Aby logy přestaly být noční můrou

Správci sítě i bezpečnostní manažeři z nich mají respekt a nezbytně je potřebují. Vedoucí pracovníci ale obvykle netuší, o co přesně jde, a systém pro zpracování logů nepodpoří, dokud nezazní klíčové slovo – shoda s regulacemi a zákonnými požadavky. Systémy na správu a vyhodnocování logů však neslouží jen k zaškrtnutí políčka „zákon o kybernetické bezpečnosti – splněno", přináší i pomoc při řešení provozních problémů.

FILIP WEBER

Existují odbory a pracovníci, kteří zpracované a vhodně archivované logy ke své činnosti nezbytně potřebují, i když každý z trochu jiného důvodu. Například správci systémů (sítí, bezpečnostních prvků, serverů a aplikací) potřebují logy prohledávat při analýze a řešení provozních problémů.

Pro bezpečnostní manažery zase představují klíč pro vyhodnocování bezpečnostních událostí. A nově, s účinností zákona o kybernetické bezpečnosti, potřebují mít logy kdykoliv připravené pro předložení organizacím zabývajícím se bezpečností – Cesnet Cerst a Cirst nebo Policii ČR.

Společné potíže

Obě skupiny však narážejí na společné problémy. Logy jsou uložené na různých zařízeních, kam mají správci rozdílně omezená přístupová práva, jsou v rozličných formátech, mají různou retenci anebo zařízení mají pro ně vyhrazenou omezenou kapacitu, takže logy jsou k dispozici jen pár dní zpět.

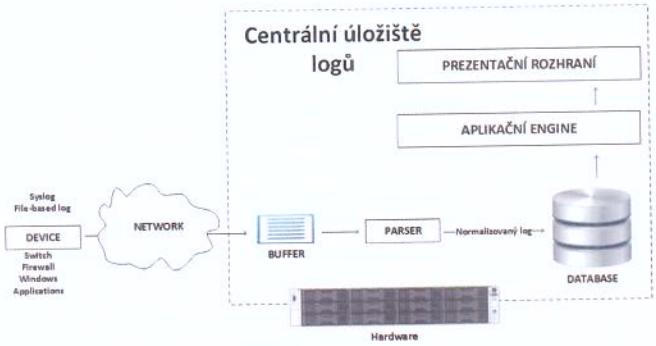
Logy uložené na různých místech lze zpochybnit, modifikovat nebo třeba také záměrně smazat. Právě mazání či pozměnění logů je jednou z činností, které útočník při průniku do systému vždy udělá, aby svoji činnost zakryl.

Centrální úložiště

Řešení spočívá ve vytvoření centrálního úložiště, kam všechna zařízení, servery, systémy, aplikace a databáze své logy ukládají. Jenže ty přicházejí v různých formátech. Síťová a bezpečnostní řešení obvykle posílají logy ve formátu Syslog, který ale není jednotný.

RFC 5424 zase popisuje pouze transportní protokol. Logy z aplikací a operačních systémů pak mají formát „file-based log" a pro něj není žádný standard. První, co tedy musí centrální úložiště tohoto typu udělat, je normalizace logů.

Ty přicházející se proženou tzv. parsery, které ze surové podoby logu rozdělí všechny informace do příslušných polí v databázi – destination IP, source port, time a další. Tím se to celé sjednotí a je možné s tím dále pracovat.



Architektura síťového úložiště logů

Parsování logů je ale činnost velmi náročná na výkon systému. Před parsovacím strojem musí být buffer, kam se ukládají data při příjmu. Síťová zařízení a systémy totiž v naprosté většině nemají implementovaný způsob ověření doručení logů. Logy se tak odesílají do „černé díry" a zařízení se nijak nestarají, zda se i doručí.

Centrální úložiště tedy musí mít dostatečný výkon pro nepřetržitý příjem – daný množstvím událostí za sekundu (EPS, Events Per Second). Definovat, kolik EPS všechna zařízení a systémy v síti vygenerují, je tak trochu jako věštění z křišťálové koule – záleží na typu produktů, množství přenesených dat, počtu přihlášených uživatelů, jestli zařízení zrovna náhodou nečelí útoku a na dalších parametrech.

Centrální úložiště logů také musí podporovat režim vysoké dostupnosti. Ten se obvykle implementuje přímo v databázovém stroji a řeší se prostým přidáváním dalšího stroje do skupiny.

V síti existuje mnoho různých zařízení, a proto je důležité si ověřit, zda se právě ta důležitá plně podporují. Parser ale musí opravdu rozluštit všechny údaje příchozího logu, nikoliv jen základní, jako jsou čas nebo IP adresy, přičemž to ostatní uloží v nezpracované podobě.

Bez vhodného zpracování bude možné ve vyhodnocovacím a reportovacím subsys využít jen ve velmi omezené míře.

Analytické a prezentační rozhraní

V podmínkách tuzemské střední a větší pc čové sítě se vygeneruje zhruba 1,5 miliardy lostí za měsíc, přičemž pro jejich uložení j třeba nejméně 10 TB. To už jsou big data, nimiž se dále pracuje – musejí se prohlíže dit, analyzovat či korelovat. Aby uživatelé seli při zadání dotazu do databáze čekat n pověď hodiny či dny, je nutné, aby úložišt mělo opravdu výkonný databázový stroj.

Prezentační rozhraní úložiště logů je tc se pracuje – tady se třídí data, filtrují, vyt dotazy. Je vhodné mít co nejvíce dotazů u pravených, aby je uživatelé nemuseli opak sami vytvářet. A k informacím je dobré se na několik kliknutí.

Co vás zajímá?

Správce sítí budou zajímat pr data. Kolik dat přenesl který tel. Kdo se připojuje na VPN? se neúspěšně snaží přihlásit p 802.1x do sítě? Jaká pravidla rewallu nejvíce zasahují? Na portech probíhá komunikace zónami? Tyto informace mus stém poskytnout na pár klinu

Bezpečnostní manažer za užije funkce SIEM (Security mation and Event Manage které jsou nadstavbou centrá úložiště logů. SIEM funkce spočívají v to správná data a položit nad nimi odpovída dotazy.

Data (eventy) jsou v centrálním úložiš lze pokládat dotazy. Třeba jak dlouho trá vatel prohlížením webu a zda stránky, na rých je celou pracovní dobu, nejsou v kat „škodlivé". Nejsou v síti neautorizované servery? Nejsou stanice nakažené červy munikují s bootnety?

Kdo porušoval pravidla o komunikaci Proč se uživatel hlásí do aplikace jiným j než jakým je přihlášen na stanici? Která na firewallu se nevyužívají, a tudíž jsou otevřená? Proč tato stanice generuje tisí jení na neexistující IP? A mnoho dalších

Centrální úložiště logů, nejlépe s fun SIEM, má svoje nezpochybnitelné místo tačové síti. Využijí jej správci sítě pro ře vozních problémů a bezpečnostní mana dohled nad bezpečností sítě a naplnění davků zákona o kybernetické bezpečnos už jen přesvědčit manažery, aby na náku nili peníze.

Autor je síťovým architektem společnosti Compu

Požadavky na centrální úložiště logů

- Standardizace formátu logů
- Výkon pro příjem tisíců událostí za sekundu
- Dostatečná kapacita pro uložení logů
- Výkonný databázový stroj pro vyhledávání v obrovských objemech dat v řádech desítek sekund až minut
- Připravené provozní a bezpečnostní pohledy na big data

CompuNe
Network Design & Supervisi

LOGmanager | *Centrální úložiště logů*

Jste připraveni
na nový Zákon o kybernetické bezpečnosti?

Od 1. 1. 2015!

LOGmanager je systém pro centralizovanou správu eventů a logů z bezpečnostních zařízení, operačních systémů, aplikačního software i aktivních síťových prvků. Je založen na zcela novém typu databáze s výkonným systémem prohledávání a prezentace nalezených dat.

LOGmanager plní požadavky Zákona o kybernetické bezpečnosti, který vstoupí v platnost již 1. 1. 2015.

www.logmanager.cz | compunet@compunet.cz | 257 211 846 | www.compunet.cz

POWERED BY HP TECHNOLOGY

Systém LOGmanager, vyvinutý společností CompuNet s. r. o., je dodáván na výkonných a spolehlivých serverech HP.

www.hp.cz