 383, 395, 539

nápravné opatření
204, 207, 213, 220, 226, 385, 389, 390

obecné povahy
144, 204, 207, 210, 212, 213, 218, 219, 224, 225, 326, 329, 330, 331, 332, 333, 362, 366, 367, 381, 382, 383, 389

bezpečnostní – viz bezpečnostní opatření

orgán veřejné moci
133, 140, 142, 145, 151, 153, 155, 214, 221, 226, 230, 245, 336, 390

osobní údaj
14, 27, 28, 31, 49, 52, 80, 96, 97, 98, 99, 101, 102, 103, 104, 105, 106, 107, 109, 110, 111, 112, 113, 120, 130, 135, 136, 151, 156, 163, 169, 185, 265, 275, 302, 304, 307, 313, 314, 377, 412, 491, 512, 532

## P

PDCA
255, 256, 260, 533, 535

penetrační test
62, 73, 292, 361, 421, 422, 444, 455

perimetr
60, 73, 282, 283, 285, 290, 291, 411, 412

phishing
62, 67, 76, 77, 79, 277, 361, 460, 462, 465, 477, 494, 495, 496, 497, 533

počítačový
systém
12, 36, 38, 42, 43, 44, 45, 46, 47, 48, 53, 57, 58, 59, 60, 61, 72, 75, 76, 77, 80, 82, 83, 87, 95, 103, 105, 108, 118, 122, 123, 141, 195, 292, 312, 360, 407, 411, 415, 416, 417, 418, 419, 420, 421, 422, 423, 424, 425, 426, 427, 428, 429, 430, 431, 432, 433, 434, 435, 436, 438, 439, 440, 441, 443, 444, 445, 446, 447, 448, 449, 450, 451, 452, 453, 454, 455, 456, 461, 462, 465, 467, 475, 476, 480, 481, 482, 483, 485, 486, 487, 488, 489, 505, 507

program
46, 72, 79, 96, 117, 123, 141, 142, 148, 159, 164, 165, 193, 278, 289, 294, 365, 368, 373, 374, 421, 422, 432, 434, 436, 440, 442, 446, 468, 469, 470, 473, 478, 479, 480, 482, 489, 497

prevence
45, 63, 69, 96, 97, 115, 131, 132, 144, 161, 258, 290, 368, 369, 372, 391, 505, 532

PROKI
29, 347, 496, 497, 498, 499, 500, 501, 502, 503, 526

přestupek
31, 109, 204, 207, 213, 214, 220, 221, 226,

230, 236, 381, 385, 386, 389, 390, 391, 392, 393, 394, 404

pseudonymizace
111, 112

působnost
místní
36, 101, 104, 114, 125

časová
125

věcná
125, 139, 140, 141, 144, 145, 148

osobní
125, 330, 332, 341, 363, 364

**R**

RACI
272, 273

rainbow tables
444, 445, 469, 470, 471, 472, 525, 531, 535

ransomware
11, 12, 67, 79, 87, 480, 483, 531, 532, 535, 537, 538

RDP
29, 482, 483

reakce
45, 50, 62, 78, 89, 91, 134, 275, 321, 326, 327, 331, 332, 333, 342, 343, 344, 358, 363, 373, 408, 443, 490, 491, 494, 497, 498, 505, 506, 507, 509, 511, 518

riziko
41, 50, 51, 58, 61, 64, 67, 68, 69, 70, 71, 74, 89, 97, 111, 112, 130, 131, 133, 139, 209, 217, 223, 228, 233, 243, 244, 245, 246, 250, 252, 253, 254, 257, 258, 259, 260, 261, 262, 263, 264, 265, 268, 269, 271, 274, 275, 278, 279, 280, 281, 297, 299, 309, 312, 342, 343, 344, 345, 358, 368, 373, 374, 399, 409, 411, 424, 426, 435, 439, 444, 448, 449, 450, 460, 464, 471, 476, 481, 482, 485, 489, 495, 505, 525, 532

**Ř**

řízení
11, 28, 30, 31, 40, 46, 47, 52, 61, 69, 89, 92, 97, 98, 99, 106, 125, 127, 130, 137, 142, 144, 149, 151, 156, 162, 176, 177, 178, 180, 181, 239, 242, 243, 244, 245, 246, 247, 250, 251, 252, 253, 254, 255, 257, 258, 259, 261, 264, 265, 266, 267, 268, 269, 270, 271, 273, 274, 275, 277, 278, 280, 284, 285, 286, 287, 288, 293, 294, 311, 314, 319, 326, 327, 328, 329, 331, 332, 333, 334, 335, 338, 344, 348, 351, 352, 353, 354, 363, 372, 388, 392, 398, 399, 400, 404, 410, 415, 438, 450, 455, 462, 463, 481, 489, 499, 493, 534, 539, 540

**S**

server
28, 60, 77, 107, 108, 157, 161, 163, 191, 282, 284, 288, 289, 290, 291, 292, 360, 361, 411, 415, 416, 417, 418, 419, 422, 423, 425, 426, 427, 428, 430, 433, 435, 436, 437, 438, 452, 454, 455, 456, 457, 458, 459, 460, 461, 462, 475, 476, 477, 478, 479, 481, 482, 483, 486, 487, 490, 492, 495, 497, 498, 501

SIEM
29, 210, 217, 234, 290, 291, 292, 411, 461, 475, 493

síť
elektronických komunikací
37, 80, 81, 82, 96, 115, 116, 118, 120, 132, 133, 134, 136, 137, 138, 139, 140, 141, 142, 143, 144, 147, 148, 149, 151, 152, 167, 168, 170, 171, 173, 174, 175, 177, 179, 180, 182, 183, 184, 185, 187, 188, 190, 198, 200, 201, 202, 203, 204, 205, 210, 212, 213, 217, 220, 223, 224, 226, 237, 241, 242, 245, 246, 248, 249, 250, 252, 299, 300, 305, 319, 320, 321, 322, 323, 327, 330, 331, 336, 338, 341, 348, 350, 362, 363, 364, 365, 366, 376, 377, 381, 382, 389, 391, 392, 396, 429

významná síť
142, 145, 167, 198, 199, 205, 206, 299, 300, 301, 302, 303, 305, 320, 322, 336, 338, 341, 349, 363, 366, 381, 382, 385, 389, 390, 391, 395, 396

služba
elektronických komunikací
79, 96, 113, 114, 115, 116, 117, 119, 132, 133, 134, 136, 137, 138, 139, 142, 144, 147, 148, 149, 194, 198, 200, 201, 202, 212, 220, 226, 241, 245, 246, 306, 319, 320, 321, 322, 325, 326, 327, 329, 330, 331, 336, 338, 341, 348, 349, 350, 363, 364, 365, 366, 381, 382, 385, 389, 391, 396, 402

základní služba
93, 99, 142, 143, 146, 154, 167, 168, 169, 170, 171, 173, 174, 176, 177, 179, 180, 182, 183, 184, 186, 187, 188, 198, 199, 222, 223, 224, 225, 226, 228, 229, 230, 241, 243, 244, 245, 247, 248, 250, 260, 295, 299, 300, 301, 302, 303, 304, 305, 307, 321, 322, 330, 337, 338, 343, 356, 359, 368, 373, 374, 375, 376, 377, 378, 382, 383, 384, 385, 386, 387, 388, 390, 394, 403, 529, 539

digitální služba
143, 189, 192, 194, 195, 198, 233, 234, 235, 236, 237, 239, 240, 242, 245, 246, 252, 301, 302, 303, 306, 337, 339, 340, 343, 346, 373, 381, 383, 390, 399, 401, 403

software
29, 58, 59, 61, 62, 72, 73, 77, 82, 101, 114, 115, 118, 122, 141, 148, 164, 193, 195, 196, 269, 282, 285, 287, 288, 289, 290, 291, 293, 301, 343, 422, 423, 434, 438, 456, 457, 487, 488, 489, 497, 498, 499

SOHO
29, 429, 436, 437, 438, 456

SSH
29, 465, 466, 481, 482, 483, 486

SSID
29, 440, 442, 443, 444, 445, 448, 449, 471

**Š**

šifrování
111, 289, 292, 293, 418, 434, 440, 441, 442, 443, 445, 446, 449, 450, 451, 458, 462, 464, 466, 476, 480, 481, 482, 485, 487

**T**

technologická neutralita
134, 145, 154, 243, 246

token
413, 414, 463

TLS
29, 476

Traffic Light Protocol / TLP
29, 49, 50, 51, 52, 538

trunk port
428

**U**

usazení
104, 237, 238, 239, 240, 241

USB
411, 418, 419, 420, 421, 422, 423, 424, 487, 538

**V**

varování
89, 132, 203, 207, 212, 219, 225, 229, 235, 236, 291, 313, 317, 319, 320, 321, 323, 324, 325, 335, 336, 344, 358, 374, 399, 400, 461, 486, 508

VLAN
30, 60, 285, 426, 427, 428, 430, 439, 462, 486

VPN
15, 30, 285, 482, 483

významný dopad
143, 228, 230, 302, 303, 307, 340, 346, 356, 358, 360, 390

**W**

web
38, 42, 106, 114, 157, 158, 161, 162, 163, 194, 195, 239, 287, 288, 292, 318, 319, 346, 361, 426, 434, 435, 436, 437, 448, 457, 458, 459, 460, 461, 468, 474, 475, 477, 479, 487, 496, 498, 502, 525, 528, 537

WEP
30, 441, 442, 443

WHOIS
494, 498, 502

Wireshark
432, 434, 440, 442, 446

WPA
30, 442, 443, 444, 445, 450, 451, 448, 525, 535, 537

WPS
30, 447, 448, 526, 540

**Z**

záplaty
73, 479, 487

zranitelnost
11, 37, 68, 71, 72, 73, 203, 207, 212, 219, 225, 229, 235, 253, 259, 262, 263, 265, 277, 279, 293, 294, 325, 340, 342, 345, 353, 356, 357, 360, 361, 425, 436, 437, 442, 450, 460, 462, 464, 478, 479, 483, 531



Tato odborná kniha byla vydána v rámci projektu „Predikce a ochrana před kybernetickými incidenty (PROKI)“ (VI20152020026), který je reaizován v rámci Programu bezpečnostního výzkumu ČR na léta 2015–2020.

Za tuto publikaci odpovídají pouze její autoři.

Recenzenti:
prof. Ing. Miroslav Vozňák, Ph.D.
doc. JUDr. Ladislav Pokorný, Ph.D.
RNDr. Radim Ošťádal, Ph.D.

**CYBERSECURITY**
doc. JUDr. Jan Kolouch, Ph.D.
Bc. Pavel Bašta
Andrea Kropáčová
Bc. Martin Kunc

Vydavatel:
CZ.NIC, z. s. p. o.
Milešovská 5, 130 00 Praha 3
Edice CZ.NIC
www.nic.cz

1. vydání, Praha 2019
Kniha vyšla jako 20. publikace v Edici CZ.NIC.

© 2019 Jan Kolouch, Pavel Bašta a kol.
Toto autorské dílo podléhá licenci Creative Commons BY ND 3.0 (http://creativecommons.org/licenses/by-nd/3.0/cz/), jeho sdílení je tedy možné za předpokladu, že zůstane zachováno označení autora díla a prvního vydavatele díla, sdružení CZ.NIC, z. s. p. o. Dílo může být překládáno a následně šířeno v písemné či elektronické formě, na území kteréhokoliv státu.

ISBN 978-80-88168-31-7 (tištěná verze)
ISBN 978-80-88168-32-4 (ve formátu EPUB)
ISBN 978-80-88168-33-1 (ve formátu MOBI)
ISBN 978-80-88168-34-8 (ve formátu PDF)

cz.nic | SPRÁVCE DOMÉNY CZ

**Summary**

We live in a time when information and communication technologies (ICT) are already inherently connected to every aspect of our existence.

As the volume of data and information stored by Internet Service Providers (ISPs) grows, questions of their effective security, transmission or deletion are increasingly being addressed, not only on the basis of a contract between the ISP and the end user, but also on the basis of the new emerging legislation.

This book focuses primarily on the issue of cyber security, especially the basic principles that every person who uses information and communication technologies should either respect or modify depending on the activity or purpose for which the principles are used.

At the same time, the book contains a partial interpretation of some legal norms that are directly related to cyber security issues. A relatively separate part of the book is a commentary on Act No. 181/2014 Coll., On Cyber Security and on Changing Related Acts (the Cyber Security Act).

Apart from the theoretical and legal part, the book also consists of a practical part which can be used especially by IT specialists who want to learn about cyber security. From the book, it is also possible to extract information about the activities of CERT, CSIRT cyber-space teams, their capabilities and limits.

In order to keep the information in the book as updated as possible, a portal has been created at: https://kyberbezpecnost.csirt.cz/. Current cyber threats or attacks will be posted on this portal, including information on how to resist them, security recommendations, hints, and instructions for both regular users and IT professionals.

Edice CZ.NIC

**O knize** Kniha CyberSecurity prezentuje základní principy, které by každá osoba, která využívá informační a komunikační technologie, měla respektovat či si je modifikovat v závislosti na činnosti a účelu, za kterým tyto technologie využívá. Kniha obsahuje dílčí výklad některých právních norem, které s problematikou kybernetické bezpečnosti bezprostředně souvisejí. Relativně samostatnou část knihy představuje komentář k zákonu č. 181/2014 Sb., o kybernetické bezpečnosti. Vedle teoretické a právní části je součástí knihy i praktická část, využitelná zejména IT odborníky, kteří se chtějí vzdělat i v problematice kybernetické bezpečnosti. Z knihy je také možné načerpat informace o činnosti bezpečnostních týmů typu CERT, CSIRT v kyberprostoru, jejich možnostech a limitech.

**O autorech** **Jan Kolouch** dlouhodobě působí jako vysokoškolský pedagog a těžištěm jeho odborného zájmu je především problematika kybernetické kriminality, bezpečnosti a aplikovatelnosti práva v kyberprostoru. Od roku 2008 působí i v rámci sdružení CESNET. Na řadě aktivit spolupracuje i se sdružením CZ.NIC a bezpečnostními týmy CERT/CSIRT. Jan Kolouch se také věnuje dalším projektům a školením v oblasti bezpečnosti v ICT, boje s kyberzločinem, ochrany uživatelů aj., jak na národní, tak na mezinárodní úrovni. Svojí činností se snaží zvyšovat informovanost laické i odborné veřejnosti zejména v oblasti kybernetické kriminality a kybernetické bezpečnosti.

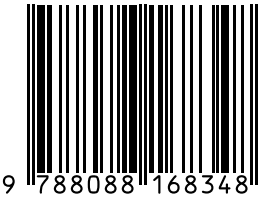
**Pavel Bašta** pracuje jako team leader a bezpečnostní analytik týmů CZ.NIC-CSIRT a CSIRT.CZ ve sdružení CZ.NIC. Problematice bezpečnosti se ve volném čase věnoval i dříve, kdy prošel různé oblasti IT, od komplexní správy sítě a serverů v menší společnosti, přes technickou podporu, konfiguraci a dohled zákaznických routerů, nebo správu zákaznických a interních serverů u internetového providera. Avšak až díky jeho působení ve sdružení CZ.NIC se mu bezpečnost stala nejen koníčkem, ale také každodenní pracovní náplní. Pavel je absolventem Bezpečnostně právních studií na Policejní akademii ČR a sám se také věnuje lektorské činnosti.

**Andrea Kropáčová** v roce 2004 vybudovala tým CESNET-CERTS, první CSIRT tým, který byl v České republice etablován a uznán světovou bezpečnostní infrastrukturou. Zkušenosti z vybudování tohoto akademického týmu uplatnila v letech 2007 až 2010 při budování pracoviště CSIRT.CZ. V současnosti se nadále věnuje vedení týmu CESNET-CERTS, rozvoji bezpečnostních služeb ve sdružení CESNET, bezpečnostní strategii sítě CESNET2 a reprezentaci sdružení CESNET v národních i mezinárodních bezpečnostních infrastrukturách. Získané vědomosti a zkušenosti využívá pro osvětovou a vzdělávací činnost.

**Martin Kunc** pracuje v týmu CSIRT.CZ jako bezpečnostní analytik. Od mládí byl fascinován počítači a svůj zájem postupně profiloval přes hry, na počítačové sítě a následně na jejich bezpečnost. Před nástupem do CSIRT.CZ pracoval v S.ICZ (I.CZ) jako specialista síťových technologií, vývojář a analytik.

**O edici** Edice CZ.NIC je jednou z osvětových aktivit správce české národní domény. Ediční program je zaměřen na vydávání odborných, ale i populárně naučných publikací spojených s Internetem a jeho technologiemi. Kromě tištěných verzí vychází v této edici současně i elektronická podoba knih. Ty je možné najít na stránkách knihy.nic.cz.

ISBN 978-80-88168-34-8




knihy.nic.cz