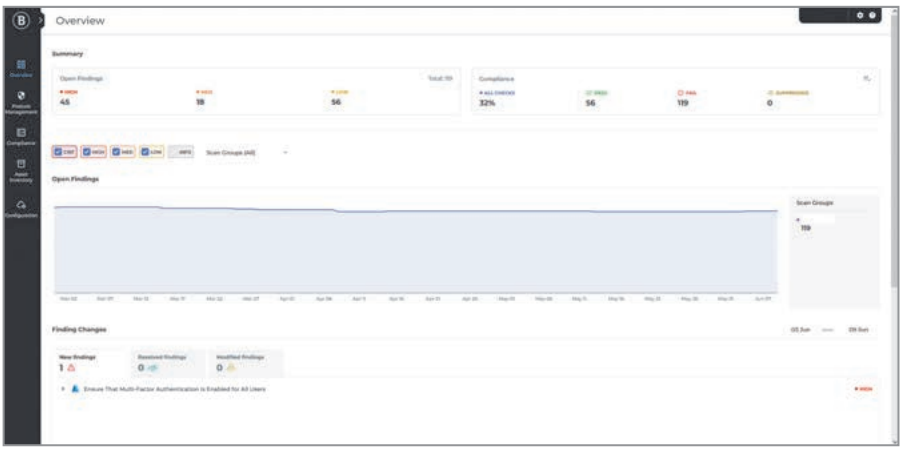
Vadí vám nepřehlednost správy rizik v cloudových službách Azure, AWS a GCP?

Chcete mít přehled o všech rizicích na jednom místě? Máme pro vás žhavou novinku.



JAROSLAV HROMÁTKA

Řízení rizik v cloudových službách typu infrastructure as a service (IaaS) je noční můrou většiny správců podnikového IT. Služby samotné mají často dost omezené schopnosti upozorňování na riziková nastavení a nedostatečná zabezpečení objektů (virtuální stroje, aplikace, kontejnery, úložiště, databáze apod.) a mají uživatelská rozhraní, která jsou nepřehledná, a často není ani po delším studiu zřejmé, jaké kroky je pro mitigaci rizika nutné podniknout.

Společnost Bitdefender dlouhodobě považuje disciplínu řízení rizik v cloudových službách jako další segment IT bezpečnosti, jehož důležitost v průběhu času bude dramaticky růst, ať už z důvodu ztráty rentability provozu on-premise řešení nebo z důvodu masivního rozvoje AI nástrojů, které si moc organizací nebude moci dovolit provozovat on-premise z důvodu příliš vysokých pořizovacích nákladů. Proto v loňském roce Bitdefender akvizoval singapurskou společnost Horangi Security, která se na řízení rizik v cloudových službách dlouhodobě specializovala, a nyní úspěšně zaintegroval celé řešení do své bezpečnostní platformy Bitdefender GravityZone včetně napojení do XDR. Není to jediný produkt či služba, která ze spojení Bitdefender-Horangi vznikla a vznikne, nicméně tomuto tématu se budeme věnovat jindy.

Jak to celé funguje

Letos byl vydán produkt Bitdefender GravityZone Cloud Security Posture Management, který, jak už název naznačuje, je součástí bezpečnostní platformy Bitdefender GravityZone. Nejen že nabízí přehledné rozhraní pro řízení a nápravu rizik v cloudech, ale též Gravityzone XDR obohacuje o postřehy o rizicích v cloudové infrastruktuře. Pokud tedy XDR detekuje útok probíhající na jakékoli části cloudové infrastruktury, CSPM dodá informace o tom, jaká rizika byla v tomto útoku zneužita, a samozřejmě též návody, jak tato rizika odstranit. Jde o další z řady urychlení reakcí na bezpečnostní incidenty, které Bitdefender GravityZone XDR obsahuje, tentokrát z kategorie, která uzavírá pomyslný kruh životního cyklu bezpečnostního incidentu návrhy vytvrzování. Právě vytvrzování je často opomíjenou součástí životního cyklu bezpečnostních incidentů, ale není o nic méně důležitá než samotné zastavení útoku. Ve chvíli, kdy úspěšně napravíme zneužitá nastavení, se stejný útok již nemůže opakovat.

Klíčová součást prevence proti útokům

Integrace CSPM s XDR je ale pouze třešničkou na pomyslném dortu. Hlavní účel celého produktu je bezpečnostním incidentům předcházet, a to se mu velmi dobře daří. Produkt sleduje stovky parametrů u všech typů objektů a ve vztazích mezi objekty a varuje před všemi zranitelnostmi, které je možné v rámci útoku na tuto cloudovou infrastrukturu zneužít, a nabízí možnosti remediace pomocí přehledného popisu, o jaké riziko jde, proč je to důležité, jaký je možný dopad na provozovanou službu, a samozřejmý je postup remediace s předpřipraveným skriptem, který riziko napraví. V mnoha případech je možné využít možnosti nápravy na jedno kliknutí (úplně automatická náprava). CSPM zároveň umí v průběhu času reportovat, zda vaše cloudové prostředí splňuje nějakou normu – ať už zákonnou nebo certifikační – např. pro GDPR, PCI DSS, ISO 27001, SOC-2, NIST-CSF aj. Pomáhá tak organizaci snadno cloudové prostředí dostat do stavu, který je v souladu s certifikací, o niž usiluje, a v takovém stavu bez námahy udržovat. Ukazuje totiž nejen celkový stav, ale i změny oproti předchozímu sledovanému období a vypisuje přesně, co se změnilo, s popisem, z jakého důvodu ke změně došlo.

Přehledné řízení rizik v IaaS

Na řízení bezpečnosti neexistuje žádná „golden bullet“, žádný univerzálně funkční postup, žádné řešení, které by zařídilo vše a bylo to bez práce. Nicméně platforma GravityZone se tímto rozrostla o další velký kus potřebný pro řízení bezpečnosti v organizacích, a jak je u Bitdefenderu zvykem, je nástroj CSPM přehledný, snadno ovladatelný a velmi urychluje a usnadňuje práci správce bezpečnosti.

TLDR; pokud využíváte cloudové služby Azure, GCP nebo AWS, kontaktujte svého Bitdefender Partnera a CSPM si vyzkoušejte.