KOMENTÁŘ

Sběrem logů bezpečnost nekončí

JIŘÍ VAŘECHA,
BEZPEČNOSTNÍ ODBORNÍK, SIRWISA

> Už jen pouhým sběrem logů ze všech aplikací lze výrazně zvýšit bezpečnost ve firmě.

Jak významnou roli hraje sběr logů v současném podnikovém zabezpečení?
Ve sběru a analýze logů z jednotlivých zařízení lze získat velmi užitečné informace. Bohužel je stále velmi málo firem, které logy vůbec sbírají, natož aby je aktivně využívaly. Už jen pouhým sběrem logů ze všech aplikací lze výrazně zvýšit bezpečnost ve firmě.

Nedojde sice k zastavení potenciálních útoků, ale správci získají informace o tom, jak k incidentu došlo a co mu předcházelo. Ať už to jsou jednoduché případy, kdy správce dohledává, který uživatel co kde smazal, nebo složitější případy, kdy se z logů zjišťuje, jakým způsobem došlo k útoku na firemní aplikaci.

SIEM bývá obvykle spojovaný s trvalou a náročnou prací administrátora, existuje snaha výrobců tento proces nějak lépe automatizovat?
Výrobci se snaží automatizovat běžné každodenní úkoly a zjednodušovat konfiguraci. Bez poctivé a mravenčí práce bezpečáka jsou ale jakékoliv bezpečnostní nástroje k ničemu. Bohužel existuje mylná představa managementu, že pořízením SIEM systému vyřeší všechny bezpečnostní problémy, koupí SIEM nicméně řešení bezpečnosti teprve začíná. Pro úspěšnou implementaci SIEM nástroje je nutné udělat zjednodušeně dva kroky.

A to nainstalovat systém pro sběr logů a posílat do něj všechny logy z aplikací a infrastruktury a ve druhém kroku vymyslet scénáře SIEM pravidel, co se musí stát v systému X a Y, aby to bylo označeno jako bezpečnostní incident.

Tato pravidla může výrobce připravit jen z části, každá firma totiž používá jiné prostředí a jiné aplikace. Je tedy nutné tato pravidla vždy definovat podle potřeb a procesů firmy. Pro analýzu těchto události by zde měl sedět opravdový bezpečák, který chápe, jak fungují firemní procesy. Jednou z jeho činností je vymýšlení nových korelačních pravidel.

Zde by bylo vhodné zdůraznit, že již zavedením „hloupého" sběru logů a jednoduchých alertů se bezpečnost firmy mnohonásobně zvedne, jelikož jsou schopni správci dohledat, proč se tomu tak stalo, kudy se útočník do sítě dostal… Druhý krok je pro firmy, které to myslí opravdu vážně a jsou schopny zaplatit tým lidí, jenž se bude věnovat jen analýze událostí SIEM.

Co by měla firma zvážit při výběru vhodného řešení pro sběr logů?
Výkon, funkce, licenční politika a v neposlední řadě složitost obsluhy a nároky na implementaci. Spousta firem používá SIEM řešení, nicméně kvůli licencím a složitosti implementace toto řešení nedělá, co by mělo, protože nebyl dostatek peněz na pořízení všech nutných licencí. Ideální systém vás licenčně nelimituje v počtu zařízení, které budete logovat, jediným limitem by měl být výkon samotného HW, na kterém systém běží. Je také nutné myslet na budoucnost, to, co potřebuji teď, nemusí odpovídat požadavkům, které budu mít příští rok. ■