# Kybernetické útoky

Jan Zdrha - Oddělení bezpečnosti operačních technologií

NÚKIB

Národní úřad
pro kybernetickou
a informační
bezpečnost

# O čem budeme mluvit



- Kdo jsme
- Vývoj počtu incidentů za poslední rok
- Rozdělení kybernetických útočníků
- Průběh kybernetického útoku
- Nejčastější cesty útočníka
- Dopady incidentů
- Řešení incidentů

# Kdo jsme

Národní úřad pro kybernetickou a informační bezpečnost

- NÚKIB je regulátor
- Nastavuje standardy v oblasti kybernetické bezpečnosti (vyhlášky a zákon)
- Analyzuje a vyhodnocuje kybernetickou bezpečností situaci

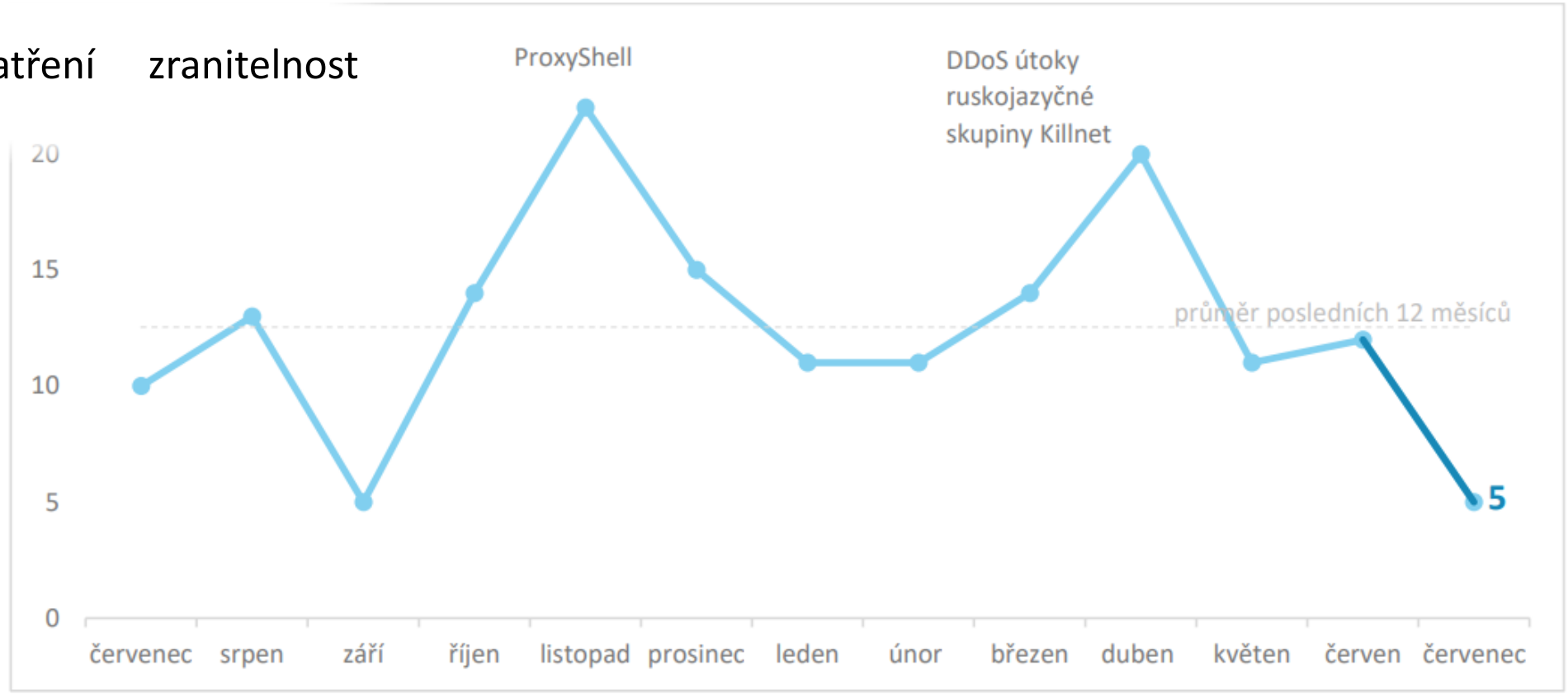
- Dohlíží na kybernetickou bezpečnost povinných osob ze ZKB
  - VIS (významný informační sytém) 583
  - KII (kritická informační infrastruktura) 125
  - PZS - systémy (poskytovatel základní služby) 180
  - Zdravotnictví 44 nemocnic

- **NÚKIB není IT dodavatel a nesupluje úlohu správce systému!**
- **Za dopad incidentu i za jeho vyřešení je vždy odpovědný správce systému!**

# Vývoj počtu incidentů za poslední rok



- Incicenty
  - 07/2021 - 07/2022
- 15. prosince 2021
  - Reaktivní opatření zranitelnost Log4Shell



# Rozdělení kybernetických útočníků

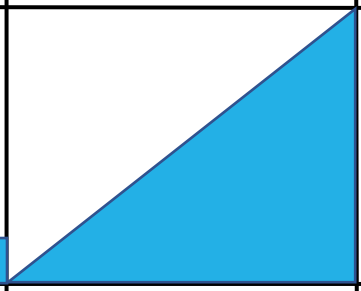


| | |
|---|---|
| 1. Script - Kiddies | WOW efekt chlubeni se před vrstevníky |
| 2. Hacker | Vybudování jména v komunitě, pomsta |
| 3. Hacker – tvůrce kódu | Vybudování jména v komunitě, finance |
| 4. Profesionální hacker (nájemný) | Finance |
| 5. Organizovaná skupina (teroristická) | Finance, politický vliv, náboženský boj |
| 6. Státní, státem podporované organizace | Politický vliv, zisk informací, ekonomický zisk, kybernetická válka |

**MOTIVACE**

# Průběh kybernetického útoku

Národní úřad pro kybernetickou a informační bezpečnost

| MOTIVACE | VÝBĚR CÍLE | ZÍSKÁNÍ PŘÍSTUPU K CÍLI | PŘÍPRAVA ÚTOKU | VLASTNÍ ÚTOK | DOPADY |
|---|---|---|---|---|---|
| | Cíl a jeho dosažení<br>Analýza cíle<br>Fyzická bezpečnost<br>Personální bezpečnost<br>Definování slabin cíle<br>Volba útoku<br>Prostředky útoku | Kompromitace zaměstnance<br>Kompromitace pomocí Phishingu<br>Kompromitace nezabezpečených prvků sítě<br>Získání privilegovaných práv k IT cíle | Mapování IT cíle<br>Nalezení cílů<br>Příprava sw nástrojů k útoku<br>Příprava sw nástrojů k zahlazení stop<br>Přenos sw nástrojů k cíli | | |
| Možnost zachycení útoku | 5% | 25% | 10% |  | |
| trvání | dny | týdny až měsíce | týdny až měsíce i roky | vteřiny - roky | |

# Nejčastější nástroje útočníka



- Phisingová kampaň
- Veřejně dostupné služby z internetu
  - Remote desktop protocol (RDP)
  - Secure Shell (SSH)
  - Virtual Private Network (VPN)
  - Webový e-mailový klient
  - Informační systémy
- Neautorizovaný přístup k vnitřní síti
  - Špatně zabezpečené Wifi
  - Nezabezpečené ethernet přípojky
- Osobní zařízení, notebooky
- Zranitelné služby

# Dopady incidentů



- IT/OT dopady
  - Kompletní ovládnutí systému
  - Krádež důležitých dat
  - Záměna dat
  - Znepřístupnění dat
  - Napadnutí HW IT/OT zařízení

- Reálné dopady
  - Organizace přestává fungovat
  - Fyzické škody na majetku a zdraví
  - Ohrožení života a zdraví
  - Reputační dopady
  - Finanční dopady

# Řešení incidentů



- Identifikace
- Snaha kontaktovat napadenou organizaci
- Zjištění základního přehledu o situaci
- Rozhodnutí o pomoci a vyslání response týmu
- Vyslání response týmu
  - Analyzuje
  - Doporučuje
  - Navrhuje opatření
- Zajištění stop, indikátorů kompromitace a jejich vyhodnocení
- Rozhodnutí o případném dalším postupu – sdílení informací o incidentu, vydání opatření, upozornění ostatních apod.

Národní úřad
pro kybernetickou
a informační bezpečnost

# děkuji za pozornost

**Jan Zdrha**
tlf: +420 720 036 693
e-mail: j.zdrha@nukib.cz