SECURITY 2011

19. ročník konference o bezpečnosti v ICT

Logy tady, logy tam, všude kam se podívám ..

Zdeněk Adamec
Volksbank CZ, a.s.

Definice problému

Co se to tu vyrojilo jako hejno vran

všude mraky serverů a networkových bran

já mám ale lepší nápad, kam až to jde hnát

všechny tyhle divný stroje ..

budem logovat !!

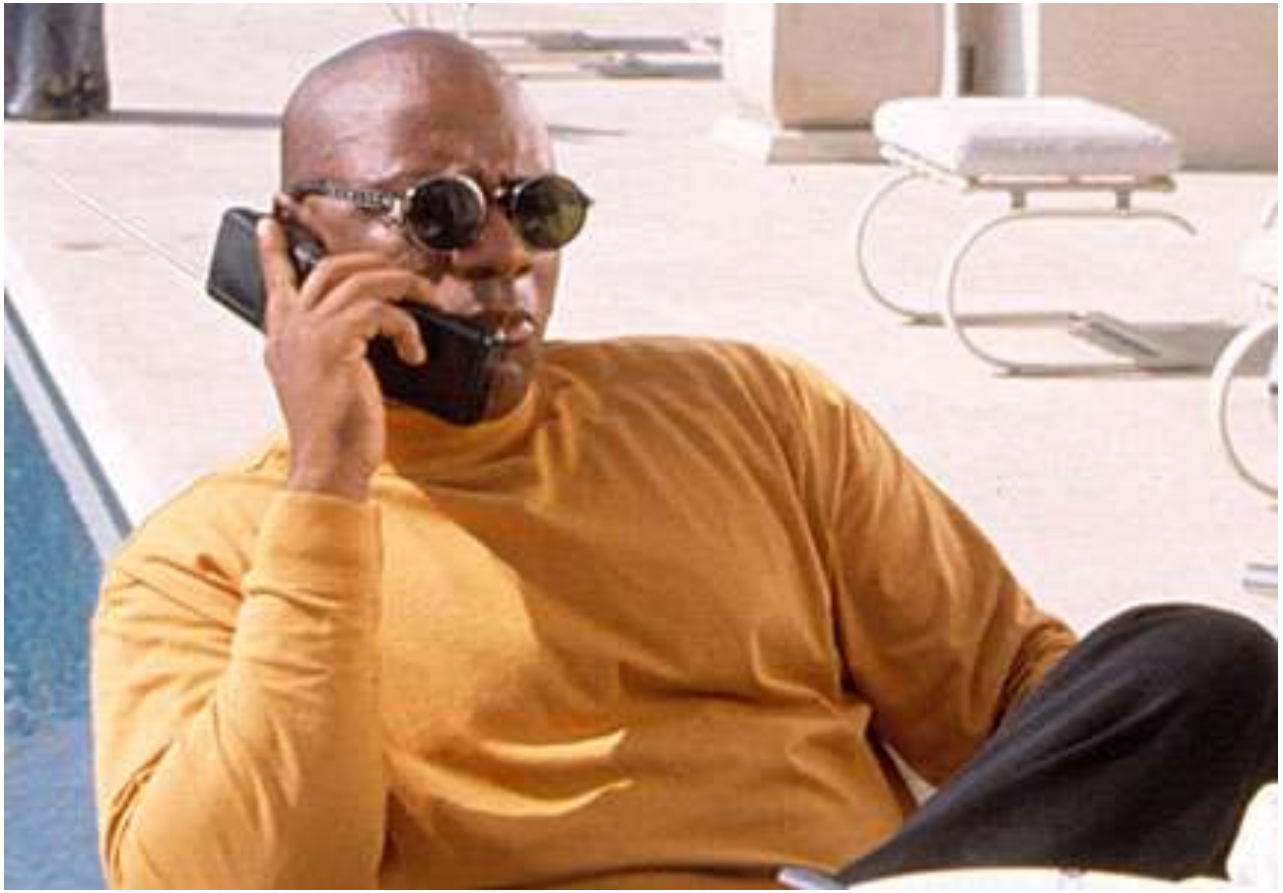
Několik čísel z Volksbank

- r. 2006
  - první implementace SIEM
  - 1000 EPS
- aktuální stav
  - 2500 EPS
  - 46 připojených IS
  - 26 různých platforem
  - měsíčně logováno cca. 250 milionů událostí
  - přes 100 customizovaných reportů

Základní otázky

1. K čemu mi to je?
2. Které systémy mám sledovat?
3. Jaké logy mám sbírat?
4. Co s tím pak mám dělat?

Nechceme myslet, chceme vědět!



SIEM je:

- prostředek reálné nezávislosti security na IT
- odpověď na legislativní požadavky
  - finanční sektor: Vyhláška ČNB č.123/2007 Sb.
    - „V oblasti bezpečnosti přístupu k informacím banka ... zajistí

      ...

      e) zaznamenávání událostí, které ohrozily nebo narušily bezpečnost informačních systémů, do bezpečnostních auditních záznamů, ochranu těchto záznamů před neautorizovaným přístupem, zejména úpravou (modifikací) nebo zničením, a jejich archivaci,

      f) vyhodnocování bezpečnostních auditních záznamů zaměstnancem, který nemá možnost upravovat (modifikovat) v informačních systémech informace související s činností, o které je bezpečnostní auditní záznam pořízen.

Dvě základní funkce SIEM

1. sběr logů na jedno místo
   - mimo dosah administrátorů jednotlivých IS
   - uchování logů pro případ šetření incidentů
   - security Quick-Win
   - další benefit: optimalizace logů na jednotlivých IS
2. analýza logů
   - tady je potenciální hlavní přidaná hodnota !!
   - časová náročnost
     - analýza logů není projekt, ale proces = trvá
   - náročnost na zdroje
     - toto za vás dodavatel sám neudělá

KSF dobré implementace

- Key Success Factors:
  - od začátku aktivně přemýšlejte a veďte dodavatele
    - SIEM je systém, který musíte CHTÍT
  - EPS stojí peníze! => využívejte je efektivně:
    - stanovte si PRIORITY vašich IS
    - sbírejte pouze informace, které jsou pro vás podstatné!
  - Bezpečnost je proces. Analýza logů také.
    - dokončením implementace teprve všechno začíná
    - počítejte s nutnými zdroji pro další rozvoj systému

Pokrytecká implementace SIEM

- trvá 2-3 dny
- napojeny všechny IS (čím více, tím lépe)
- generují se všechny předdefinované reporty
  - zejména reporty typu Basel II, ISO27000 apod.

- nasbíraná data aktivně nikdo nestuduje
- netvoří se žádné customizované reporty
- nevznikají žádné bezpečnostní kontroly

Zkušenosti z praxe - závěr

- jakákoliv kapacita EPS se brzy vyčerpá
  - využívejte optimálně EPS
  - držte priority systémů a aktualizujte je
  - vyhodnocujte sbíraná data, laďte datový tok

- neztrácejte z očí váš cíl
  - nenechte se zavalit daty z připravených reportů
  - řešte *informační bezpečnost*
  - vytvářejte si vlastní reporty na míru

SECURITY 2011

19. ročník konference o bezpečnosti v ICT

Děkujeme za pozornost.

Ing. Zdeněk Adamec, CISM
Volksbank CZ, a.s.
adamec.zdenek@volksbank.cz