BusinessIT.cz
ebook

Moderní správa IT ve firmě

redakce BusinessIT

Moderní správa IT ve firmě. Edice BusinessIT ebooks 2011.

Moderní správa IT ve firmě

BusinessIT.cz

Edice: BusinessIT ebooks
Autoři: Redakce BusinessIT.cz

Vydáno v roce 2011 v Bispiral, s.r.o.

web: www.BusinessIT.cz

Tentokrát jsme pro naši elektronickou knihu zvolili poněkud jinou strukturu než obvykle; vzhledem k faktu, že je správa IT tématem, u kterého nedává příliš velký smysl vysvětlovat její základní principy (IT manažeři je znají a vedení firem zpravidla nemá důvod do jejich tajů dopodrobna pronikat, protože pro něj jsou důležité výsledky), rozhodli jsme se začít jinak – pohledem na strategické řízení IT. Jde tedy

opět o text vhodný i pro manažery mimo IT – věnuje se totiž pohledu na správu IT z nadhledu – zabývá se potenciálem informačních technologií a tipy pro plánování na delší časové období.
V dalších částech se pak již tradičně vydáváme k praktickým záležitostem, kterými jsou tentokrát nasazení IPv6 a nejzajímavější open-source nástroje pro správu IT. Současně přidáváme i kapitoly zaměřené na správu mobilních zařízení a na možnosti nasazení cloudu, které jsme publikovali již v našich e-knihách Mobilní zařízení pro lepší byznys a Cloud Computing od B do Y, ale které nepochybně patří i sem. Věříme, že to přivítají především ti z vás, kteří zmíněné knihy zatím nečetli.

Redakce BusinessIT.cz

IT oddělení v roli makléřů, aneb Strategické řízení IT

Analytici společnosti Gartner v říjnu roku 2011 na svém sympoziu ITxpo mimo jiné upozornili, že je nyní – více než kdykoli dříve – nutno začít přetvářet roli informačních technologií ve firmách. Běžný způsob modernizace IT podle nich již nestačí, protože v současném byznysu se lze se zákazníky setkat naprosto všude – a tomu se firmy – v úzké kooperaci s IT – musejí přizpůsobit. Možná, že to zní jako příliš vznešené myšlenky, ale rozhodně vybízejí k jednomu důležitému kroku – totiž k zamyšlení se nad způsobem řízením IT ve firmách z většího nadhledu, než bývá obvyklé.

Část IT oddělení se podle analytiků v budoucnu posune do role takzvaných makléřů cloudu, kteří služby nakoupené na běžném trhu přizpůsobují potřebám svých firem. Šéfové informatiky – budou-li chtít uspět – se budou muset naučit riskovat – a doporučovat inovativní řešení. A všechna IT oddělení budou muset poskytovat co nejjednodušší služby tak, aby je klienti mohli snadno využívat prostřednictvím

jakéhokoli koncového zařízení.

Nový pohled na budoucí byznys

“Postmoderní byznys kompletně mění status quo a nutně musí řešit dramaticky nový vztah se zákazníky, dodavateli i partnery,“ vysvětluje Daryl Plummer, viceprezident společnosti Gartner. Váš byznys v současném postmoderním světě není omezen žádnými zdmi; musí být všude a musí se měnit tak, jak se mění zákazníci. „V postmoderním byznysu zapomenete na pojmy, jako je business architecture, a chopíte se nových pojmů, jako je spokojenost zákazníka nebo zapojení zákazníka do byznysu. V postmoderním byznysu se zákazník a požadavky na vás budou měnit rychleji než nějaké vaše architektury.“

IT lídři musejí podle Gartneru uspokojit zákazníky, kteří jsou nyní daleko informovanější o jejich produktech – a to v situaci, kdy se trhy mění rychleji, než kdykoli dříve. Zákazníci chtějí vědět, že se firmy zajímají o jejich starosti, a tak šéfové informatiky musejí zachytit aktivitu zákazníků – byť se projevuje jen v krátkém časovém úseku - a reagovat na ni. Ano – je to role CIO, protože právě on má (nebo by

měl mít) nejlepší přehled o možnostech IT – a protože právě prostřednictvím IT dnes zákazníci s firmou velmi často komunikují.
„Ve světě, kde průměrná firma vydrží jen deset let, může každý bod navíc ve spokojenosti zákazníka přidat vašemu byznysu jeden rok života," říká Plummer. „Postmoderní byznys nevynakládá všechny peníze na zajištění loajality zákazníků, ale investují do loajality firmy vůči zákazníkům."

Trendy, které musí sledovat IT

Rychlost změn nutí dnešní firmy – a jejich IT oddělení – sledovat aktuální trendy a využívat možnosti, které nabízejí. Jedním z nich je pochopitelně cloud computing a jednou z mnoha otázek s ním spojených je budoucí role IT oddělení ve firmě.
Podle Plummera se IT oddělení mohou nově stát jakýmisi makléři, kteří nakoupí cloudové služby od velkých poskytovatelů a zajistí jejich propojení a úpravy podle potřeb firmy, pro kterou pracují. Výhodou bude skutečnost, že poskytovatelem základní cloudové služby je firma, která se na danou oblast specializuje a poskytuje ji ve velkých objemech; ale klient – lidé z byznysu ve firmě – bude

mít k dispozici řešení šité na míru podle vlastních potřeb. Plummer odhaduje, že do role „cloud brokerů“ se postupně dostane až 30 % IT organizací. Dalším zásadním trendem je snaha o jednoduchost, která se podle Plummera odráží i v nástupu využívání mobilních zařízení. “V roce 2015 počet projektů na vývoj mobilních aplikací pro chytré telefony a tablety přečíslí PC projekty v poměru 4:1. PC už nadále není králem,“ upozorňuje Hung LeHong, viceprezident Gartneru pro výzkum trhu. „IT oddělení musejí být součástí tohoto vývoje. Věci musejí být tak jednoduché, aby lidé mohli dělat, cokoli potřebují, na jakémkoli přístroji,“ říká LeHong.

Je třeba být inovativní

„Většina IT organizací věnuje 70 % a více svého času, peněz a úsilí na zajištění spolehlivosti svých systémů, na prosté udržení věcí v chodu,“ poznamenává Tina Nunnová, analytička a viceprezidentka Gartneru. To se podle ní musí konečně změnit. IT oddělení se budou muset přizpůsobit požadavkům byznysu na zajištění nové funkčnosti, která zcela novými způsoby podpoří podnikání firmy. „Je skvělé, že je řada IT oddělení

považována za dobrého poskytovatele služeb, ale jejich budoucí role by měla být podstatně aktivnější," upozorňuje Nunnová. Správné IT oddělení by podle ní mělo radit vedení firmy, jak využít potenciál nových technologií.

Skuteční IT lídři budou muset podle analytiků Gartneru vsadit při řízení IT nejen na perfekcionismus, ale také na kalkulované riziko. „Pokud nikdy neriskujete, znamená to, že jste předpověditelní a stáváte se snadným terčem pro konkurenci," upozorňuje Nunnová. „Odvažte se jít do kalkulovaného rizika a překvapte jak lidi kolem sebe, tak konkurenci."

5 tipů pro moderní CIO

Nastavte si priority tak, aby odpovídaly prioritám vedení firmy.

Zajistěte soulad mezi vašimi prioritami a financemi určenými pro jednotlivé projekty.

Nepodporujte projekty a aplikace, které se nepodílejí na příjmech firmy.

Omezte přerostlé projekty zaměřené na update podnikových aplikací nebo technické infrastruktury.

Doporučujte vedení kroky, díky kterým IT přímo přispěje k lepším výsledkům firmy.

Kdy a jak přejít z IPv4 na IPv6

V roce 2015 bude využívat IPv6 méně než třetina nových uživatelů internetu (přesně to má být 28 %; a 17 % stávajících uživatelů; tvrdí to loňská předpověď společnosti Gartner). To jsou zjevně nižší čísla, než by leckdo po posledních zprávách ze světa IPv4 očekával. Životnost staršího protokolu je ale stále prodlužována, a to navzdory některým nevýhodám, které to s sebou přináší.

Aktuální průzkum GNKS Consult mezi 1600 organizacemi poskytujícími internetovou infrastrukturu ve 135 zemí světa ukázal, že 70 % z nich plánuje nasadit IPv6 v roce 2012 (a jen 7 % z nich s tím začne až později). Z těch, kteří s nasazením IPv6 infrastruktury již začali, přes 80 % využívá takzvaného konceptu dual stack, tedy provozování IPv4 i IPv6 na stejném hardwaru. Americký NetworkWorld se zase letos v létě mimo jiné ptal zástupců amerických firem, kdy hodlají nabídnout své webové stránky i přes IPv6. 72 % dotazovaných tak hodlá učinit do dvou let, 53 % nejpozději do roka. Jak tedy přistoupit k přechodu z

IPv4 na IPv6?

IPv4 vs. IPv6

IP (Internet Protocol) je základním protokolem používaným pro přenos dat prostřednictvím internetu. Jeho původní verze, IPv4, je postupně nahrazována verzí novější, IPv6. Adresní prostor IPv4 byl na globální úrovni vyčerpán v únoru 2011, adresy přidělené regionálním správcům budou zřejmě vyčerpány nejpozději v roce 2012.

Adresy IPv4 mají délku 32 bitů, takže jsou schopny rozlišit přes čtyři milardy adres; to – i vzhledem k nehospodárnému využití – ovšem nestačí aktuálním potřebám. IPv6 disponuje 128bitovými adresami a má tedy prostor pro 3,4 x 1038 adres. Při změně z IPv4 na IPv6 se mění formát datagramů, většina ostatních protokolů se nijak měnit nemusí (pokud ovšem nepracují s adresami síťové vrstvy).

Kromě výrazně většího adresního prostoru přináší IPv6 i řadu dalších vlastností, mimo jiné podporu větších paketů, nativní podporu multicastu nebo IPsec, či automatickou konfiguraci hosta ve směrované IPv6 síti. Na rozdíl od IPv4 neobsahuje již IPv6 kontrolní součet hlavičky, což by mělo urychlit

směrování.

Potíže soužití IPv4 a IPv6

Než vůbec – někdy v budoucnu – dojde ke kompletnímu nahrazení IPv4 novějším IPv6, musejí spolu oba protokoly v síti nějakým způsobem koexistovat. Noví klienti i servery jsou dnes již zpravidla schopni komunikovat prostřednictvím obou protokolů, pokud je však třeba přenášet IPv6 pakety po infrastruktuře podporující pouze IPv4, je třeba to řešit zapouzdřením IPv6 paketů do IPv4, kdy pak IPv4 funguje jako linková vrstva pro IPv6 (u čísla protokolu je pak v IPv4 uvedeno 41).

Problém s nedostatkem adres IPv4 je již déle řešen překladem adres. Vzhledem k omezenému počtu využitelných portů (65536) a obvyklému počtu session na jednoho uživatele (podle statistik NTT – Nippon Telephone and Telegraph – jich uživatelé běžně potřebují několik stovek současně) zde však existuje poměrně výrazné omezení, obzvláště u větších sítí. Nicméně při využívání IPv4 k privátní komunikaci v rámci firmy není na první pohled třeba s přechodem na IPv6 nijak spěchat.

Kdy a jak přecházet na IPv6

Rychlý přechod na IPv6 je ovšem nutný v některých speciálních případech. Třeba u poskytovatelů vybavení a služeb, pokud to vyžadují jejich významní klienti. Například federální úřady USA mají za cíl podporovat IPv6 ve všech svých veřejně poskytovaných internetových službách do konce září 2012, australské úřady pak do konce téhož roku. A třeba Indie počítá již s březnem 2012.

Dalším případem, kdy je třeba zajistit rychlou podporu IPv6, jsou aplikace, které s IPv4 nefungují. Jde především o služby, které vyžadují přímou adresaci velkého množství zařízení.

Společnost Infoblox pak varuje i před poskytováním webového obsahu na IPv4 klientům s IPv6 prostřednictvím překladu adres z IPv4 na IPv6. Z hlediska funkčnosti tam sice není žádný problém, poskytovatel ale podle ní přijde o některé klíčové informace o svých klientech, které se extrahují z logů webového serveru, které vyžadují nativní podporu IPv6.

Zástupci společnosti Cisco pak v souvislosti s přechodem na IPv6 upozorňují, že se někdy setkávají s mýtem, že je třeba v organizaci přejít na IPv6

naráz. Opak je podle nich pravdou. Pokud se rozhodnete přejít z IPv4 na IPv6, je vhodnější rozdělit celý proces do několika fází. Nejprve je vhodné zajistit přechod u systémů, které poskytují služby směrem do internetu. Následovat by měla interní síťová infrastruktura, intranet a přístup k internetu. Jako poslední pak zůstává zajištění plné podpory IPv6 na straně koncových stanic.
Cisco rovněž doporučuje zabývat se nejen nutnými kroky pro přechod stávajících služeb, ale také prozkoumat všechny nové příležitosti, které nový protokol firmě nabídne. A to z hlediska fungování síťové infrastruktury, ale také z hlediska možných nových služeb.

Možné zádrhele přechodu na IPv6

Proces přechodu na IPv6 v sobě skrývá řadu rizik, která je dobré znát. Již zmínění zástupci Infobloxu dávají v tomto ohledu několik doporučení. Jako první krok přitom doporučují ověření, jak v síti přidělujete a sledujete IP adresy. Rozhodně je podle nich třeba to dělat prostřednictvím automatizovaných nástrojů a nevyužívat náhradních manuálních řešení, která snad

mohla stačit pro IPv4.
Je rovněž třeba zkontrolovat architekturu DNS a její podporu IPv6. Pokud jsou adresy přidělovány prostřednictvím DHCP, musí samozřejmě i DHCP server podporovat IPv6 a být zajištěna vzájemná kompatibilita obou systémů. Zástupci Cisca v této souvislosti upozorňují, že třeba DHCP server Windows 2003 není schopen poskytovat IPv6 adresy.
S nástupem IPv6 musejí dopředu počítat pravidla pro údržbu a zabezpečení síťové infrastruktury. Problémem může být třeba řada starších firewallů, které IPv6 nepodporují. Je třeba rovněž ověřit, že budou fungovat i služby třetích stran. Příkladem mohou být třeba antispamové databáze, které nyní fungují na principu blokace adres IPv4. Společnost Microsoft s ohledem na bezpečnost doporučuje využívání autentizace prostřednictvím IEEE 802.1X pro všechny počítače připojující se do sítě přes IPv6. Teprve po úspěšné autentizaci pak mohou využít protokolů NDP nebo DHCPv6 k získání IPv6 adresy a komunikovat tak v síti.
Zástupci společnosti Cisco připomínají rovněž nutnost zajistit příslušná školení všem

zaměstnancům, jejichž práce se přechod z IPv4 na IPv6 dotkne. Ve větších firmách to mohou být desítky zaměstnanců – od bezpečnostního architekta sítě po osobu zodpovědnou za IP kamery stážící objekt organizace.

K dalším nezbytným krokům patří kompletní inventura aktuální síťové infrastruktury, aby se ověřilo, že všechny její prvky podporují přechod na IPv6. Infoblox zde upozorňuje, že třeba pobočková ústředna Asterisk je kompatibilní s IPv6 teprve od podzimu loňského roku. A nejde o jediný případ opozdilce.

Rovněž je třeba ověřit, že všechny nástroje pro monitoring a správu sítě jsou updatovány tak, aby podporovaly novou technologii. Speciálním případem jsou nejrůznější databáze, jejichž tabulky nemusejí vždy pojmout delší adresy IPv6.

A dopředu je třeba počítat také s možnými výkonnostními problémy, protože zdaleka ne všechna síťová zařízení, která protokol IPv6 podporují, jsou pro něj také optimalizována. Jelikož optimalizaci je třeba zpravidla realizovat na hardwarové úrovni, bude třeba provést výměnu těch zařízení, která nepostačí výkonnostním nárokům.

Nejlepší open-source nástroje pro správu IT

Stojíte-li právě před otázkou, jaké nástroje použít ke správě sítě i další IT infrastruktury ve své organizaci, a přitom vám omezený rozpočet nedovoluje se pořádně rozmáchnout, zkuste některé z open-source nástrojů. Některé jsou zcela zdarma, u dalších si za vybrané vychytávky připlatíte; i tak ale budete mít šanci získat za své peníze velmi slušnou protihodnotu. A co je nejdůležitější – pokud zatím vhodný nástroj nemáte, díky těmto produktům si nejspíš poměrně rychle a snadno výrazně usnadníte život. Dost ale úvodních řečí, pojďme se podívat na jednotlivé nástroje.

Nagios Open Source pro monitoring IT

Nagios Open Source je bezplatné řešení pro monitoring IT infrastruktury v jakékoli organizaci. K dispozici jsou nástroje pro sledování aplikací, služeb, operačních systémů, síťových protokolů, zvolených systémových metrik a síťového hardwaru. V případě definovaných událostí jsou odesílána varování (e-

mailem nebo přes SMS, s možností eskalace), případně podniknuty potřebné kroky k nápravě (například automatický restart aplikace nebo serveru).
Celý balík Nagios Open Source se skládá z několika různých skupin projektů, které zajišťují jeho funkčnost. Konkrétně jde o Nagios Core, základní monitorovací engine a webové rozhraní, Nagios Plugins, sloužící k monitorování jednotlivých aplikací nebo služeb, Nagios Frontends, nabízející pokročilejší rozhraní, a Nagios Addons, což jsou různá další rozšíření. Nagios je k dispozici pro běžné serverové operační systémy (ve formě obrazů pro virtuální stroje, na nichž je spuštěn CentOS 6.x).
Zvolit lze i balík Nagios XI, což je komplexní monitorovací řešení postavené na výše zmíněných komponentách. Jeho použití je zdarma pouze pro menší IT prostředí (do sedmi hostitelských počítačů), pro vyšší počet monitorovaných zařízení je licence placená.

Netdisco pro správu sítě

Kořeny projektu Netdisco sahají do roku 2003 a jeho autoři se již od začátku zaměřili na správce sítí

velkých firem a univerzit. Data ze sítě jsou sbírána prostřednictvím SNMP a uživateli předkládána prostřednictvím webového rozhraní. K typickým způsobům využití podle autorů patří lokalizace počítače v síti a určení portu přepínače, ke kterému je připojen, inventarizace síťového hardwaru (výrobce, model, firmware, operační systém apod.), zobrazení topologie sítě nebo statistiky využití síťových portů přepínačů.

Autoři projektu uvádějí, že nejlépe jsou jejich produktem podporována zařízení společností Cisco a HP, do jisté míry jsou však samozřejmě podporována všechna zařízení komunikující prostřednictvím SNMP. Netdisco je vyvíjeno na FreeBSD, podle dostupné dokumentace by ale mělo běžet na jakémkoli systému, na kterém lze spustit Postgres, Perl, Apache, a Net-SNMP. Netdisco je šířeno zdarma s volitelnou registrací.

Just For Fun NMS není jen pro zábavu

Just For Fun Network Management System, nebo zkráceně JFFNMS, je dalším bezplatným nástrojem pro monitorování síťové infrastruktury. Je kompletně napsán v PHP5 a podle autora by měl být

provozovatelný na jakémkoli operačním systému, který PHP verze 5 podporuje. JFFNMS nabízí webové uživatelské rozhraní a podporuje množství protokolů potřebných pro sběr informací ze sítě (kompletní seznam najdete na stránkách projektu). JFFNMS je aktuálně ve verzi 0.9.1 (čímž se nenechte zmást, rozhodně nejde o nějaký syrový systém) a je k dispozici pod licencí GNU GPL.

I Velká sestra ohlídá vaše systémy

Projekt Big Sister byl původně zaměřen čistě na monitorování sítě, postupem času se však rozrostl o prvky zajišťující správu a monitoring dalších IT systémů. Aktuálně pod hlavičkou Big Sister najdete Big Sister Network Monitor, produkt pro monitorování sítě zajišťující zobrazení aktuálního stavu, ukládání informací o událostech v síti a varování v případě předdefinovaných rizikových stavů, Big Sister Web Application Framework, zajišťující funkcionalitu dynamického webové rozhraní pro další produkty Velké sestry, a Node Director, což je aplikace pro správu uživatelů, distribuci softwaru, správu konfigurací, LDAP management, a to včetně automatizovaných akcí v

reakci na definované události.
Součásti projektu Big Sister jsou k dispozici pro platformy Linux a Windows. Jsou šířeny zdarma.

OpenNMS s klientem pro mobilní telefony

Autoři projektu OpenNMS, který vznikl v roce 1999, se chlubí tím, že je 100% open-source. Šířen je pod licencí GNU-GPL, ale firmy, kterým tato licence nevyhovuje, si mohou koupit i licenci komerční.
Jde o systém pro sledování a správu sítě, který je schopen automaticky zjistit zařízení připojená k síti, nebo je načíst z externí databáze, sledovat dostupnost a výkonnost síťových služeb od těch webových přes e-mailové až po mobilní nebo reagovat na definované události – odesláním e-mailu nebo SMS, případně provedením určeného skriptu. K dispozici je rovněž záznam časového průběhu přenášených dat prostřednictvím protokolů HTTP, SNMP, JMX a WMI i jejich grafická prezentace.
Kromě běžného webového rozhraní nabízí OpenNMS i klientskou aplikaci pro iPhone, iPod Touch a iPad.

Open-source, ale placené

K dispozici je rovněž řada produktů, které jsou částečně nebo zcela postaveny na open-source softwaru, ale jsou poskytovány za poplatek. K těm nejznámějším patří systémy pro kompletní monitorování a správu IT infrastruktury Big Brother (pro nekomerční účely zdarma, pro komerční je k dispozici je 30denní zkušební verze), GreatNMS (k dispozici je rovněž 30denní zkušební verze) nebo systém pro monitoring dostupnosti a výkonnosti sítě Groundwork Monitor Enterprise (pro demoverzi je nutné kontaktovat dodavatele).

Uvedený přehled produktů ukazuje, že nabídka open-source produktů pro monitoring a správu sítě, případně celé IT infrastruktury, je opravdu velmi široká. Pokud máte svůj preferovaný produkt, případně můžete nabídnout zajímavé zkušenosti s open-source produkty tohoto typu, budeme rádi, když se o ně podělíte s ostatními v diskusi nebo s redakcí na naší e-mailové adrese.

(Odkazy na stránky všech uvedených nástrojů najdete v příslušném speciálu na stránkách BusinessIT.cz.)

Bezpečnost a správa mobilních zařízení

Ano, klidně můžete nechat své uživatele mobilních zařízení jejich osudu. Nestarat se o to, jaká firemní data mají na svých smartphonech a tabletech, jak na nich pracují, ani co si do nich instalují. Vážně neříkáme, že to tak nejde. Ale zpravidla to nebude dobrý nápad, stejně jako většinou není dobrý nápad nechat zaměstnancům naprostou volnost v používání pracovního počítače. Pojďme se tedy společně podívat na možnosti správy mobilních zařízení. Na funkce podporované samotnými zařízeními i na balíky typu MDM (Mobile Device Management).

Koncová zařízení: Apple vs. Google

U koncových zařízení se budeme věnovat především produktům s operačními systémy iOS od Apple a Android od Google, protože právě ony jsou aktuálně na trhu nejpopulárnější. Lze samozřejmě namítnout, že na firemní uživatele daleko dříve mířily přístroje Blackberry, že druhá pozice na trhu chytrých telefonů podle posledních výsledků (druhé čtvrtletí 2011) patří

Symbianu, nebo že zajímavý jednou bude i Windows Phone 7 (v Nokiích), ale vzhledem k aktuálnímu stavu trhu dáme přednost prvním dvěma zmíněným systémům. Nicméně řada údajů v následujícím textu platí obecně pro všechny platformy.

Jak operační systém iOS od Apple, tak Android od Google, udělaly od svého vstupu na trh velký pokrok z hlediska možností centrální správy. U Androidu je ovšem nepříjemnou komplikací skutečnost, že jsou aktuálně na trhu k dispozici zařízení se značně odlišnými verzemi tohoto operačního systému, takže nabízejí různé schopnosti.

Samotný systém iOS disponuje nástroji, které dávají IT oddělením možnost poměrně snadno mobilní telefony a tablety od Apple vzdáleně konfigurovat, sledovat shodu jejich chování s firemními bezpečnostními pravidly a v případě potřeby zařízení zamknout nebo kompletně vymazat. V iOS je možno provést širokou škálu nastavení, je možné mimo jiné zakázat používání vestavěného fotoaparátu nebo pořizování screenshotů, nepovolit instalaci nových aplikací nebo provádění nákupů z aplikací již nainstalovaných, případně zakázat používání vybraných aplikací.

Android přinesl rozšířené možnosti správy v rámci firemní infrastruktury s příchodem své verze 2.2. Také u něj mohou administrátoři na dálku smazat všechna data ze ztraceného nebo ukradeného zařízení, zamknout přístup k zařízení po určité době nečinnosti, případně vyžadovat používání hesla na každém zařízení a nastavit jeho minimální požadovanou délku (případně si vynutit, aby heslo obsahovalo jak znaky, tak číslice). Tyto možnosti jsou k dispozici, pokud je na zařízení nainstalována aplikace Google Apps Device Policy od Google, která je zdarma ke stažení na Android Marketu. Nutno ovšem říci, že výše uvedeným výčtem možnosti vzdálené správy v podstatě končí (a ve srovnání s většinou ostatních platforem, včetně iOS, jsou tak podle analytiků výrazně chudší).

V této souvislosti stojí ještě za zmínku pravidla pro způsob odemykání smartphonu. Použití nějaké formy gesta namísto zadání alfanumerického hesla v sobě skrývá nebezpečí, že možný nálezce nebo zloděj telefonu odhalí kód ze šmouh na displeji. Nabízí se tedy vynucení zadání alfanumerického hesla, ale má to své „ale“. Ne vše, co zajistí vyšší bezpečnost, je oblíbeno u uživatelů. Třeba z komentářů uživatelů

smartphonu HTC Sense na internetu zjistíte, že s radostí používají aplikaci LockPicker, která je povinného alfanumerického hesla zbaví.

Antimalware pro smartphony

Společnost AVG, známý výrobce bezpečnostních řešení mj. i pro mobilní zařízení, varuje, že počet útoků – především na zařízení s operačním systémem Android – strmě roste. Pokud tedy nechcete spoléhat jen na zodpovědné chování uživatelů těchto zařízení, bude pro vás zřejmě dávat instalace některého z antimalwarových produktů dobrý smysl.

Již zmíněná společnost AVG nabízí svůj software AVG Mobile Security, který těží z dřívější akvizice společnosti DroidSecurity, která se specializovala právě na bezpečnost mobilních zařízení. Mobile Security kontroluje obsah stahovaných aplikací, mailů, SMS a webových stránek na přítomnost škodlivého softwaru, případně dodatečně proskenuje mobilní zařízení na viry, které je schopna i odstranit. Je rovněž schopna být nápomocna při lokalizaci ztraceného nebo ukradeného přístroje, případně při jeho zamčení, či při vymazání jeho

obsahu.
Podobnou funkcionalitu nabízí i ESET Mobile Security (pro Android je nyní k dispozici verze Release Candidate), jehož výrobce se chlubí i funkcí takzvaného bezpečnostního auditu, který by měl odhalit potenciální bezpečnostní rizika, nebo Kaspersky Mobile Security, který si zase zakládá na funkci speciální ochrany vybraných citlivých kontaktů.
Z dalších výrobců mobilních antimalwarových řešení jmenujme ještě alespoň firmy McAfee, F-Secure, Symantec (Norton) nebo Trend Micro.

Software pro správu

Komplexní systém pro správu mobilních zařízení (MDM) by měl podle definice analytiků společnosti Gartner nabízet především správu softwaru – včetně instalace, updatu, smazání nebo blokování mobilních aplikací, správu zabezpečení i pravidel využívání zařízení a správu souvisejících telekomunikačních služeb. Od MDM lze rovněž očekávat, že správcům IT poskytne podklady pro softwarový audit mobilních zařízení, pro bezpečnostní audit i pro rozúčtování nákladů.

K dispozici je skutečně pestrá nabídka MDM produktů od řady firem, z nichž některé se na tento segment trhu specializují, pro jiné tvoří doplněk jejich širšího produktového portfolia. Z první skupiny jmenujme například firmy Absolute Software, AirWatch, BoxTone, MobileIron, Tangoe nebo Zenprise. Do druhé skupiny patří například McAfee, Microsoft, Motorola Solutions, Research In Motion nebo Sybase (nyní SAP). Všechny běžně nabízené produkty jsou schopny spravovat mobilní telefony s různými operačními systémy (typicky iOS, Android, OS Blackberry, Windows Mobile, Symbian a některé i WebOS).

Správa je realizována v modelu klient/server, kdy na mobilních telefonech běží agent, jenž poskytuje serverové části, s níž pracují správci, potřebné informace, a zajišťuje provádění zaslaných instrukcí (nastavení smartphonu apod.). Agent přitom může být součástí operačního systému nebo může být do přístroje nahrán dodatečně. Obecně lze říci, že pokud systém pro správu spoléhá na integrovaného agenta, je omezen schopnostmi dané platformy tak, jak už jsme je zmiňovali výše.

Agent prostřednictvím dostupných komunikačních

kanálů nejen přijímá instrukce a odesílá informace o stavu telefonu, ale může také hlídat, zda nedošlo k nějaké z definovaných situací, na kterou je třeba podle dříve nastavených pravidel zareagovat. Tak lze například v okamžiku, kdy se telefon ocitne v roamingu, zakázat nebo omezit přenosy dat.

Odlišnosti různých řešení

Jednotlivé MDM se od sebe liší nejen škálou nabízených funkcí a rozhraním (typicky webové, k dispozici je zpravidla API a někdy desktopová aplikace), ale také způsobem poskytování (jako běžný software, SaaS, appliance), rozsahem podpory, škálovatelností, podporou adresářových služeb (typicky je podporován Active Directory, často i Open Directory) nebo prací s profily uživatelů. Většina systémů je schopna detekovat práci s nepovolenými aplikacemi v iOS nebo jailbreak iOS (úprava iOS, při které uživatel k telefonu získá plná přístupová práva, a může tak například instalovat neautorizované aplikace, různá rozšíření apod.; obecně, bez ohledu na operační systém, je tato úprava označována jako rooting).

Dodejme ještě, že řada IT oddělení používá k

základní správě mobilních zařízení ve firmě Microsoft Exchange Server a ActiveSync, se kterým jsou dnes mnohá mobilní zařízení schopna nativně komunikovat. Toto řešení umožňuje mimo jiné vzdálené vymazání obsahu telefonu (mobilního zařízení) nebo nastavení vymazání po určitém počtu neúspěšných pokusů o odemknutí telefonu, nastavit pravidla pro heslo (délku, složitost apod.) nebo délku neaktivity uživatele, po které dojde k zamčení telefonu (a pro odemčení je třeba užít heslo). Nastavit lze rovněž třeba pravidla pro šifrování dat v telefonu a na paměťových kartách.

Úskalí systémů MDM

Společnost Gartner ve své letošní zprávě o MDM varuje před některými úskalími těchto systémů. První z nich již bylo naznačeno výše – některé z mobilních operačních systémů výrazně limitují možnosti správy, a tak nelze očekávat, že všechny chytré telefony ve firmě – pokud pracují na různých softwarových platformách – nabídnou stejnou úroveň správy. Gartner přitom varuje především před nevyzrálostí platformy Android.

Současně upozorňuje, že ačkoli je Blackberry

historicky nejvýznamnější platformou chytrých telefonů pro použití ve firmách, ne všechny MDM systémy podporují integraci s BES (Blackberry Enterprise Server). Pokud tedy používáte mimo jiné i zařízení Blackberry, je vhodné být v tomto ohledu ostražitý.
Ohledně správního rozhraní systémů MDM Gartner doporučuje pečlivě zkoumat, zda nabízí vše, co bude při práci třeba – a upozorňuje, že některé systémy nabízejí jen velmi omezené možnosti reportingu a nástrojů BI (Business Intelligence). K dispozici by podle analytiků měly být jak textové, tak grafické výstupy, a to jak předpřipravené, tak uživatelsky definované.

Ještě několik poznámek

Za jeden z nejvýraznějších celosvětových trendů dneška bývá označován přístup, kdy si zaměstnanci přinášejí do zaměstnání svá vlastní mobilní zařízení – vybraná dle vlastních preferencí – a je jim z nich umožněn – v různé míře – přístup k firemním IT zdrojům. Za hlavní výhodu tohoto stavu je označována vyšší produktivita, nevýhody jsou však

zřejmé: Heterogenní IT prostředí se hůře spravuje, a pokud má být učiněno bezpečnostním pravidlům zadost, je třeba omezit činnosti, které uživatel může se svým zařízením provádět. Přitom se ale nelze stoprocentně spolehnout na to, že nasazená ochrana nebude uživatelem překonána. I když aktuální vývoj mobilních platforem i systémů pro jejich správu naději, že se tento problém v budoucnu podaří do značné míry vyřešit, rozhodně to nelze očekávat v horizontu několika málo měsíců.

Nasazení cloudu v praxi

Služby cloudu lze využívat různými způsoby pro různé účely a my se v následujícím příspěvku podíváme na několik příkladů. Řeč bude jak o významné open source platformě, jejímž prostřednictvím lze vybudovat vlastní privátní cloud, tak o veřejných cloudech poskytujících různé typy služeb, typicky aplikace nebo infrastrukturu formou služby.
I když nejsnazší je zpravidla použití cloudu nabízejícího služby typu software ve formě služby (SaaS), my začneme z druhého konce, totiž od řešení pro vybudování vlastníhou cloudu. Proč? Právě proto, že služby typu SaaS jsou dnes již poměrně známé a zpravidla snadno použitelné, nechceme vás hned v úvodu nudit něčím, co nepředstavuje tu správnou výzvu.

OpenStack: Open Source software pro vlastní cloud

Za jeden z nejvýznamnějších (ne-li vůbec nejvýznamnější) open source cloudový projekt je označován OpenStack, za kterým zpočátku stála

společnost RackSpace a NASA, ale postupně se v něm začala angažovat asi stovka dalších firem, mimo jiné Citrix, Dell, AMD, Intel nebo Cisco. OpenStack bývá označován za Linux světa cloudu (v pozitivním slova smyslu).

Z hlediska uživatelů jsou pochopitelně podstatné nejen vlastnosti, které jsou de facto definicí cloudu (škálovatelnost, spolehlivost apod.), ale také jednoduchost nasazení. Zatím poslední významný krok tímto směrem učinila v létě 2011 společnost Dell, která uvolnila jako open source svůj Crowbar - softwarový framework, který umožňuje nainstalovat víceuzlový cloud během několika hodin či dokonce minut. (Na konferenci CloudConnect předvedla nasazení šesti uzlů s OpenStack Compute a Object Storage během necelé půlhodiny.)

OpenStack se skládá ze tří základních částí: OpenStack Compute (kódové označení Nova), OpenStack Object Storage (kódové označení Swift), a OpenStack Image Service (kódové označení Glance).

OpenStack Compute zajišťuje správu rozsáhlé sítě virtuálních strojů, čímž vytváří základ škálovatelné cloudové platformy s redundantními zdroji. Tento

software poskytuje jednak grafické správní rozhraní, jednak API potřebné pro využití cloudu – včetně zajištění běhu instancí softwaru nebo přístupu uživatelů. Podstatné je, že OpenStack Compute je navržen bez vazby na konkrétní hypervisor nebo hardware.

OpenStack Object Storage, jak už název napovídá, zajišťuje dlouhodobé ukládání dat, a to v mnohapetabajtových objemech. Jde o distribuovaný, široce škálovatelný systém. Výstižný je i název posledního základního prvku OpenStacku, totiž Image Service. Ten samozřejmě zajišťuje práci s obrazy systémů uložených v různých úložištích, jejich ukládání, vyhledávání i streaming.

Jak na vlastní cloud

Při instalaci vlastního cloudu na platformě OpenStack budete pochopitelně potřebovat řadu podkladů ze stránek tohoto projektu. We wiki projektu OpenStack jsou k dispozici odkazy na různé instalační balíky OpenStacku umožňující vytvoření cloudového prostředí pod linuxovými operačními systémy Ubuntu, CentOS, Fedora a Red Hat Enterprise, následované instrukcemi – od postupné

instalace systému od vytvoření příslušných diskových oddílů až po odkaz na podrobnou dokumentaci Novy, která se po instalaci zřejmě stane vaším startovním bodem další práce. Manuály ke všem třem základním prvkům OpenStacku naleznete zde – ve formě pro prohlížeč i v PDF.
A stránky projektu Dell Cloud Edge najdete zde. Je tu k dispozici již zmíněný produkt Crowbar usnadňující nasazení OpenStacku. Případně můžete pro automatizaci nasazení cloudu využít produkt Chef.
Abychom nebyli pouze jednostranně zaměření, zmiňme ještě další významnou open source cloudovou alternativu, totiž projekt Eucalyptus, který byl – do vzniku OpenStacku – obecně považován za nejvýznamnější projekt tohoto typu. Rozhodnutí, kterému z nich dnes patří pomyslné vítězství, s dovolením ponecháme na vás.

Veřejný cloud od Amazonu

Pokud chcete dát přednost službám veřejného cloudu a potřebujete nikoli hotové aplikace, ale výpočetní výkon, pak zřejmě při zkoumání možností neminete nabídku společnosti Amazon, která nabízí

jednu z nejznámějších (ne-li vůbec nejznámější) služeb tohoto typu. Její Amazon Elastic Compute Cloud (EC2) je službou, která uživateli poskytuje škálovatelnou výpočetní kapacitu podle jeho potřeb. Platit budete za skutečně spotřebované zdroje, resp. za dobu běhu příslušné instance a za přenesená data.

Ale buďme konkrétní. Prostřednictvím webového správního rozhraní si můžete během několika minut vytvořit novou instanci virtuálního serveru s jedním z nabízených operačních systémů (různé varianty Linuxu, Windows Server nebo OpenSolaris) a začít na něm provozovat svou aplikaci. Využít přitom můžete jak některý z předpřipravených diskových obrazů (AMI, Amazon Machine Image), tak obraz upravený dle svých potřeb – s vlastním nastavením, s potřebnými aplikacemi, případně s daty.

Instancí si můžete vytvořit tolik, kolik je potřeba, zvolit lze i jejich provozování v jedné nebo v různých lokalitách. Vytváření a zavírání jednotlivých serverových instancí lze pochopitelně realizovat i prostřednictvím API a tedy zcela automatizovat. EC2 je součástí kompletnější cloudové infrastruktury

Amazonu, do které patří ještě Amazon Simple Storage Service (Amazon S3), Amazon Relational Database Service (Amazon RDS), Amazon SimpleDB a Amazon Simple Queue Service (Amazon SQS); tyto prvky jsou odpovědí na (zatím zde nevyřčené) otázky ohledně ukládání a zpracování větších objemů dat.
A zmiňme zde ještě několik vlastností cloudu Amazonu, jako jsou Elastic IP Addresses, což jsou statické IP adresy spojené nikoli s konkrétní instancí serveru, ale s vaším účtem – a lze je dynamicky přemapovat – například v okamžiku výpadku – na funkční část cloudu. Elastic Load Balancing, jak už název napovídá, automaticky distribuuje příchozí požadavky na nejméně vytížené instance EC2 a zajišťuje, aby provoz nebyl směrován na instance, které mají problémy. Amazon Virtual Private Cloud zajišťuje bezpečné propojení mezi vaší firemní IT infrastrukturou a externím cloudem Amazonu. A zmiňme i službu VM Import, která umožňuje importovat do EC2 virtuální stroje z vašeho interního IT prostředí.

Aplikace v cloudu

Z hlediska klienta nejjednodušší použití nabízejí cloudové služby typu SaaS, tedy Software as a Service. Výborným příkladem je v tomto případě Google a jeho Google Apps, Zoho, případně MS Office 365. Pro naše účely si zde vyberme snad nejtypičtějšího zástupce, totiž Gmail pro firmy. Jeho výhodou pro naše účely je fakt, že všichni hned vědí, o čem je řeč – webové e-maily zná každý. A Gmail pro firmy vypadá úplně stejně, jako běžný Gmail.

I když i běžný Gmail nabízí odesílání z jakýchkoli jiných e-mailových adres, než je ta základní (typicky jmeno.prijmeni@gmail.com), v hlavičce zprávy je stále uvedeno, že mail byl odeslán z Gmailu – a v některých e-mailových klientech se to i zobrazí. Proto je vhodné se při profesionálním využití zaregistrovat k balíku služeb Google Apps a provozovat Gmail na vlastní doméně. Celým procesem vás přitom Google provede a největší „složitostí“ je tak změna MX záznamů u registrátora doménového jména. Vše je záležitostí několika minut.

Odpadá tak instalace a správa vlastního e-mailového serveru. Lze přitom zvážit i využívání dalších aplikací; zkušenosti ukazují, že uživatelé jsou zpravidla konzervativnější, pokud jde o hlavní

kancelářské aplikace (které jsou v on-line provedení značně omezené), nicméně e-mail, kalendář nebo interní webové stránky pro sdílení informací mají v cloudové podobě své kouzlo i pro ně. A to mimo jiné díky snadnému sdílení potřebných informací v rámci firmy i díky snadnému přístupu z mobilních zařízení.
Výraznou výhodou bývala i cena – Google nabízel možnost využívat Apps zdarma s až padesáti uživateli, což znamenalo de facto bezplatné řešení pro řadu menších firem; letos (2011) byl však limit pro nově registrované organizace snížen na 10. Při vyšším počtu uživatelů činí cena za uživatele 40 eur ročně (v době psaní tohoto textu, tedy v srpnu 2011).
Na závěr ještě dodejme, že Google nabízí kromě svých standardních balíků aplikací v rámci Google Apps také možnost pořídit si cloudové aplikace od třetích stran – běžící v cloudu Google, případně si vyvinout a provozovat v něm aplikace vlastní.

Cloud není jen módní hit

Společnost Gartner na své letošní letní „hype“ křivce přidělila technologiím cloudu několik pozic. Zatímco privátní cloud a cloud ve smyslu nabídky veřejné infrastruktury se pohybují na jejím prvním vrcholu, tedy

v oblasti přehnaných očekávání – s předpokládaným uvedením do praxe během následujících dvou až pěti let, cloudové webové platformy se nacházejí v následující části vyhrazené technologiím, kde uživatelé propadli deziluzi. Mimochodem – rovněž s očekávanou dobou nasazení dva až pět let. Zdá se tedy, že stále není kam spěchat. Nicméně i dnes už nepochybně cloud má na mnoha místech své opodstatnění a přináší své ovoce.

Uvedená trojice příkladů si samozřejmě v žádném případě nedělá ambice na úplnost. Různých řešení a služeb spojených s Cloud Computingem je na trhu nepřeberné množství a pokud se podíváte na takřka jakéhokoli z dalších (zde dosud nejmenovaných) významných hráčů na poli podnikové informatiky (a tím opravdu nemáme na mysli jen HP, IBM, Microsoft nebo Oracle), v jeho nabídce bude zpravidla řada s cloudy souvisejících produktů. V tomto článku nám šlo o to, nabídnout pohled na tři základní přístupy ke cloudu a na tři konkrétní možná řešení; že je variant daleko více, je nezpochybnitelné.