Proč začít log managementem, a ne hned se SIEM?

Víte, jaké největší chyby se dopouští většina bezpečnostních manažerů při implementaci SIEM? Chtějí mít všechno a hned a musí to fungovat samo. K plně funkčnímu řešení SIEM ale vede poměrně obtížná cesta.

FILIP WEBER

Při výběru plnohodnotného SIEM řešení se vše točí kolem licencí a implementace a nemalých nákladů. Většina renomovaných výrobců řešení SIEM počítá licence podle množství zdrojů odesílajících logy a podle schopnosti přijímat určité množství událostí za sekundu.

Potřebné funkce

Velké SIEM systémy navíc často obsahují řadu zbytečných funkcí jako třeba reporty shody s americkými zákony a nařízeními. K čemu jsou českému úřadu reporty shody, jako jsou Basel II, HIPAA nebo NIST?

Opravdu potřebujete hned v úvodu korelovat data z mnoha různých zdrojů? Většina systémů SIEM umí sice pomocí svých sběračů logů sbírat data z mnoha zařízení, ale jakmile chcete data korelovat, poskytnutá licence dovolí využít jen dva tři zdroje pro korelaci. A za každý další si draze zaplatíte.

Funkce automatického sledování podvodů a chování uživatelů, sledování nestandardní činnosti administrátorů, případně porušení best practice pravidel nebo obecných norem jsou určitě úžasná věc, nicméně opravdu je nezbytné je teď všechny řešit? Vždyť zatím nemáte ani logy uložené na jednom místě.

Otázka správy

Máte vlastního bezpečnostního operátora schopného psát regulární výrazy a pokládat dotazy na různé zdroje dat a vymýšlet korelační podmínky? A pak vyhodnocovat výsledky? Nemáte? Připravte si v rozpočtu hodně peněz na implementaci a provoz.

Aby SIEM opravdu fungoval, tak jej musí někdo hodně znalý a hodně drahý nastavit. A také vyhodnocovat.

SIEM určitě nespočívá v rozsvěcení nějakých kontrolek, případně v přehazování výhybek, kudy data tečou, nebo v automatickém sepnutí blokování toku dat, když se sejdou definované události. Z toho jsou jen plané poplachy.

Není možné nadefinovat předem charakteristiku DDoS útoku na datové centrum a na základě splnění podmínek automaticky odstříhnout datové centrum od určitého rozsahu vnějších adres. Tak to opravdu nefunguje – vždy musí příznaky útoku a samotný útok vyhodnotit operátor.

Máte ale takového operátora? SIEM opravdu není samospasný a automatický systém, vždy je k němu potřeba chytrá hlava s úsudkem.

Postupné zavádění

Začněte postupně. Dnes máte logy uložené na zařízeních a systémech, ti pokročilejší je možná ukládají někam na syslog server nebo do databáze.

Vytvořte si datový sklad na logy – můžete například jen posílit svůj současný syslog, můžete přejít na moderní open source dokumentovou databázi, nad kterou si rozběhnete také open source grafický nástroj na přehledy nad daty. To všechno lze zvládnout vlastními silami nebo za pomoci externích programátorů.

Rozumnější je ale odhodlat se pořídit ucelený systém pro log management. Takový, který detailně parsuje/standardizuje příchozí logy, má jednotné konfigurační rozhraní, dostatečný výkon, kapacitu a zabezpečení uložených dat.

Má přednastavené dashboardy, reporty či alerty a je připravený pro integraci s plnohodnotným SIEM systémem.

To znamená, že podporuje nějaký standardní formát výměny dat mezi SIEM systémy. A až budete mít rozjetý systém pro ukládání a analýzu logů, tak se pusťte do plnohodnotného SIEM.

A důležitá věc, kterou si málokdo při pořizování centrálního úložiště logů nebo i SIEM systému uvědomí. Centrální úložiště logů by nemělo běžet na virtuálním stroji a mělo by být na samostatném hardwaru.

Proč? Systém musí první nabíhat a poslední se vypínat, systém musí být připraven přijímat logy okamžitě po najetí prvního ze serverů nebo zařízení a musí uložit poslední log při vypínání. Co je platný systém pro uložení logů na virtuálu, který se vypne dávno před vypnutím virtuální platformy, firewallů a switchů? ■

Autor pracuje ve společnosti Compunet.