Behatolás védelem IBM-ISS eszközökkel - szerver és hálózat védelmi megoldások a pénzügyi szektorban

IBM IT biztonsági szeminárium
2012. június 12.

Tóth Vencel

NOREG
Információvédelmi Kft.
SZIGORÚAN BIZALMAS

•Fő védelmi körök

- Határvédelem
- Kibővített határvédelem
- Belső védelem

•Határvédelem

- Alap hálózati IPS – GX4004
- Menedzsment – SiteProtector
- További kérdés:
  - Titkosított forgalom, pl. SSL védelem

•Kibővített határvédelem

- Alap hálózati IPS – GX4004
- LAN oldali nagyobb sávszélesség kezelése – gigabites IPS-ek – GX5000-es sorozat
- Fontosabb DMZ és LAN szerverek védelme hoszt IPS-sel – Server Protection
- Menedzsment – SiteProtector

•Kibővített határvédelem

- Kérdések:
  - Nagyobb sávszélességek kezelése
  - Támogatott operációs rendszerek
  - További hálózatvédelmi funkciók:
    - Virtual Patching
    - DoS és DDoS védelem
    - Web Application Security
    - Content Analyzer - DLP
    - SNORT signatures

•Belső védelem

- Kibővített határvédelem +
  - Core nIPS védelem (10 Gbps) – GX7000-es sorozat (akár 20+ Gbps)
  - További szerverek hIPS védelme
  - Virtuális környezetek védelme – Virtual Server Protection
  - Desktop védelem – Proventia Desktop + Endpoint Protection

•Belső védelem

- További kérdés:
  - Támogatott rendszerek
  - További védelmi funkciók használata:
    - Firewall
    - Buffer Overflow Exploit Prevention
    - File Integrity Monitoring
    - Application Control
    - Inter-VM traffic analysis and transparant intrusion prevention
    - VM Rootkit Detection
    - Virtual network segmentation and network access control
    - Virtual infrastructure auditing

•Összefoglaló

- Teljes körű közös menedzsment
- Hálózati védelem
- Széles körű hoszt oldali védelem
- Virtuális rendszerek védelme
- Széles körű integrálhatóság SIEM rendszerekbe – pl. QRadar

- Kérdések?

NOREG
Információvédelmi Kft.
SZIGORÚAN BIZALMAS