KOMENTÁŘ

Křišťálová koule

FILIP WEBER,
SÍŤOVÝ ARCHITEKT,
COMPUNET

> Obvykle nezbude, než pozvat externího experta.

Tak kolik EPS bude ta vaše síť dávat? Odhaduji to na 4 500 událostí za sekundu, můžu to tak nechat? Odhad potřebného výkonu systému pro sběr logů nebo SIEM je věštěním z křišťálové koule.

Potřebujete se dostat k výsledku, kolik EPS (Events Per Second) vygenerují zařízení v počítačové síti a jak velký prostor událostí zaberou. Nejlepší je stanovit tyto hodnoty pro všechny aplikace, servery, počítače, přepínače, prostě vše, co je k počítačové síti připojeno. A udělat odhad, co budete v dohledné době přidávat. Vyjde astronomické číslo. Pak si z celkové množiny zdrojů vyberete jen ty zdroje, které jsou zajímavé. Z hlediska bezpečnosti obchodních aplikací to budou všechny kritické aplikace a systémy, které je sledují, třeba DLP. Z hlediska čisté bezpečnosti potřebujete firewally, IPS, antiviry. A z hlediska provozu jsou to servery, na kterých běží kritické obchodní aplikace, ale také AD servery, systémy pro 802.1x a přepínače. Je na zvážení, zda potřebuji sbírat data opravdu ze všech zdrojů, nebo si definovat vlastní množinu.

Jenže jak se dostat k informaci, kolik který zdroj dává EPS. Výrobce nebo autor aplikace to neprozradí, sám to neví.

Musíte udělat studii proveditelnosti (proof of concept). Nejlepší je získat požadované údaje na základě měření. To znamená nasadit zkušebně zařízení pro sběr logů. A sbírat logy ze všech zdrojů a po určité době, obvykle jeden až dva měsíce, sběr vyhodnotit. Pak sestavit tabulku požadovaných zdrojů logů a na základě měření ji doplnit o EPS a velikost, jakou jednotlivý záznam v databázi zabere.

Zní to jednoduše. Sehnat zařízení pro sběr, případně externí experty je ta jednodušší část. Jak ale donutit všechny správce serverů a aplikací, bezpečáky a síťaře, aby nastavili na zasílání logů na dočasný systém pro sběr logů? Že jim prostě vydáte pokyn? Tak hodně štěstí, tudy cesta, v opravdu velké počítačové síti, obvykle nevede.

Nezbude, než stanovit kapacitu odhadem podle seznamu zdrojů logů. Vyčistit od duplicit a zkontrolovat, zda tam nic nechybí. To zabere klidně několik dní práce.

Jak stanovit EPS a velikost záznamu pro jednotlivé zdroje? Obvykle nezbude, než pozvat externího experta.

Ten si zdroje rozdělí do skupin podle druhu – pracovní stanice, servery, aplikace provozní, vývojové a testovací, přepínače, bezpečnostní zařízení, firewally externí a interní a další. Každé skupině přiřadí hodnotu EPS a velikost záznamu.

Kde ty hodnoty získal? Lety praxe a expertní zkušeností. Bezpečnostní a síťová zařízení, ta jsou celkem odhadnutelná, servery a stanice ještě také. Zato kritické obchodní aplikace, to je bez měření opravdu věštění z křišťálové koule.

Výsledkem bude množina zdrojů, odhad EPS a velikosti záznamu. Z těchto údajů si už spočítáte důležité hodnoty – EPS a velikost místa, jakou zprávy zaberou, a také retenci logů při daném úložném prostoru. Podle množiny zdrojů logů a EPS také stanovíte potřebné licence, jsou-li potřeba.

A pak přijde DDoS útok na externí firewally a křišťálová koule se rozprskne na tisíce malých střípků. ■