IT Systems
www.SystemOnLine.cz
Číslo 5/2023
Ročník 25
130 Kč/5,65 €
Květen/Máj

Drobečky nejsou na e-shopu maličkost

Navigační prvky ovlivňují zákaznickou zkušenost

Bez AI bychom dnes nemohli fungovat,

říká Ondřej Nešpor, technický ředitel tržiště Biano

Nová generace platebních řešení

Jaké výhody nabízí A2A platby?

DTM Connector

usnadní digitalizaci map

Komunikace ve firmách

stále čeká na digitální disrupci

Chyby v konfiguraci cloudu

vedou k problémům se zabezpečením

Příloha IT pro výrobní podniky 1/2023

9 771212 456008 05

Quo vadis, e-commerce? • Transformace e-commerce díky AI • Cloud je motorem digitální transformace • ESG a nefinanční reporting • Role DevOps v digitální transformaci • Vývoj UPS pomáhá bezpečnosti i udržitelnosti • Bezpečnost při zavádění kontejnerů • Synology Surveillance Station

Chyby v konfiguraci cloudu představují zranitelná místa a vedou k problémům se zabezpečením

Petr Kocmich

Zahraniční, ale i české organizace pokračují s přesunem svých IT systémů a dat do cloudového prostředí. Přechod do cloudu však není jen o migraci dat, ale i o změně přístupu správců, a to mnohdy přináší nové výzvy a konfigurační postupy. Pak se jednoduše může stát, že se při migraci něco opomene ošetřit, nastavit či obecně nakonfigurovat podle „best practice“. Tak vznikají tzv. miskonfigurace a díky nim firmy následně zbytečně čelí většímu počtu útoků, než tomu bylo dříve a nedokáží se jim adekvátně bránit.

Jak cloudové, tak on-premise řešení nabízí jasné výhody a řeší konkrétní výzvy a potřeby organizací. Vzít a přesunout kompletně lokální IT infrastrukturu bez potřebných změn do cloudu (tzv. Lift & Shift přístup) je však častou chybou, které se dopouštějí. Oba typy prostředí – ať už on-premise či cloudové – přinášejí výhody i nevýhody, a proto se lze u zákazníků často setkat s hybridními prostředími. Důvodem pro toto řešení bývá buď legislativní požadavek (z pohledu citlivosti dat a toho, kde se taková data smějí či nesmějí nacházet), nebo architektury a komplexity legacy aplikací, které se nedají v cloudu provozovat vůbec, či s nutnou, avšak nepřiměřenou investicí a vypětím sil.

Ohýbání stavu není přijatelné

Migrace do cloudu může organizacím pomoci snížit náklady na IT (v případě správného využívání cloudových prostředků), získat kdykoliv vyšší, a hlavně škálovatelnější výkon, zvýšit flexibilitu úložiště, zjednodušit a zrychlit nasazení systémů a aplikací a zároveň získat přístup k datům a systémům odkudkoliv, kdykoliv, a to 365 dní v roce.

Nasazení cloudu z kybernetického hlediska však může zvýšit pravděpodobnost napadení organizací. Pokud padne rozhodnutí „pojďme do cloudu“, musí se k němu přistupovat zodpovědně. V první řadě je zapotřebí si uvědomit, že cloud jako takový je sdílená zodpovědnost mezi poskytovatelem cloudových služeb a zákazníkem, cloud tedy není nikdy samospasný. Můžeme se samozřejmě bavit o výběru správného modelu (IaaS/PaaS/SaaS), ale pokud chceme ulevit internímu IT/SEC týmu, správnou cestou by měl být model PaaS a SaaS, kde většina zodpovědnosti spadá právě na poskytovatele cloudových služeb. Příležitost přechodu do cloudu se navíc musí pojmout jako šance na přechod k modernímu a bezpečnému řešení firemní infrastruktury. Zároveň se nesmí zapomenout zapojit bezpečnostní oddělení, které by mělo být fundamentální a integrální součástí každého podobného projektu.

Bohužel většina cloudových migrací mnohdy znamená jen ohýbání a přesun stávajícího stavu. Z toho vyplývá, že je zapotřebí začít využívat ideálně nativních cloudových prostředků, což v mnoha ohledech znamená přeměnu stávajících monolitických aplikací. V opačném případě obyčejným přesunem systémů a dat společnosti nic nezískají, a s největší pravděpodobností je to bude stát více finančních prostředků než původní řešení v on-premise.

V hlavní roli miskonfigurace

Zatímco v případě on-premise řešení jsou dnešní společnosti poměrně dobře vybaveny nástroji pro monitoring stavu a kontrolu zabezpečení z pohledu zaběhlých a ověřených standardů, pro migraci do cloudu tomu tak být nemusí. Chybné konfigurace cloudu představují zranitelná místa, která čekají, až si jich útočníci všimnou. Jde o vstupní brány, prostřednictvím kterých je možné infiltrovat nejen cloudovou infrastrukturu, ale díky propojení a hybridnímu režimu i laterálně přesunout do stávající on-premise části infrastruktury, kde je pak možné exfiltrovat data, přístupové údaje, telemetrická data strojů v OT prostředí, zdravotní záznamy či osobní údaje, a to vše třeba zakončit nasazením ransomwaru.

Podle odborníků má průměrný podnik každý rok stovky chybných konfigurací, ale o převážné většině z nich jejich IT oddělení vůbec netuší. Všechny chybné konfigurace jsou přitom výsledkem lidské chyby a chybějících nástrojů na kontrolu konfiguračního stavu cloudu (např. tzv. CSPM – Cloud Security Posture Management).

Dopad chybné konfigurace cloudu na zabezpečení systému

Při migraci systémů dost často dochází i k tomu, že vybrané služby, které byly dostupné v rámci on-premise řešení jen

interně, jsou po migraci vystaveny veřejně na internetu, bez filtrování a blokování externího síťového provozu. Tímto nešvarem trpí mnoho společností, a dokonce mnoho z nich spadajících pod kritickou infrastrukturu. Může se tedy stát, že se na internetu objeví veřejně dostupné konzole pro ovládání průmyslových řídících systémů. Nedávno jsme takto detekovali konzoli ICS systému pro ovládání výrobní a montážní linky – bez nutnosti ověření. Běžným folklórem jsou služby obsahující zneužitelné zranitelnosti bez dodatečného zabezpečení, které bylo nasazeno v on-premise řešení, ale v cloudu se již nebo ještě neimplementovalo (např. chybějící WAF – Web Application Firewall) a dále služby s výchozími přístupovými údaji a služby sloužící ke vzdálené správě interních systémů zákazníka nebo dokonce volně přístupná data citlivého charakteru.

Proto, přičemž statistiky našeho dohledového centra to jen potvrzují, následně dochází k desítkám až stovkám incidentů měsíčně. Chybné bezpečnostní konfigurace se stávají snadným cílem útočníků, kteří dobře vědí, že je má téměř každý podnik. Toto zanedbání může mít katastrofální následky. Útočníkům pomáhá v rekognoskaci a infiltraci do zákaznického prostředí, vytvoření permanentních vazeb pro vzdálený přístup, ovládnutí systémů, exfiltraci dat, ale například i přihlašovacích údajů, které jsou následně prozrazeny nebo prodány a použity k dalším útokům. Případně otevírá dveře postranním ransomware nebo cryptojacking útokům, při nichž jsou zneužívány cloudové výpočetní zdroje k podpoře kryptotěžebních aktivit.

Kroky pro minimalizaci rizik miskonfigurací

Správa, a především sledování konfigurace, vyžaduje mnohostranný přístup.

Organizace by měly zavést osvědčené bezpečnostní postupy, jako je pravidelné hodnocení stavu zabezpečení cloudu (Cloud Security Posture Management), které pomohou odhalit řadu bezpečnostních prohřešků a miskonfigurací. Je nutné dodržovat zásadu Least-Privilege a průběžně monitorovat a auditovat cloudové systémy.

Udržování dostatečné viditelnosti cloudových aktiv by mělo být prioritou, stejně jako v rámci on-premise. Dále pomůže silný Identity & Access Management, který umožní škálovat oprávnění, aby byla zajištěna správná úroveň přístupu ke cloudovým službám.

Identifikací různých chybných konfigurací při migraci do cloudu a jejich vyvarování podnikům pomůže odstranit hlavní bezpečnostní problémy. S tím dokážou pomoci specializované firmy, které organizaci provedou celým procesem a vše správně nastaví. ■

Petr Kocmich

Autor článku je Global Cyber Security Delivery Manager ve společnosti Soitron.

Nejslabším článkem zabezpečení firem a rizikem pro jejich data jsou stále zaměstnanci

-tz-

Nejslabším článkem zabezpečení firem jsou stále zaměstnanci. Většinou neúmyslně. Mohou klikat na nebezpečné odkazy nebo otevírat zavirované přílohy. Neuváženě mohou předávat firemní data nedůvěryhodným zdrojům, v krajním případě i hackerům, nebo rovnou podvodníkům posílat firemní finanční prostředky. Nově na ně útočí i umělá inteligence v podobě naprogramovaných chatbotů, jejich kvalita roste stejně jako riziko, že nás obelstí. Novým rizikem je populární nástroj ChatGPT, do kterého zaměstnanci vkládají citlivá firemní data, aniž by si uvědomovali, že se tak stávají součástí tréninkových dat umělé inteligence.

Nebezpečné klikání stále vede

Podle výsledků simulovaných útoků v rámci testování odolnosti firem, pětina zaměstnanců klikne na odkaz ve zprávě, aniž by si prověřila, kam směřuje. Přitom phishingové léčky mohou způsobit firmám katastrofální škody. Zacílení na jednotlivce je velmi účinná technika, mnoho zaměstnanců stále kliká na phishingové e-mailové odkazy a stahuje přílohy se škodlivými soubory.

„Riziko pro firemní data a celkovou bezpečnost, které přichází od zaměstnanců je stále velmi vysoké. A phishingové útoky, které hackeři vedou přes zaměstnance jsou velmi účinné. Firmy mají stále ve vzdělávání svých