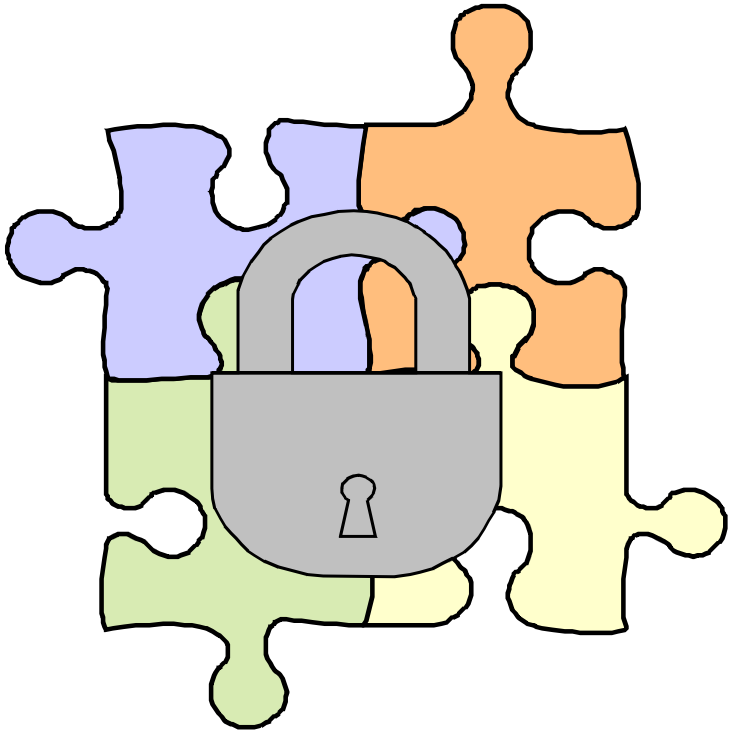
Trendy a řešení v oblasti analýzy a monitoringu bezpečnostních incidentů



Ing. Adrian Demeter

Technical Director

GC System a.s.

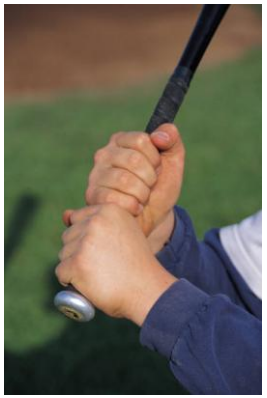
Potenciální oblasti rizik

Ztráta dat jako následek útoku nebo jiného incidentu (např. porucha)

Únik důvěrných informací jako následek útoku nebo podvodu

Nedostupnost ICT služby jako následek útoku

Nedodržení zákonů nebo nařízení jako následek opomenutí vývoje



Potenciální způsoby útoků

- Lidský faktor a vnitřní incidenty („omyly“, „pokusy“, „úmysl“, „nedbalost“)
- Zneužití nebo následky chyb v organizaci a řízení ICT
- Zneužití chyb produktů a poruchy (software, hardware)
- Podvody na uživatele (phishing, pharming, spyware, virus, ...)
- Zneužití vlastností nebo nedokonalostí architektury, protokolů
- Cílený útok, špionáž (sledování komunikace, prolomení šifry výpočtem, ...)
- Odcizení komunikační komponenty (inteligentní mobil, ...)

Většinu útoků lze detekovat před samotným prolomením bezpečnosti –
- hledáme odchylky od standardního stavu nebo výskyt charakteristických situací

Oblasti řešení

- Bezpečnostní mechanismy operačních systémů (MLS, EAL4+, ...)
- IPS/IDPS (Intrusion /Detection/ Prevention Systems) – NIPS, WIPS, HIPS, NBA
- DLP (Data Loss Prevention) - @network/DiM, @storage/DaR, @endpoint/DiU
- SIEM (Security Information and Event Management)
- NetFlow (RFC 3954), IPFLIX (RFC 5101, RFC 5102, vychází z NetFlow)

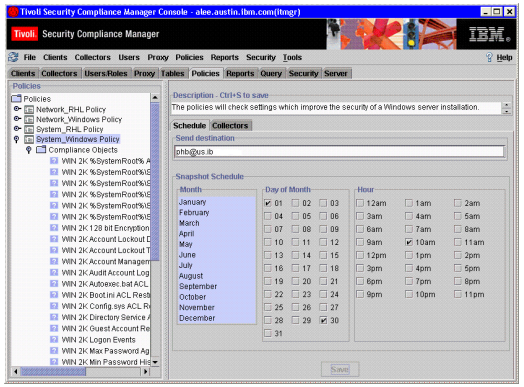
  Jflow/Cflowd (Juniper), NetStream (3Com/HP, Huawei), Cflowd (Alcatel), ...
- Compliance Management (PCI, FISMA, Basel II, SOX, HIPAA, ISO27001)
- Aplikační bezpečnost
- Identity & Access Management
- Šifrování, podpisy a certifikáty, správa klíčů (3DES, AES, RSA, DSA, ...)
- Firewally, antiviry, ...
- Fyzická, personální a administrativní bezpečnost

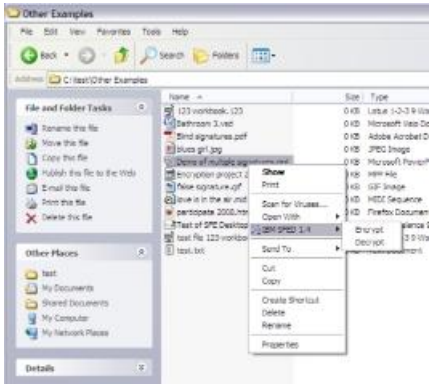
Produkty

- Mechanismy operačních systémů (MLS, EAL4+, SELinux, ...)
- IBM: Tivoli – SIEM, Identity, Access, zSecure, Security Policy,
  Key LifeCycle, Security Compliance,
  Rational AppScan, PolicyTester
  ISS (Internet Security Systems), Proventia (NIPS)
- HP: ArcSight SIEM, HP S Intrusion Prevention System (IPS) N Series,
  HP Security Management System Appliance Series
- CISCO: Virtual Security Gateway, ASA (Adaptive Security Appliance), IPS
- CheckPoint: 61000 Security System, IPS-1, DLP-1, VSX-1, SafeOffice
- Symantec, Fortinet, Juniper, INVEA Tech
- Ruckus Wireless, Safenet

Konkrétní řešení

- ✓ Identity Management – Tivoli Identity Management
- ✓ Access Management – Tivoli Access Manager + SSO
- ✓ SIEM – Tivoli Security Information and Event Manager
- ✓ Compliance – Tivoli Security Compliance Manager
- ✓ IPS – Proventia Network IPS
- ✓ E-mail – Proventia Network Mail Security System
- ✓ Encryption – IBM Secure File Encryption for Desktops (SFED)





Konkrétní high-end řešení

IBM System z (mainframe) + zOS + RACF + DB2

Tivoli zSecure Alert for ACF2/RACF

Tivoli zSecure Audit for ACF2/RACF

Tivoli zSecure Audit for TopSecret

IBM Security zSecure Admin

Thank you

Ing. Adrian Demeter
demeter@gcsystem.cz

GC System a.s.

Na Strži 3/342
Praha 4
140 00

T: 225987987

Špitálka 41
Brno – město
602 00

T: 543537111

Výstavní 1928/9
Ostrava
702 00

T: 599505120

info@gcsystem.cz

www.gcsystem.cz