SECURITY 2012

20. ročník konference o bezpečnosti v ICT

Monitorování a audit databází v reálném čase

Ing. Jan Musil

IBM Česká republika

Jsou naše data chráněna proti zneužití ?

Ano, pokud ...


Nepoužitelné
Steve Mandel, Hidden Valley Observatory
http://apod.nasa.gov/apod/ap010809.html

Jsou naše data chráněna proti zneužití ?

1) vůbec připustíme,
   že můžeme být obětí útoku

2) víme, co bychom měli chránit

Ano, pokud

3) víme, kdo může být útočník

4) víme, jaké prostředky použít
   pro ochranu

Jaká je realita ?

- 86% útoků se oběti dověděli až od třetích stran (třeba od svých zákazníků ...)
- Pouze 6% útoků bylo odhaleno aktivními interními prostředky
- 92% útoků bylo podniknuto zvenku
- 17% útoků bylo provedeno zevnitř podniku
  - 85% zaměstnanci
  - 3% systémoví a síťoví administrátoři
- 89 % obětí nesplňovalo v době útoku standard PCI DSS, i když mu podléhali

Zdroj: Verizon Business 2011 Data Breach Investigations Report:
http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf

Proč nejsou databázové útoky odhaleny ?

Příčina: Není prováděn vůbec žádný audit a monitoring nebo naopak audit se provádí na vše a nikdo nikdy již neprovede analýzu

Řešení: Zvolení **vhodného** prostředku a **vhodných** postupů

Příčina: Neomezený přístup k datům privilegovanými uživateli a možné zneužití citlivých dat

Řešení: Zvolení na privilegovaných uživatelích zcela nezávislého prostředku pro audit s možností blokování přístupu

Příčina: Aplikační uživatelé mají přístup k neúměrně velkému množství dat

Řešení: Odejmutí práva PUBLIC pro všechny databázové objekty a systém varování pro případ, že uživatel zpracuje neúměrně více záznamů, než obvykle

Proč nejsou databázové útoky odhaleny ?

Příčina: Neexistuje komplexní pohled na míru zabezpečení jak databázového systému tak prostředí, ve kterém pracuje

Řešení: Použití detailně propracovaného a automatizovaného systému kontroly zranitelnosti systému

Příčina: Neautorizované přidávání a modifikace uživatelských účtů

Řešení: Audit DCL (grant, revoke) příkazů

Příčina: Přístup k datům mimo pracovní dobu resp. přístup prostřednictvím neschválených komunikačních kanálů

Řešení: Dynamická změna pravidel auditu v čase a sledování i dalších informací než pouze SQL operace (např. IP a MAC adresy klientů, typ klientské aplikace)

Co dalšího je třeba sledovat ?

- Neschválené změny databázových systémů
- Změny konfigurace systémů za účelem zhoršení výkonnosti nebo havárie systému
- Záplatování produkčních systémů nesprávnými záplatami nebo v nevhodnou dobu

Jaké nástroje pro ochranu
databází musíme hledat ?

Proč není vhodný
nativní databázový audit ?

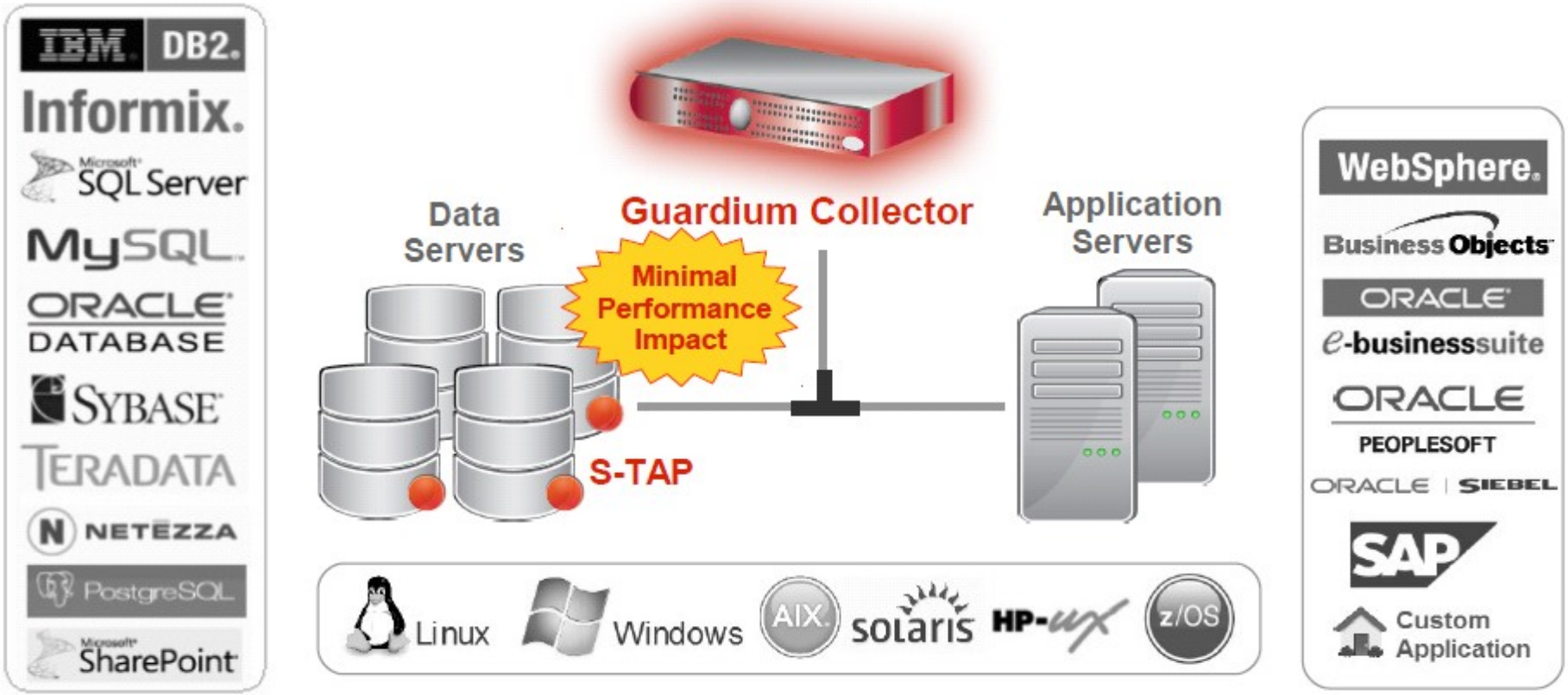
Problémy nativního db auditu

- Výrazný vliv na výkonnost databáze
- Neumožňuje aktivní opatření v reálném čase
- Vyžaduje časově náročnou analýzu sebraných dat (ovšem až po případném incidentu)
- Výstupy nejsou uloženy bezpečně
- Neumožňuje dostatečně oddělit role (administrátor vs. auditor)
- Nelze identifikovat skutečného koncového uživatele ve vícevrstvé architektuře
- Nekonzistentní v případě použití různých databázových platforem

Vlastnosti požadovaného nástroje

- Nezávislost na privilegovaných uživatelích
- Monitorování a audit v reálném čase
- Aktivní zamezení přístupu k citlivým datům
- Aktivní systém varování
- Minimalizace vlivu na výkonnost databázových serverů
- Rychlé zjištění neautorizovaných nebo podezřelých aktivit v reálném čase
- Automatizované workflow řešení incidentů
- Bezpečné uložení auditních záznamů
- Jednotná forma tvaru auditních záznamů pro všechny podporované db platformy
- Audit a monitorování skutečných koncových uživatelů

IBM InfoSphere Guardium



- **Kolektor** – Neinvazivní zařízení, které prosazuje dodržování politik, žurnáluje databázové aktivity a spouští reporty a auditní procesy
- **S-TAP sonda** – Na databázích nezávislý SW agent, který posílá monitorované databázové aktivity do kolektoru pro další analýzu a případné žurnálování

Případová studie

- **Zákazník:** Globální telekomunikační mobilní operátor
- **Důvod implementace:** Zabezpečení záznamů o hovorech z důvodu naplnění zákona o ochraně citlivých dat
- **Prostředí:** 15 geograficky oddělených datových center
  - Oracle, SQL Server, Informix, Sybase
  - SAP, Remedy
  - Vlastní aplikace "na klíč"
- **Zvažované alternativy:** Nativní audit, konkurenční řešení
  - *Nevýhody nativního auditu:* vliv na výkonnost, není dostatečně detailní
  - *Nevýhody konkurenčního řešení:* nebylo možné nasadit v heterogenním prostředí databází více dodavatelů, nepodporuje starší verze databázových serverů

Případová studie – dosažené výsledky

- Pro prvních 12 datových center nasazeno pouze za 2 týdny!
- I přes vysoký objem přenášených dat řešení úspěšně monitoruje veškeré aktivity celého prostředí
- Centralizace monitorování a auditu heterogenního prostředí
- Prostředí prošlo úspěšně několika externími audity

Případová studie – názor zákazníka

„Nyní jsme schopni detekovat interní a externí přístupy k fakturačním a PCI záznamům“

„Víme, kdo a kdy mění schémata databází“

„Okamžitě zjistíme, pokud autorizovaná osoba stahuje neobvyklé množství citlivých informací o našich zákaznících“

„Neúměrně vysoký počet neúspěšných přihlášení do systému nebo velký počet SQL chyb nám signalizují možný útok na systém“

Děkujeme za pozornost.

Jan Musil
IBM Česká republika
jan_musil@cz.ibm.com