SECURITY 2012

20. ročník konference o bezpečnosti v ICT

Bezpečnost jako cibule
Vícevrstvá ochrana ICT

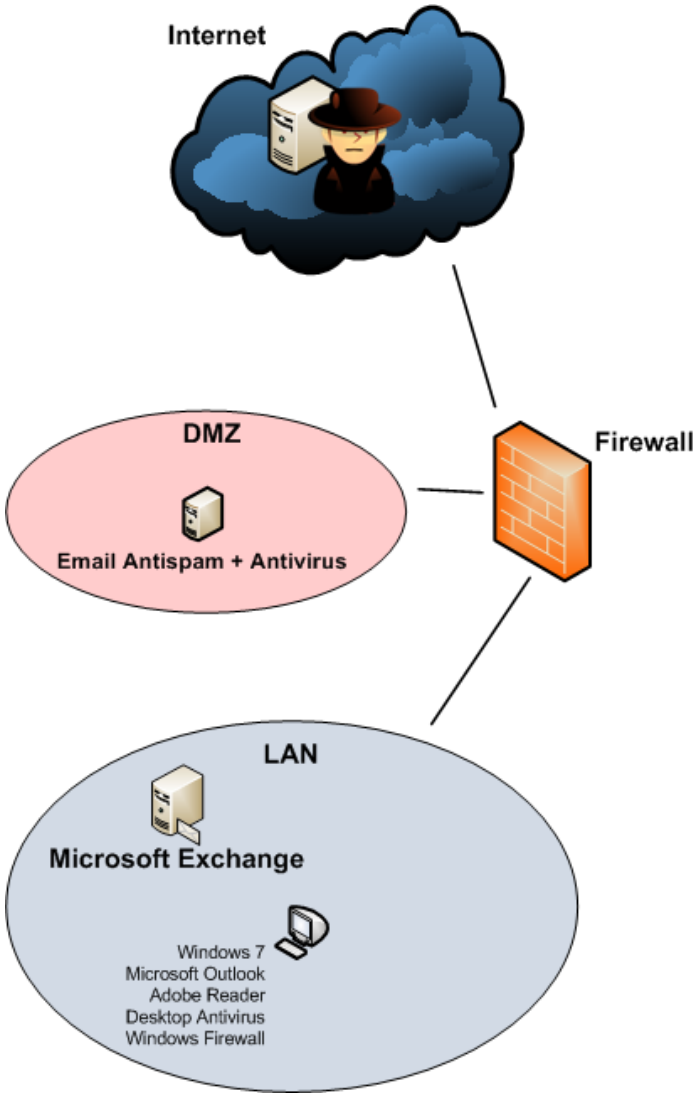
Michal Mezera a Robert Šefr

COMGUARD a.s.

Ochrana před cílenými útoky

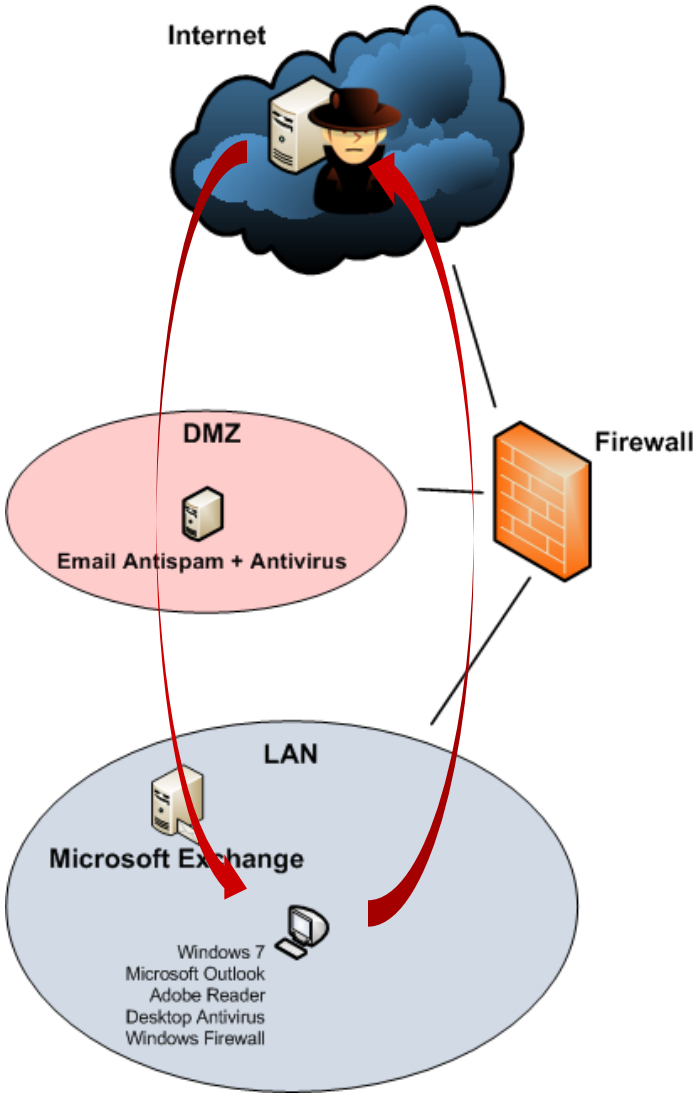
- **Otázky, na které bychom měli nalézt odpovědi:**
  - Poskytují standardní AV technologie založené na detekci pomocí signatur účinnou ochranu proti cíleným (APT) útokům?
  - Jsou tyto útoky lehce odhalitelné?
  - Jakým způsobem poskytuje centrální reporting ucelený přehled o stavu sítě z pohledu jejího zabezpečení?

Předpokládaná topologie cíle



- Základní bezpečnostní prvky
  - Perimetrový stavový firewall
  - Filtrování emailového provozu na bráně pomocí Antispamu a Antiviru
  - Antivirus na koncové stanici

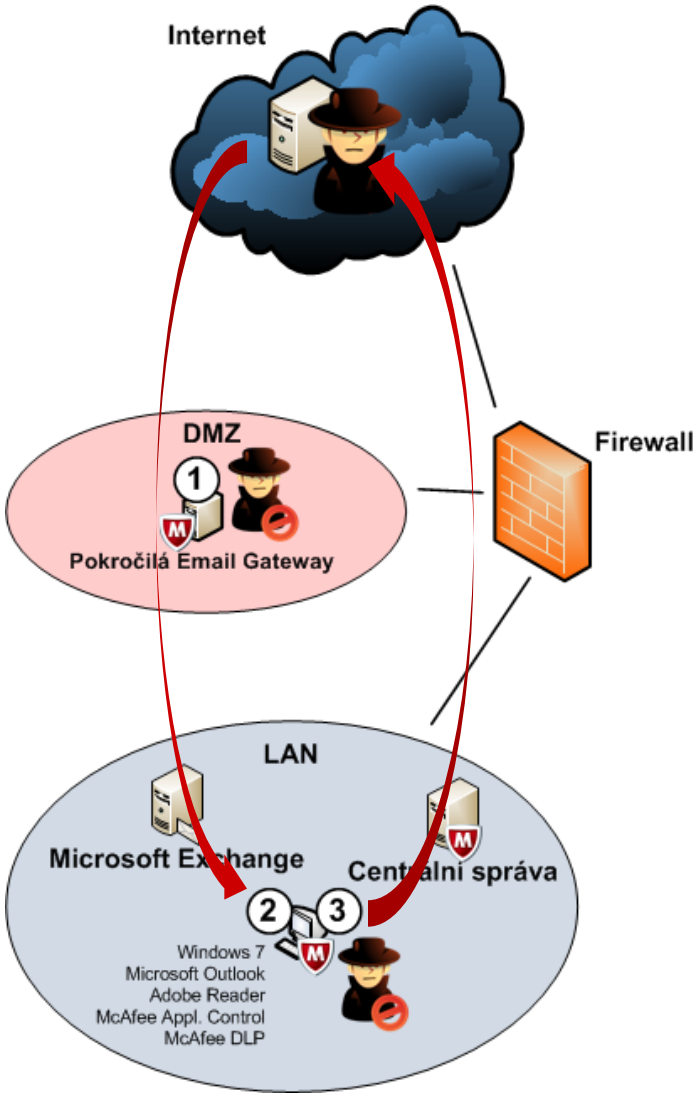
Simulace útoku



- **Spear-phishing** – cílený phishing útok na konkrétní osobu
- **Infiltration** – získání kontroly nad stanicí pomocí podvržených dat
- **Exfiltration** – získání citlivých firemních dat

Ukázka…

Simulace ochrany



1. **Spear-phishing** – cílený phishing útok na konkrétní osobu
2. **Infiltration** – získání kontroly nad stanicí pomocí podvržených dat
3. **Exfiltration** – získání citlivých firemních dat

Ukázka…

Ochrana před cílenými útoky

- **Odpovědi na stanovené otázky:**
  - Standardní perimetrový FW je vůči APT slepý
  - Běžná AV/AS ochrana emailové komunikace nestačí
  - Tradiční AV založené na detekci pomocí signatur jsou proti APT bezzubé
  - Bez pokročilého reportingu není APT prakticky odhalitelný

- **Jak ochránit citlivá firemní data před cílenými útoky?**
  - Ve vazbě na ukázky…
    - Pokročilá Email Gateway (hloubková ochrana emailové komunikace)
    - Application Control (spustitelné pouze známé aplikace)
    - Host Data Loss Prevention (ochrana citlivých dat)
    - Centrální správa zabezpečení (správa a reporting)
  - Přemýšlet jako útočník
    - Zvýšit nároky na překonání ochrany případnému zisku
  - Bezpečnost jako cibule, tj. vícevrstvá ochrana ICT
    - Jeden produkt není spasitelný
    - Všechna omezení jsou překonatelná

Možnosti Kompetenčního centra

- **Nabízí možnost podrobit různé bezpečnostní nástroje detailnímu testování v reálném prostředí včetně jejich kooperace a možností centrální správy v oblastech:**
  - Ochrana koncových stanic a serverů
  - Ochrana virtualizovaných prostředí (servery, desktopy)
  - Ochrana mobilních zařízení
  - Ochrana sítí (Firewally, IPS, NAC)
  - Ochrana webové a emailové komunikace
  - Ochrana citlivých dat (DLP, Device Control), Šifrování dat
  - Autentizace, PKI (HW klíčenky, Smartcard, SMS)
  - Vzdálené přístupy (SSL VPN, IPSec)
  - Správa zranitelností
  - Log Management (SIEM)

SECURITY 2012

20. ročník konference o bezpečnosti v ICT

Děkujeme za pozornost.

Michal Mezera a Robert Šefr
COMGUARD a.s.