Život je změna a změna je život...

K bezpečnosti cloudu přistupujme komplexně a s rozmyslem

Petr Nádeníček

Jak cloud změnil během posledních let náš přístup k informační a ICT bezpečnosti a jak se změnila samotná bezpečnost, aby se vypořádala s novými výzvami, které stále zvyšující se podíl cloudových služeb přináší?

Pod pojmem cloud si můžeme představit poměrně široké spektrum služeb od poskytování určité aplikace (SaaS) až po outsourcing systémových zdrojů, případně další rozmanité varianty. V tomto článku řešíme cloud z pohledu organizace, nikoliv cloudové služby určené primárně pro jednotlivé soukromé uživatele.

Cloud? Raději ne!

Stejně jako v životě i v bezpečnosti nastane čas od času nějaká změna, která věci a potažmo i náš přístup podstatným způsobem změní. Cloud a cloudové služby můžeme za jednu z tohoto druhu změn oprávněně považovat.

Vzpomínám si, že já sám jsem cloud v začátcích neměl ani trošku rád, spíše naopak. A zdůvodňoval jsem si to právě zejména „bezpečností“. Prostě jsem si myslel, že něco, co je vystrčeno úplně mimo fyzický perimetr organizace a mimo její chráněnou síťovou infrastrukturu, je zákonitě nebezpečné, a tedy špatné. Byl jsem „vychováván“ v duchu zásad, že firewall je základ a síť musí být od okolního internetu co nejlépe oddělena, aby data organizace byla v dokonalém bezpečí. Čím víc je síť otevřená, tím větší je i riziko potenciálního průšvihu. Prvotním úkolem bezpečnosti je zajistit se vůči externím hrozbám, další prioritou je ochrana proti možným vnitřním útočníkům, takže nezapomenout na zabezpečení koncových bodů... To byly základní postuláty, díky kterým mi něco jako cloud přišlo z bezpečnostního hlediska jako naprostý nonsens.

Jak šel čas, cloudů, cloudových služeb i jejich uživatelů postupně přibývalo. A bezpečnost tomuto rozmachu kupodivu nebyla překážkou. Ano, jako vždycky byla částečně ignorována, silnějšími argumenty ale asi byla provozní hlediska a náklady. Současně se bezpečnost novému trendu začala pomalu přizpůsobovat. Bezpečnostní specialisté a IT architekti sáhli hluboko do svého arzenálu a obrnili cloudy a jejich obsah takovými prostředky, jako je například silná kryptografie, sofistikované autentizační metody apod. Praxe ukázala, že i cloud lze zabezpečit tak, abychom se vůči existujícím rizikům dostatečně chránili.

Takže, světe, div se, dnes není vůbec neobvyklé, že cloudové služby mají své místo i u organizací, jako jsou banky, které jsou jinak považovány za poměrně konzervativní. Osobně jsem se v dosavadním profesním životě potkal s řadou cloudových řešení a musím uznat, že jejich zavedení pro organizace a jejich IT většinou znamenalo určitý pokrok a dostalo je tak říkajíc na další (vyšší) úroveň, a to při zachování potřebné úrovně bezpečnosti. Zaměstnanci IT většinou oceňují, že se nemusí starat o fyzický hardware, koncovým uživatelům zase vyhovuje snadnější dostupnost IT služeb, vedení organizace si pak v ideálním případě mne ruce nad úsporami.

Funguje to, ale proč?

Úspěch cloudových řešení lze poměrně dobře pochopit z provozního hlediska, ale jak je vůbec možné, že to funguje i v oblasti bezpečnosti? Ano, čas od času se potkáme i s nějakým významnějším průšvihem, který se týká většinou cloudových řešení, která jsou určena pro koncové uživatele (viz např. aktuální kauza vydírání společnosti Apple kvůli jejich službě iCloud), ale celkově se zdá, že tento koncept prostě funguje.

Sám sebe se často ptám, jak je to možné, že jsme se byli schopni s cloudem vypořádat i na poli bezpečnosti. Co je v zabezpečení cloudu jiné než v zabezpečení vlastní infrastruktury?

V první řadě si myslím, že je nutné především změnit svoje myšlení. Je třeba se odpoutat od tradičního uvažování, tedy snahy primárně se zabezpečit tím, že izolujeme svůj perimetr před okolním světem. Naším hlavním objektem zájmu totiž už není naše infrastruktura, aplikace apod., ale především naše informace. Nezabezpečujeme prostředí, zabezpečujeme informace.

Abychom to dokázali, musíme v první řadě znát jejich životní cyklus – kde vznikají, kde se všude vyskytují, kdo k nim má mít přístup, jak je daná informace citlivá, jak moc záleží na její integritě (správnosti) a jak moc musíme zajistit její dostupnost. Tyto parametry nezjistíme sami od sebe nebo jen v rámci IT, ale musíme bezpodmínečně vyjít z požadavků businessu a z jeho procesů.

Kde začít?

Se zabezpečením pak musíme začít u cloudu samotného a u jeho poskytovatele. Jinými slovy, co pokazíme při výběru samotného cloudu a při smluvním zajištění vztahu dodavatel–odběratel, to pak jinými prostředky budeme napravovat většinou obtížně. To znamená, že základní bezpečnostní aspekty a garance musí být již součástí cloudu samotného a jejich garance musí být součástí smlouvy. Sem patří např. základní SLA týkající se dostupnosti služeb, technické podpory, fyzického zabezpečení (např. datových center poskytovatele), zálohování apod.

Dále nesmíme zapomenout na zabezpečení infrastruktury, která zůstala přímo v organizaci, a také na zabezpečení koncových bodů, potažmo jejich uživatelů. Zde se dostáváme k další noční můře dnešních bezpečáků, který se obecně označuje jako BYOD (Bring/Buy Your Own Device). S tímto trendem a také třeba s tím, jak se pořád častěji ve firmách využívá Home Office nebo

obecně práce odkudkoliv, se dále rozvolňují hranice perimetru, ve kterém se data organizace vyskytují a chrání.

Se správnými nástroji

Zde už nám nezbude nic jiného, než sáhnout do repertoáru ověřených technických bezpečnostních opatření. Nezbytným základem je samozřejmě kvalitní řešení pro zabezpečení endpointů (antivirus, personal firewall, případně další ochrany a dohledy, jako např. hlídání aktuálnosti OS a SW) s kvalitní centrální správou, které se musí podrobit i uživatelé vlastních zařízení.

Samostatnou kapitolou je šifrování a šifrovací nástroje. Pokud pracovní stanice cestuje se svým uživatelem, tak kompletní šifrování je zcela na místě. Nezapomínejme ale na možné problémy, které nás mohou ve firemním prostředí potkat, jako je např. ztráta šifrovacích klíčů nebo „nespolupráce“ uživatele v různých vyhrocených situacích. Šifrování dat je často nejlepší ochranou také přímo v samotném cloudu. Ten ho však ne vždy musí podporovat nebo být pro jeho nasazení vhodný.

Dále můžeme, ať již v cloudu nebo mimo něj, ochranu našich informací posílit dalšími nástroji, jako je např. DLP (Data Loss Prevention) nebo SIEM (Security Incident Event Monitoring). Pomocí DLP můžeme efektivně chránit informace a jejich šíření jak na úrovni koncových stanic, tak i na úrovni centrálních komunikačních uzlů. SIEM nám zase pomůže udržet kontrolu nad širokým perimetrem a přehled nad různými událostmi včetně souvislostí mezi nimi.

Nezapomínejme na člověka

I při zabezpečení cloudu nesmíme zapomenout na roli běžného uživatele – člověka. Tím, jak naše informace pouštíme do širšího perimetru bez striktně vymezených hranic, více záleží na tom, aby uživatelé měli dostatečné bezpečnostní povědomí a dokázali s nimi správně zacházet, aby je zbytečně nevystavovali rizikům.

Proto, i když se většina IT organizace nachází „někde v oblacích“, se nevyhneme opakovanému přízemnímu školení uživatelů o tom, jak mají se systémy a aplikacemi zacházet, co mohou a co nesmí v žádném případě dělat a jak se mají zachovat v mezních situacích, když se děje něco nežádoucího.

Něco chytrého nakonec

I když by někdo mohl z cloudu a jeho zabezpečení dělat vědu, v praxi to tak složité určitě být nemusí. Zásadní je, dle mého názoru, zbavit se zažitých a přežitých přístupů a myšlení z doby, kdy jsme ještě měli všechno pěkně zamknuté ve vlastní serverovně. Místo úzkostlivé snahy o maximální izolaci svého IT se musíme zaměřit na to, co je opravdu důležité, což jsou informace. Jednotlivá bezpečnostní opatření pak musíme nasměrovat tímto směrem.

Dalším specifikem zabezpečení tak komplexního řešení, jakým je cloud, je nutnost řešit i bezpečnost komplexně již od samotného začátku. Bezpečnostní požadavky musíme definovat již předtím, než začneme vhodného poskytovatele hledat. Dále je musíme prosadit i do samotného cloudového řešení a hlavně do smlouvy, abychom mohli jejich naplňování účinně vyžadovat.

Byť, jak jsem psal na začátku tohoto článku, se může zdát, že cloud a bezpečnost jsou věci těžko slučitelné, není tomu tak. Bezpečnosti cloudu a v cloudu se bát nemusíme, především v případě, že jsme schopni k problematice přistupovat komplexně a s rozmyslem. A to platí nejen u cloudu... ■

Petr Nádeníček

Autor článku působí na pozici Senior IT Security Consultant ve společnosti AEC, a. s.