Bezpečnostní analýzou cloud prostředí můžete předejít velkým komplikacím

Karin Gubalová

V předchozím dílu našeho seriálu o bezpečnosti cloudu (IT Systems 6/2021, str. 46–47) jsme se věnovali problematice zajištění bezpečnosti cloudu z obecného hlediska. V aktuálním dílu se zaměříme na to, co by si měla organizace ujasnit ještě před tím, než vůbec začne cloudové služby využívat, a jaké konkrétní kroky musí podniknout, aby bylo jejich provozování co nejbezpečnější.

Rizika cloudového prostředí

Minule jsme si ujasnili přehled technických hrozeb v cloudovém prostředí. Pojďme se teď blíže podívat na možná rizika související s governance a na jejich příčiny.

Většina organizací umí dobře posuzovat rizika tzv. on-prem prostředí, tedy v interně provozovaných datacentrech, případně u osvědčeného dodavatele. Pokud se tu objeví nějaký problém, lze ho zpravidla vyřešit s příslušným obchodním zástupcem, protože většinu potřebných oblastí pokrývá outsourcingová smlouva.

V případě cloudových služeb si je potřeba uvědomit, že co se týče smluvních ujednání, tahá naprostá většina zákazníků oproti obřímu globálnímu poskytovali za výrazně kratší konec. Změna standardizovaných smluvních podmínek není často možná dokonce ani v případě, že kontrakt vyjednává nadnárodní mateřská společnost. To nemusí být zásadní problém, je však třeba s tím počítat a příslušná rizika adresovat i jinak než běžnými smluvními ujednáními. V zásadě jde o strategii organizace, o to, jak ke cloudovému řešení přistoupí a jak dobře dokáže definovat svoje požadavky a očekávaní.

Oproti běžnému provozu on-prem se cloudové služby liší v několika základních parametrech:

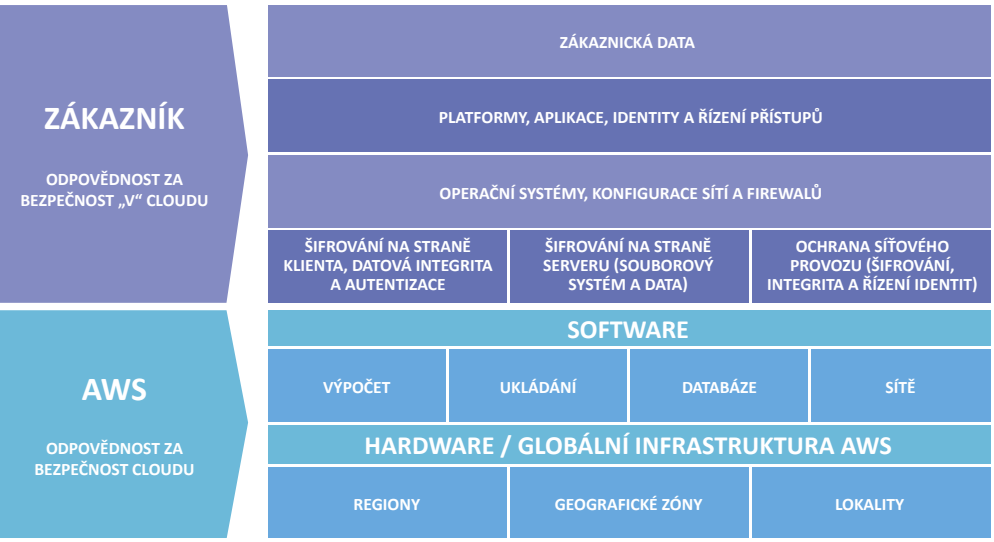
- Sdílení odpovědností mezi zákazníkem cloudové služby a jejím poskytovatelem;
- technický design a provozní řízení cloudové služby v rukou poskytovatele;
- nová rozhraní mezi zákazníkem a jednou nebo více cloudovými službami;
- vlastnictví informací a přístupová práva k uloženým datům, nové otázky týkající se duševního vlastnictví a práva na přístup k datům, která můžou mít regulační a právní orgány.

Dobrá zpráva je, že většina velkých poskytovatelů cloudových služeb bere bezpečnost velice vážně a problematiku závazků a odpovědnosti se svými zákazníky transparentně komunikuje. Například AWS prosazuje tzv. Model sdílené odpovědnosti, kde zákazník dostane přesnou informaci o rozdělení odpovědnosti mezi poskytovatelem a uživatelem. Na obrázku 1 je znázorněno zjednodušené schéma tohoto modelu.

Ujasněte si přístup

Ještě před tím, než padne definitivní rozhodnutí o vstupu do cloudu, si musí společnost zodpovědět i několik ryze strategických dotazů. Ty se však, možná překvapivě, netýkají cloudové technologie jako takové, ale především celkového přístupu organizace ke cloudu. Také proto probíhají tyto úvodní diskuze hlavně na manažerské úrovni, jakkoli je zapojení architektů a specialistů více než žádoucí.

- **Jaká je naše primární motivace?** Například ušetřit, zpřehlednit cashflow, zdokonalit úroveň poskytovaných služeb, možnost využívat řešení, která nejsou dostupná on-prem, zlepšit flexibilitu, předejít masivním investicím, protože je potřebná obnova infrastruktury atp. Motivátorů je celá řada, proto je nutné si hned v úvodní fázi ujasnit, které jsou pro organizaci primární.
- **Co všechno přesuneme do cloudu?** Ačkoliv ve světě existují společnosti, které převedly do cloudu veškerou infrastrukturu, přece jenom je dnes běžnější hybridní model. Zároveň je důležité mít jasno



Obr. 1: Model sdílené odpovědnosti – přehled rozdělení odpovědnosti mezi poskytovatelem a uživatelem cloudu. Zdroj: AWS Shared Security Responsibility Model

v tom, jak bude nové řešení napojené do stávající infrastruktury. Tady se poprvé objevuje aspekt bezpečnosti, protože některá data a procesy jsou pro přechod do cloudu vhodnější než jiná.

- **Jaká omezení plynoucí z příslušných regulačních předpisů se na nás vztahují?** Nevyhnutelná otázka, kterou je potřeba řešit nejenom ve společnostech svázaných celou řadou regulí. GDPR se dnes vztahuje prakticky na všechny, další komplikaci pak může představovat například využívaní asijských datacenter.

Na tomto místě bych ráda zmínila jeden důležitý problém, na který s kolegy z AEC pravidelně narážíme, a to napříč různými společnostmi. Business se často zhlédne v cloudové službě typu SaS (software as a service) a vzhledem k tomu, že technologická implementace je velice snadná, nemá žádnou potřebu kontaktovat IT nebo jiný odpovědný útvar. Potíž je však v tom, že business útvary často v dané věci nedisponují potřebnou odborností a nedovedou dohlédnout všech následků takového rozhodnutí.

Příslušné technické útvary se tak mnohdy dostanou k věci až ve chvíli, kdy je kontrakt dojednaný, nebo v okamžiku, kdy vyvstanou první velké problémy a na bezbolestnou a levnou nápravu už je většinou pozdě. Technické útvary mohou velice dobře pomoci s definicí požadavků na řešení, a proto je prozíravé zapojit je do daného procesu hned od začátku.

Jak řídit rizika v cloudovém prostředí

Jak už bylo řečeno, cloudové služby generují rizika specifických parametrů. Na druhou stranu, pro úplný pohled je třeba vyzdvihnout i nezanedbatelné bezpečnostní benefity těchto služeb. Organizace se může v některých případech přesunem do cloudu určitým stávajícím rizikům úplně vyhnout nebo je alespoň minimalizovat tím, že implementuje bezpečnostní technologie, které nemusejí být pro in-house produkty dostupné. Typickým případem je řízení kontinuity a recovery procesů, kde velcí poskytovatelé v rámci standardního kontraktu nabízejí úroveň záruk, která je pro malá datacentra prakticky nedostižná.

Analýza rizik v cloudovém prostředí by měla zohlednit metodiku využívanou ve společnosti. Důvodem je možnost srovnání rizik a jejich vývoje v čase. Pokud to zdroje umožní, není úplně od věci provést analýzu stávajícího i nového řešení a oba rizikové profily porovnat.

Prvním krokem je, tak jako obvykle, identifikace aktiv. V případě cloudových služeb se postačí zaměřit na obchodní procesy, resp. služby organizace a na informace, kterých se může využití cloudu týkat. Pro každý business case doporučujeme provést samostatné hodnocení z hlediska celkových dopadů na organizace. Oblasti, kde by měla analýza proběhnout, zahrnují organizační a compliance rizika, právní/smluvní a technická rizika. Pravděpodobně zjistíte, že někde bude situace komplikovanější, jinde dojde naopak ke zlepšení rizikového profilu (viz např. zmiňovaná odolnost vůči výpadkům u velkých poskytovatelů).

Určitě je vhodné zahrnout i některá provozní rizika, např. personál, stávající SLA či technickou podporu dodavatele. Nezapomeňte ani na hrozby související s ukončením využívání služby. Všechna data, která společnost přenese do cloudu, jsou v jejím vlastnictví. Avšak již při podepisování smluv a během implementace řešení je vhodné si k nim zajistit možnost přístupu i v případě, že služby vypovíte. Organizace by měla mít vždy takový přístup ke svým datům, který jí v případě potřeby umožní jejich efektivní export.

Poté, co si ujasníte bezpečnostní dopady přechodu do cloudu, přichází na řadu mitigace a řízení rizik. V případě tohoto kroku by se mohla nabízet bezmyšlenkovitá akceptace rizika. My však svým klientům vždy důrazně doporučujeme zamyslet se nad možnými technickými a organizačními řešeními stávající situace. Mnohá z těchto opatření mívají dopad na uživatele a zavádějí procesy, na které nebyli zvyklí. Příkladem může být odlišný způsob ověření uživatele v cloudové službě nebo zavedení klasifikace informací a stanovení pravidel pro jejich zpřístupňování v rámci cloudových služeb. To je typicky potřeba velmi dobře popsat a nastavit v případě využívaní služeb Microsoft O365.

Z technického pohledu je nutné do řízení rizik zapojit architekty, specialisty na síťovou bezpečnost a bezpečnostní monitoring, kteří pomohou navrhnout optimální soubor technických opatření. Dnes je drtivá většina velkých cloudových provozovatelů ve stavu, kdy nabízí velkorysá bezpečnostní řešení. Otázkou však zůstává cena. Podstatné je rozumné využívaní nabízených technologií, případně posouzení každého use casu zvlášť. To zvládne vlastními silami jen málo společností, pozitivní však je, že pokud se obrátíte na odborníky, je velmi pravděpodobné, že vám to do budoucna ušetří finanční prostředky.

Součástí implementace cloudového řešení musí být jednoznačná akceptace rizik a navrhovaných opatření včetně odpovědnosti za průběžné monitorování. Důležité je mít přitom na paměti, že proces řízení rizik je nikdy nekončící aktivita. ■

Karin Gubalová

Autorka článku vede divizi Risk & Compliance ve společnosti AEC a.s.