Bezpečnostní architektura cloudu

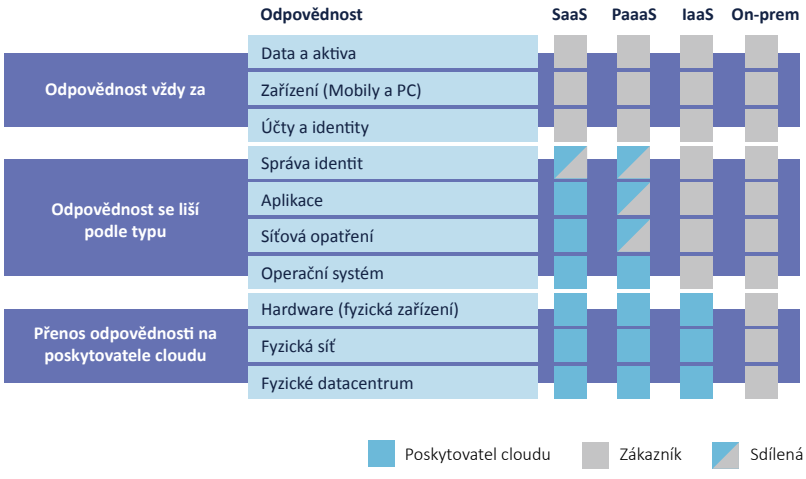
Matej Kačic

Není pochyb o tom, že cloud computing dnes mění výrazným způsobem dynamiku byznysu a firmám otevírá dosud netušené příležitosti. Problém je, že řada společností má za to, že přechod do cloudu je zbavuje nutnosti starat se o bezpečnost. Opak je pravdou. Zákazník cloudu zůstává i nadále vlastníkem svých dat a své identity. Jednou z nejzajímavějších možností, jak je ochránit, je využít bezpečnostní koncept Zero Trust, jehož hlavní zásadou je nikomu a ničemu nevěřit.

Rozdělení zodpovědnosti

Náročnost zabezpečení dat a rozdělení zodpovědnosti za bezpečnost a provoz cloudových služeb mezi providerem a firmou se odvíjí podle použitého modelu cloudu. Zjednodušeně řečeno, odpovědnost se liší v závislosti na tom, zda je práce hostována v softwaru jako služba (SaaS), v platformě jako služba (PaaS), infrastruktuře jako služba (IaaS) nebo v místním datovém centru.

Obr. 1: Rozdělení odpovědnosti podle typu cloudu.



Porovnáme-li zabezpečení dat v případě standardní infrastruktury a bezpečnost poskytovanou datovými centry (kdy musíme řešit bezpečnost na celé frontě), zjistíme, že s posunem do cloudu nám řada problémů odpadá. Ale zdaleka ne všechny. Přehled na obrázku 1 znázorňuje, jak se liší zodpovědnost podle typu cloudu.

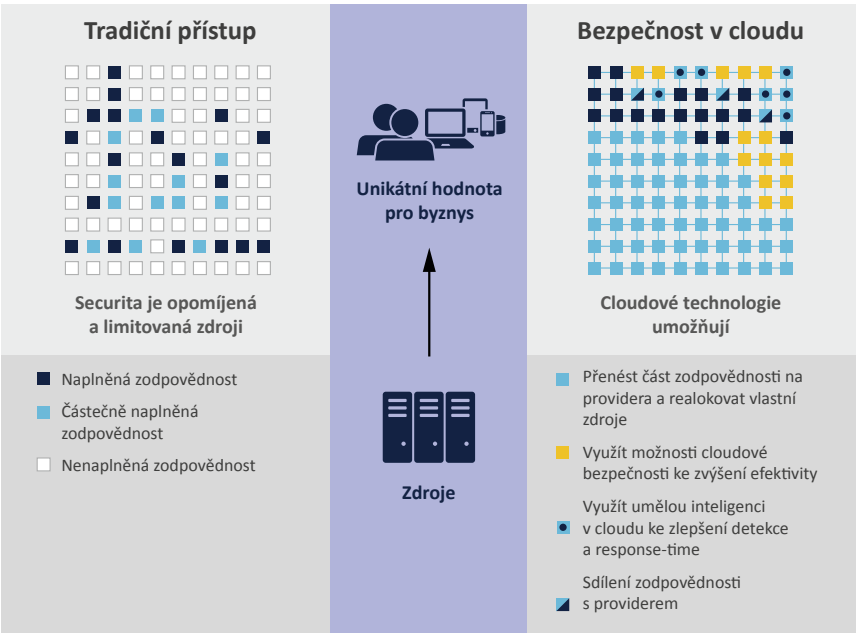
Některé firmy se stále domnívají, že přechod do cloudu je zbaví nutnosti starat se o bezpečnost. Opak je však pravdou. Ať už jste v cloudu, nebo ne, vždy a za každých okolností musíte mít na zřeteli bezpečnost svých dat, své identity, své koncové stanice. Další schéma (obr. 2) ukazuje, jak se liší tradiční přístup, při němž téměř nikdy nedosáhneme na úplnost bezpečnostních opatření, od přístupu v cloudu, v rámci něhož nám velkou část bezpečnostních opatření zajistí cloud provider.

Zákazníci cloudu by v žádném případě neměli propadnout pocitu, že cloud je vždy a za každých okolností bezpečný. Právě naopak, zodpovědnost za vlastní bezpečnost je naprosto zásadní a nikdy by neměla být brána na lehkou váhu.

Společnost Microsoft v jednom ze svých komentářů ke sdílené odpovědnosti v cloudu zdůrazňuje: „U všech typů cloudového nasazení vlastníte svá data a identity. Jste zodpovědní za ochranu zabezpečení svých dat a identit, místních zdrojů a cloudových komponent, které ovládáte... Bez ohledu na typ nasazení si vždy ponecháte následující povinnosti: data, koncové body, účet a řízení přístupu.“

Zero Trust model

Jak už sám název napovídá, hlavní zásadou Zero Trust modelu je nedůvěřovat nikomu a ničemu a vždy všechno ověřovat. Mějte na paměti, že útočníci jsou dnes všude – uvnitř i vně sítě. To znamená, že počítače ve výchozím nastavení, ale ani samotní uživatelé by z principu nikdy neměli být automaticky důvěryhodní. Musíte předpokládat, že veškerý provoz, bez ohledu na to, jakým způsobem je řešený, vás může ohrozit. Vždy znovu ověřujte, autorizujte, kontrolujte, zajišťujte.



Obr. 2: Schematické znázornění rozdílů mezi tradičním přístupem k bezpečnosti, při němž téměř nikdy nelze dosáhnout na úplnost bezpečnostních opatření, od přístupu v cloudu, v rámci něhož velkou část bezpečnostních opatření zajistí cloud provider.

Zero Trust propaguje princip at-least-priviledge, umožňující uživatelům přístup pouze k těm zdrojům, které potřebují k plnění svých povinností. Problém je, že dnešní moderní aplikace navíc často poskytují rozsáhlá oprávnění ke komponentám, které tvoří distribuovanou architekturu, tato oprávnění však zůstávají ve standardním nastavení. V horším případě se oprávnění pouze přidávají a vznikají tzv. super uživatelé.

Webové aplikace jsou obzvláště zranitelné. Pokud vývojář například neblokuje porty na firewallu konzistentně nebo implementuje nevhodným způsobem oprávnění, bude mít hacker, který aplikaci převezme, oprávnění načítat a upravovat data z přímo z databáze.

Zero Trust navíc v případě síťové vrstvy využívá mikrosegmentaci, tedy způsob vytváření drobných bezpečných zón v datových centrech nebo v cloudech. Tyto zóny mohou být plně kontrolovány například IPS systémem. Granularita bezpečnostních politik je tím pádem výrazně větší a zabezpečení sítě mnohem podrobnější, protože tím získáme větší vizibilitu.

Zero Trust model účinně minimalizuje útoky a zajišťuje celou řadou sofistikovaných způsobů bezpečnosti. Ta je díky tomuto řešení všudypřítomná a – což je mimořádně důležité – v celém prostředí proaktivní.

Jak definovat správné bezpečnostní požadavky?

Při zajištění bezpečnosti v cloudu doporučujeme aplikovat plný Zero Trust model, který poskytuje ochranu:

- **Uživatelů** – zajišťuje, aby přístup k vašim datům byl udělen výhradně oprávněným osobám, a to pouze poté, co byla jejich identita důkladně ověřena pomocí jednotného přihlašování (Single Sign-On) a silné kryptografie. Při ověřování zohledňujeme i kontext geografické polohy připojení a chování uživatele při přihlašování a následnou detekci anomálií.
- **Sítí** – v rámci tohoto řešení nasazujeme granulární segmentaci sítě napříč veřejným i soukromým cloudem a v případě hybridního prostředí i LAN. Bezpečnostní politiky jsou unifikovány ve všech prostředích a řídí se z jedné centrální správy. Zajišťujeme detailní náhledy uživatelů, skupin, aplikací, zařízení a všech typů připojení k internímu prostředí. Model vynucuje princip „at Least Privileged" na úrovni síťové vrstvy tak, aby k firemním aktivům měli přístup pouze oprávnění uživatelé a prověřená zařízení.
- **Zařízení** – infikovaným zařízením blokujeme přístup k firemním datům a aktivům, a to včetně mobilních zařízení a pracovních stanic zaměstnanců, zařízení IoT a průmyslových řídicích systémů.
- **Dat a aktiv** – model proaktivně chrání data před krádeží, jejich poškozením či neúmyslným smazáním, kdekoliv jsou uložena. Data musí být šifrována, a to jak data in-rest, tak data in motion.
- **Výpočetních služeb** – sem patří například virtuální infrastruktura v cloudu, Docker kontejnery, aplikace apod. Tyto typy prostředků jsou v cloudu vysoko distribuované a škálovatelné, přičemž životnost kontejnerů je často velmi krátká (dochází znovu k postupnému znovuvytvoření celé infrastruktury). Zabezpečení ochrany těchto prostředků je realizováno formou rozhraní API, která jsou integrována přímo na vývojový proces a bezpečnostní workflow.

Zero Trust model akcentuje 3 základní principy:

- **Úplnost** – bezpečnostní opatření musí být úplné a na každé úrovni. Částečné nasazení se nepřipouští. Vždy vycházíme z předpokladu, že nám každý okamžik a na jakémkoli místě hrozí bezpečnostní problém.
- **Efektivita** – bezpečnost musí být účinná a snadno udržitelná; optimálně by neměla nijak významně zvyšovat požadavky na pracovní sílu, protože zavádí prvky automatizace.
- **Prevence** – bezpečnostní opatření jsou preventivní a okamžitá, předpokládá se vyspělá ochrana proti Zero Day hrozbám a pokročilým útokům.

Cloud nezná hranice

Naše základní premisa zní: cloud je všude. Cloud jako takový nemá hranice. V enterprise prostředí se stává běžnou praxí použití multicloud strategie k zajištění vysoké dostupnosti, geo dostupnosti a minimalizaci vendor locku. Tento přístup s sebou však přináší další problémy – musíme vynutit konzistentně bezpečnostní politiku napříč všemi prostředími. Tato prostředí musíme bezpečným způsobem navzájem propojit. Důležité je, abychom byli schopni zajistit v multicloud prostředí plnou vizibilitu do všech částí a aby byla správa bezpečnostních politik a vyhodnocování bezpečnostních incidentů realizována z jednoho místa.

Jako hardening je označován proces zabezpečení konfigurace systému takovým způsobem, který omezí výskyt zranitelností využitelných útočníkem. V dnešní době je hardening systémů jedním ze základních bezpečnostních opatření pro ochranu informací a informačního systému společnosti.

Automatizace

Automatizace v cloudu je široký pojem, který označuje procesy a nástroje, které organizace používá ke snížení manuálního úsilí

spojeného se zajišťováním a správou cloudových prostředků. Součástí automatizace je i nasazení bezpečnostních opatření včetně hardeningu, firewallových pravidel, distribuce certifikátů a podobně.

V případě nasazení automatizace bezpečnosti redukujeme v těchto operacích lidský faktor. Máme-li takové bezpečnostní opatření nasazeno a otestováno, můžeme se spolehnout, že je tomu tak natrvalo a bezchybně. Dalším dobrým příkladem je nasazení rychlého protiopatření jako reakce na detekovanou hrozbu nebo útok. Představme si, že systém pro detekci zranitelností objevil kritickou zranitelnost v aplikačním serveru, který je použit v Docker infrastruktuře skládající se z více než tisíce uzlů v multicloudovém prostředí. Automatizační úkol může být navázán na tuto detekci a okamžitě aplikuje IPS pravidlo, které tuto zranitelnost mitiguje.

Důležité je, aby bezpečnostní architektura podporovala automatizační procesy již od samého začátku. V optimálním případě doporučujeme vystavět a spravovat cloud infrastrukturu výhradně pomocí automatizace. Tak vzniknou konfigurační a bezpečnostní šablony, které jsou aplikovány dynamicky a adaptivně, bez zásahu člověka. Daný přístup zároveň může z velké části nahradit technickou dokumentaci prostředí.

Nejčastější bezpečnostní problémy firem v cloudu

V rámci služeb jsme již realizovali několik bezpečnostních auditů cloudu v různých segmentech. Zde uvádíme nejčastější bezpečnostní problémy:

- **Chybná autentizace uživatelů** – autentizace druhým faktorem není vynucena pro všechny uživatele a administrátory, nově zakládaní uživatelé nemají tuto ochranu automaticky vynucenou, případně je nasazena pouze sms autentizace, které se důvěřuje. Není použit princip SSO.
- **Administrátoři cloudu nemají rozdělené role** – řada ze zákaznických prostředí nemá v rámci administrace cloudu nasazen princip Segregation of Duties. Pro běžnou správcovskou činnost používají administrátora s nejvyšším oprávněním.
- **API rozhraní nejsou dostatečně zabezpečená** – autentizace v rámci API používá sdílená hesla (secret) a nepoužívá silné certifikáty. API mají většinou všechna práva, i když je nepotřebují. I zde doporučujeme použít at least privileged přístup.
- **Nulová vizibilita** – provozní i bezpečnostní logy nejsou analyzovány a v některých případech ani sbírány. Zde je nutné si uvědomit, že administrační konzole cloudu neposkytuje plnohodnotné pohled na logy, je tedy nutné nasadit nástroje, které nám to zajistí.
- **Není prováděn konfigurační bezpečnostní audit** – zákazník se skoro vždy po migraci do cloudu nebo po nasazení nové funkcionality soustřední pouze na stránku provozu, a nikoli na bezpečnost. Je nutné si uvědomit, že cloud je stále se měnící prostředí, a proto je nutné sledovat, jak se dané moduly změnily. Mnohokrát se stalo, že již nasazená bezpečná konfigurace se po aktualizaci, respektive po změně v cloudu stala nebezpečnou.
- **Není nasazen management zranitelností** – veřejný cloud obsahuje mnoho zranitelností, které sice nemůžeme záplatovat, ale je možné pomocí konfigurace minimalizovat riziko do té doby, než je poskytovatel cloudového prostředí opraví. Zranitelnosti obsahuje například i vlastní kód nebo kontejnery operačních systémů stažené z oficiálních stránek.
- **Nedostatečné řízení přístupových oprávnění** – většina zákazníků využívá spolupráce v rámci cloudu ke zvýšení efektivity práce. Na druhé straně však stojí nekontrolovatelné sdílení v rámci organizace i mimo ni.
- **Nedostatečně ošetřený hostitelský (guest) přístup** – v rámci cloud prostředí se předpokládá spolupráce mezi organizacemi. Špatné procesy a nastavení způsobují, že externí entita má přístup k interním aktivům organizace.
- **Uživatel používá prostředky cloudu na neautorizovaném zařízení** – není vynucována autentizace pracovních stanic a zařízení. Uživatel po přihlášení může používat například OneDrive na svém soukromém zařízení. To znamená, že je zcela legitimně schopen odsychronizovat firemní data ven.
- **Není kontrolován bezpečnostní stav zařízení** – po migraci do cloudu organizace zapomínají na zabezpečení koncových stanic, na kterých se může objevit malware nebo ransomware. Je nutné, aby byla stanice před přístupem k citlivým datům prověřena a označena za bezpečnou.
- **Cloud data nejsou zálohována** – 90 % zákazníků má zpočátku mylnou představu o tom, že data v cloudu jsou zálohována. V případě výpadku nebo chyby cloud poskytovatele může dojít k úplné ztrátě dat. Proto doporučujeme zálohovat všechna data v cloudu (OneDrive, SharePoint, Teams, e-mail, databáze) do offline lokality.

Závěr

Výše uvedený přehled bezpečnostních problémů firem v cloudu zahrnuje jen ty nejpalčivější. I tak se jedná o celkem názornou ukázku toho, s čím mohou být uživatelé cloudových služeb denně konfrontováni. Je zřejmé, že jediným správným přístupem odpovídající možnostem, které cloud computing poskytuje, není bohorovný klid, ale naopak proaktivní přístup. Řešením je trvalé úsilí vedoucí ke kvalitnímu zabezpečení dat a zařízení, ideálně za pomoci ověřeného bezpečnostního modelu, a dále ke správnému nastavení procesů a jasnému rozdělení kompetencí. ■

Matej Kačic

Autor článku působí na pozici Head of Security Technologies Division ve společnosti AEC.