Log management – základ Security Information management riešenia

Juraj Polak, IBM Tivoli Sales
juraj.polak@sk.ibm.com

Mnohé z nariadení vyžadujú kontrolu účinnosti riadenia IT bezpečnosti podniku. Bezpečnostní manažéri potrebujú preskúmať podozrivé security incidenty, čo znamená zbierať dáta v reálnom čase ako aj v historickom prehľade.

Nie je možné spoznať a ovládnuť to o čom neviete, že existuje, teda ak nemáte spoľahlivý log management systém na zber logov systémov a aplikácií. Log management systém preto musí nevyhnutne zvládať zber, ukladanie, vyhľadávanie, skúmanie a reportovanie security udalostí.

Je dôležité poznamenať, že zber správnych udalostí je rovnako dôležité ako povolenie auditu logov – súčasné odporúčanie NIST (1) odporúča organizáciám „definovať... požiadavky a ciele pre výkon logovania a monitorovania logov vrátane aplikovateľných právnych predpisov, nariadení autorít a existujúcich organizačných predpisov.“ Nie všetok obsah logov má rovnakú hodnotu pre rozpoznanie bezpečnostných udalostí. Preto prvým krokom k log managementu je rozhodnutie ktoré logy je potrebné zbierať a uchovávať.

SCHOPNOSŤ ZBIERAŤ A ROZUMIEŤ

Ďalším dôležitým kritériom, ktoré je potrebné zvážiť, je schopnosť zbierať a rozumieť rôznym typom logov. Tu je namieste otázka či máte kapacitu resp. schopnosť analyzovať a prehliadať rôzne log formáty generované systémami a zariadeniami? Ak aj áno takáto práca sa nepokladá za činnosť s vysokou pridanou hodnotou a preto zváženie automatizácie takejto činnosti je veľmi dôležité.

V nemenšej miere organizácie musia byť schopné voči audítorom preukázať, že použitý proces je spoľahlivý a verifikovateľný a poskytuje kompletné, zrozumiteľné a kontinuálne sady logov.

Pre Log management v IT dnes existujú dva základné dôvody:

1. Prevádzka potrebuje audítovať, monitorovať a upozorňovať na neadekvátne správanie sa používateľov z pohľadu základných bezpečnostných predpisov.
2. Nemenej dôležitá je schopnosť preukázať súlad s nariadeniami regulačných orgánov a autorít.

NIST SP 800-92 popisuje základnú hodnotu log managementu pre organizácie.

AKÉ SÚ BEZPEČNOSTNÉ RIZIKÁ?

Súčasné štúdie ukazujú že až 87 % interných bezpečnostných incidentov je spôsobených internými privilegovanými používateľmi, menovite administrátormi, outsourcermi, konzultantmi a tzv. power usermi. Takéto incidenty stoja spoločnosti približne 6 % ich hrubého obratu.

Zoznam potenciálnych incidentov, ktorých sa najčastejšie dopúšťa menovaná skupina používateľov:

1. Sabotáž informácií privilegovaný-

mi používateľmi.
2. Zneužitie informačných zdrojov, ako sú napr. informácie o kreditných kartách alebo zoznamy zákazníkov či iné.
3. Inštalovanie nepovoleného softvéru alebo hardvéru, čo môže vyústiť až do logických, alebo časových bômb, trojských koní a back doors.
4. Manipulácia slabín TCP/IP protokolu ako je DNS spoofing and TCP_SYN flooding.
5. Manipulácia kódu v návrhu aplikácií samotných.

Okrem bezpečnostných rizík je tu ešte „compliance" – potreba zabezpečenia zhody s regulačnými autoritami ako je SOX Sarbanes Oxley Act, Health Insurance Portability Accountability Act (HIPAA), a Gramm-Leach-Bliliey Act (GLBA) Všetky tieto nariadenia majú jedno spoločné – ak spoločnosť nezaručí zhodu je automaticky obmedzená vo svojom pôsobení alebo musí spĺňať iné kritérium obyčajne finančné. (napr. BASEL II v prípade nezhody banka musí zvýšiť hotovostné rezervy, čo ju, samozrejme, zaťažuje a znižuje jej flexibilitu). Preto je splnenie regulačných predpisov pre spoločnosť veľmi dôležité a na IT kladie nové požiadavky – kontroly činnosti používateľov prostredníctvom sledovania log záznamov.

Charakteristika efektívneho Log Management Systému

- ★ Automatizácia
- ★ Konfigurácia nastavení audit parametrov
- ★ Spoľahlivý, verifikovateľný zber logov a reporting
- ★ Princíp palubnej dosky pre rýchly prehľad a reakciu, asistovaný prieskum
- ★ Originálny log storage
- ★ Rychly systém pre dopyt a rešerš

POTREBA AUTOMATIZÁCIE

Z technického pohľadu každé zariadenie v sieti generuje sériu logov. Každý log systém je svojím spôsobom unikátny. Logy sú často kryptované a špecializované, čo tvorí vysoké nároky na expertízu ak im chceme porozumieť. Všetky tieto faktory zapríčiňujú, že systémoví administrátori sú pri manuálnej kontrole logov neefektívni a dopúšťajú sa príliš mnoho chýb. Navyše si treba uvedomiť, že korelácia udalostí viacerých zdrojov (rádovo +100ky) je ručne vlastne nemožná!

Log management systém musí byť preto automatizovaný – management systémov je inak nemožný. Automatizácia zberu a ukladania logov prináša so sebou vysokú spoľahlivosť a zabezpečuje aj kontinuitu logov, čo dáva IT bezpečnostným špecialistom istotu dokázania porušení predpisov a schopnosť splniť požiadavky audítorov efektívne bez potreby manuálnej práce. Dnes základný log management systém umožňuje zber, uloženie a dopyt na log súbory s cieľom zistiť security eventy. Sofistikovanejšie systémy (ako IBM Tivoli InSight Security manager) umožňujú konsolidovať, normalizovať, skúmať, reportovať, a varovať pri porušení predpisov, identifikovaných pomocou pokročilých korelačných a analytických mechanizmov.

Tivoli Compliance Insight Manager okrem sofistikovaného log managementu, audit a compliance schopností – plug-in compliance moduly – umožňujú kontinuálne monitorovať a reportovať súlad biznis požiadavek s „best practices":

- ★ Sarbanes Oxley
- ★ Basel II
- ★ HIPAA
- ★ GLBA
- ★ PCI DSS
- ★ SAS70
- ★ NISPOM
- ★ FISMA
- ★ DCID
- ★ ISO17799
- ★ Všeobecné bezpečnostné kritériá ■