Aktuální trendy kybernetických útoků

Jan Kopřiva
ALEF CSIRT

jan.kopriva@alef.com

ALEF

Jaké útoky jsou vidět?

- Komerčně motivované útoky
- Hacktivistické aktivity
- Cílené útoky a technicky vyspělé hrozby – APT, státní aktéři

Komerčně motivované útoky

- Ransomware
- Útoky na mobilní platformy a IoT
- Botnety
- Automatizované „low-tech“ útoky

ALEF

Hacktivismus

- Defacementy
- DDoS útoky

ALEF

Cílené útoky a vyspělé hrozby

- Cílené útoky nemusí být vždy high-tech
  - Spear phishing
- Krádeže citlivých dat
- Útoky na infrastrukturu
- Kyberšpionáž

ALEF

Co vidět není?

- 0-day hrozby
- Činnost APT a státních aktérů
- Moderní techniky
  - Útoky na ALSR
  - Uložení malwaru do podepsaných souborů
  - Malware cílený na PLC
  - Útoky na zranitelnosti HW
  - Pokročilé exfiltrační techniky

Reálné hrozby z každodenní praxe

- Malware
  - Exploit kity, trojské koně, ransomware,…
- Útoky na webové aplikace
- Tradiční automatizované skeny a útoky
- Phishing

Co přinese budoucnost?

- Stále více automatizovaných útoků
- Komplexní malware
- Útoky pomocí sociálního inženýrství
- Vzdělávání

Prostor pro Vaše dotazy

ALEF

Děkuji Vám za pozornost

ALEF