Jak náročné je nasadit SIEM?

Proč ve firmě implementovat logovací nástroj a jak vypadá nasazení a provoz takového řešení ve větší organizaci, ukazuje příspěvek, který pro Security World připravil René Pisinger, vedoucí systémové podpory v České televizi.

Logovací systém či také syslog představuje řešení pro centralizovanou správu eventů a logů z libovolných síťových aktivních prvků, bezpečnostních zařízení i operačních systémů a aplikačního softwaru. Nástroj má ve svém nitru databázi s určitou kapacitou a systémem prohledávání a následné prezentace nalezených dat.

Podstatou většiny takových systémů je sběr všech relevantních eventů (událostí) a logů (protokolů) v organizaci, jejich ukládání do centrálního úložiště s předem definovanou retencí a možností prohledávat enormní množství dat v čase.

Výstupy prohledávání se prezentují v podobě, jakou systém umožňuje – většinou jde o textovou či grafickou podobu. Syslogy by měly rovněž umožnit uchovávat data – i několik let zpětně podle kapacit úložiště a typu nástroje na prohledávání dat. To se hodí třeba pro potřeby shody s předpisy, požadavky pro forenzní analýzu či případné bezpečnostní audity.

Většinou nejde o systém, který se stará o bezpečnost IT ve firmě – vhodný je spíše pro operativní provoz IT, jehož pracovníkům umožňuje formou interakce oproti databázi událostí nalézt například podstatu nefunkčnosti systému, identifikovat možné závady a rychle dohledat události popisující příčinu konkrétního problému, ztráty dat nebo výpadku komunikace.

Donedávna televize provozovala zastaralý logovací nástroj, který uměl logovat záznamy pouze do 256 znaků, ostatní ořezával. Není tedy těžké pochopit, že v současném IT světě je takový nástroj k ničemu. Vzhle-

Kritéria pro výběr syslogu v České televizi

1. Sběr událostí

- Zpracování událostí z předdefinovaných zdrojů logu napříč OS, SW i HW.
- Otevřené řešení pro snadnou integraci systémů, které nejsou podporované přímo výrobcem.
- Možnost sběru událostí minimálně ve formátech raw, syslog.
- Agent pro Windows pro zajištění sběru nemodifikovaných událostí.
- Možnost zakázat mazání nebo filtrování přijímaných a uložených zpráv administrátorem.

2. Úložiště událostí & správa

- Konsolidace logů na centrálním místě
- Snadné vyhledávání událostí (ad hoc) bez nutnosti programování.
- Grafické znázornění událostí (grafy událostí).
- Grafické znázornění top událostí za určité časové období.
- Unifikované vyhledávání napříč všemi typy dat a zařízení.
- Možnost uložení filtrů, výsledků vyhledávání pro budoucí zpracování.
- Reportovací nástroj s přednastavenými nejběžnějšími reporty a možností vlastních úprav.
- Aktualizace reportů a pohledů výrobcem.
- Škálovatelné do budoucna a rozšiřitelné v případě potřeby.
- Monitoring stavu systému – alertování při překročení prahových hodnot nebo chybě systému, přeposlání upozornění pomocí SMTP nebo syslog.
- Možnost dotazování externím monitorovacím systémem pro další zpracování alertů a prahových hodnot.
- Webová konzole pro správu.
- Možnost ověřovat uživatele systému na externím LDAP serveru.

3. Parametry softwaru

- Webová konzole pro vzdálenou správu.
- Průměrný příjem alespoň 5 tis. událostí/s.
- Licenčně neomezený počet zařízení pro příjem zasílaných událostí.
- Podpora následujících zařízení na úrovni rozčlenění událostí na jednotlivé položky událostí a uložení ve strukturovaném formátu: Aktivní prvky Cisco a HP, firewally Cisco a Check Point, Windows a Linux, bezpečnostní logy 802.1x s možností dopsání parseru pro výše neuvedená zařízení.

4. Požadavky na logování:

- *Syslogy ze zařízení:* Switche Cisco a HP, Wi-Fi Cisco a HP, firewall CheckPoint, HP ILO.
- *File-based-logy:* Windows servery, Windows stanice, Linux servery, Apache servery, SAP, Docházkové systémy, UPS, Tiskárny, Kamery, Bezdrátové spoje, SecureEnvoy, Radius server na OS linux.

Požadovala se také podpora výrobce na aktualizaci systému alespoň na pět let a potvrzení o shodě s normou ISO 27001:2005.

dem k tomu, že bylo nutné neustále zpětně dohledávat problémy, které vznikaly provozem systémů, dohodli se v televizi na nákupu nového logovacího systému, a to podle přesných parametrů a požadavků.

Takto sestavené podklady se pak přednesly nadřízeným. Doplněné přitom byly o informace, jaké problémy se obnovou nástroje v budoucnu vyřeší, a také o průzkum trhu na toto téma. Přesvědčit vedení firmy pak nebyl až tak velký problém.

Nasazení a správa

Po výběrovém řízení přišla samotná implementace, kdy server s logovacím nástrojem dodavatel poskytl během 14 dnů od podpisu smlouvy. Za pomoci technika dodavatelské firmy se základní nastavení a implementace zvládly zhruba za dva týdny, přičemž to, co se v pilotním provozu logovacího nástroje nasadí, bylo jasné už předem.

Vzhledem k tomu, že jde o nástroj z české provenience, implementace byla i pro neznalé anglického jazyka jednodušší v tom, že nástroj je plně lokalizovaný do češtiny a obsahuje poměrně srozumitelnou a podrobnou dokumentaci.

Implementace zahrnovala instalaci serveru do racku, oživení, připojení do sítě, dále nasměrování všech síťových zařízení na IP adresu logovacího serveru a vytvoření pravidla Group Policy pro instalaci logovacího systému event sender a její aplikace na vybraná zařízení podle předimplementační domluvy. Procházejí se i všechna ostatní zařízení a přesměrovávají na logovací nástroj.

Při tzv. access integraci probíhá vše bez problémů, v případě trunk propojení je nutné dávat pozor, aby nedošlo ke ztrátě konfigurace logovacího zařízení. Konfigurace prvků podle návodu probíhá v pořádku, při konfiguraci integrace např. se zařízením Check Point musí mít správce vyšší znalosti těchto systémů.

Při provozu logovacího systému je nutné průběžně kontrolovat, zda logování probíhá na všech prvcích, které se s logovacím systémem integrovaly (převážně Windows a Check Point integrace se ale občas přeruší).

V současnosti se v České televizi loguje zhruba 300 zařízení, denně přibude v průměru 62 GB dat, což je v tomto prostředí cca 79 milionů záznamů denně. Používá se interní alertovací sytém, který rozesílá kritické události na e-mailové adresy systémových techniků. Nástroj již od roku 2012 vypomáhá provozním účelům IT.

Logovací nástroj v současnosti spravují dva lidé na 2 % svého pracovního času. Jde převážně o přidávání či ubírání systémů, přidávání alertů nebo o obecné využívání nástroje. ■