IT biztonsági logelemzés

Ragó István
CISA, CISM
osztályigazgató

Raiffeisen BANK

Tartalom

- Mit?
- Miért?
- Hogyan?
- Hol?

IT biztonsági logelemzés

Raiffeisen BANK

Mit?

- Log-források:
  - IT biztonsági eszközök
  - Alkalmazások
  - Operációs rendszerek
  - Adatbázisok
  - Hálózati eszközök
  - Nem IT biztonsági rendszerek
- Kockázatelemzés

IT biztonsági logelemzés

Raiffeisen BANK

Miért?

- Törvényi háttér:
  1996. évi CXII. Törvény (Hpt.)
- Felügyeleti elvárások
- Tulajdonosi elvárások
- COBIT
- ISO 17799:2000
- ISO 27001:2005

IT biztonsági logelemzés

Raiffeisen BANK

Miért?

- Rendelkezésreállási problémák korai felismerése
- Biztonsági incidensek felismerése
- Incidensek utólagos elemzése

IT biztonsági logelemzés

Raiffeisen BANK

Hogyan?

- Előszűrés
- Trend-elemzés
- Minta-alapú észlelés

Raiffeisen BANK

Hogyan? - Előszűrés

- Audit
- Incidenskezelés

- Szakértői erőforrások kiegészítése

Raiffeisen BANK

Hogyan? - Trendelemzés

- A felhasználói és rendszer viselkedési szokások elemzése
- Öntanuló rendszerek
- Szakértői üzemeltetést igényel

IT biztonsági logelemzés

Raiffeisen BANK

Hogyan? - Minta-alapú észlelés

- Előre definiált szabályokon alapszik
- Tanítható rendszerek
- Téves riasztások kezelése

- Szakértői üzemeltetést igényel

IT biztonsági logelemzés

Raiffeisen BANK

Hol?

- IT
- Biztonsági szervezet
- Outsourcing

Kérdések?

istvan.rago@raiffeisen.hu

Raiffeisen BANK

Köszönöm a figyelmet!