MYSQL GDPR BEST PRACTICES A REÁLNÉ PŘÍKLADY

Peter Rus
Team Leader - Oracle
peter.rus@techdata.com

MySQL

- Plnohodnotný RDBMS
- Celosvětově druhá nejpoužívanější databáze na světě (db-engines.com)
- Tradičně součást LAMP
- Community edice je dostupná zdarma, k dispozici jsou i edice s předplatným podpory (Standard, Enterprise, Cluster Carrier Grade)
- Funkce popisované na dalších stranách vyžadují min. Enterprise edici

ORACLE

TechData

Posouzení vlivu (články 35, 90, 91)

- Analýza účtů a reporting
- Identifikace bezpečnostních rizik (díry, slabá místa)
- Porovnání konfigurace s centrální politikou
- Analýza dat – detekce osobních dat
- Monitorování uživatelů, hesel a privilegií
- Správa uživatelů prostřednictvím Pluggable Authentication Modules – Linux, Kerberos, Microsoft Active Directory

- MySQL publikuje „Security Best Practices Guidelines“, nejste na to sami.

- Workbench, Enterprise Monitor

Prevence (články 32, 83, 28, 26, 5, 20, 27, 30, 64)

- Transparentní šifrování dat (vč. záloh)
- Firewall (SQL Injection, IDS), IP whitelisting

- Ent. Security, Firewall

Detekce (články 30, 82, 33)

- Audit log
- Detekce nevhodného použití DB
- Alerts – např. v případě nevhodného přístupu k osobním datům
- Hashe, podpisy, šifrování (AES, SHA-1&2, RSA, DSA, DH)

- Enterprise Audit, Oracle Audit Vault

Případová studie

- Zákazník, společnost v jihovýchodní Evropě, provozuje 2 velké portály
  pro zaměstnance/zaměstnavatele (5 serverů),
  a pro přímý prodej vozidel (4 servery).
- Back end a front end byl provozován na DB Percona (fork MySQL se službami)
- Při studii dopadů GDPR na systémy bylo identifikováno několik situací, které stávající řešení nemohlo vyřešit:
  - Bylo možné šifrovat data, ale klíče musí být uloženy na stejném serveru
  - Nebylo možné dostatečně podrobně kontrolovat přístup k datům, a jejich užívání
  - Nalezená dílčí řešení způsobila dramatický pokles výkonu
  - Zálohy dat, s ohledem na šifrování

Případová studie - pokračování

- „Režim učení“ – MySQL monitoruje uživatele a jejich dotazy, a postupem času vytvoří „White list“ schválených činností. Činnosti mimo White list spustí Alert.
- Oracle Audit Vault – pro uchování záznamů Auditu
- Oracle Key Vault – pro správu klíčů
- MySQL nativní nástroje:
  - Backup – šifrované zálohy,
  - Enterprise Monitor – dohled na systém, detekce rizik
  - Firewall – prevence přístupu k DB, SQL Injection

7

Postřehy z implementace

- MySQL „našel" na podobné akci, jaká je ta dnešní.
- Vliv na výkon byl označen jako „akceptovatelný", cca 10% pokles.
- Během spolupráce musely být nahrazeny některé šablony z CMS, kvůli bezpečnostním rizikům
- Činnosti byly rozděleny na dva kroky:
  1. Zajistit, aby technologie poskytovala šifrování, přístup k datům, audit, monitorování, a firewall. (Hotovo)
  2. Zabránit zneužití dat, prostřednictvím nastavení rolí. Nyní lze zjistit, kdo k jakým datům přistoupil, ale tento krok aktivně omezí data, která jednotlivé role budou moci z DB získat.

8

Není třeba čekat

… 25. května 2018

9