# Jaké bezpečnostní nástroje potřebujeme v cloudu?

Matej Kačic

Cloud nemá hranice a z pohledu bezpečnosti to platí dvojnásob. Řešením zabezpečení v cloudu je automatizace, která redukuje případné negativní vlivy lidského faktoru a zároveň umožňuje provádět veškerá bezpečnostní opatření nativně, rychle a efektivně. Tři základní typy technologií, které dokážou nahradit řešení známá z on-premise prostředí a zajistí bezpečnost v cloudu, jsou Cloud Security Posture Management, Cloud Workload Protection Platform a Cloud Access Security Broker.

## Bezpečnostní prostředky cloudu na všechno nestačí

Podle společnosti Gartner bude do roku 2025 více než 99 % všech bezpečnostních chyb v cloudu způsobeno jeho zákazníky. Prognóza amerických specialistů, kteří se dlouhodobě zaměřují na výzkum a poradenství v oblasti ICT technologií, se opírá o současný trend, kdy je řada uživatelů cloudu přesvědčená, že toto prostředí je samo o sobě bezpečné, že neobsahuje žádné zranitelnosti, a tudíž se o jeho bezpečnost není třeba starat. Máloco je vzdálenější pravdě.

Spoléhat se v dnešní době pouze na bezpečnostní prostředky cloudu nestačí. Jeho prostředí je velmi flexibilní, a to, co zde platí dnes, už nemusí platit zítra. Zabezpečení dat, aktiv, zařízení, účtů nebo identity spadá plně do zodpovědnosti zákazníka, žádný cloudový provider za ně odpovědnost nenese. Míra zodpovědnosti se přitom liší podle režimu, který si konkrétní zákazník zvolí. Naopak na providera lze přenést částečně správu identit, dále síťová opatření, správu operačních systémů, případně fyzickou bezpečnost.

## Klíčem je centralizace a automatizace bezpečnostních řešení

Jaká bezpečnostní řešení se nám nabízejí v případě on-premise prostředí? Samozřejmostí je nasazený antivir, dále je tu EDR řešení a SIEM, které ideálně monitoruje osvědčený security operations tým. Je zde síťová ochrana, jako je Next Generation Firewall (NGFW) nebo Web Aplications Firewall (WAF). Provádíme hardening, patch management, aplikujeme řešení Data Lost Prevention (DLP) a chráníme své servery pomocí Email Gateway. Tyto nástroje a technologie však nemůžeme použít v cloudu. V případě cloudového prostředí máme k dispozici tři základní typy technologií, které nám zajišťují bezpečnost a zároveň nahrazují řešení známá z on-premise:

- Cloud Security Posture Management (CSPM), který obstarává compliance a hardening celého cloudového prostředí.
- Cloud Workload Protection Platform (CWPP) zajišťující vizibilitu a ochranu před hrozbami.
- Cloud Access Security Broker (CASB), což je jakási brána mezi on-premise prostředím a cloudovým prostředím.

Zabezpečení v cloudu je typickou ukázkou toho, že v bezpečnosti je nutná centralizace, a právě proto se v tomto případě klade tak velký důraz na automatizaci. Automatizace by měla být součástí bezpečnosti cloudu od samého začátku. Už jen proto, že díky ní si můžeme být jistí, že vše bylo hned na startu nasazeno správně a že to funguje tak, jak má. Neméně důležitým aspektem včasného nasazení automatizace je i možnost použít daný playbook jako dokumentaci ke cloudovému řešení.

## CSPM se stará o vizualizaci nedostatků v zabezpečení

Cloud Security Posture Management má několik základních funkcí, které dokážeme dobře využít právě při zabezpečování cloudu. Jde o nástroj, který vidí do konfigurace jakéhokoli našeho cloudového prostředí, ať už se jedná o Microsoft Azure, Amazon Web Services nebo Google Cloud Platform. CSPM nám umožňuje kontrolovat konfiguraci vůči nějakému předem definovanému standardu – může jít o CIS Benchmarks, o doporučení ISO, NIST, případně o PCI DSS a další. Takový nástroj dokáže vyhodnotit rizika a rovněž stanovit, jakým způsobem bude vhodné namapovat vhodná opatření tak, aby byla zajištěna bezpečnost. CSPM zároveň všechny nedostatky vizualizuje, a my tak máme vždy přehled o bezpečnosti našeho cloudového prostředí.

V případě hardeningu cloudu je třeba pokrýt šest základních oblastí:

- Identity and Access Management (správa identit a přístupu uživatelů);
- Logging and Monitoring (logování a monitoring všech aktivit, které v cloudu

probíhají, včetně průběžného auditování a alertingu, resp. implementace systému varování);
- Network (síťová bezpečnost v cloudu);
- Storage (bezpečnost a spolehlivost úložiště);
- Databases;
- Virtual Machines (zabezpečení za pomoci virtuálních strojů, v rámci virtualizace, kterou v cloudu provozujeme).

Některá nastavení není možné vykonávat pomocí běžného grafického prostředí tak, jak jsme zvyklí, ale je nutné přistupovat k nim prostřednictvím produktu PowerShell. Cloud jako takový je extrémně dynamický. Množství nastavení cloudového prostředí se neustále mění, mění se standardní hodnoty, ne vždy najdeme vše tam, kde očekáváme a kde jsme zvyklí. To, co umíme nastavit začátkem měsíce, už nemusí být možné na jeho konci.

V rámci standardu, který používáme při hardeningu, lze hovořit právě o CIS Benchmarksu, o PCI DSS, případně o standardech od úřadu NIST. Pro zajištění compliance je vhodné mít nástroj typu Check Point CloudGuard, který pomůže zaručit compliance celého cloudového prostředí. K dispozici je řada předdefinovaných šablon pro tři základní cloudy: Microsoft Azure, Amazon Web Services i Google Cloud Platform, včetně novinky v podobě Kubernetes. Najdeme tu šablony jak pro PCI DSS, tak vůči dalším standardům.

Každá politika má předem stanovená pravidla. Nástroj zprostředkovává odkazy na příslušnou dokumentaci s instrukcemi, jak a co správně v rámci nálezu nastavit. Všechna data jsou přehledně vizualizována. Je zde možné podívat se na základní manažerský přehled, případně se dostat na úroveň jednotlivých pravidel a ověřit si, jaké konkrétní položky v rámci dané konfigurace cloudu nejsou splněny. Nález lze přímo eliminovat na jedno kliknutí, což je mimořádně cenné, protože v mnoha případech nelze pro odstranění použít grafické rozhraní, ale musí se zadat příkaz například v PowerShell konzoli.

## Nástroje typu CWPP pomáhají identifikovat zranitelnosti v aplikacích

CWPP zajišťuje vizibilitu do toho, co se v cloudu děje. V tomto případě nemáme vizibilitu do konfigurace, ale do veškerých aktivit v rámci cloudu. Pojem Workload zde značí jakékoli aktivity, respektive jakékoli zdroje, které v cloudu máme. Může se jednat o virtuální stroje, může jít o databáze, ale stejně tak i o kontejnery, což je důležitý rozdíl oproti běžnému on-premise prostředí.

Nástroje typu CWPP pomáhají identifikovat zranitelnosti v aplikacích, ať už jde o nativní aplikace nebo aplikace vyvíjené v rámci kontejnerizace. Dokážou tyto kontejnery monitorovat a zajišťují tzv. Shift Left přístup, což znamená, že bezpečnost vyvíjených aplikací se tu posouvá přímo k samotnému vývojáři. Nástroje typu CWPP jsou zároveň vhodné i pro security operations týmy, protože právě díky nim dokáže tým správně detekovat typ problému a vypátrat celý bezpečnostní incident.

I v rámci CWPP poskytuje své funkce už zmíněný nástroj Check Point CloudGuard. Ten dokáže vyhodnotit severitu všech událostí, které se v rámci cloudu dějí, poskytne popis zranitelnosti a především pro SOC týmy představuje výhodu i v tom, že umí všechny tyto aktivity namapovat na tzv. Mitre Att&ck Framework.

Bavíme-li se o cloudu, lze bezpečnost rozdělit do tří částí: 1. bezpečnost v cloudu, která je zajišťována produkty CSPM, 2. bezpečnost v cloudu, kterou zajišťují nástroje CWPP, a 3. bezpečnost mezi cloudem a on-premise prostředím, tedy jakási pomyslná brána mezi těmito dvěma prostředími, což zajišťují nástroje CASB.

Jedná se o lokální nebo cloudový software nainstalovaný mezi spotřebitelem cloudových služeb a jejich poskytovatelem. CASB slouží jako nástroj pro vynucování bezpečnostních zásad organizace za pomoci identifikace rizik a dodržování předpisů, kdykoli se přistupuje k datům uloženým v cloudu. Tento hlídací nástroj je jedním z nejdůležitějších doplňků zabezpečení organizace, protože zabraňuje krádežím dat a brání malwaru a dalším hrozbám v pronikání do systému.

Mnohé společnosti si uvědomují rizika spojená s přechodem do cloudu, vědí, že potřebují specializovaná cloudová bezpečnostní řešení, ale nejsou si jisté tím, jaká přesně. V případě, že by se CASB ukázalo jako nedostatečné pro udržování bezpečnostních politik a ochranu jejich aplikací v cloudu, mohou využít nástroj Secure Access Service Edge. SASE poskytuje všechny možnosti CASB, ale navíc i další bezpečnostní řešení a možnosti nasazení modelu Zero Trust, které přesahují cloud.

## Závěr

Bezpečnost v cloudu nelze brát při přechodu z on-premise prostředí jako samozřejmost. Bezpečnostní produkty cloudových poskytovatelů často nebývají dostačující, obzvláště pokud zákazník používá princip multicloudu. V takovém případě je vhodné zvolit řešení od třetí strany, které dokáže spravovat a zajistit bezpečnost všech vašich cloudových platforem. Přitom je nutné myslet i na správnou konfiguraci cloudového prostředí, a to především s ohledem na různé standardy, které odpovídají požadavkům vaší společnosti. V neposlední řadě je vhodné zachovat již zmíněný Zero Trust Model. ■

Matej Kačic

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