ORACLE

Ste očkovaní proti ransomware?

Marián Kuna
Oracle Slovensko

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Ransomware is a type of malicious attack where attackers encrypt or steal organization's data and demand payment to **restore access** or to not **disclose data publicly**.

Príklady ransomware útokov

Marec 2021

- > 30,000 napadnutých organizácií
- Zraniteľnosť v MS Exchange serveri
- Administratívny prístup k serverom obetí

Máj 2021

- Zastavená distribúcia paliva na východnom pobreží
- Výkupné vo výške $5 mil.
- Kompromitované VPN heslo
- Chýbajúca dvojfaktorová autentifikácia

December 2020

- Škodlivý kód vložený do Solarwinds Orion aplikácie
- >18,000 napadnutých organizácií (Microsoft, VMWare, Cisco)
- Komplexná séria aktivít na oklamanie systému na detekciu rizík

Typický útok ransomware

Vektor útoku :
Získanie prihlasovacích údajov, nové/známe zraniteľnosti, phishingové emaily, ...

Získanie prístupu:
Lokálny prístup, prístup k sieti, prístup k serverom, privilegovaný prístup...

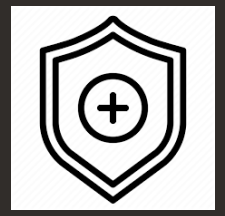
Útok na úložisko a dáta:
Manipulácia s dátami za účelom vydierania

Prístup k zálohám:
Horizontálne šírenie ransomware pre prístup k ostatným systémom vrátane záloh

Zaplatenie výkupného

Spustenie útoku:
Heker spustí útok z „command & control“ centra

Ochrana proti ransomware



Prevencia

Zúženie priestoru na útok

- Hardening systémov
- Pravidelné aktualizácie
- Autentifikácia a riadenie prístupu
- Monitorovanie a alerty
- Bezpečnostné „best pactices“

Zotavenie

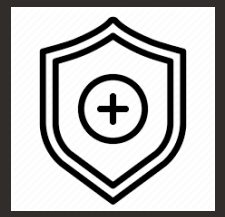
Zálohovanie a obnova

- Silne zabezpečený systém na zálohu a obnovy
- Testovanie obnovy zo zálohy

Ochrana pred únikom citlivých dát

- Šifrovanie dát (produkčné, testovacie, zálohy,...)

Ochrana dát v Oracle databáze



Prevencia

Zúženie priestoru na útok

- Hardening systémov
- Pravidelné aktualizácie
- Autentifikácia a riadenie prístupu
- Monitorovanie a alerty
- Bezpečnostné „best pactices“

ORACLE®

- Linux na Exadate má len 700 balíkov (bežná linux distribúcia > 5000)
- Microkernel len 38 MB (štandardne > 150MB)
- Oracle Database Vault pre riadenie prístupu k dátam
- Database Firewall pre odhalenie útokov
- Database Audit a alerty pre včasné varovanie

Ochrana dát v Oracle databáze

Zotavenie

Zálohovanie a obnova

- Silne zabezpečený systém na zálohu a obnovy
- Testovanie obnovy zo zálohy

Ochrana pred únikom citlivých dát

- Šifrovanie dát (produkčné, testovacie, zálohy,...)

ORACLE®

- Oracle Recovery Appliance
  - Automatická kontrola obnovy
  - Izolovaný „air-gapped“ vault
  - Offsite záloha typu WORM
- Transparent Data Encryption
  - Transparentné šifrovanie dát vrátane záloh
  - Key vault alebo HSM pre bezpečné uchovanie šifrovacích kľúčov

Typický útok ransomware

Vektor útoku :
Získanie prihlasovacích údajov, nové/známe zraniteľnosti, phishingové emaily, ...

Hardened infrastructure, silná autentifikácia a riadenie prístupu, Oracle database Vault

Získanie prístupu:
Lokálny prístup, prístup k sieti, prístup k serverom, privilegovaný prístup...

Oracle Audit Vault a Database Firewall

Útok na úložisko a dáta:
Manipulácia s dátami za účelom vydierania

Transparent Data Encryption

Prístup k zálohám:
Horizontálne šírenie ransomware pre prístup k ostatným systémom vrátane záloh

Recovery appliance, izolovaná záloha, offsite WORM zálohy

Zaplatenie výkupného

Spustenie útoku:
Heker spustí útok z „command & control“ centra

NEPLATTE VÝKUPNÉ !!!
Úplná obnova bez straty dát

Ďakujem za pozornosť

marian.kuna@oracle.com

ORACLE