Chce bezpečnostní manažer cloud?

Vedle jasných přínosů cloud computingu přináší jeho využívání i nová bezpečnostní rizika, která je nutné pokrýt. Požadavky na bezpečnost cloudu by měly vzejít od bezpečnostního manažera. Ten musí umět řídit ochranu dat i mimo firemní perimetr. Jeho neznalost však mnohdy vzbuzuje neopodstatněný strach a obavy.

Zákazníci i dodavatelé cloudu si uvědomují rizika, která plynou z umístění systémů na sdílené infrastruktuře nebo ve vzdálené fyzické lokalitě. Bezpečnostní manažeři zejména na zákaznické straně jsou znepokojeni riziky cloudu, protože přenosem odpovědností za provoz informačních systémů ztrácejí mj. i přímou kontrolu nad bezpečností dat, kterou nelze jednoduše delegovat na provozovatele cloudu.

Vedle rizik však cloud computing přináší také benefity v podobě úspor nákladů na bezpečnost. Implementace a provozování bezpečnostních opatření může být ve větším rozsahu levnější než dílčí ochrana. Pro poskytovatele cloudu je velmi efektivní mít centrální patch management, provozovat současně několik vzájemně záložních lokalit nebo řešit řízení zranitelností jednou technologií přes tisíce serverů.

Sjednocení řízení bezpečnosti je jednou ze základních výhod cloudu pro poskytovatele i zákazníky. Standardizace různých bezpečnostních vrstev vede opět ke snížení nákladů, ale také umožňuje efektivní a transparentní řízení a implementaci bezpečnostních technologií.

Bezpečnost cloudu je věcí, kterou řeší řada CISO, ale bohužel hodně z nich postrádá znalosti o možnostech ochrany dat, která jsou uložena mimo „jejich“ lokalitu, neboli mimo správu organizace. Tato neznalost se bohužel následně projevuje striktním odmítáním přesunu systémů a dat k poskytovateli cloudu.

Moderní bezpečnostní manažer však musí umět reagovat na požadavky IT a ekonomů, kteří v cloudu vidí úsporu nákladů. Není možné se cloudu vyhnout a trvale ho odmítat.

Rizika cloudu

Identifikace a vyhodnocení rizik cloudu je základem pro rozhodnutí, zda do něj jít nebo ne. Řada bezpečnostních manažerů však vidí cloud jako jedno velké nové riziko, které nelze pokrýt. Je to možné, jen je nutné znát charakteristiku rizik, detailní profil hrozeb a možnosti ochrany před ztrátou, únikem a zneužitím dat. Pokud CISO ví, jak vyhodnocovat rizika cloudu, nemůže ho a priori odmítat.

Cloud computing není nová technologie, ale jen nový způsob využívání informačních prostředků. I přesto s sebou přináší určitá externí rizika, která lze částečně odvodit z vnitřních bezpečnostních hrozeb. Je však nutné se na ně dívat z jiného pohledu. Cloud nedovoluje využít běžné postupy hodnocení rizik, jako když je systém v plné správě interní organizace IT. Zvládání rizik musí být rozšířeno o další činnosti, které zajistí ochranu rozhraní, dodržení souladu, řádnou kontrolu mazání dat apod.

Charakter konkrétních rizik je také velmi závislý na způsobu využívání cloudu – IaaS (Infrastructure as a Service), PaaS (Platform as a Service), SaaS (Software as a Service). Jednotlivým variantám se věnoval článek [1]. Každá varianta definuje jiné hranice mezi cloudem a organizací a bezpečnostní manažer musí přesně nastavit procesy ochrany tak, aby korespondovaly s nastaveným rozhraním.

Pokud není dostatečně zajištěna kontrola cloudu, nemůže organizace prohlásit, že má detailně zmapována všechna rizika. Je věcí bezpečnostní-

ho manažera si prosadit do smlouvy prostředky pro monitorování, nástroje patch managementu a řízení technických zranitelností, testování zálohovacích procedur a zajištění procesů řízení incidentů a kontinuity. Všechna tato opatření mají významný vliv na skutečný profil rizik.

Na druhou stranu je skutečně otázkou, zda použití cloudu přináší rizika zcela nová a do této doby organizaci neznámá. Řada potenciálních hrozeb je stejná jako v případě, kdy je systém provozován ve vlastním prostředí. Je běžné, že uživatelé používají notebooky a podobná zařízení pro práci s firemními daty. A používají je v externím prostředí, které nemá bezpečnostní manažer pod kontrolou.

Je vcelku standardní, že obchodní zástupce přistupuje z veřejné kavárny v obchodním centru přes VPN přímo k CRM databázi obsahující citlivé údaje o zákaznících. Kopii této databáze má u sebe na počítači. A kdo ví, kdo se mu dívá přes rameno? Důležité je, že komunikace mezi notebookem a serverem je dostatečně šifrovaná a pro přístup se používá vícefaktorová autentizace. Jaký je potom rozdíl, když celá databáze bude „někde“ v cloudu?

Obdobné to je s fyzickou a environmentální bezpečností. Při procházení kvalitním českým hostingovým centrem je možné zjistit, že tato oblast bezpečnosti je zajištěna mnohem lépe, než v serverovnách některých českých bank.

Vedle rizik, do určité míry shodných s interním prostředím, je možné při analýze cloudu identifikovat specifická rizika, která vyžadují rozdílný přístup k jejich pokrytí. Ucelený seznam rizik vydala organizace ENISA a asociace Cloud Computing Security. I když jsou rizika různě identifikována, jejich celkový obsah je téměř shodný. Viz jednotlivé boxy.

TOP rizika cloudu podle ENISA **BOX 1**

- *Ztráta governance nad bezpečností*
- *Závislost na poskytovateli (Lock-in)*
- *Chyba oddělení v cloudu*
- *Nedodržení souladu*
- *Nezabezpečené rozhraní*
- *Ochrana dat*
- *Nedostatečné a neúplné mazání dat*
- *Interní útoky*

http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment

Důvěryhodnost poskytovatele cloudu

Poskytovatelé cloudu nabízejí svým zákazníkům neomezené výpočetní kapacity, sítě a úložné prostory, které jsou velmi často spojeny s rychlým registračním procesem. Díky němu je možné využívat cloud téměř anonymně a bez jakékoli identifikace konkrétní existující organizace nebo osoby. Navíc někteří poskytovatelé nabízí zkušební využití cloudu zdarma, a to už se jedná o anonymitu opravdu stoprocentní. Benevolence poskytovatelů cloudu s úspěchem využívají útočníci k zasílání spamu. Autoři škodlivých kódů a jiní pachatelé mají díky cloudu možnost provádět svou nekalou činnost prakticky beztrestně.

Těmito útoky jsou tradičně nejvíce poškozeni poskytovatelé PaaS, nicméně hackeři útočí i na dodavatele IaaS. Stále častější jsou případy z oblasti zneužití hesel, útoky DDOS, dynamické útoky z více bodů, hostování škodlivých kódů, útoky botnetů, rainbow tables nebo využívání prostředků cloudu k rozluštění CAPTCHA.

Vysoká důvěra v cloud je tedy zásadním parametrem při rozhodování organizace, jakého poskytovatele si vybrat. Pokud si poskytovatel pustí do svého prostředí anonymní „zákazníky“, kteří nejsou schopni dodržovat základní bezpečnostní (a vlastně i etická) pravidla, nemůže očekávat velké solventní zákazníky.

Poskytovatel si musí sám prosadit monitorování aktivit, aby identifikoval a dokázal zabránit zneužití své infrastruktury. A bezpečnostní manažer zákazníka by měl požadovat prokázání takového monitorování ze strany poskytovatele. Na druhou stranu je otázkou, do jaké míry může poskytovatel cloudu sledovat aktivity svých zákazníků. Nicméně poskytovatel musí být schopen sledovat svůj cloud a podezřelou síťovou komunikaci, aby mohl efektivně zmařit případné útoky.

Bezpečnost rozhraní

Poskytovatelé cloudu nabízí přístup prostřednictvím různých softwarových rozhraní, přes které mohou zákazníci řídit a spravovat nabízené služby. Správa, řízení, organizování, monitorování a spouštění nebo ukončování služeb, to všechno je prováděno prostřednictvím rozhraní, na kterých závisí bezpečnost a dostupnost poskytovaných služeb.

Rozhraní pro autentizaci, řízení přístupu, šifrování nebo monitoring musí být navrženo tak, aby v maximální míře zajišťovalo ochranu před úmyslnými útoky nebo obcházením bezpečnostních politik. Rozhraní jsou obvykle přístupná volně přes internet a nabízí přístup k rozsáhlým zdrojům a funkcionalitám. K riziku rozhraní nutno připočíst též zranitelnost webových prohlížečů.

Navíc mohou zákazníci cloudu poskytovat přidané služby svým zákazníkům prostřednictvím dalších rozhraní (typicky e-shop). Tato situace vyžaduje zajištění bezpečnosti na několika vrstvách API, protože organizace jsou nuceny dávat

TOP rizika cloudu podle Cloud Security Alliance BOX 2

- *Zneužití a nekalé využívání cloudu*
- *Nezabezpečené rozhraní a API*
- *Úmyslné interní útoky*
- *Sdílené technologie*
- *Ztráta a únik dat*
- *Neoprávněné získání účtu nebo služby*
- *Neznámý profil rizik*
- *Interní útoky*

http://www.cloudsecurityalliance.org/

oprávnění dalším třetím stranám. Tak se např. riziko ztráty důvěryhodnosti může stát problémem na několika úrovních.

Bezpečnostní manažer musí po poskytovateli požadovat silnou, ideálně vícefaktorovou autentizaci k rozhraní pro správu systému. Zároveň musí zajistit, nejlépe už v návrhu aplikace, aby registrace všech zákazníků byla bezpečná, důvěryhodná a transparentní. Rozhraní pro přístup zákazníků nesmí obsahovat známé zranitelnosti webových aplikací a musí zajistit bezpečný způsob přihlášení i komunikace.

Úmyslné interní útoky

Hrozba „vnitřního nepřítele“ se netýká jen cloud computingu, ale je to hrozba známá ve všech organizacích. Do cloudu přistupuje mnoho uživatelů a riziko je zesíleno tím, že v jedné lokalitě, na jedné platformě a často v jedné logické doméně se vyskytuje několik různých zákazníků. Pokud je tato situace doplněna nedostatkem transparentnosti v procesech a činnostech poskytovatele cloudu, může mít bezpečnostní manažer zaděláno na velký problém.

Zatímco je toto interní riziko méně pravděpodobné, jeho dopady jsou obvykle závažnější, protože interní útočník zná mnohem lépe prostředí, ve kterém se pohybuje. Navíc může zneužít různé role, které mu zajišťují oprávněný přístup do různých úrovní cloudu.

Bezpečnostní manažer navíc zpravidla oponuje, že přístup k datům mají neidentifikovatelní pracovníci poskytovatele cloudu. Je ale opravdu důvěryhodnější správce serveru – zaměstnanec nebo správce poskytovatele pracující na základě SLA? Má CISO opravdu detailní přehled o přístupech jednotlivých administrátorů systémů, které jsou provozovány lokálně? Mnohem větší sankce za porušení důvěryhodnosti lze aplikovat prostřednictvím SLA než v pracovní smlouvě.

Zákazníci obvykle nepožadují, aby jim poskytovatel cloudu představil svoje vnitřní procesy, jak jeho zaměstnanci získávají logický a fyzický přístup k zařízením, jak jsou monitorovány aktivity v systému nebo jak je hodnocena a reportována shoda s požadavky. Pro kvalitního a transparentního poskytovatele cloudu toto přeci nemůže být problém.

Bezpečnostní manažer by měl požadovat detailní reporting všech aktivit systému včetně těch realizovaných zaměstnanci poskytovatele. Zákazník musí požadovat transparentnost v procesech řízení a ve správě cloudu. Určitou záruku kvality a důvěryhodnosti poskytovatele mohou poskytnout i certifikace nebo obdobné způsoby prokázání určité úrovně bezpečnosti.

Sdílené technologie a nedostatečné oddělení

Souběžný pronájem a sdílené zdroje představují základní charakteristiky cloud computingu. Riziko nedostatečného oddělení pokrývá selhání mechanismů separace serverů, síťových segmentů a chyby ve směrování. Spadají sem i tzv. guest-hopping útoky, kdy útočník využije situace provozování několika virtuálních strojů na jednom fyzickém zařízení.

Základním opatřením je prosazení strategie defense-in-depth, která musí zahrnovat zajištění bezpečnosti pro výpočetní a úložná zařízení, sítě i monitorovací nástroje. Musí být zavedeno důsledné oddělení jednotlivých kapacit a zařízení tak, aby jednotliví zákazníci nebyli ovlivněni případnými problémy jiných nájemců sdílených částí cloudu. Zásadním opatřením je také silné řízení přístupu, a to i ke zrušeným a vymazaným datům.

Zde, více než jinde, je potřebné monitorování aktivit v systému a bezpečnostní dohled nad jednotlivými alerty, které mohou znamenat potenciální narušení bezpečnosti. Toto opatření však není nic speciálního pro cloud. Pokud je monitoring důsledně realizován, je prakticky jedno, zda je systém pod správou organizace nebo u poskytovatele cloudu. Bezpečnostní manažer si v obou případech musí zajistit, že bude mít přístup ke všem logům a bude dostávat bez prodlení všechny informace o nestandardních událostech v systému. Praxe ukazuje, že tyto požadavky na monitoring je mnohem snazší realizovat v rámci SLA než interním pravidlem, které budou kolegové z IT ignorovat.

Bezpečnostní manažer by měl také prosadit, aby smlouva s poskytovatelem cloudu zahrnovala možnost pravidelného skenování technických zranitelností a audit konfigurace pronajímaných zařízení a systémů.

Ztráta a únik dat

V cloudu existuje mnoho možností ztráty dat. Vymazání nebo chybná změna v datech, která nebyla zálohována, jsou obvyklými případy ztráty dat v cloudu.

Pokud jsou data uložena na nespolehlivém zařízení nebo médiu, může i ztráta malého množství dat způsobit nečitelnost v mnohem širším kontextu. A architektura a provozní vlastnosti cloudu tato rizika ještě znásobují.

Např. ztráta šifrovacích klíčů je dokonalým prostředkem k definitivní ztrátě všech uložených dat. Je velmi jednoduché zapnout transparentní šifrování na úrovni MS SQL, ale řízení přístupu nebude díky šifrování výrazně bezpečnější. Navíc je nutné zajistit několikanásobnou zálohu šifrovacích klíčů, aby byla zajištěna obnova dat v případě havárie.

Významným rizikem úniku dat může být jejich nedostatečná likvidace. Mazání dat v cloudu nemusí být plně v souladu s požadavky zákazníka a pro poskytovatele není jednoduché prokázat, že data byla nenávratně zničena. Zejména pokud má být mazání dat rychlé a operativní. Riziko velmi souvisí se sdílením kapacit cloudu.

Přiměřené či včasné odstranění dat může být také nemožné a to buď proto, že existují další nadbytečné kopie dat, které však nejsou pro zákazníka přístupné (např. z důvodu zálohy), nebo proto, že na disku určenému k fyzickému zničení jsou uložena rovněž data jiných klientů.

Efektivním opatřením proti ztrátě nebo úniku dat je řádné zálohování, přísné řízení přístupu prostřednictvím kvalitních rozhraní a dostatečné zajištění integrity dat. Pokud je využíváno šifrování, musí být klíče uloženy v různých lokalitách a ideálně i na technologicky různých médiích. Pochopitelně i sem patří možnost, aby bezpečnostní manažer prostřednictvím SLA měl možnost kontrolovat postupy zničení dat a médií.

Neoprávněné zneužití účtu nebo služby

Stejně jako pro jiné běžné (lokálně provozované) systémy jsou i pro cloud relevantní běžné hrozby phishingu, podvodů, zneužití technických zranitelností apod. Uživatelská ID a hesla jsou často opětovně používána pro různé přístupy a tato situace ještě zvyšuje potenciální rizika neoprávněného zneužití.

Řešení cloudu však přináší i nová bezpečnostní rizika. Pokud útočník získá přístupové údaje uživatele, může tajně monitorovat jeho aktivity, transakce, manipulovat s daty, vracet falešné informace na dotazy a přesměrovávat komunikaci na jiné servery. Získá-li hacker neoprávněný přístup ke službám cloudu, může ho využít jako svou základnu pro další útoky, jak bylo zmíněno výše. V takovém případě může dojít ke ztrátě dobrého jména zákazníka i poskytovatele cloudu.

Bezpečnostní manažer musí požadovat a prosadit, aby byla zavedena vícefaktorová autentizace, zákaz sdílení přístupových oprávnění mezi uživateli a službami a zajištění aktivního monitoringu všech částí cloudu.

Požadavky definuje CISO

CISO musí umět prosadit bezpečnostní požadavky na všechny funkce a vrstvy systému, které budou zajištěny poskytovatelem cloudu. Protiopatření jsou prosazována smlouvou a CISO musí umět detailně popsat požadavky včetně technologických řešení. Měl by se účastnit celého procesu přesunu systémů do cloudu – od návrhu až po provoz.

Mezi základní bezpečnostní opatření spadá řízení přístupu, ochrana komunikace mezi zákazníkem a poskytovatelem, bezpečnost rozhraní, šifrování uloženého obsahu, separace systémů v rámci cloudu, zajištění řádné likvidace použitých médií, důsledný bezpečnostní monitoring, pravidelné skenování zranitelností a efektivní řízení kontinuity.

Prakticky všechna tato opatření jsou zajištěna bezpečnostními technologiemi, které musí CISO důkladně ovládat. Ne proto, aby si uměl z dohledového systému vyjet report o neúspěšných přihlášeních, ale zejména z důvodu, že to je on, kdo musí na poskytovatele cloudu klást požadavky týkající se technologického zabezpečení.

Předsudky stranou

Řada bezpečnostních manažerů se bojí cloudu a naivně si myslí, že systém provozovaný samotnou organizací je více bezpečný. Toto přesvědčení však v mnoha případech plyne z neznalosti bezpečnostních technologií a procesů zajišťování bezpečnosti.

Mnoho CISO brečí nad tím, že v jejich organizaci je velmi těžké prosadit bezpečnost, protože se proti ní bouří uživatelé i správci IT. Stěžují si, že nemají dostatečnou podporu managementu. Budou si zřejmě ještě muset osvojit zkušenost, že prosadit bezpečnostní strategii je jednodušší v SLA než interní směrnicí.

Jan Mikulecký
mikulecky@rac.cz

Ing. Jan Mikulecký, Ph.D., CISM, CGEIT, CRISC

Absolvent ČVUT Praha, od roku 1999 pracuje v RAC jako konzultant pro řízení rizik, ISMS, BCMS a penetrační testy. Člen komise ISACA CISM TES, rady ISACA ČR a redakční rady DSM.

POUŽITÉ ZDROJE

[1] http://www.cloudsecurityalliance.org/
[2] http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment