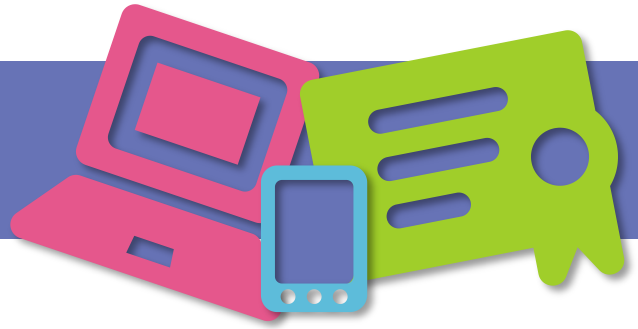
SECURITY 2014

22. ročník konference o bezpečnosti v ICT



Praktické zkušenosti se zaváděním monitoringu zranitelností IS

Karel Nosek, Zdeněk Sloupenský

ING Životní pojišťovna

Obsah

- Začínáme
  - Co vlastně potřebujeme?
  - Hledáme vhodný nástroj
- Implementace
  - Jak na to?
  - Hlavně na nic nezapomenout
  - Reporting
- Vždy je prostor pro zlepšení

Začínáme

- Co vlastně potřebujeme?
  - Analýza současného stavu
  - Komplexita řešení
  - Ohodnocení systémů, prioritizace
- Hledáme vhodný nástroj
  - Kritéria výběru
  - Jeden nebo více nástrojů?
  - Nejlepší je praktická zkušenost

Implementace

- Zapojení všech oddělení
  - Důležitá dohoda s IT
  - Synchronizace celého procesu
- Hlavně na nic nezapomenout
  - Nemáme jen interní síť
  - Bez práv to nejde
- Reporting
  - IT vs. management

Nasazení

- Hlavní nástroje: Tenable Security Center + Nessus Vulnerability Scanner
- Externí perimetr – Internet
  - Vulnerability scan – Nessus
  - Weby – HP Web Inspect
  - Další nástroje a služby dle potřeby
- Interní perimetr (LAN + DMZ):
  - Pravidelné skeny s autentizací, bez autentizace, kontrola nastavení systémů – compliance check
  - Stanice – Nessus
  - Servery – Tenable security center
  - Ostatní infrastruktura – kombinace dle BIA ratingu - Tenable nebo Nessus
  - DMZ – Tenable Security Center

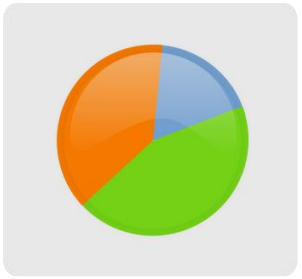
Policy Compliance audity

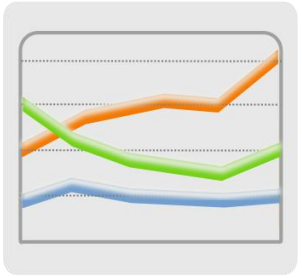
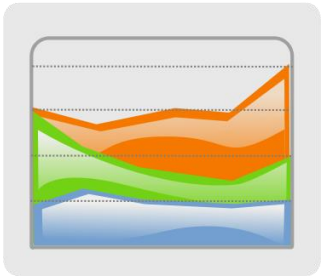
- Kontrola bezpečného nastavení systémů
- Základem je kvalitní OSG
- Ne každý má specialisty na hardening všech systémů
- Auditní skripty vytvořeny společně s OSG za pomoci externí firmy
- Vždy je nutná spolupráce se správcem systému
- Ne vše lze kontrolovat automatem
- Vlastní auditní skripty pro: operační systémy, databáze, VMware, síťová zařízení, Apache, atd.

Drobné nedostatky

aneb vždy je co zlepšovat:

- Správa účtů
- Flexibilita reportů
- Compliance nálezy v TSC



Další rozvoj

- Implementace nikdy nekončí
- Stále je co zlepšovat
- Vlastní auditní skripty pro každý typ serveru a zařízení
- Připojení dalších zařízení

- Napojení na SIEM
- PVS

SECURITY 2014

22. ročník konference o bezpečnosti v ICT

Děkujeme za pozornost.

Karel Nosek, Zdeněk Sloupenský

ING Životní pojišťovna

karel.nosek@ing.cz

zdenek.sloupensky@ing.cz