

IBM: Bezpečnost v cloudu zůstává nadále výzvou

Cambridge, 17. července 2020 – Společnost IBM zkoumala hlavní výzvy a hrozby, které mají dopad na zabezpečení cloudu. Snadnost a rychlost nasazení nových cloudových nástrojů může mnohdy ztěžovat týmům zabezpečení kontroly nad jejich používáním. Podle údajů průzkumu společnosti IBM a analýzy případové studie zůstávají základní problémy s bezpečnostním dohledem, včetně zranitelností a chybných konfigurací, hlavními rizikovými faktory, které by organizace měly řešit, aby pomohly zabezpečit své stále čtenější používání cloudu. Případová studie bezpečnostních incidentů za poslední rok také osvětluje, jak se kybernetičtí zločinci zaměřují na cloudová prostředí pomocí přizpůsobeného malwaru, ransomwaru a dalších.

Přechod do cloudu a bezpečnost

Vzhledem k tomu, že podniky rychle přecházejí na cloud, aby vyhověly požadavkům na vzdálenou pracovní sílu, je pro řízení rizik nezbytné pochopit jedinečné bezpečnostní výzvy, které tento přechod představuje. I když cloud umožňuje mnoho důležitých obchodních a technologických možností, jeho přijetí ad-hoc a správa cloudu může také přinést komplikace pro týmy IT a kybernetické bezpečnosti. Podle společnosti IDC více než třetina společností zakoupila v roce 2019 30+ typů cloudových služeb od 16 různých dodavatelů. Toto distribuované prostředí může vést k nejasnému vlastnictví bezpečnosti v cloudu a zranitelnosti IT.

S cílem získat lepší představu o nové bezpečnostní realitě, když se společnosti rychle přizpůsobují hybridním, multi-cloudovým prostředím, prozkoumaly IBM Institute for Business Value (IBV) a IBM X-Force Incident Response and Intelligence Services (IRIS) jedinečné výzvy, které mají dopad na bezpečnostní operace v cloudu a také hlavní hrozby zaměřené na cloudová prostředí.

Co všechno má vliv na bezpečnost?

Až 66 % dotázaných uvedlo, že se spoléhají ohledně základního zabezpečení na poskytovatele cloudu; přesto se vnímání zabezpečení respondenty značně lišilo napříč konkrétními cloudovými platformami a aplikacemi.

Nejobvyklejší cestou pro zločince ke kompromitaci cloudových prostředí byly aplikace založené na cloudu, což představuje 45 % incidentů v případových studiích souvisejících s cloudem IRIS IBM X-Force IRIS. V těchto případech využívali kybernetičtí zločinci chyby v konfiguracích a zranitelnosti v aplikacích, které často zůstaly nezjištěny kvůli zaměstnancům, kteří si sami postavili nové cloudové aplikace mimo schválené kanály.

Zatímco krádež dat byla hlavním dopadem studovaných cloudových útoků, hackeři se také zaměřili na těžbu kryptoměn a ransomware, a pomocí cloudových zdrojů zesílili účinek těchto útoků.

„Cloud má obrovský potenciál pro efektivitu podnikání a inovace, ale může také přinést mnoho komplikací, pro organizace a firmy, které používají cloudová prostředí od mnoha dodavatelů,“ říká Abhijit Chakravorty odpovědný ve společnosti IBM za bezpečnost Cloudu. „Když to uděláme správně, cloud může učinit bezpečnost škálovatelnou a přizpůsobivější, ale nejdřív musí organizace opustit staré návyky a musí začít uplatňovat nové bezpečnostní přístupy navržené speciálně pro tyto nové technologie, využívající automatizaci všude, kde je to možné.“ Organizace, které jsou schopny zefektivnit cloudové a bezpečnostní operace, mohou snížit své riziko prostřednictvím jasně definovaných zásad, které se vztahují na celé IT prostředí.

Hlavní hrozby v cloudu: Krádež dat, těžba kryptoměn a ransomware

Abychom získali lepší představu o tom, jak útočníci cílí na cloudová prostředí, provedli odborníci na odezvu incidentů X-Force Incident Response and Intelligence Services hloubkovou analýzu případů souvisejících s cloudem, na které tým reagoval v uplynulém roce. Analýza zjistila, že finančně motivovaní kyberzločinci byli nejčastěji pozorovanou kategorií nebezpečných skupin zaměřujících se na cloudové prostředí v případech reakce na incidenty IBM X-Force, přestože přetrvávajícím rizikem jsou také národní aktéři.

Nejběžnějším vstupním bodem pro útočníky byly cloudové aplikace, včetně taktiky, jako je násilné zneužití zranitelných míst a nesprávná konfigurace. Zranitelnosti často zůstaly nezjištěny kvůli „stínovému IT“, když zaměstnanec jde mimo schválené kanály a postaví zranitelnou cloudovou aplikaci.

Ransomware byl nasazen 3x více než jakýkoli jiný typ malwaru v cloudových prostředích v případech incidentů, následovaly těžba kryptoměn a malware z botnetu.

Kromě nasazení malwaru byla krádež dat nejčastější hrozbou, kterou IBM pozorovala v porušených cloudových prostředích za poslední rok, od osobních identifikačních informací (PII) po e-maily související s klienty.

„Na základě trendů v našich případech odezvy na incidenty je pravděpodobné, že se případy malwaru zaměřující se na cloud budou i nadále rozšiřovat a vyvíjet se zvyšujícím se přijetím cloudu,“ poznamenal Charles DeBeck z IBM X-Force Incident Response and Intelligence Services. Průzkum od IBM Institute for Business Value zjistil, že reagující organizace, s vysokými znalostmi v oblasti cloudu a zabezpečení, byly schopny identifikovat porušení dat rychleji než kolegové, kteří byli stále v raných fázích své cesty k přijetí cloudu. Pokud jde o dobu odezvy na narušení dat, nejrozvinutější zkoumané organizace byly schopny identifikovat a omezit porušení údajů dvakrát tak rychle jako nejméně zralé organizace (průměrná životnost hrozby 125 dní vs. 250 dnů).

Jak zlepšit bezpečnost v cloudu

Přijměte sjednocenou strategii, která kombinuje cloudové a bezpečnostní operace napříč vývojáři aplikací, IT operací a zabezpečení. Určete jasné zásady a odpovědnosti za stávající cloudové zdroje i za získávání nových cloudových zdrojů.

Zhodnoťte druhy pracovního vytížení a data, která plánujete přesunout do cloudu, a definujte vhodné zásady zabezpečení. Vytvořte plán pro postupné zavádění cloudu.

Využijte zásady a nástroje pro správu přístupu ke cloudovým prostředkům, včetně multifaktorového ověřování, abyste zabránili infiltraci pomocí odcizených údajů. Omezte privilegované účty a nastavte všechny skupiny uživatelů na nejméně požadovaná oprávnění, abyste minimalizovali poškození způsobené kompromitováním účtu (model nulové důvěryhodnosti).

Zajistěte, aby nástroje pro monitorování bezpečnosti a odezvy byly účinné ve všech prostředcích cloud a on-premise. Zvažte přechod na otevřené technologie a standardy, které umožňují větší interoperabilitu mezi nástroji. Implementace účinné automatizace zabezpečení ve vašem systému může pomoci zlepšit možnosti detekce a reakce.

Více o studii najdete: [zde](#).

Pro další informace kontaktujte:

IBM Česká republika

Vladislav Doktor

External Communications Manager

Tel.: + 420 733 149 624

E-mail: vladislav.doktor1@ibm.com

<https://cz.newsroom.ibm.com/2020-07-17-IBM-Bezpecnost-v-cloudu-zustava-nadale-vyzvou>