Polygon operačních technologií na NÚKIB v 0.2

Jan Zdrha - Oddělení bezpečnosti operačních technologií

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

O čem budeme mluvit

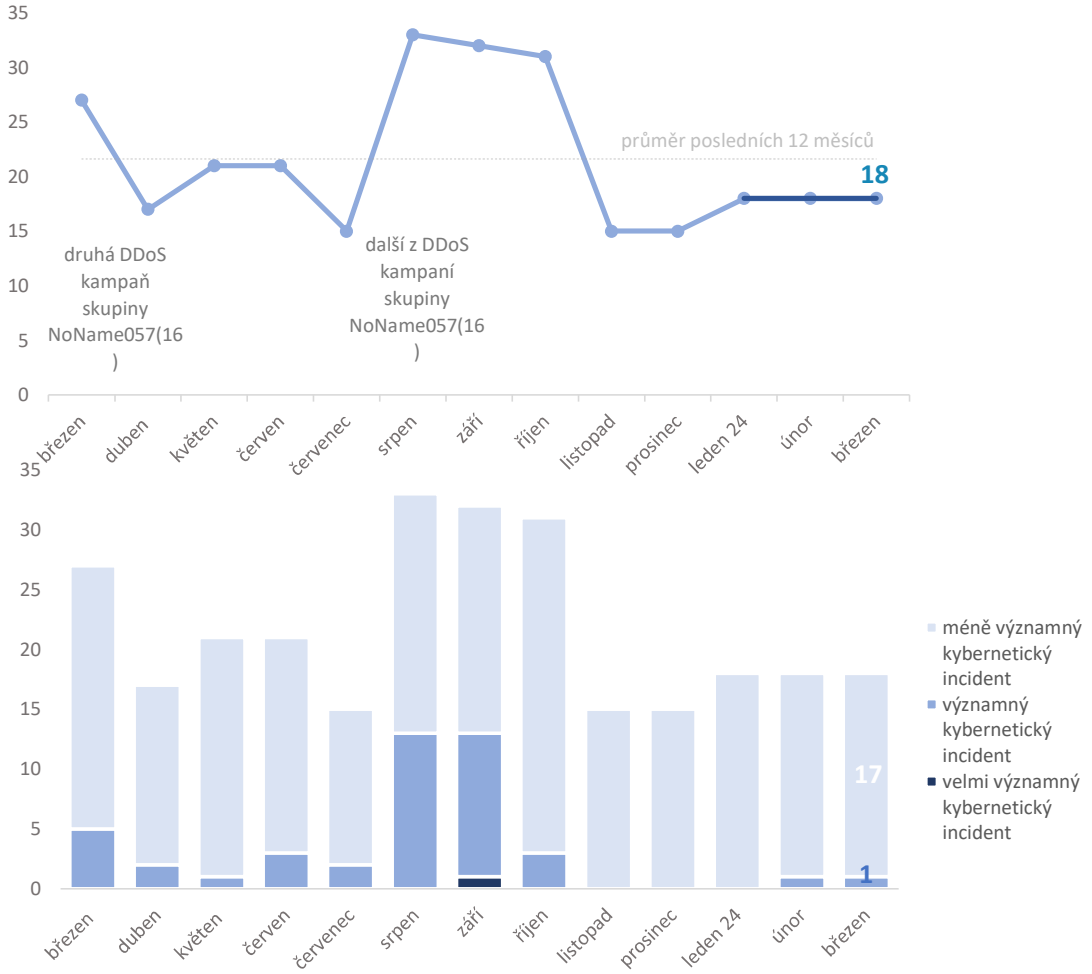
Národní úřad
pro kybernetickou
a informační bezpečnost

- Kybernetické incidenty pohledem NÚKIB
- Polygon operačních technologií

Kybernetické incidenty pohledem NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

- Počet a závažnost kybernetických bezpečnostních incidentů nahlášených NÚKIB



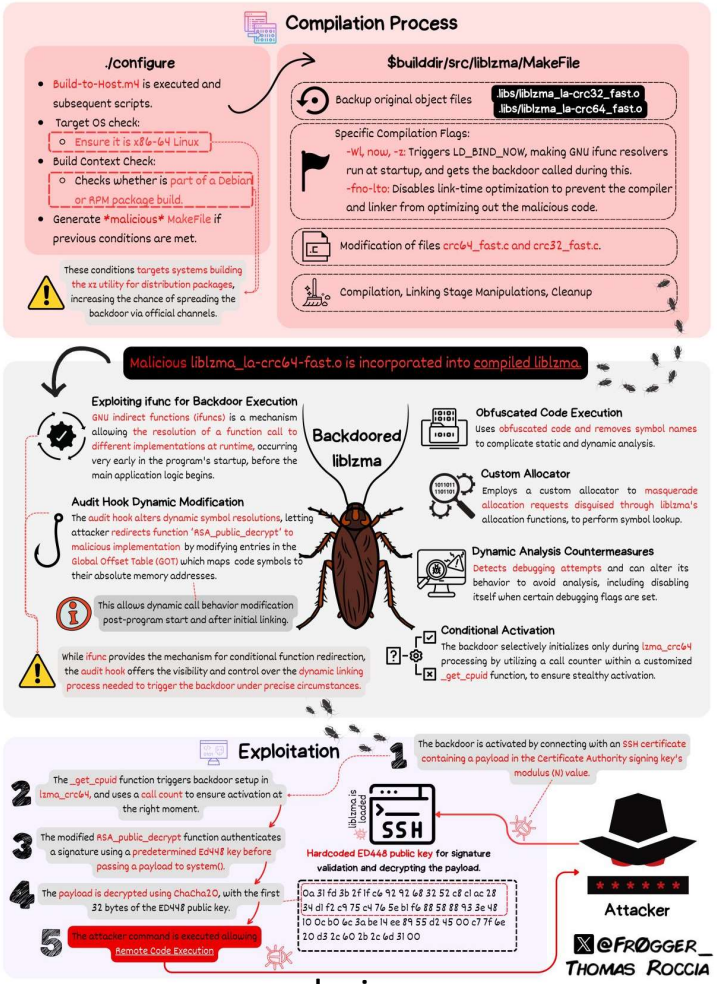
Kybernetické incidenty pohledem NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

- Trendy v kybernetické bezpečnosti pohledem NÚKIB
  - Phishing, spear-phishing a sociální inženýrství
  - Malware
  - Ransomware
    - Skupina LockBit 3.0
  - Zranitelnosti
    - Ivanti
    - Nástroj XZ
  - DDoS

Kybernetické incidenty pohledem NÚKIB

- Kompromitace rozšířeného nástroje systémů na bázi Unix
  - linuxový nástroj XZ (open-source nástroj pro kompresi dat)
  - Backdoor cílený na distribuce linuxu **Debian** a **Fedora**
  - Zranitelnost je označována jako CVE-2024-3094 s kritičností CVSS 10



zdroj: x.com

Kybernetické incidenty pohledem NÚKIB

- Zneužití PLC Unitronics používaných ve vodárenství CyberAv3ngers
  - Produktovou řadu Vision kombinované PLC s HMI
  - 27. listopadu 2023 útok na vodárenské subjekty
  - 28. listopadu 2023 CISA
    - Systémy vystavené do internetu
    - Defaultní heslo „1111“
  - 18. prosince 2023 vydáno doporučení na aktualizaci FW

Datum	Počet zařízení
únor 2023	105
začátek prosince 2023	84
12. prosince 2023	76
18. prosince 2023	62
22. prosince 2023	42
16. dubna 2024	32

Polygon operačních technologií

Národní úřad pro kybernetickou a informační bezpečnost

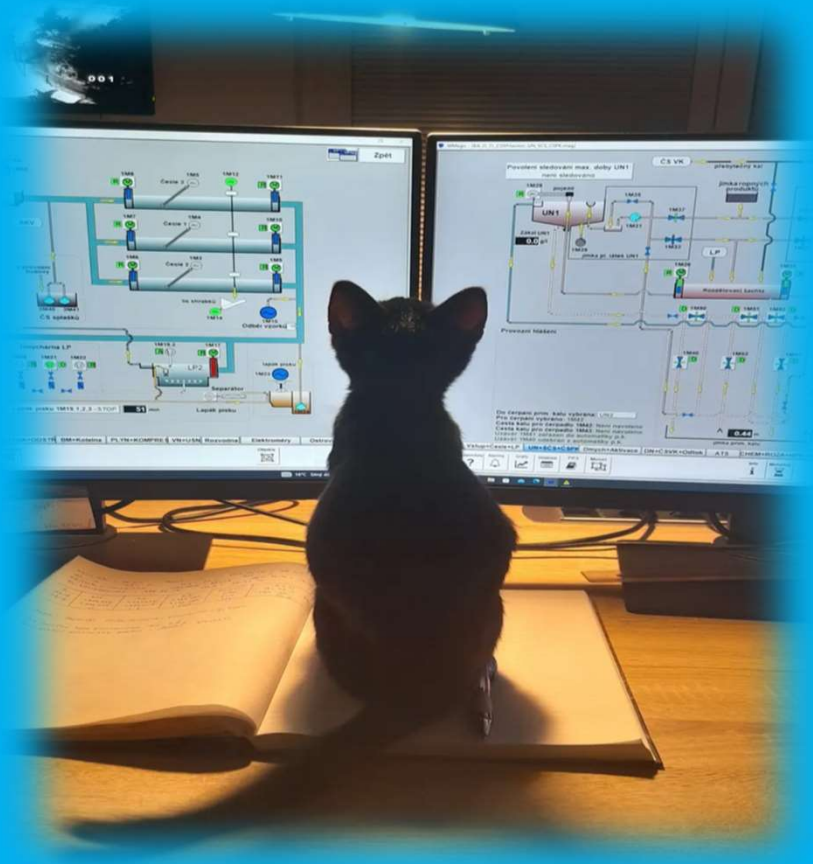
- Model uhelné elektrárny
  - Pasový dopravník S7 1200
  - Turbína elektrárna S7 1200
  - Rozvodna Siprotec 5 + RTU Sicam A8000
- Podpůrné technologie
  - Podpůrné technologie Wago, Schneider electrics
  - 3D model elektrárny s vizualizací stavů 3D tisk
  - Databáze Historian PostGreSQL
  - Zobrazení stavu technologie SCADA vizualizace a scoring bot .NET + ASP





Národní úřad
pro kybernetickou
a informační bezpečnost

děkuji za pozornost



Jan Zdrha
tlf: +420 541 110 762
e-mail: jan.zdrha@nukib.cz