Implementácia eTrust Network Forensics v praxi

Ing. František Boda
OTP Banka Slovensko, a.s.
31.5.2005

OTP Banka Slovensko

Projekt Centrálneho monitorovania bezpečnosti

Ciele projektu:

- splniť požiadavky kladené na bezpečnosť
  - Bezpečnostná doktrína OTP Banky Slovensko, a.s.
  - Bezpečnostná architektúra IS OTP Banky Slovensko, a.s.
  - Manuál bezpečnosti OTP Banky Slovensko, a.s.
  - Bezpečnostný projekt ochrany osobných údajov v zmysle Zákona č. 428/2002
  - legislatíva SR a EÚ
- naplniť opatrenia vedúce k zníženiu hrozieb

Realizácia na báze produktov Computer Associates

- eTrust Security Command Center,
- eTrust Access Control
- eTrust Policy Compliance
- eTrust Network Forensics

Dôvody

Potreby OTP Banky Slovensko, a.s.

- monitorovať aktuálny stav bezpečnosti IS
- zvýšiť úroveň bezpečnosti IS

Legislatíva SR

- Zákon o ochrane pred legalizáciou príjmov z trestnej činnosti
- Zákon o bankách
- Odporúčanie č. 3/2003 úseku bankového dohľadu Národnej banky Slovenska
- spolupráca s orgánmi činnými v trestnom konaní

Medzinárodná legislatíva a štandardy

- požiadavky legislatívy EÚ a regulačné požiadavky
- bazilejské kritériá Basel II (metodológia merania a riadenie rizík v bankách)
- Sarbanes-Oxley Act (požiadavky na účtovníctvo a výkazníctvo)
- Gramm-Leach-Biley (požiadavky na ochranu osobných finančných údajov)
- OLAF

Interná legislatíva

- riadiace dokumenty bezpečnosti

Úloha eTrust Network Forensics

– podpora systému na identifikáciu neštandardných obchodných operácií

– analýza podozrivých finančných tokov

– vizualizácia realizovaných finančných transferov a väzieb medzi účastníkmi transakcií

Implementácia eTrust Network Forensics

Základné fázy

- analýza požiadaviek kladených na výstupy eTrust Network Forensics
- definovanie požiadaviek na výstupy z bankového systému
- externé predspracovanie údajov
- úprava parametrov eTrust Network Forensics

Riešené problémy

- absencia jednoznačnej metodiky na identifikáciu neštandardných obchodných operácií
- nutnosť externého predspracovania údajov
- limity produktu vo zvolenej konfigurácii (notebook, Single Platform inštalácia)

Implementácia eTrust Network Forensics

Dosiahnuté výsledky

- zefektívnenie identifikácie neobvyklých obchodných operácií
- zjednodušenie procesu analýzy
- zvýšenie používateľského komfortu pri analýze finančných transakcií
- získanie jednoduchých a prehľadných informácií v grafickej forme
- splnenie legislatívnych požiadaviek a priblíženie sa k medzinárodným štandardom
- skvalitnenie procesov na identifikáciu obchodných operácií
- rozvoj internej metodiky a procesov na identifikáciu neobvyklých obchodných operácií

Zhrnutie – záver

eTrust Network Forensics
je analytický nástroj,
ale **bez dobrého analytika** nemá „dušu“

Implementácia eTrust Network Forensics v praxi

Ing. František Boda
OTP Banka Slovensko, a.s.
31.5.2005

OTP Banka Slovensko