BusinessIT.cz
ebook

Bezpečnost IT: Nepodceňujte rizika

Redakce BusinessIT
a kolektiv autorů

Bezpečnost IT. Edice BusinessIT ebooks 2012.

Bezpečnost IT: Nepodceňujte rizika

BusinessIT.cz

Edice: BusinessIT ebooks
Autoři: Redakce BusinessIT.cz a autoři uvedení u kapitol

Vydáno v roce 2012 v Bispiral, s.r.o.

web: www.BusinessIT.cz

Málokteré téma je tak rozporuplné jako bezpečnost IT: Na jednu stranu se o ní stále mluví a všichni si uvědomujeme, kde případně může hrozit průšvih, na druhou stranu řada z nás prostě doufá, že bude mít zase štěstí a průšvih nenastane. Ještě chvíli nám to štěstí musí vydržet, ale pak, pak už dokončíme všechny plánované bezpečnostní projekty a všechno

bude OK. Ale co když nás štěstí opustí? V této knize vám nabízíme pohled na vybraná rizika, a to z pohledu statistik i ve formě přehlídky možných řešení.
V následujících příspěvcích se věnujeme mimo jiné problematice zaměstnanců, jejichž nedbalost, ale i špatné úmysly jsou velkým rizikem pro bezpečnost dat, problematice cílených útoků zvenčí, vybraným bezpečnostním technologiím (za všechny jmenujme NBA – Network Behavior Analysis) nebo přetrvávajícím slabinám softwaru. A nabízíme vám i pohled partnerů této knihy, kteří nabízejí svá řešení problémů, které možná ohrožují i vás.

Redakce BusinessIT.cz

Počet cílených útoků na IT roste

Denní počet cílených útoků na IT infrastrukturu je na

vzestupu, přičemž nejčastěji bývá napadána veřejná správa; druhé místo pomyslného žebříčku patří chemickému a farmaceutickému průmyslu, třetí průmyslu zpracovatelskému. Cílem útoků je podle komentátorů vytvoření trvalého přístupu do sítě napadené organizace, v mnoha případech jde rovněž o vytvoření vzdáleného přístupu k důvěrným datům. A útoky se samozřejmě nevyhýbají ani organizacím v tuzemsku.

Výše uvedené údaje jsou jen částí výstupů ze zprávy Symantec Intelligence Report (SIR), ve které společnost Symantec koncem minulého roku shrnula trendy za uplynulých 11 měsíců. Provedená analýza mimo jiné potvrdila, že velké společnosti s více než 2500 zaměstnanci čelily největšímu průměrnému počtu útoků. Denně jich blokovaly v průměru 36,7. Menší organizace s počtem zaměstnanců do 250 pak denně blokovaly průměrně 11,6 útoků.

„Cílené útoky jsou navrženy pro sběr informací, krádeže důvěrných dat nebo obchodních tajemství. V případě útoků typu Stuxnet narušují provoz, případně ničí kritickou infrastrukturu," varuje Paul Wood, senior intelligence analyst, Symantec.cloud. „Je

důležité si uvědomit, že bez silného sociálního inženýrství nebo techniky ‚head-hacking' nemohou uspět ani technicky velmi sofistikované útoky. Většina z nich proto využívá sociální inženýrství," dodává Wood a upřesňuje: „Pracují s informacemi, které o sobě zveřejňujeme na sociálních sítích a na stránkách sociálních médií. Pokud útočníci mohou znát naše zájmy a koníčky, ví, s kým se stýkáme a kdo je v naší síti, potom jsou schopni vytvořit velmi uvěřitelné a přesvědčivé útoky."

Průběh útoků

Útočníci podle další zprávy Symantecu věnované loňskému útoku Nitro (zaměřeného na chemický průmysl) cílené útoky zpravidla pečlivě plánují. V každé napadené organizaci byl v tomto případě e-mail typicky zaslán jen malému počtu zaměstnanců. Výjimkou byly tři organizace, z nichž v jedné dostalo e-mail takřka 500 příjemců a v dalších dvou více než 100.
Obsah e-mailů byl velmi různý, dva typy však vyčnívaly nad ostatní: Jedna skupina se tvářila jako

pozvánka na setkání se známým obchodním partnerem, druhá pak jako bezpečnostní update (tento druhý typ e-mailů zpravidla dostala širší skupina příjemců). E-maily pak obsahovaly buď spustitelný soubor, který se názvem a ikonou maskoval jako textový dokument, nebo zaheslovaný archiv se spustitelným souborem – s heslem uvedeným v e-mailu. V obou případech obsahoval spustitelný soubor trojského koně Poisonlvy, vyvinutý zřejmě čínsky mluvícím programátorem.
Po spuštění se škodlivý kód nainstaloval, šifrovaně se spojil s C&C serverem (command-and-control server) a poté již plnil příkazy zadané prostřednictvím tohoto serveru. Typicky odeslal útočníkovi informace o dalších počítačích v síti a hashe hesel z Windows. S využitím získaných informací pak útočník zamířil na další počítače v síti.
Útok Nitro postihl 29 firem – a podle uvedené zprávy napadl rovněž tři počítače v ČR. (Lokalita napadených počítačů byla určena podle IP adres strojů připojujících se k C&C serveru.) Útočícími počítači byly VPS servery v USA využívané z Číny.

Nebezpečí v číslech

Zpráva SIR dále uvádí, že jeden phishingový útok připadal loni v listopadu na 302 e-mailů (0,33 %) a globální míra e-mailů šířících viry činila 0,39 % (jedna postižená zpráva na 255,8 bezproblémových). 40,2 % e-mailů šířících viry obsahovalo odkazy na infikované webové stránky.

Analytici každý den identifikovali v průměru 4915 webových stránek, které obsahovaly škodlivý kód (včetně spyware a adware) a obecně nejčastěji blokovaným malwarem byl kód WS.Trojan.H. (Jde o soubory zachycené obecnou cloudovou heuristickou detekcí, u nichž nebyla klasifikována konkrétní hrozba.)

Pokud vás zajímá, jak jsou na tom jednotlivé regiony, pak třeba podíl spamu se typicky pohybuje ve většině uváděných zemí okolo 70 % e-mailové komunikace. V USA činí podle zprávy 69,9 %, v Kanadě 69,5 % (stejně jako ve Velké Británii), v Nizozemsku 70,5 %, v Austrálii 68,6 % a naopak v Brazílii 74,3 %. Nejčastějším cílem phishingových útoků se stala Jižní Afrika – jeden z 96,2 e-mailů byl identifikován jako phishing, druhé místo připadlo

Velké Británii s jednou ze 167 zpráv. V USA šlo o jednu z 461,8 zpráv a třeba v Německu o jednu z 426,2 zpráv.

Bezpečnost informací ohrožují hlavně vlastní zaměstnanci

Nedbalost, ale i špatné úmysly zaměstnanců jsou velkým rizikem pro bezpečnost dat ve firmách. Dokazuje to řada analýz, z nichž vyplývá například fakt, že více než polovina zaměstnanců má přístup k datům, k nimž by se vůbec neměla dostat, a 40 % zaměstnanců bez skrupulí poškodí zaměstnavatele či nadřízeného, budou-li z toho mít osobní prospěch. Výsledky nejzajímavějších z těchto studií vám nabízíme v tomto textu spolu s tipy, jak se proti zmiňovaným rizikům účinně bránit.
Výsledky studie The Insecurity of Privileged Users (TIPU) provedené Ponemon Institute na zakázku HP ukazují, že 52 % respondentů má přístup k chráněným a utajovaným podnikovým informacím nad rámec svých kompetencí či pracovní pozice a

více než 60 % dotázaných uvádí, že privilegovaní uživatelé přistupují k citlivým nebo tajným datům spíše ze zvědavosti, než kvůli pracovním povinnostem. 40 % účastníků průzkumu si není jistých, zda má jejich firma přehled o specifických přístupových právech napříč celou podnikovou sítí, případně zda stávající práva splňují definovanou úroveň zabezpečení na jednotlivých stupních oprávnění přístupu k datům.

Společnost S&T CZ na základě analýzy DAP Services varuje, že 40 % zaměstnanců bez skrupulí poškodí zaměstnavatele či nadřízeného kvůli osobnímu prospěchu. Pravděpodobnost útoku zevnitř je přitom podle jejích zástupců třikrát vyšší než zvenčí. „Interní pletichy, tedy snaha získat nekalým způsobem nějakou výhodu uvnitř firmy, patří mezi nejrozšířenější bezpečnostní rizika. V závěsu je vynášení strategických informací mimo firmu, například podrobnosti o nabídkách klíčových tendrů," upozorňuje Petr Hněvkovský, bezpečnostní expert S&T CZ.

Za únikem dat způsobeným zaměstnanci ale nemusí být vždy jen zlý úmysl. Další analýza Ponemon

Institute – tentokrát provedená na zakázku Kingston Technology a zaměřená na stav zabezpečení USB disků – nabízí rovněž varující pohled: 62 % organizací podle ní uvádí, že během posledních dvou let jejich zaměstnanci ztratili důležité informace uložené na USB discích a 75 % zaměstnanců v evropských organizacích používá USB disky bez povolení zaměstnavatele.
A konečně ze studie Cisco Connected World Technology Report plyne, že 70 % zaměstnanců, kteří jsou obeznámeni s bezpečnostními pravidly firmy, připouští jejich občasné porušení, přičemž třetina z nich to odůvodňuje přesvědčením, že nedělají nic špatného. Zhruba 22 % jich uvádí, že potřebují přístup k nepovoleným programům a aplikacím, aby mohli dokončit svoji práci. A 19 % respondentů tvrdí, že dodržování pravidel není vynucováno.

Intriky ve firmách

„K intrikaření dochází v každé firmě," tvrdí Petr Hněvkovský a dodává: „Vynést tajnou informaci

mimo firmu a ještě ji zpeněžit je rizikové a náročné, to si běžný zaměstnanec netroufne. U interního zneužití je to ale jinak: Upevnit svou pozici uvnitř firmy chce každý, s rostoucí nezaměstnaností budou interní pletichy narůstat.“

„Češi jsou poměrně soutěživí a ambiciózní, bohužel až 40 procent z nich bez skrupulí poruší pravidla hry, pokud jim to přinese osobní výhodu. Může za to přijetí neetických forem chování v české populaci jako zcela běžné součásti života,“ vysvětluje psycholog Jiří Šimonek z DAP Services. Vyplývá to z testování 84 tisíc zaměstnanců během posledních pěti let, které tato společnost provedla.

Pokud dojde ke krádeži dat, nejčastěji podle S&T CZ jde o rozvojové plány, informace o platech a odměnách, nabídky v rámci tendrů a o některé další klíčové informace užitečné k upevnění vlivu uvnitř firmy.

„Setkáváme se často s nulovým zabezpečením interních dat. V případě jejich zneužití se pak velmi těžko hledá viník, a i pokud se najde, bez pádných důkazů nelze takového pracovníka kvůli zneužití interních informací propustit,“ upozorňuje soudní znalec Ivan Janoušek ze znaleckého ústavu Apogeo

Esteem. Nízké zabezpečení lze zřejmě mnohdy přičíst na vrub i faktu, že si manažeři neradi připouštějí zrádce ve vlastním týmu: „Je to přirozené: Stejně jako každý rodič vidí (i manažer) vlastní děti v lepším světle než okolí. O to více je třeba být na pozoru, protože intriky mohou rozložit celý pracovní tým," vysvětluje Šimonek.

Situace se ale postupně mění a firmy investují do řešení, která jejich data pomáhají chránit i před nebezpečím zevnitř. „Zaznamenáváme meziročně zhruba 30procentní nárůst prodejů. Tyto systémy monitorují a vyhodnocují všechny události, které by mohly mít vliv na bezpečnost firmy – od pohybu osob po přístup k citlivým datům a využívání různorodých informačních zdrojů," vysvětluje Hněvkovský. Lze tak snadno zjistit aktivity jednotlivých uživatelů a včas vyhodnotit nestandardní situace.

„Nová generace zaměstnanců obohacuje firmy o nové myšlenky, metody práce i netradiční pohled na řešení pracovních úkolů. Zároveň má ale svá očekávání ohledně používání informačních technologií, která se mohou významně promítat do firemní IT bezpečnosti," říká Jiří Devát, generální ředitel Cisco Česká republika, a dodává: „Pro firmy

nastal čas přizpůsobit svá bezpečnostní pravidla nastupujícím trendům a modelům chování – odměnou jim kromě vyšší bezpečnosti bude také větší produktivita a spokojenost zaměstnanců.“

Jak se lze bránit

Organizace se podle Ponemon Institute snaží udržet problém s oprávněností přístupů k datům pod kontrolou různými způsoby. Dvacetsedm procent respondentů průzkumu TIPU prozradilo, že jejich organizace ke kontrole sdílení správcovských oprávnění či zvýšených oprávnění vybraných uživatelů využívá technologie monitorující správu identit a přístupů, u 24 % organizací se pak kombinují tyto technologie s dalšími procesy. Zároveň však 15 % respondentů přiznalo, že přístupy nejsou zcela kontrolované a v 11 % případů nejsou organizace schopny vůbec detekovat nesprávné sdílení přístupových práv.
Hlavní překážku pro lepší kontrolu přístupových práv privilegovaných uživatelů představují podle respondentů neustálé změny požadavků,

nekonzistentní schvalovací procesy, vysoké náklady na sledování přístupů a složité ověřování změn oprávnění. Zlepšení aktuálního stavu pak může přinést sledování privilegovaných uživatelů v případě jejich použití administrátorských oprávnění, identifikace porušení bezpečnostních pravidel a centrální správa přístupů v celé organizaci. Téměř 80 % respondentů uvedlo, že nasazení řešení pro správu bezpečnosti informací a aktivit (SIEM) bylo rozhodující pro podstatné zlepšení správy, administrace a sledování přístupových práv privilegovaných uživatelů.

Představitelé společnosti HP, která si provedení průzkumu u Ponemon Institute objednala, ihned upozorňují na své léky řešící uvedenou situaci: Nabízejí komplexní bezpečnostní řízení a správu privilegovaných uživatelů prostřednictvím nástroje Security Intelligence Platform, jež je podle nich klíčovou součástí řešení HP IT Performance Suite, které umožňuje IT administrátorům optimalizovat provoz a vylepšit výkon síťové infrastruktury. HP IT Performance Suite nabízí ucelený přehled o celé IT infrastruktuře a automatizuje její správu.

Řešení z tuzemských laboratoří

Své řešení zaměřené na ochranu firem před hrozbami ze strany jejich zaměstnanců nabízí i česká společnost Safetica Technologies, a to konkrétně se svým produktem Safetica Endpoint Security. Safetica podle svých autorů chrání před únikem dat a dohlíží na pracovní činnost zaměstnanců. Cílem je odhalit rizikové chování zaměstnanců dlouho před tím, než mohou firmu ohrozit. Pokud se problém objeví, software by měl zabránit nejhoršímu – tedy vynesení citlivých informací z firmy či poškození zájmů společnosti. Klientovi podle představitelů výrobce software současně zajistí cenné důkazní materiály pro případný spor s problémovými zaměstnanci.

Safetica Endpoint Security nabízí manažerům neustálý přehled o dění ve společnosti a především o tom, kdo pracuje s jakými daty. Nezatěžuje je však zbytečnými detaily; zasílá pravidelné souhrny výsledků a v případě nebezpečí je ihned varuje. Každý manažer si přitom sám může vybrat, na co bude upozorněn – a detaily může zkoumat až v

okamžiku reálného podezření.
V současné době produkt Safetica Endpoint Security distribuují partneři výrobce ve 45 státech světa. A plánována je další expanze.

Ochrana USB disků

Také pohled na USB disky a nutnost jejich zabezpečení se postupně mění. Podle výše zmíněného průzkumu Ponemon Institute v současnosti 34 % USB disků používaných v evropských organizacích používá šifrování dat, přičemž 49 % evropských organizací tvrdí, že jejich USB disky vyhovují hlavním bezpečnostním standardům.
A ještě pohled z jiného úhlu: 68 % zaměstnanců podle Ponemon Institute potvrzuje, že jejich organizace má nějaká pravidla pro používání USB disků – ale 37 % evropských organizací prý tato pravidla nevynucuje. 46 % zaměstnanců pak nedodržuje důležitá bezpečnostní pravidla pro práci s USB disky, mezi která podle představitelů společnosti Kingston Technology patří: používání

hesel, blokování USB portů (pro neschválená zařízení), kontrola zařízení na viry a další malware, monitorování USB disků a šifrování dat.
Kingston Digital Europe samozřejmě také nabízí své řešení pro zajištění bezpečnosti USB disků: Koncem loňského roku představila rodinu USB flash disků Kingston DataTraveler 6000, které chrání citlivá data podle požadavků normy FIPS 140-2 (Federal Information Processing Standard), v jejímž rámci je certifikován pro Level 3. DataTraveler 6000 využívá patentovanou technologii Secured by Spyrus, která podporuje 256bitovou šifru AES na hardwarovém základě s využitím režimu blokového kódování XTS. Podle výrobce jde o nejbezpečnější USB flash disk na současném trhu a splňuje předpisy pro nakládání s uloženými daty v organizacích poskytujících finanční služby a ve vládních úřadech. Pro své chráněné USB disky nabízí Kingston i software určený pro jejich centrální správu v organizaci.

Nikdo není dokonalý

Společnost Gallup, která se zabývá výzkumem a

poradenstvím v oblasti psychologie, managementu a sociologie, člení zaměstnance ve firmách na základě svých anket typicky do třech skupin. V první z nich jsou zaměstnanci, kteří pracují se zájmem a nadšením pro danou věc. Ti zpravidla řídí rozvoj a inovace ve společnosti a je jich cca 27 %. Druhou skupinou jsou zaměstnanci, kteří pracují bez vášně a zájmu o úspěch společnosti a nevyužívají plně svůj potenciál. Takových je podle výzkumu Gallupu 59 %. A poslední skupinu tvoří zaměstnanci aktivně vystupující proti společnosti. Do práce chodí negativně naladění, snaží se škodit v tom, co dělají oni i jejich spolupracovníci, a často se tak mstí za domnělé křivdy jim způsobené. Těch je dle výzkumu 14 %.

Ani další dostupné statistiky nejsou zcela optimistické. Podle IDC 30-40 % přístupů na internet v pracovní době není stráven pro účely související s prací. Podle průzkumu Morse se pak 57 % dotázaných pracovníků v práci věnuje osobním aktivitám na sociálních sítích. Dle staršího průzkumu KPMG (z roku 2009) skončí 70 % ukradených dat u konkurence.

I když připustíme, že podobná varování hrají do noty

poskytovatelům bezpečnostních produktů a služeb, vždy stojí za to položit si otázku, nakolik může některý z nastíněných problémů existovat i v mé organizaci. A pokud není dosud řešen, zda a jak vážně může ohrozit její fungování.

Chraňte svou síť s odlehčenou technologií NBA

Technologie NBA – Network Behavior Analysis není na trhu žádnou horkou novinkou, přesto však rozhodně nelze tvrdit, že by povědomí o ní bylo dostatečně rozšířené. Jde přitom nepochybně o jednu z velmi efektivních cest vedoucích k odhalování provozních a bezpečnostních problémů v počítačových sítích. A i když tomu tak dlouho bylo, nyní již nejde o řešení vhodné jen pro velké organizace.
Systémy založené na technologiích NBA pracují na principu detekce anomálií a nežádoucího chování v datových sítích, která je založena na permanentním

vyhodnocování statistik o provozu na síti. Integrovaná inteligence těchto systémů je schopna na základě provedených analýz odhalit například problémy typu průniku škodlivého kódu do sítě, útoku DDoS nebo zneužívání infrastruktury interními zaměstnanci organizace.
Hlavní výhodou proti běžným IDS systémům či SNMP monitoringu je orientace na celek – na komplex chování zařízení na síti – a to umožňuje administrátorům získat ucelený pohled na spravovanou IT infrastrukturu a reagovat i na dosud neznámé či specifické hrozby.
Mezi výrobce, kteří se na využití technologií NBA specializují, patří třeba Arbor Networks s platformou Peakflow nebo Lancope se systémem StealthWatch. Produkty využívající technologií NBA však nabízí i řada dalších hráčů, například IBM, která mimochodem nedávno dokončila akvizici Q1 Labs, firmy vyvíjející některé prvky NBA, nebo třeba Riverbed, které k příslušným technologiím pomohla akvizice firmy Mazu Networks.

NBA řešení od tuzemských vývojářů

Až do nedávné doby nasazovaly produkty založené na NBA zejména velké společnosti, a to především z důvodu relativní složitosti implementace a následné obsluhy i celkové finanční náročnosti těchto řešení. To se rozhodla změnit mladá česká firma AdvaICT, která vyvinula odlehčené řešení s NBA, které je dostupné i pro střední a malé firmy.

Inovativnost nového řešení spočívá podle představitelů AdvaICT zejména v rychlosti a jednoduchosti jeho nasazení do sítě, které lze zvládnout za 30 až 60 minut – a výstupy pak má firma k dispozici ihned. Díky rychlosti nasazení tohoto řešení je v současné době možné využívat NBA také formou jednorázové služby auditu provozu v síti.

„Služba Network Traffic Audit umožňuje odhalit anomálie a bezpečnostní rizika, navrhuje optimální rozložení síťových kapacit, určuje kritická místa sítě, detekuje vnitřní i vnější útoky a určuje, které služby a kteří uživatelé síť nejvíce vytěžují. Je možné ji jednoduše nasadit v různých prostředích bez ohrožení standardního chodu síťové infrastruktury," vysvětluje Pavel Minařík, ředitel vývoje společnosti

AdvaICT. Řešení FlowMon ADS přitom obsahuje také takzvaný učící režim, který umožňuje naučit jej, jaká komunikace je považována za standardní, byť by v základním nastavení byla pokládána za anomálii.

Audit je postaven na analýze provozu, který se v síti skutečně vyskytuje. Z tohoto pohledu hodnotí stav sítě a způsob práce s ní bez ohledu na používané nástroje, směrnice či bezpečnostní politiky firmy. Popisuje tak nejen stav sítě a jejích bezpečnostních prvků, ale nepřímo také pracovní morálku zaměstnanců nebo dodržování SLA ze strany poskytovatele připojení k internetu a dalších služeb. U nalezených incidentů či problémů poskytuje detailní podklady pro jejich rychlé a efektivní řešení. O jaké problémy se typicky jedná? „Jde například o slovníkové útoky proti serverům, skenování sítě, vzdálený management, šíření malware, nebo odesílání spamu," vyjmenovává Minařík. „Takto detekované incidenty lze vyřešit dříve, než ovlivní chod celé organizace a eskalují na úroveň nejvyššího managementu." Dalším krokem na základě odhalených útoků je nastavení prostředí tak, aby se již nemohly opakovat.

Produkt od AdvaICT už využívají například Masarykova univerzita, Český statistický úřad, Agrofert Holding nebo Veletrhy Brno. „Řešení FlowMon ADS jsme nasadili s cílem zvýšit bezpečnost a kontrolu nad naší infrastrukturou. Díky monitorování provozu datové sítě máme pod dohledem vytížení a způsob využití našeho datového centra i a připojených společností k síti internet. V případě problémů jsme schopni efektivně diagnostikovat jejich příčinu. Navíc FlowMon ADS permanentně vyhodnocuje veškerý provoz a upozorňuje nás na potenciální bezpečnostní incidenty.," komentuje využití produktu ICT ředitel Agrofert Holding, Martin Poláček.

Audit lze zrealizovat i bez vzdáleného přístupu k používanému zařízení a všechna data získaná v průběhu monitoringu sítě jsou podle dodavatele při ukončení auditu nenávratně smazána. Služba tak splňuje nároky na bezpečnost dat zákazníků. Díky nízkým nákladům je přitom možné audit objednat rychle a bez typicky komplikovaného schvalování na několika úrovních. „První výstupy, které budou použity pro vypracování auditní zprávy, jsou generovány nejvýše do hodiny od vstupu do

serverovny a je možné je okamžitě konzultovat," upřesňuje Pavel Minařík. „Auditní zpráva je hotová s ohledem na trvání auditu během čtrnácti dnů nebo jednoho měsíce."

Nasazení řešení NBA

Obecně se doporučuje nasadit jakékoli systémy s NBA poté, co jsou na místě další standardní prvky ochrany na perimetru sítě – firewally a IPS (Intrusion Prevention System). A stejně jako u jiných řešení i zde platí, že pokud IT oddělení firmy nemá s výběrem a nasazením NBA dostatek zkušeností, je vhodné je řešit s využitím externích odborníků, kteří jsou schopni zhodnotit existující síťovou infrastrukturu, doporučit a poté i nasadit řešení, které v ní bude schopné efektivně pracovat.
Protože NBA systémy obecně vyžadují pečlivé nastavení, doporučuje se rovněž nasazované řešení nejprve v organizaci – přímo v provozním prostředí – pečlivě otestovat, než se přistoupí k plné implementaci. Jako vhodnou alternativu bohužel nelze doporučit testování v laboratorních

podmínkách, protože touto cestou nelze získat potřebné poznatky z chování ve vlastní infrastruktuře. Právě vzhledem k náročnosti, kterou obvykle nasazení „velkého“ NBA řešení představuje, může být dobrou volbou využití odlehčeného řešení, které může přinést potřebné informace bez toho, aby byla jeho implementace přehnaně časově, finančně a organizačně náročná.

NBA: Příklady z praxe

Poměrně častým problémem bývá v organizacích zahlcení lokální sítě nebo zpoždění aplikací způsobené zahlcováním spojení mezi pobočkami. Jeden z řady konkrétních případů vedl k situaci, kdy se firmě problém svépomocí nepodařilo vyřešit, nepomohla ani výměna podezřelých aktivních prvků či zavedení restriktivních opatření. Po nasazení specializovaného monitorovacího zařízení se ukázalo, že na vině je aplikace vzdáleného dohledu stanic na pobočkách, která po třech letech bezproblémového provozu vypověděla službu a začala mezi pobočkami přenášet zcela neočekávané objemy dat. Audit provozu datové sítě

tak dokázal rychle a přesně lokalizovat problém, který firma standardními prostředky nebyla schopna odhalit.
Další příklad se týká bezpečnosti. Firmy, které mají infrastrukturu navrženou dle doporučených pravidel a postupů, včetně ochrany perimetru a důsledné antivirové kontroly, si jsou někdy až příliš jisty svou bezpečností. Typickým výstupem auditu v tomto případě bývá identifikace infikovaných zařízení, která se snaží rozesílat spam nebo porušování bezpečnostní politiky zaměstnanci používáním služeb jako ICQ nebo rapidshare. Dalším příkladem odhaleného incidentu je masivní používání služeb pro sdílení multimediálních dat (BitTorrent) a internetových úschoven ve firmě, jejímž největším bohatstvím je průběžně vytvářené duševní vlastnictví.

Deset let staré slabiny v počítačovém softwaru

Autorem kapitoly je Jiří Nápravník, Salamandr

Hledáte vysvětlení dlouhé doby skrytého působení viru Stuxnet, případně dalších virových infekcí? Přemítáte, jak se virus mohl dostat do relativně dobře zabezpečených počítačů uživatelů internetbankingu? Jedno z vysvětlení nabízí pohled na způsob nakládání se zdrojovými kódy počítačových programů ve spojení s mnoho let neopravenými chybami v operačních systémech a prohlížečích.

Slabiny, díry nebo zadní vrátka se v operačních systémech, prohlížečích a dalších programech objevují stále. Vedle jejich závažnosti je důležité i to, jak dlouho se nalezená slabina v systému nacházela a kdo ji mohl objevit dříve, než byla zveřejněna. Pokud se v operačním systému nebo v nadstavbové aplikaci objeví kritická slabina, která se vyskytuje pouze v poslední verzi konkrétního programu, je to nepříjemné, ale kdo z vás by dokázal takovou slabinu ve zdrojovém kódu najít, otestovat a následně vytvořit s využitím takové slabiny i škodlivý program? Kolik času byste potřebovali? 3 měsíce, 6 měsíců nebo celý rok? Musíte být rychlí, velmi rychlí, jinak se může stát, že dříve, než celý úkol dokončíte, může být konkrétní slabina odhalena někým jiným a

následně opravena. V případě slabin, které jsou v programu více než 3500 dnů mají ovšem počítačoví podvodníci mnohem více času na své aktivity.

Přístup ke zdrojovým kódům programů

S rychlostí, jakou může být slabina odhalena, úzce souvisí i přístupnost zdrojových kódů konkrétního operačního systému nebo aplikace. V případě veřejně přístupného zdrojového kódu jsou možnosti všech vyrovnané. Ke zdrojákům mají přístup všichni zájemci. Přesněji všichni, kteří se zapojí do vývojového týmu, což ale není překážkou. Všichni zájemci mají možnost zkoumat zdrojové kódy. Takže tuto možnost mají i ti, kdo hledají slabiny z důvodů vylepšení konkrétního programu a současně i ti, kdo by chtěli takovou slabinu zneužít.
Druhým přístupem je striktní utajování zdrojového kódu. V takovém případě jsou možnosti všech zájemců mimo firmu, která program vytvořila, opět vyrovnané. Pominu fakt, že počítačoví podvodníci mají vždy větší zájem hledat a následně zneužívat slabiny a zadní vrátka. To ale platí pro všechny

způsoby nakládání se zdrojovými kódy.
Velmi zvláštní situace existuje v případě, kdy ke zdrojovým kódům mají přístup pouze vybrané týmy. To znamená, že takové programátorské týmy mají přístup k jinak nepřístupným zdrojovým kódům. To je třeba případ společnost Microsoft a jejího Government Security Programu. Na základě příslušných dohod mají již minimálně od roku 2003 vybrané partnerské země a vysoké školy přístup k vybraným zdrojovým kódům Windows, MS Office, Internet Exploreru, atd. Mezi státy, které měly nebo mají přístup ke zdrojovým kódům, patří například Norsko, Austrálie, Velká Británie a také Ruská federace a Čína.

Rozdílný přístup ke zdrojovým kódům

V analýze slabin, kterou jsme zveřejnili počátkem ledna 2012, jsou jasně vidět dva přístupy ke zdrojovým kódům počítačových programů. Bohužel těmto dvěma přístupům přesně odpovídají i výsledky analýzy slabin.
V operačním systému Windows 7 bylo v průběhu let

2010 a 2011 zveřejněno a opraveno 176 slabin. Přičemž 137 slabin bylo společných s verzí Windows Vista a XP. Dalších 31 dokonce s Windows 2000. Stejná situace platí i v případě prohlížeče Microsoft Internet Explorer. V obou případech byly zveřejněné slabiny v programech více než deset let, více než 3600 dnů.

V prohlížečích Mozilla Firefox nebo Google Chrome jsou také slabiny – a dokonce jich tam je na první pohled více, než v programech společnosti Microsoft. Jenže doba existence jednotlivých slabin byla několik týdnů (Google Chrome) a v nejhorším případě u prohlížeče Firefox 8.0 se jednalo o 500 dnů.

Při tvorbě analýzy slabin zveřejněných v roce 2011 jsme zjistili „dlouhověkost“ slabin v operačním systému Windows a prohlížeči Microsoft Internet Explorer. Nerevidovaný zdrojový kód, který se používá v mnoha po sobě jdoucích verzích stejného programu (Windows 7, Vista, XP a 2000) ve spojení s tím, že k těmto zdrojovým kódům má přístup pouze vybraná skupina státních úředníků, případně studentů, je prostorem pro vytváření sofistikovaných škodlivých programů.

Specializované škodlivé programy mohou být vytvořeny a vyvíjet svoji činnost právě proto, že v programech jsou dlouhodobě neopravené slabiny a současně pouze vybraná skupina odborníků má možnost analyzovat zdrojové kódy a mohou v nich hledat nová zadní vrátka.

Existující rizika a možné cesty dál

Jedním z důvodů pro vytvoření naší analýzy slabin v operačních systémech a prohlížečích byla existence případů, kdy uživatelům někdo zneužil jejich elektronický podpis, vykradl účet přes internet banking a v neposlední radě i působení viru Stuxnet, který mimochodem zneužíval několik do té doby neznámých slabin v operačním systému Windows. Z výsledků analýzy je patrné, že slabiny zveřejněné v roce 2011, které se týkají Windows 7, se současně týkají i Windows Vista a XP. Běžný programátor nebo analytik nemá možnost prozkoumat zdrojové kódy Windows nebo Internet Exploreru a musí jako jakýkoliv jiný uživatel spoléhat na prohlášení tvůrce Windows a MSIE, že nový operační systém,

prohlížeč nebo další program jsou lepší a bezpečnější než předchozí verze.
Využívání počítačů nabývá stále více na významu a existují proto i významné tlaky na řešení bezpečnosti jednotlivých uživatelských počítačů, firemních sítí i počítačů, které řídí výrobní technologie. To vše se děje v prostředí, kdy autoři operačního systému používají bez revizí části nebo celé počítačové moduly více než deset let. Současně ovšem jinak chráněné zdrojové kódy dávají k dispozici zástupcům zemí, které jsou podezřelé z organizování počítačových útoků.
Za takových podmínek je řešení bezpečnosti v podmínkách internetbankingu a dalších obchodních aplikací složitý úkol. Možná je to náhoda, ale Ruská federace i Čína již před časem oznámily, že prosazují jako hlavní operační systém ve státní správě obou zemí vlastní distribuce Linuxu. Že by to byla pouze náhoda?
Analýzu slabin zveřejněných v roce 2011 si můžete stáhnout z tohoto článku na BusinessIT.cz.

čitelné.)

Průšvih za 34 milionů dolarů

Autorem kapitoly je Dr. Larry Ponemon, který se specializuje na problematiku ochrany dat a informační etiku. V roce 2002 založil Ponemon Institute, výzkumné centrum zaměřené na pokročilé metody ochrany dat a soukromí. Mezi jeho další aktivity patřila nebo patří spolupráce s významnými soukromými i veřejnými organizacemi na projektech spojených s hodnocením rizik a s ochranou dat. V listopadu 2011 zpracoval Dr. Larry Ponemon pro společnost Kingston Technology nezávislou studii „Stav bezpečnosti USB v Evropě“, která zkoumala úroveň USB bezpečnosti v deseti evropských státech.

Naši společnost si firemní zákazníci často zvou, když u nich dojde k nějakému průšvihu spojenému s krádeží nebo s únikem dat; případ, o kterém tady bude řeč, je ale opravdu unikátní. Tentokrát jde totiž

o průšvih ďábelských rozměrů - o krádež finančních dat obsahujících mimo jiné informace o pěti tisících velmi bohatých klientech; a škoda, která byla způsobena, dosáhla 34 milionů dolarů.
Ale nechci začínat od prostředka, a proto se teď raději vrátím k okamžiku, kdy se celý problém zrodil. A kdy ještě nikdo neměl tušení, jak velký vlastně bude. Ani jeho pachatel, ani další zaměstnanci firmy, jíž se dotkl. Mimochodem - dotčena byla společnost, která je opravdu velkým poskytovatelem finančních služeb. Působí po celém světě, zaměstnává více než 30 tisíc lidí a dále popisované trable se odehrály v její divizi zaměřené na správu investic.

Máte vyhazov

Celý příběh začal v okamžiku, kdy se jeden manažer z oddělení privátního bankovnictví dozvěděl, že se jeho oddělení zavírá - a že všechny investiční operace budou zajišťovány z jiné země formou outsourcingu. Muž se rozhodl, že to nenechá jen tak - a o několik dní později si zkopíroval jména, kontaktní údaje a další data nejbohatších klientů společnosti

na svůj USB disk. Mimochodem - tento seznam obsahoval záznamy řady skutečně důležitých lidí, politiky počínaje a nejrůznějšími celebritami - včetně známých sportovců - zdaleka nekonče.
Zaměstnanec, který se rozhodl ukrást data své firmy, měl za sebou více než 15 let práce v oboru a více než 5 let působil na své současné pozici. Vždy odváděl velmi dobrou práci a svými nadřízenými byl kladně hodnocen. Neexistoval ani malý náznak, že by mohl spáchat krádež tohoto druhu. I proto měl zřejmě velmi široká práva přístupu do některých kritických informačních systémů.

Klienti si stěžují a začíná vyšetřování

Krádež dat byla objevena asi 3 měsíce poté, co se odehrála. Jak se to stalo? Několik z oněch velmi bohatých zákazníků si stěžovalo, že je oslovila konkurenční firma. A ne ledajak: Vše podle nich nasvědčovalo tomu, že její makléři mají k dispozici důvěrné informace o jejich účtech, o posledních obchodech i o preferencích, které nikdo neměl znát. Tedy - nikdo kromě nich a firmy, která byla okradena

o data.
Firemní oddělení IT bezpečnosti zahájilo ve spolupráci s externími auditory pečlivé vyšetřování, při němž byl zjištěn download dat ze systémů. Ukázalo se rovněž, že jej provedl bývalý zaměstnanec, který nyní pracuje u té konkurenční firmy.
Škoda, kterou způsobil, zahrnovala poškození dobrého jména firmy, náklady na obhájce, náklady na konzultace a také ztráty způsobené odchodem klientů. Nebylo jich málo: Mimo jiné odešlo přibližně osm procent velmi významných firemních zákazníků. Celková škoda tak byla odhadnuta na 34 milionů amerických dolarů.

Je třeba přijmout opatření

A právě v době, kdy se problém provalil a firma začala zvažovat, jak napříště podobným událostem zabránit, jsme vstoupili na scénu my. Prostudovali jsme všechny dostupné informace ohledně práce firmy s daty i o celém incidentu. Podle našeho názoru mu bylo možné zabránit a v tomto smyslu

jsme informovali i klienta.
V důsledku celé události pak byla přijata řada zásadních opatření. Ředitel firmy ve spolupráci s jejím představenstvem iniciovali vznik nových pravidel ochrany dat a vytvoření oddělení zodpovědného za jejich ochranu. Vznikla pozice šéfa ochrany dat na mezinárodní úrovni. Firma nyní provádí intenzivní audity monitoringu a shody s pravidly. Byly rovněž nasazeny systémy SIEM (Security IntElligence systeMs), které pomáhají v reálném čase identifikovat podezřelé transakce, a to především u privilegovaných uživatelů.
Jakkoli jsem v úvodu zmínil, že šlo o unikátní případ, nelze tvrdit, že se podobné problémy vyskytují zřídka. I když v nich ale třeba nejde o tak bohaté klienty a celebrity, případně škoda nedosahuje takových rozměrů, pro firmy jsou vážné. Smutné je, že bezpečnostní opatření jsou mnohdy zaváděna nikoli preventivně, ale až dodatečně.

Bezpečný veřejný cloud

Tato kapitola je partnerským příspěvkem. Jejím autorem je David Matějů, RSA Presales Engineer, RSA, The Security Division of EMC, www.rsa.com

Důležitou a nedílnou součástí přechodu k veřejnému cloudu je přesun jeho zabezpečení mimo kontrolu podniku směrem k poskytovateli daného cloudu, což vede k potřebám změn v pojetí informační bezpečnosti. Jedná se o sdílení řízení bezpečnosti, které je naprosto nezbytné pro další rozvoj důvěryhodných vztahů mezi odběrateli a poskytovateli cloudových služeb. Těmi nejdůležitějšími procesy jsou z pohledu bezpečnosti zejména řízení přístupu, ochrana dat a shoda s předpisy a zákony, tzv. compliance.

Identity

Správa identit, autentizační služby a federovaná identita hrají v bezpečnosti cloudu klíčovou roli. Ochrana identit zajišťuje integritu a důvěrnost dat i aplikací a zpřístupňuje je autorizovaným uživatelům. Podpora výše zmíněných funkcí je nedílnou součástí všech typů cloudu včetně toho veřejného.

Z pohledu řízení přístupu do cloudu je třeba se soutředit zejména na silnou autentizaci. Pokud má veřejný cloud sloužit k provozu podnikových aplikací, je bezpodmínečně nutné využít silnější autentizaci uživatelů, než je již dávno překonané uživatelské jméno a statické heslo. Standardem v této oblasti je použití ověřených technologií pro silnou autentizaci (multifaktorová autentizace na bázi jednorázového hesla), federovanou (delegovanou) identitu pro důvěryhodné sdílení identit mezi různými subjekty, a „risk-based“ autentizaci založenou na chování uživatele, kontextu a mnoha dalších faktorech. Vhodnou kombinací a vrstvením těchto autentizačních metod lze zajistit jak dodržení bezpečnostních SLA, tak jednoduchost použití pro všechny typy uživatelů.

Informace

V tradičním datovém centru je bezpečnost řešena nejen IT prostředky, ale současně fyzickým zabezpečením přístupu k hardwarové infrastruktuře. Tato bariéra ale s příchodem veřejného cloudu mizí.

Místo stavění bariér je třeba se soustředit na řízení bezpečnosti konkrétních informací. Data putující po cloudu i mimo něj tak mají vlastní zabezpečení, které je po celou dobu chrání. K dosažení této „information-centric“ bezpečnosti je třeba vyřešit několik oblastí:

• Oddělení dat: Ve veřejných cloudech, kde se zpracovávají data mnoha nájemců, musí být data izolována. Virtualizace, šifrování a granulární řízení přístupu významně pomohou v izolaci dat mezi nájemci, jednotlivými skupinami či uživateli.

• Granulární bezpečnost dat: Se zvyšující se citlivostí informací a jejich počtem se musí prohloubit i klasifikace dat a důslednost ve vynucování jejich výhradně oprávněného použití. Ve veřejném cloudu je bezpečnost dat tak kritická, že její granularitu musíme řešit už na úrovni souboru, tabulky či sloupce v databázi. S tím také přichází inspekce dat (sledování obsahu), jejich tokenizace či šifrování a bezpečná správa šifrovacích klíčů po celý jejich životní cyklus.

• Klasifikace dat: Nalézt v cloudu ideální poměr mezi uživatelským komfortem a požadavky na jeho zabezpečení není jednoduché. Důležitými kroky k

nalezení toho správného poměru je klasifikace dat a fungující procesy pro jejich vyhledávání, monitoring toku a použití. V této oblasti významně pomáhají systémy pro vyhledávání a ochranu citlivých dat, tzv. „data loss prevetion“ (DLP).
• Monitoring a audit: Prostředí všech systémů, ve kterých se pracuje s citlivými informacemi, musí být z pohledu bezpečnosti kompletně monitorováno a pravidelně auditováno. Ideálním řešením této oblasti je systém pro sběr a analýzu logů z klíčových systémů (tzv. SIEM) s reportingem do podnikového GRC (governance, risk, compliance) řešení pro řízení podnikových procesů a rizik.

Infrastruktura

Celá infrastruktura cloudu musí být už v jádru bezpečná, nezávisle na tom, zda stavíte privátní či veřejný cloud. To vyžaduje:
• Komplexní bezpečnost: Cloud musí již být navžen jako bezpečný, postaven z bezpečných komponent, implementován dle odpovídajících bezpečnostních „know-how“, bezpečně komunikující s okolím, a

podporujícím potřebná bezpečnostní SLA.
• Bezpečnou integraci: Tam, kde dochází ke komunikaci mezi jednotlivými částmi cloudu, je třeba vynucovat dodržování bezpečnostních politik pro sdílení dat, aby byla zajištěna jejich integrita a důvěrnost.
Všechny výše uvedené oblasti jsou důležité nejen pro pro privátní a veřejný cloud, ale také pro služby IAAS (infrastructure as a service), PAAS (platform as a service) a SAAS (software as a service). Dobrou zprávou je, že všechna popsaná řešení jsou již dnes k dispozici a další se samozřejmě vyvíjejí a testují, aby mohla splnit stále náročnější požadavky trhu.

Původní české řešení pro dohled a správu datové sítě

Tato kapitola je partnerským příspěvkem.
Produkty a služby společnosti AdvaICT jsou určeny ke zjednodušení a zrychlení správy IT infrastruktury. Původní české řešení FlowMon ADS kombinuje

hlavní funkce pro sledování výkonu (Network Performance Monitoring), zvýšení bezpečnosti (Network Security) a dohledu uživatelů (User and Application Control). Profesionální služba analýzy provozu datové sítě Network Traffic Audit je určena pro nezávislou kontrolu stavu bezpečnosti datové sítě a její provozní kontrolu. Výstupem služby je přehledná zpráva shrnující zjištěné nedostatky spolu s návrhem opatření na jejich odstranění.

Jihomoravské inovační centrum

Jihomoravské inovační centrum opakovaně řešilo problémy s umísťování veřejné IP adresy společnosti na blacklisty, které mělo za následek nemožnost odesílat a přijímat emaily v rámci celé sítě JICu v řádu několika hodin. Každé umístění na blacklist navíc vyžadovalo složité odstraňování IP adresy z blacklistu. V říjnu 2011 proběhl audit provozu datové sítě s cílem tento problém analyzovat a vyřešit.
V rámci auditu byla identifikována stanice patřící jedné z inkubovaných firem, která byla infikovaná malwarem způsobujícím umísťování veřejné IP

adresy JICu na blacklisty. Problém se podařilo vyřešit odpojením infikovaného počítače ze sítě. Uživatel počítače dlouhodobě neprováděl pravidelný antivirový test počítače a o přítomnosti malwaru na svém stroji neměl tušení.

V rámci auditu provozu v síti JIC byla dále provedena standardní analýza provozu v síti a chování jednotlivých zařízení v síti, na základě které byla doporučena následující opatření:

• Prozkoumat podezřelé anomálie poštovního provozu v segmentu inkubovaných firem
• Opravit odhalené drobné konfigurační problémy v síti
• Doplnit reverzní DNS záznamy k místním IP adresám pro zpřehlednění sítě

Vypracovaná auditní zpráva zároveň poskytla zákazníkovi potřebný vhled do dění v síti, především o využívání sítě inkubovanými firmami. Dále zákazník získal podklady pro systematický rozvoj sítě a její efektivní správu. Výsledky auditu hodnotí manažer ICT společnosti, Ing. Jiří Vala:

"Umísťování na blacklisty pro nás znamenalo značné komplikace jak z pohledu zaměstnanců, tak z pohledu partnerů a zákazníků naší společnosti.

Řešením problému jsme trávili řádově desítky hodin, ale příčinu problému se nepodařilo odhalit. Nezbylo nám než při každém incidentu pracně odstraňovat naši IP adresu z blacklistů. Pomocí služby auditu sítě jsme problém vyřešili ještě v den nasazení řešení FlowMon ADS do naší sítě. Na základě této zkušenosti jsme se rozhodli pořídit řešení FlowMon ADS pro trvalý monitoring naší sítě, abychom podobným problémům v budoucnu dokázali efektivně předejít.“
Jihomoravské inovační centrum dnes již patří ke stálým uživatelům řešení FlowMon ADS nasazeném v prosinci 2011 pro trvalý dohled datové sítě.

AGROFERT HOLDING, a.s.

AGROFERT Holding, a. s., sdružuje více než 230 subjektů ze sektoru chemie, zemědělství, potravinářství a pozemní techniky s vlastním kapitálem převyšujícím 34 mld. Kč. Jedná se o největšího privátního zaměstnavatele v České republice. Jednotlivé společnosti provozují vlastní IT infrastrukturu připojenou prostřednictvím MPLS sítě

do datového centra, které poskytuje výpočetní výkon zejména pro informační systémy a podpůrné aplikace na platformě operačních systémů Microsoft včetně webových portálů.
Požadavky zákazníka:
• Sledovat zatížení a propustnost sítě datového centra
• Monitorovat míru a způsob využívání připojení k síti internet
• Měřit využívání jednotlivých služeb
• Účinně kontrolovat dodržování bezpečnostních směrnic a předpisů
• Dokladovat skutečnou kvalitu služeb, zpoždění sítě a služeb
• Eliminovat nežádoucích aplikace, sdílení obsahu
• Detekovat potenciálně nežádoucí chování
• Průběžně optimalizovat konfiguraci sítě a síťových zařízení

Nasazení řešení FlowMon ADS

Předmětem monitoringu jsou provozní a bezpečnostní parametry datového centra a komunikace všech podniků do internetu. Zejména

jde o rozsah využívání jednotlivých služeb a výkonnostní parametry z hlediska propustnosti datové sítě. Dvojice sond FlowMon Probe 1000 monitoruje veškerý provoz datového centra a přípojky k síti internet. Data jsou zasílána na FlowMon Collector s kapacitou 2 TB. Veškerý provoz vyhodnocuje FlowMon ADS s cílem automaticky rozpoznat potenciální provozní a bezpečnostní problémy. FlowMon Reporter a HTTP Logger sestavuje přehledy o míře a způsobu využívání služeb datového centra a sítě internet jednotlivými podniky.

Hodnocení zákazníka

Ing. Martin Poláček, ICT ředitel, AGROFERT HOLDING, a.s., hodnotí řešení FlowMon ADS nasazené v prostředí datové sítě společnosti po půlroční zkušenosti:
"Řešení FlowMon ADS jsme nasadili s cílem zvýšit bezpečnost a kontrolu nad naší infrastrukturou. Díky monitorování provozu datové sítě máme pod dohledem vytížení a způsob využití našeho datového centra a připojených společností k síti internet. V

případě problémů jsme schopni efektivně diagnostikovat jejich příčinu. Navíc FlowMon ADS permanentně vyhodnocuje veškerý provoz a upozorňuje nás na potenciální bezpečnostní incidenty."
Mezi další vybrané uživatele řešení FlowMon ADS v České a Slovenské republice patří Veletrhy Brno, Masarykova univerzita, Pražské vodárny a kanalizace, Konica Minolta, AT Computers, Generální ředitelství hasičského záchranného sboru ČR nebo dm drogerie markt.
Více informací získáte na AdvaICT.cz.

Nadace Naše dítě: Ochraňte sebe i své okolí!

Tato kapitola je partnerským příspěvkem.
Nadace Naše dítě pomáhá dětem z problémových rodin, z kojeneckých, diagnostickýcha výchovných ústavů, zneužívaným, týraným i handicapovaným dětem již od roku 1993. Zakladatelkou Nadace je

Ing. Zuzana Baudyšová. V následujícím příspěvku vám nabídneme pohled na to, jak tato nadace nyní chrání svá citlivá data.

Důvěra, bezpečnost a ochrana spolu souvisí

„Chceme se plně věnovat ochraně dětí a jejich zájmů, a proto nám zajišťují správu ICT odborníci z externí firmy," začíná své vyprávění Michaela Maxová, manažerka fundraisingu Nadace Naše dítě. „Děti, rodiče, jejich sousedi, známí i lidé anonymně se nám svěřují v oblasti vztahů nebo se nás na tuto oblast ptají především prostřednictvím telefonních linek či emailů. Vážíme si důvěry našich klientů a partnerů. Uvědomujeme si důležitost dat, které využíváme, a proto se potřebujeme komplexně chránit."
Změnit způsob ochrany svých dat se Nadace rozhodla na základě doporučení a referencí nového dodavatele IT, společnosti UNITEC CS a.s. Svého kroku Nadace nelituje. Ba, naopak! Hlavními kritérii pro nové řešení bylo sjednocení operačních systémů pro firewall, zajištění vyšší ochrany, možnost

konfigurace přes grafické rozhraní, spolehlivost, intuitivní ovládání a dobré reference. Kerio Control splňuje všechny požadavky, a proto jím bylo nahrazeno původní řešení nakonfigurované na operačním systému Linux.
Kerio Control je efektivním nástrojem pro zabezpečení sítě a sledování komunikace při minimálním zatížení operačního systému. Jeho konfigurace zabere jen několik minut. Vestavěný průvodce komunikačními pravidly umožňuje prostřednictvím jediné přehledné tabulky snadné nastavení paketového filtru, NAT, mapování portů a kontroly. Sebemenší porušení bezpečnostních pravidel je pak zapsáno v záznamu Security.

Bezpečí komunikace

„Nejužitečnějšími vlastnostmi firewallu od Keria jsou dokonalá antivirová kontrola, monitorování internetové aktivity, filtrování HTTP a možnost omezení šířky pásma," popisuje své několikaleté zkušenosti s Kerio Control IT specialista společnosti UNITEC CS a.s.

Kerio Control nabízí několik způsobů antivirové ochrany. Lze použít vestavěný antivirový modul Sophos, některý z podporovaných externích antivirů nebo obě možnosti ochrany zkombinovat.
V Nadaci Naše dítě využívá Kerio Control s integrovaným antivirem Sophos osm uživatelů. Hlavní výhodou integrované verze antiviru je správa antivirového programu přímo z administrační konzole, a následná úspora času i peněz.
Samostatné sdružení Linka bezpečí a mládeže také využívá Kerio Control, avšak s podporou antivirového systému Avast! for Kerio. Bezpečná komunikace je zajištěna v Kerio Control kontrolou veškeré příchozí i odchozí pošty včetně příloh a přezkoumáváním obsahu webové komunikace včetně HTML stránek a všech souborů stahovaných přes HTTP nebo FTP.
Internetovou aktivitu, tedy informace o navštívených webových stránkách a čase na nich strávených, zadaných dotazech v internetových vyhledávačích, použitých protokolech, přenosech velkých souborů apod., lze díky rozhraní Kerio StaR snadno sledovat. Informace jsou prezentovány velmi přehledně prostřednictvím barevných grafů a report lze zobrazit

i vytisknout za každého uživatele ve zvoleném časovém období.

„Naše zkušenost s Kerio Control je výborná. Pro zabezpečení sítě a komunikace ho doporučujeme všem," shodují se závěrem oba zástupci Nadace Naše dítě.

Kerio Control – přehled základních funkcí:

- Unifikované zabezpečení
- Detekce a prevence útoků (IDS/IPS)
- Antivirová kontrola
- Řízení přístupu uživatelů
- Filtrování obsahu – Kerio Web Filter
- Statistiky a reporty
- Kvalita služeb (QoS)
- VPN server
- K dispozici jako software, hardware či Virtual Appliance
- Jednoduchá správa
- Dvojitá antivirová kontrola
- StaR – Statistiky a Reporty
- Integrovaný antivirus Sophos

Více informací najdete na www.kerio.cz.