Preukazovanie súladu stavu ochrany osobných údajov s legislatívnymi požiadavkami v automatizovaných informačných systémoch

Október 2011

Ladislav Nyíri
lnyiri@novell.com

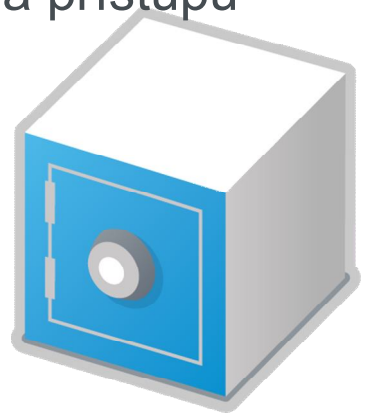
Novell®

Ako je to s bezpečnosť ou

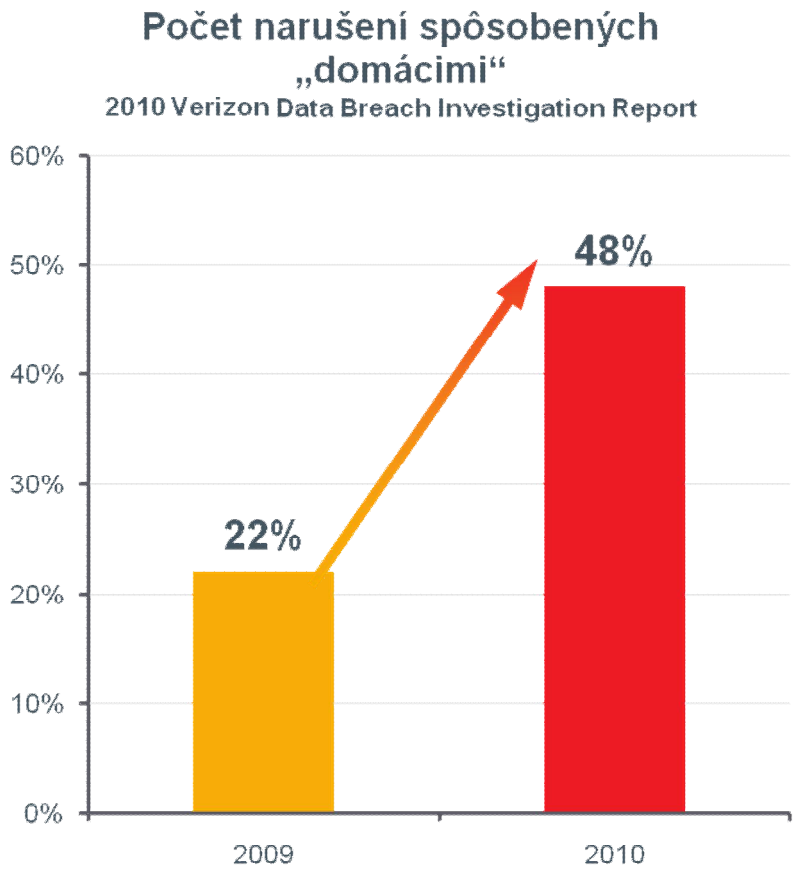
- V priebehu uplynulých 6 rokov podľa správy spoločnosti Verizon Business Data Breach Investigation Report (DBIR) bolo evidovaných viac ako 900 narušení, 900 miliónov záznamov bolo zneužitých
- Skladba narušení v minulom roku (podľa DBIR)
  - 70% záznamov bolo na kompromitovaných externých zdrojoch
  - 48% narušení spôsobili „domáci“
  - 32% narušení malo vážne dopady na obchodných partnerov
- 96% týchto prípadov bolo možné ošetriť pomocou jednoduchého riadenia a monitorovania prístupu

Kde sa nachádzame?

- Vyberte si najhodnotnejšie údaje vo vašej organizácii
  - Implementovali ste riadenie prístupu, aby ste si ich ochránili
  - Je takmer nemožné, aby sa k nim dostal niekto neoprávnený
- Aby však mohli byť údaje užitočné, niekto k nim musí pristupovať
  - „domáci“ sú najväčším bezpečnostným rizikom
  - Útočníci sa snažia objaviť slabiny ošetrenia prístupu intenzitou, ako nikdy predtým
- Ako riešite túto výzvu?



Bezpečnostné riziko „Domáci“

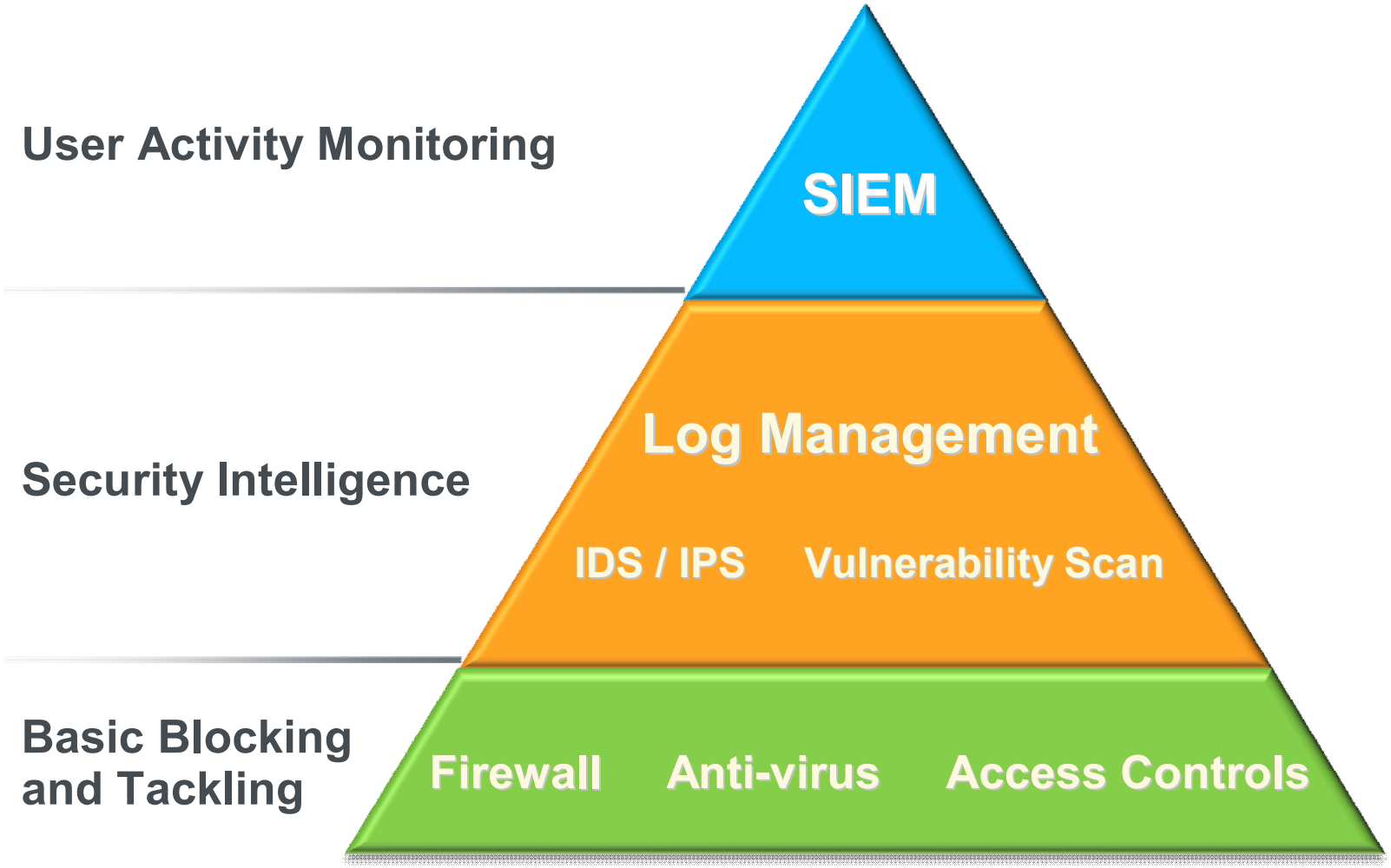


- Nárast v počte narušení „domácimi“ používateľmi
  - Niekedy je nutné sprístupniť údaje, ale…
    - Stanice niekedy nie sú zabezpečené adekvátne
    - Niekedy existujú iné dôvody (úplatky,...)
    - Chyby v riadení
- Externí narušitelia však nezmizli (len ich nárast je nižší)

Skutočná výzva

- Všetky systémy a aplikácie v rámci organizácie generujú záplavu informácií
- Zákazníci musia z tejto záplavy vyselektovať adekvátnu vzorku, aby zodpovedali kritické otázky:
  - "Som zabezpečený?" a "Ako bezpečné sú moje systémy?"
  - "Som v súlade s legislatívou [PCI-SS/SOX/BASELII/HIPAA]?"
  - "Kto pristupoval k týmto údajom?"
  - "Ktoré systémy mám zraniteľné?"
- Rôznorodosť systémov a objem informácií potrebných spracovať je prekážkou rýchlych odpovedí

Základný recept na bezpečnosť



Čo je „Log Management“?

- Nástroj pre zber a uchovávanie obrovského množstva bezpečnostných logov so schopnosťou vyhľadávania a reportovania
- Štandardne sa zavádza ako odpoveď na legislatívne požiadavky, ako sú
  - PCI
  - Sarbanes Oxley (SOX)
  - HIPAA

„Log Management“ – Základná funkčnosť

- **Zber** logov z rôznych sieťových zariadení, bezpečnostných aplikácií a podnikových aplikácií
- **Uchovávanie** týchto logov počas definovanej periódy ideálne za najnižšie náklady
- **Umožnenie vyhľadávania** vo všetkých uložených logoch na základe podnetov za účelom nájdenia anomálií a súvislostí
- **Posielanie** pravidelných správ určeným osobám za účelom naplnenia legislatívnych požiadaviek

Prečo „Log Management“?

- Auditori vyžadujú správy o stave zabezpečenia systémov, ale **prečo**?
  - Používajú informácie z logov na zistenie, či bezpečnostná infraštruktúra je funkčná a či pracuje podľa očakávaní
  - V prípadoch narušenia bezpečnosti útočníci vždy zanechávajú “digitálny otlačok”
- V prípade narušenia je potrebné preukázať ho, zanalyzovať aktivity aby bolo možné:
  - Obnoviť funkčný stav po narušení
  - Zistiť závažnosť narušenia (akých údajov sa týka)
  - Preukázať osobnú zodpovednosť účastníkov

Použitie Log Managementu pre prevenciu

- Log management poskytuje transparentnosť potrebnú pre odhaľovanie potencionálnych hrozieb a zraniteľností
  - Vyžaduje istú dávku bdelosti
- Použitím log management-u je možné objaviť:
  - Nesprávnu konfiguráciu programov a zariadení
  - Kto pristupuje k údajom
  - Kto mení konfiguráciu
  - Kto má prístup k senzitívnym údajom
  - Ktorí správcovia si zdieľajú heslo a nedbajú na bezpečnosť

Použitie Log Management-u pre detekciu

- Log management môže byť nápomocný pri zistení, či došlo k narušeniu
  - Exaktne vedieť , že došlo k narušeniu je často veľmi obtiažne
- Aktívna správa logov vám preukáže:
  - Či bol neočakávane vytváraný nový používateľ
  - Kto si zvýšil privilégiá
  - Či intenzita útokov stúpa
  - Či bol cieľom útokov neošetrený zraniteľný systém
  - Či niekto pozmenil konfiguráciu a kto to bol

Použitie Log Mangementu pre vyšetrovanie

- Udalosti zachytené v logoch môžu byť nápomocné v rekonštrukcii narušenia
  - Log Management poskytuje transparentnú viditeľnosť celou IT infraštruktúrou
  - Umožňuje zistiť základnú príčinu, ktorá umožnila narušenie
- Správa logov sa môže použiť na zistenie čo a ako sa stalo, a na základe týchto informácií je možné navrhnúť správnu obnovu po narušení, či znížiť následky narušenia:
  - Ktoré systémy a aplikácie boli kompromitované
  - Vektor použitého útoku
  - Ktorý bezpečnostný systém zlyhal
  - Či bol útok identifikovaný alebo nie
  - Či útok bol vedený zvonku, alebo k nemu prispeli aj „domáci“

Použitie Log Managementu pre preukazovanie zhody s legislatívou

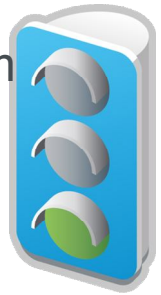
- Log management zjednodušuje preukazovanie zhody s predpismi poskytovaním:
  - Zákaznícky definovateľných predpripravených reportov
  - Priestoru pre úschovu logov počas požadovanej doby
  - Možnosťou vyhľadávania súvislostí medzi rôznymi udalosťami a systémami
  - Schopnosť preukázať efektívnosť riadenia bezpečnosti.

SIEM: Kedy potrebujem takéto riešenie?

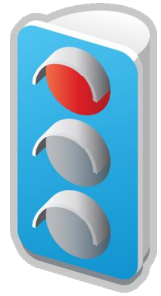
- Požiadavka na kontinuálny monitoring aplikácií, systémov na bezpečnostné anomálie
- Realizovanie odoziev takmer v reálnom čase keď je aktívna bezpečnostná anomália
- Požiadavka na kontinuálny monitoring IT alebo riadenia prevádzky
- Je vhodné mať doplnkovú jednoduchú správu logov za účelom operácií nad historickými údajmi

SIEM/Log Management Best Practices

- Nesprávny vstupný údaj = nesprávny výstupný údaj
- Príliš veľa údajov spôsobuje preťaženie systémov
- Začínajte s menšími implementáciami, moderné technológie sú škálovateľné
- Použite systém na správu logov na filtrovanie údajov postupujúcich do systému SIEM
- Skôr ako začnete riešiť problematiku SIEM, musíte porozumieť vášmu prostrediu, údajom ktoré vie poskytovať
- Postupujte v systematických krokoch s potrebou vyhodnotenia úspechu každého z nich
- Použite SIEM/LM na preukazovanie poskytovaných služieb iným úsekom v organizácii / partnerom
- Dbajte na ochranu osobných údajov



Nedoporučené postupy pre SIEM/LM



- Vynechanie fázy definovania požiadaviek na systém SIEM/LM
- Ponechanie definovania odhadu náročnosti spracovania udalostí zo systémov až po kúpe riešenia SIEM/LM
- Jediné kritérium výberu cena
- Očakávať, že vám výrobca povie, čo máte zapisovať do logov
- Domnievať sa, že celý SIEM/LM uvediete do prevádzky bez zainteresovania ostatných vo vašej organizácii
- Ignorovanie vašeho právneho oddelenia
- Nasadzovanie riešenia SIEM/LM „hurá systémom“ a nie vo fázach
- Vynechanie školení, lebo rozhranie je intuitívne
- Očakávanie okamžitej redukcie práce po nasadení riešenia SIEM/ LM

Nástroje pre správu bezpečnosti od spoločnosti Novell

Novell® Sentinel™

“Zhoda s predpismi a bezpečnosť”

Log Management

- Audit / reporty zhody s predpismi
- Zber, uchovávanie, analýza
- Pokročilá analýza

Security Monitoring and Remediation

- Monitorovanie v reálnom čase
- Historická analýza
- Automatizovaná obnova po narušení

User Activity Monitoring

- Správa rizika používateľských prístupov
- Monitorovanie krádeže identity
- Komplexný prehľad o stave bezpečnosti a zhody s predpismi

Corporate Headquarters
1800 South, Novell Place
Provo, Utah 84606

801.861.7000 (Worldwide)
800.453.1267 (Toll-free)

Join us on:
www.novell.com

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. Novell, Inc. may make improvements in or changes to the software described in this document at any time.