KOMENTÁŘ

Bát, či nebát se cloudu?

Bezpečnostní požadavky na cloud computing by měly vzejít od bezpečnostního manažera, který by měl umět řídit ochranu dat i mimo firemní perimetr. Jeho neznalost však mnohdy vzbuzuje neopodstatněný strach a obavy. Bezpečnost cloudu je věc, kterou řeší řada manažerů na pozici CISO (Chief Information Security Officer), ale bohužel postrádají znalosti o možnostech ochrany dat, která jsou uložena mimo „jejich" lokalitu, neboli správu organizace. Tato neznalost se naneštěstí následně projevuje striktním odmítáním přesunu systémů a dat k poskytovateli cloudu. Před rokem 1903 se lidé také báli létat, protože nikdo nevěděl, že je možné vznést se na motorovém stroji těžším než vzduch.

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

> Řada bezpečnostních manažerů se bojí cloudu a naivně si myslí, že systém provozovaný samotnou organizací je bezpečnější.
>
> **JAN MIKULECKÝ,** KONZULTANT PRO ŘÍZENÍ RIZIK, ISMS, BCMS A PENETRAČNÍ TESTY, RISK ANALYSIS CONSULTANTS

Hledání pravdy

Je otázkou, zda použití cloudu opravdu přináší organizaci mnoho nových bezpečnostních rizik. Řada potenciálních hrozeb je stejná jako v případě, že systém je provozován ve vlastním prostředí. Je běžné, že uživatelé využívají notebooky a podobná zařízení pro práci s firemními daty. A používají je v externím prostředí, které nemá bezpečnostní manažer pod kontrolou. Je vcelku normální, že obchodní zástupce přistupuje z veřejné kavárny v obchodním centru přes VPN přímo k CRM databázi obsahující citlivé údaje o zákaznících. A kdo ví, kdo se mu dívá přes rameno. Důležité je, že komunikace mezi notebookem a serverem je dostatečně šifrována 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. Pokud se půjdete podívat do kvalitního hostingového centra, zjistíte, že tato oblast bezpečnosti je zajištěna mnohem lépe než serverovny některých českých bank.

Dalším předmětem diskuze je také důvěra v poskytovatele cloudu. Neznalý bezpečnostní manažer zpravidla oponuje, že přístup k datům mají neidentifikovatelní pracovníci poskytovatele cloudu. Je 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.

Důkladná kontrola klíčem...

Jedněmi ze základních opatření jsou monitoring aktivit v systému a bezpečnostní dohled nad jednotlivými alerty, které mohou znamenat potenciální narušení bezpečnosti. 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. A toto je opět obvykle mnohem snazší prosadit v rámci SLA než interním pravidlem, které budou kolegové z IT ignorovat.

CISO by tedy měl umět prosadit bezpečnostní požadavky na všechny funkce a vrstvy systému, které budou zajištěny poskytovatelem cloudu. Drtivá většina protiopatření je prosazena skrze smlouvu, a proto je nutné, aby bezpečnostní manažer uměl detailně popsat požadavky včetně technologických řešení. Také by se měl účastnit celého procesu přesunu systémů do cloudu, od návrhu až po provoz.

Mezi základní bezpečnostní opatření spadají řízení přístupu, ochrana komunikace mezi organizací a poskytovatelem cloudu, bezpečnost rozhraní, šifrování uloženého obsahu, separace systémů v rámci cloudu, zajištění řádné likvidace použitých médií a důsledný bezpečnostní monitoring.

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

CISO by si měl také prosadit, aby mu poskytovatel cloudu pravidelně a bez prodlení zasílal aktuální reporty o technických zranitelnostech systémů a zařízení, pochopitelně včetně jejich vyřešení. Stejně tak by poskytovatel měl prokázat, že jeho procesy řízení kontinuity jsou efektivně zavedené a pravidelně je testuje.

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 kolikrát jednodušší v SLA než interní směrnicí.

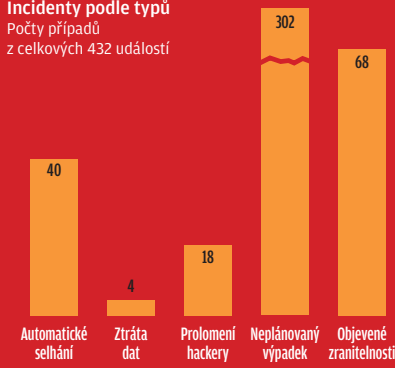
(mar) 110001

Výpadky cloudů

Organizace Open Security Foundation provozuje na adrese *www.cloutage.org* databázi nahlášených a známých problémů s cloudovými službami.

Celkem bylo k prvnímu lednovému týdnu roku 2011 v databázi zaznamenáno 432 událostí a incidenty jsou rozděleny do pěti základních typů: Automatické selhání zapříčiněné zejména problémy s aktualizací softwaru, ztráta dat či informací způsobená převážně nedostatečně zvládnutými procesy záloh a obnov, dále pak prolomení služby hackery, neplánovaný výpadek (který je nejčastějším problémem) a také objevené zranitelnosti.

Incidenty podle typů
Počty případů z celkových 432 událostí



Zdroj: Open Security Foundation, leden 2011

> Cloudu se není možné vyhnout a trvale ho odmítat.
>
> **JAN MIKULECKÝ,** KONZULTANT PRO ŘÍZENÍ RIZIK, ISMS, BCMS A PENETRAČNÍ TESTY, RISK ANALYSIS CONSULTANTS