Útok, který by bez SIEM zůstal skrytý

Kybernetické útoky se dnes rozdělují na plošné a méně sofistikované a na cílené, sofistikovanější. Firmy i veřejné instituce proto stojí před zásadní otázkou: jak zajistit, aby dokázaly útok nejen zastavit, ale také pochopit, co se v jejich prostředí skutečně stalo?

PETR KOCMICH

Právě zde přicházejí do hry nástroje jako SIEM, log management, vulnerability scanning, patch management a další. Každý z nich řeší jinou část skládačky, ale dohromady tvoří systém, který dokáže organizacím dát kontrolu nad tím, co se v jejich IT prostředí děje.

Security Information and Event Management (SIEM) je centrálním prvkem moderní bezpečnostní architektury. Jde o „srdce detekce a reakce", protože SIEM nejenže sbírá logy z různých systémů, jako jsou např. koncové body, servery, firewally, a ze síťových prvků nebo nástrojů pro správu identit, případně z e-mailových a antispamových systémů a dalších cloudových služeb a workloadů, ale ty následně analyzuje a vyhodnocuje v reálném čase. Nad nimi pracují korelační pravidla, která dokážou odhalit anomálie – třeba neobvyklé chování administrátora o víkendu nebo masivní export dat z firemního úložiště. Většina SIEM řešení zároveň často k pokročilé korelaci a doplnění kontextu využívá umělou inteligenci a strojové učení.

Velký význam rovněž zastává MITRE ATT & CK framework, shromažďující a kategorizující různé typy strategií, technik a postupů, které používají kybernetičtí útočníci. Díky němu SIEM dokáže pospojovat jednotlivé události do souvislostí a ukázat, že v prostředí probíhá reálný útok a nejde jen o náhodný výkyv – často právě pomocí využití AI a ML. Pokročilé SIEM lze navíc napojit na SOAR (Security Orchestration, Automation and Response), což umožňuje reagovat na některé incidenty automaticky. Například izolovat počítač, na kterém byl detekován malware, dříve než infikuje zbytek sítě.

Bez logů není příběhu

Často se můžeme setkat s architekturou, kdy před samotný SIEM předřazujeme centrální log management. Ten zajišťuje sběr, normalizaci a dlouhodobé ukládání logů z celé infrastruktury. To je důležité nejen pro detekci hrozeb, ale i pro forenzní analýzu. Útoky jsou totiž často odhaleny až s odstupem – mnohdy i po několika měsících. Pokud má například organizace k dispozici záznamy pouze z posledních třiceti dnů, nemá šanci zpětně dohledat, jak útok začal a k jakým datům se útočníci dostali. Právě proto regulace (např. ZKB či NIS2) vyžadují uchovávání logů typicky až po dobu osmnácti měsíců (pro ty společnosti, kterých se konkrétní úroveň regulace týká).

Z praktického hlediska dává log management smysl i ekonomicky. SIEM je licencován podle množství zpracovávaných dat, a proto je výhodné do něj posílat jen bezpečnostně relevantní logy, zatímco kompletní archiv je uložen v levnějším log managementu.

Neustálé hledání slabých míst

Dalším pilířem kybernetické bezpečnosti je vulnerability management, tedy proces identifikace a prioritizace zranitelností v prostředí organizace. Specializované skenery dokážou otestovat servery, aplikace i síťová zařízení a porovnat je se známými databázemi zranitelností. Tato data je ideální zpětně integrovat do SIEM.

Výstupem je seznam slabých míst, který je nutné prioritizovat – ne všechny slabiny jsou totiž stejně nebezpečné. Kritická je například zranitelnost, která umožňuje vzdálené ovládnutí zařízení z internetu, případně ta, jež je právě aktivně zneužívána útočníky. K vyhodnocení takovýchto dat využíváme tzv. threat intelligence data, která často můžeme integrovat se samotným SIEM řešením, a obohacovat tak potřebná data k lepším výsledkům detekce a prioritizace.

Záplatování jako nepřetržitý proces

Na vulnerability management navazuje patch management, tedy pravidelné nasazování záplat na odhalené zranitelnosti. Bez něj by byly výsledky skenování jen seznamem problémů.

Standardní cyklus zahrnuje měsíční aktualizace. Záplaty se nejprve testují na vybraných testovacích strojích a prostředích, aby neohrozily běžný chod systémů, a až poté se nasazují do produkce. V urgentních případech, třeba u zero day zranitelností, musejí firmy reagovat okamžitě a nasadit záplaty bez čekání, mnohdy bez potřebného času na testování, a provést tzv. emergency patching.

Proč to celé dává smysl i z pohledu byznysu

Mohlo by se zdát, že jde o složité a drahé nástroje. Jenže v praxi jejich přínos přesahuje čistě technickou rovinu:

- **Plnění regulací** – GDPR, ZKB nebo NIS2 ukládají povinnost nejen útoky nahlásit, ale také přesně vědět, co se stalo. Bez SIEM a log managementu to není možné.
- **Minimalizace dopadů incidentů** – rychlé odhalení a izolace útoku může ušetřit miliony korun za odstávku nebo ztrátu dat.
- **Forenzní schopnosti** – logy a analýzy ze SIEM dávají firmám možnost přesně určit, zda došlo k úniku dat, což je zásadní při komunikaci se zákazníky i úřady.
- **Zvýšení důvěry a dobrého jména** – zákazníci i partneři oceňují, když organizace dokáže prokázat, že má prostředí pod kontrolou.
- **Efektivita provozu** – automatizované reakce a lepší přehled a viditelnost nad prostředím snižují náklady na manuální správu.

Bezpečnost není jednorázový projekt

SIEM, log management, vulnerability scanning a patch management tvoří vzájemně provázaný systém, kde každý prvek má svou roli a navazuje na ostatní. Log management poskytuje data a důkazy, SIEM je analyzuje a odhaluje souvislosti, vulnerability scanning identifikuje slabiny a patch management je následně odstraňuje.

V době, kdy jsou kybernetické útoky stále cílenější a sofistikovanější, je právě tato komplexní spolupráce bezpečnostních technologií klíčem k efektivní ochraně. Nejde jen o splnění regulací, ale o schopnost udržet ochranu dat, provozní kontinuitu a důvěru zákazníků.

Autor je bezpečnostní expert skupiny Soitron