Inteligentný nástroj na ochranu vášho podnikania

Security Information and Event Management, skrátene SIEM, je integrovaný balík produktov na zber, správu a inteligentnú interpretáciu udalostí v IT infraštruktúre. Pomáha pri odhaľovaní incidentov, ktoré môžu ohroziť podnikanie organizácií.

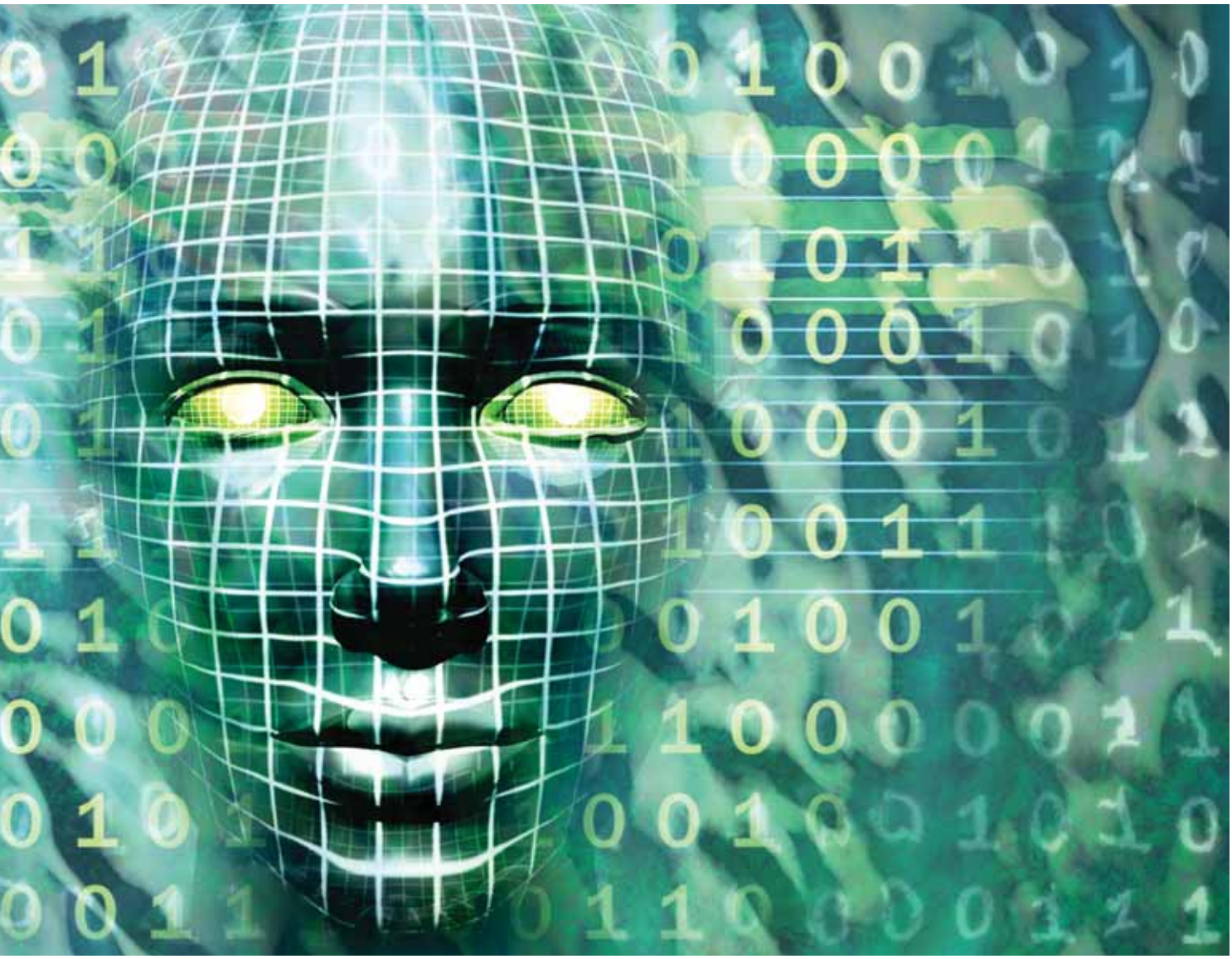
Miroslav Sciranka
pre-sales konzultant TEMPEST
miroslav_sciranka@tempest.sk

Zariadenia v IT infraštruktúre spravidla vykonávajú záznamy o prichádzajúcich požiadavkách i o reakciách na ne. Zjednodušene ich nazývame logy. Na základe týchto záznamov možno odvodiť viacero ďalších veľmi cenných záverov, ktoré môžu pomôcť odhaliť úsilie o odcudzenie informácií, pomôcť s dodržiavaním bezpečnostných noriem a legislatívnych požiadaviek. Organizácie spravidla nemajú vytvorené a implementované metódy, ako účinne interpretovať logy. Keďže sa táto schopnosť firiem stáva čoraz dôležitejšou pre odhaľovanie nebezpečných incidentov, neraz siaha do top priorít mnohých CIO a CSO. Nasadenie metód, či best practices na analýzu udalostí prináša organizáciám obrovskú pridanú hodnotu vo forme zníženia a efektívneho riadenia bezpečnostných rizík i vo forme zhody s legislatívnymi požiadavkami.

RIZIKÁ STRATY UPOZORNENÍ

Riešenia pre bezpečnostný manažment informácií v súčasnosti umožňujú zhromažďovať, korelovať, analyzovať a interpretovať udalosti (logy) v celej IT infraštruktúre tak, aby online poukázali na zdroj útoku, jeho priebeh a cieľ. SIEM môže dosiahnuť svoj plný potenciál len v prípade, keď bude integrovaný do všetkých aplikácií a nástrojov na zabezpečenie siete. Ako príklad by sme mohli uviesť použitie na monitorovanie aplikácií ako sú SAP, e-mailová komunikácia, internet banking a podobne s cieľom odhaliť podvod (fraud detection) alebo konania vedúceho k ohrozeniu zvnútra (insider attack). Spoločnosti začínajú nasadzovať SIEM bok po boku s ich tradičnými bezpečnostnými riešeniami alebo nástrojmi. Výsledkom nasadenia, teda zhromažďovania a analýzy udalostí môžu byť zistenia, ktoré poukazujú

Malé a stredné podniky majú rovnaké bezpečnostné problémy ako veľké spoločnosti, ak sú konfrontované s úlohou chrániť svoje podnikanie.



na podvod, odcudzenie senzitívnych informácií, zneužitie osobných údajov alebo kreditných kariet.

Ak je riešenie nasadené správne, správa hrozieb sa stane oveľa jednoduchšia a účinnejšia. Veľakrát majú podniky zavedené postupy a procesy na sledovanie udalostí, ale jednoducho ich nestačia spracúvať, správne interpretovať a zmerať ich význam pre bezpečnosť aj biznis firmy v reálnom čase. Inštalované bezpečnostné systémy (FW, IDS/IPS, AV, VPN atď.) generujú také množstvo informácií, že je namáhavé určiť, ktoré zraniteľnosti si vyžadujú okamžitý a vysoko prioritný prístup. Neraz je na túto činnosť v spoločnosti určených pár pracovníkov, ktorí musia používať separátne nástroje na prezeranie informácií z rôznych pohľadov s rôznymi prístupmi. Napríklad, ak jeden výrobca firewallov pokladá udalosť za kritickú, iný výrobca IDS systému tú istú udalosť môže pokladať za neškodnú. Takže hoci máme príslušné nástroje, môžu sa niektoré udalosti strácať a stále existuje v celom bezpečnostnom systéme nezanedbateľná miera rizika straty dôležitých upozornení. Preto je dôležité mať k dispozícii nástroj – takú SIEM platformu, ktorá má vlastnú, pre váš biznis prispôsobenú logiku na identifikáciu, stanovenie priorít a zmiernenie hrozieb. Sú tu však už aj prvé náznaky plnej integrácie a niektorí výrobcovia začali spájať alebo integrovať Security Information and Event Management s ostatnými časťami z ich portfólia, vrátane IAM (Identity and Access Management), správy systémov, správy rizík ako aj s riadením zhody s legislatívnymi predpismi či

Nasadenie metód na analýzu udalostí prináša organizáciám obrovskú pridanú hodnotu vo forme zníženia a efektívneho riadenia bezpečnostných rizík i vo forme zhody s legislatívnymi požiadavkami.

požiadavkami. Rovnako neoddeliteľnou súčasťou musí byť riadenie bezpečnosti, správa záznamov a rozsiahly reporting (napr. COBIT, GLB, HIPPA, PCI či Sarbanes Oxley).

MANAŽMENT INFORMÁCIÍ ALEBO LOGOV?

Správa záznamov (log management) je tradične určená na sledovanie záznamov z firewallu o povolení alebo zamietnutí prístupu k sieťovým zdrojom, na sledovanie zmien konfigurácie operačného systému, vypnutie alebo reštart systému, povolenie, či zamietnutie prístupu k súboru. Log management tak tvorí základ na odhaľovanie potenciálnych incidentov, teda pre komplexný Security Information and Event Management. Jemné detaily, ktoré poskytuje log management sa stávajú čoraz viac užitočné v kombinácii s korelačnými schopnosťami SIEM-u. Podľa spoločností The InfoPro a Gartner integrácia oboch technológií je len ďalším logickým krokom. Log management umožňuje používateľom získavať záznamy, špecifické systémové udalosti a oznámenia generované operačnými systémami, zariadeniami a aplikáciami. Všetky tieto dáta sú umiestnené centrálne. Nástroje log managementu sú zamerané na posudzovanie, reporting a umožňujú používateľom vidieť udalosti ex post. Produkty bezpečnostného manažmentu informácií pridávajú vrstvu inteligencie prostredníctvom korelácií, redukcie udalostí, varovaní a analýzy v reálnom čase. Tieto riešenia porovnávajú a analyzujú všetky záznamy, udalosti a transakčné informácie s cieľom nájsť potenciálne bezpečnostné hrozby a riziká. Dá sa povedať, že SIEM vznikol evolúciou zo správy log záznamov.

Výsledkom nasadenia, teda zhromažďovania a analýzy udalostí môžu byť zistenia, ktoré poukazujú na podvod, odcudzenie senzitívnych informácií, zneužitie osobných údajov alebo kreditných kariet.

VHODNÝ AJ PRE MALÉ A STREDNÉ PODNIKY

Hoci sa nástroje pre Security Information and Event Management zdokonaľujú z verzie na verziu, stále sa môžu zdať príliš komplikované, a to najmä v prípade veľkých podnikov, keď zložitosť ich implementácie dramaticky narastá s veľkosťou a zložitosťou infraštruktúry. Malé a stredné podniky majú rovnaké bezpečnostné problémy ako veľké spoločnosti, ak sú konfrontované s úlohou chrániť svoje podnikanie. Kľúčové je, že majú spravidla menej prostriedkov na ich riešenie a menej prostriedkov na špičkových expertov so znalosťami z oblasti bezpečnosti. SIEM šitý na mieru menším firmám musí byť jednoduchý a ľahko použiteľný. Práve kvôli tomu tieto menšie spoločnosti potrebujú automatizované riešenie, ktoré odbremení zamestnancov od manuálneho triedenia nahromadených dát.

PRÍNOSY PRE BEZPEČNOSTNÝ MANAŽMENT INFORMÁCIÍ

- účinné odhaľovanie a predchádzanie neautorizovanému prístupu k informáciám, zníženie rizika bezpečnostného prieniku do systémov a tým ochrana značky, vzťahov so zákazníkmi a ochrana dobrého mena spoločnosti;
- jednoduché a rýchle zrekonštruovanie nepovoleného prieniku do systému, odhalenie príčin jeho vzniku. SIEM výrazne napomáha zastaviť útoky pred ich zintenzívnením, čím zmierňuje škody a šetrí finančné náklady. Pomáha rýchlejšie vykonať obnovu systému a odstrániť škody;
- jednoduché zavádzanie zhody s legislatívnymi požiadavkami (compliance);
- zníženie nákladov na monitoring ako aj nákladov na bezpečnostný personál.

Spoločnosť TEMPEST a.s. implementovala a v súčasnosti poskytuje podporu v oblasti Security Information and Event Management riešení organizáciám z oblastí telekomunikácií, energetiky i finančníctva. TEMPEST má skúsených odborníkov od viacerých svetových výrobcov ako Cisco, Enterasys alebo RSA (Security division EMC).

ZOPÁR TIPOV AKO ZAČAŤ

- **Začnime so základným pochopením svojich bezpečnostných udalostí**
  Ešte pred výberom nástroja musíme urobiť ohodnotenie rizík. Tak by sme mali zistiť, čo vlastne potrebujeme. Pozrime sa na každý typ udalosti, ktorý prebieha v IT prostredí a posúďme mieru ohrozenia. Okrem toho sa utvrďme v tom, že rozumieme upozorneniam ako aj stratégii zmierňovania hrozieb.
- **Neodhryznime si príliš veľký kus**
  Začnime pomaly – táto rada platí pri nasadzovaní SIEM riešenia vari dvojnásobne. Najprv si skúsme nainštalovať produkt v testovacej časti domácej siete. Ono totiž často produkt na papieri „vie“ ďaleko viac ako v skutočnej prevádzke.
- **Vytvorme si systém, ako nakladať s výstrahami**
  Ak nemáme vytvorené a zavedené pravidlá alebo procesy ako vybavovať výstrahy a záznamy, tak SIEM riešenie našu situáciu nijako výrazne nezlepší. Pokiaľ nemáme plán pred nasadením, môžu sa naše investície do SIEM riešenia minúť účinkom.
- **Zaangažujme vedúcich pracovníkov**
  Správne si definujme svoj mandát, svoje právomoci a nechajme si ich schváliť vedením organizácie. IT tímy totiž budú musieť pracovať so záznamami, ktoré by mohli byť citlivé alebo by mohli mať dôverný charakter.