# SECURITY 2011

19. ročník konference o bezpečnosti v ICT

## Co (ne)přináší DLP systémy

Petr Javora
AEC, spol. s r.o.

## Obsah prezentace

- **Obsah:**
  - Ztráta dat
  - DLP systémy – požadavky
  - Bezpečnostní koncepce
  - Chráněné kanály, podporované platformy
  - Politiky, reporty
  - Detekce citlivého obsahu
  - Napojení na SIEM
  - Implementační postupy
  - Inteligentní telefony
  - Omezení DLP



## Citlivá data

- **Ztráta dat**
  - Úmyslná – zcizení dat
  - Neúmyslná – špatná e-mailová adresa, ztráta zařízení.
- Jedná se nejen o finanční ztráty, ale i poškození pověsti společnosti, možné nároky na odškodnění, atd.



## DLP systémy

- **DLP (Data Loss Prevention) -** ochrana před ztrátou a zneužitím citlivých dat.
  - Systémy schopné identifikovat, monitorovat a chránit data.
- **Ochrana:**
  - používaných dat (data in use)
  - přenášených dat (data in motion)
  - dat v úložištích (data at rest)



## DLP systémy

- **Primární požadavky na DLP systémy:**
  - Znemožnění uživatelům neoprávněně vynášet citlivá data z firemní sítě
  - Dodržení schody s legislativními požadavky (PCI DSS, HIPAA, FISMA, GLBA, SOX,…)
  - Propracované možnosti reportování událostí
- **Sekundární požadavky:**
  - Vyhodnocení chování zaměstnanců
  - Dohled nad tokem dat
  - Správa výměnných zařízení



## Přínosy DLP

- **Přínosy řešení:**
  - Úklid datových úložišť
  - Změna chování zaměstnanců
  - Konsolidace bezpečnostních pravidel a postupů
- **Omezení řešení:**
  - Omezení práce zaměstnanců
  - Velké nároky na správu systému
  - Nepokrytí specifických požadavků

## Bezpečnostní koncepce

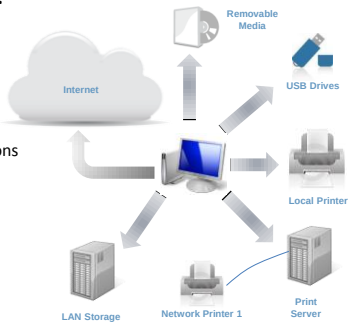
- **Ochrana citlivých informací a dat**
  - Není možné zobecnit pouze na DLP. Je to jeden z nástrojů pro dosažení cíle, ale vyžaduje další podpůrné prostředky a správné nastavení celého systému.
  - Ochrana koncových stanic (Host DLP) vs. ochrana síťového provozu (Network DLP)



## Chráněné kanály

**Kanály host řešení:**

- Email
- Web
- FTP
- Lokální/síťové tiskárny
- Copy/paste
- Endpoit Applications
- CD Burning Apps
- Removable Media
- Instant Messager
- Lan Storage
- P2P Apps
- (Porty počítače)

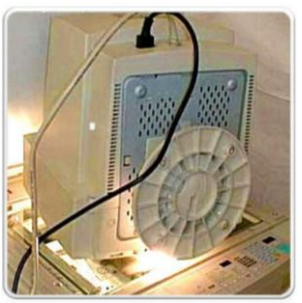





## Chráněné kanály

- Obraz
- Zvuk
- Video

!





## Chráněné kanály

- **Network řešení:**
  - Pasivní monitoring provozu
  - Aktivní kontrola síťového provozu
  - Kontrola HTTP/HTTPS, FTP, POP3, IMAP, SMTP, IM
- Možnost karantény, šifrování, pozdějšího dohledání incidentů.



## Chráněné platformy

- Ochrana primárně pro platformu Microsoft Windows.
- Podpora 64-bitových OS. U většiny výrobců v průběhu roku 2011.
- Koncepčně je potřeba zabezpečit všechny stanice. Vhodná je kombinace s produkty na kontrolu přístupu do sítě (Network Access Control).



## Bezpečnostní politiky

- Konzistentní politiky pro celou organizaci a pokud možno pro všechny komunikační kanály.
- Špatná nebo příliš obecná pravidla vedou ke generování velkého množství incidentů –> zahlcení obsluhy!
- Úrovně incidentů
  - Proměnné meze (Low, Medium, High) podle typu dat, konkrétního oddělení ve firmě.

## Reportování incidentů

- **Bezpečnostní administrátoři** mají kompletní přístup k citlivým interním datům (osobní údaje, údaje o platech zaměstnanců, kontakty,…)
- Postup vyhodnocení incidentů má více kroků, může být časově náročný. (analýza dat, hledání vlastníka dat, nadřízený pracovník analyzuje incidenty )
- Monitoring opakování události v časovém intervalu.



## Možné reakce

- BLOKOVAT VŠE?

Pravidla:

- Povolit (monitorovat)
- Potvrdit (notifikace)
- Umístit do karantény
- Vynutit šifrování
- Blokovat
- Speciální skripty, emailové notifikace, smazat, přesunout



## Reportování incidentů

- **Eskalace událostí**
  - Nadřízený nebo bezpečnostní správce
  - Nutné řešit falešné detekce s uživateli, dočasné výjimky, úprava politik
- **Reporty**
  - Možnosti pokročilého vyhledávání
  - Pravidelné generování, archivace



## Metody detekce

- Každý zákazník má jiná (jedinečná) citlivá data a proto je nutné upravovat řešení „na míru“.
- **Detekce citlivých dat pomocí:**
  - Umístění (lokalita)
  - Obsahu (regulární výraz,…)
  - Formát dat
  - Otisk (Fingerprint)
  - …



## Datové úložiště

- Je potřebné chránit veškerá úložiště citlivých dat.
- Pravidelné vyhledávání ve firemní síti:
  - Databáze
  - Diskový prostor uživatelů
  - Síťová uložiště (Fileshare/Sharepoint)



## Dohledové systémy

- **Napojení na návazné systémy**
  - E-mailové a sms upozornění, export incidentů, SIEM (Security Information and Event Management) - enVision
- DLP vs. Right Managment

## Implementace

- **Předpoklady:**
  - Potřeba mít dopředu vypracovanou koncepci.
  - Časové požadavky na plné zprovoznění jsou řádově měsíce, dle zvolených modulů a velikosti sítě.
- **Postup:**
  1. Analýza
  2. Instalace + nastavení
  3. Monitoring provozu a chování uživatelů
  4. Ladění politik a systému
  5. Finální provoz



## Inteligentní telefony

- Stále rozšířenější, s dokonalejšími možnostmi.
  - Synchronizace firemní pošty a dat.
  - Ukládání obsahu
  - Odeslání informací na internet



## Co DLP nezachytí

- Speciální malware s cílem získat citlivá data není zjistitelný – nutné použití antivirového programu, FW, gateway,…
- Uživatelé s administrátorskými oprávněními dokáži jednoduše DLP systémy na koncových stanicích obejít!
- Fyzické zcizení zařízení!



## Otázky?



## SECURITY 2011

19. ročník konference o bezpečnosti v ICT

## Děkuji za pozornost.


Ing. Petr Javora
AEC, spol. s r.o.
petr.javora@aec.cz