Analýza rizik ISP infrastruktury

z pohledu kyberbezpečnosti a NIS2

FLOWCUTTER

Mgr. Matej Pavelka PhD.
Ing. Filip Sklenár

Proč rizika probírat?

300 ISP, kt jsou kritickou infrastrukturou ČR

- **Kyberbezpečnost = preventivní přístup k rizikům**
- **Příklady rizik, jejich dopadů a protiopatření**
- **NIS2 framework, (ale taky ISO27001)**

Co nebudeme probírat

- Nikoliv “incident response”
- Nikoliv “recovery plan”
- Nikoliv procesy a papíry, co je třeba mít v pořádku

Pouze analýza rizik pro infrastrukturu

NIS2 framework

Názvosloví, kt používá NUKIB, ale intuitivní

NIS2 framework

- **Primární aktiva = kritická služba, kt poskytujete**

  co musí poskytovatel chránit, aby mohl i nadále poskytovat bezpečné, spolehlivé a zákonné služby

- **Sekundární aktiva = BGP router, radiový spoj, …**

  podporují bezpečný provoz internetu, např. monitorovací systémy (zbx, FC)

- **Ohrožení těchto aktiv je “scope”**

NIS2 framework

- **Důvěrnost** - Zkoumá, zda má k informacím přístup jen ten, kdo má.
- **Integrita** - Sleduje, zda jsou data správná, úplná a nezměněná.
- **Dostupnost** - Zjišťuje, zda-li systémy jsou dostupné, když jsou potřeba.
- **Hodnocení hrozeb** - Odhaduje, jak často hrozí (měsíc, rok, 5 let).
- **Hod. zranitelností** - Pravděpodobnost zneužití a účinnost opatření.
- **Hodnocení rizika = finální skóre**

NIS2 framework

Úroveň	
Nízká	1
Střední	2

- Důvěrnost
- Integrita
- Dostupnost
- HZ = skóre
- HH Hodnocení hrozeb
- HZ Hodnocení zranitelností

max(Dů,In,Do) * HH * 3

Hodnocení rizika = finální skóre

Zdroje hrozeb

pro kritická aktiva operátora

Zdroje hrozeb pro ISP

- Vně sítě ~ z internetu
- Uvnitř od zákazníků
- Ze strany zaměstnanců - naštvaný technik

Postup při analýze

- **Pojmenovat riziko a popis scénáře**
- **Klasifikovat (NIS2 framework)**
- **Opatření, jak** **a) omezit pravděpodobnost**

  b) nebo omezit dopad
  - např. dozvědět se o hrozbě včas

- **Příklad z ISP praxe**

Hrozby vnější

Hrozby, které mají původ mimo síť ISP

Hrozby vnější

- Příchozí DDoS
- Zranitelnosti služeb na perimetru ISP
- BGP miskonfigurace
- Útok na servisní porty (ssh, telnet, mikrotik winbox)
- …

Úroveň
Nízká
1
Střední
2

Riziko

Incoming DDoS

Příchozí DDoS

- Cílení, rozsah dopadu (celá síť nebo část)
- Frekvence / délka útoku - ročně / 30m
- Hodnocení rizika = 12HR

dů 1, int 1, dost 4, hrzb 1, zrn 4

max(d,i,d) * HH * HZ

4 * 2 * 4 = 32 bez opatření

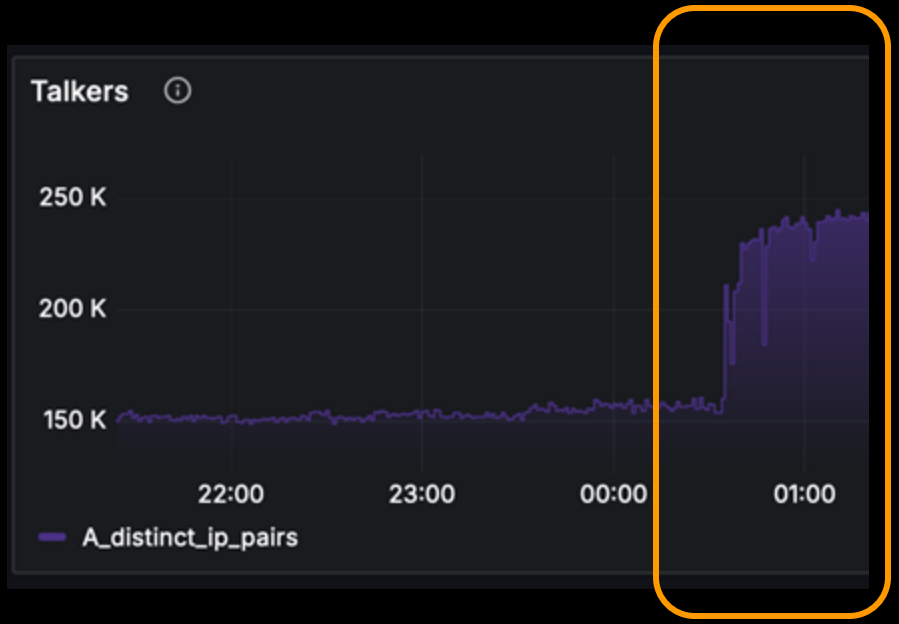
4 * 2 * 2 = 16 po opatření

Úroveň
Nízká
1
Střední
2
Vysoká
3

Hodnocení rizika

Hodnocení rizik			Hodnocení rizik
Úroveň		Popis	Proces zvládání rizika
Nízká	**< 7**	Riziko je považováno za akceptovatelné.	Riziko akceptuje MKB. Dále jej monituruje.
Střední	**8 <= HR < 15**	Riziko může být sníženo méně náročnými opatřeními nebo v případě vyšší náročnosti opatření je riziko akceptovatelné.	Riziko může akceptovat MKB ve spolupráci s garantem aktiva. Opatření navrhuje architekt kybernetické bezpečnosti ve spolupráci s MKB.
Vysoká	**16 <= HR < 31**	Riziko je dlouhodobě nepřípustné a musí být zahájeny systematické kroky k jeho odstranění.	Způsob zvládání rizika schvaluje Výbor pro kybernetickou bezpečnost, kterému rizika a opatření prezentuje MKB. Opatření pro snížení rizika navrhuje architekt kybernetické bezpečnosti ve spolupráci s MKB.
Kritická	**>= 32**	Riziko je nepřípustné a musí být neprodleně zahájeny kroky k jeho odstranění.	Způsob zvládání rizika schvaluje Výbor pro kybernetickou bezpečnost, kterému rizika a opatření prezentuje MKB. Opatření pro snížení rizika navrhuje architekt kybernetické bezpečnosti ve spolupráci s MKB.

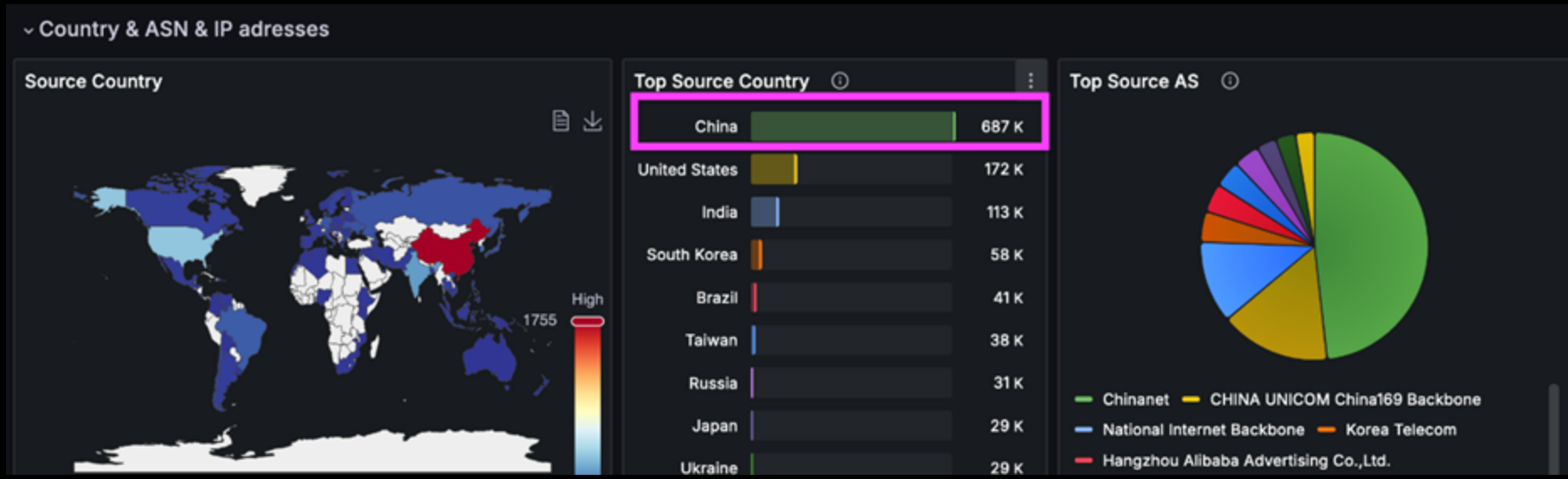
Detekce z flows



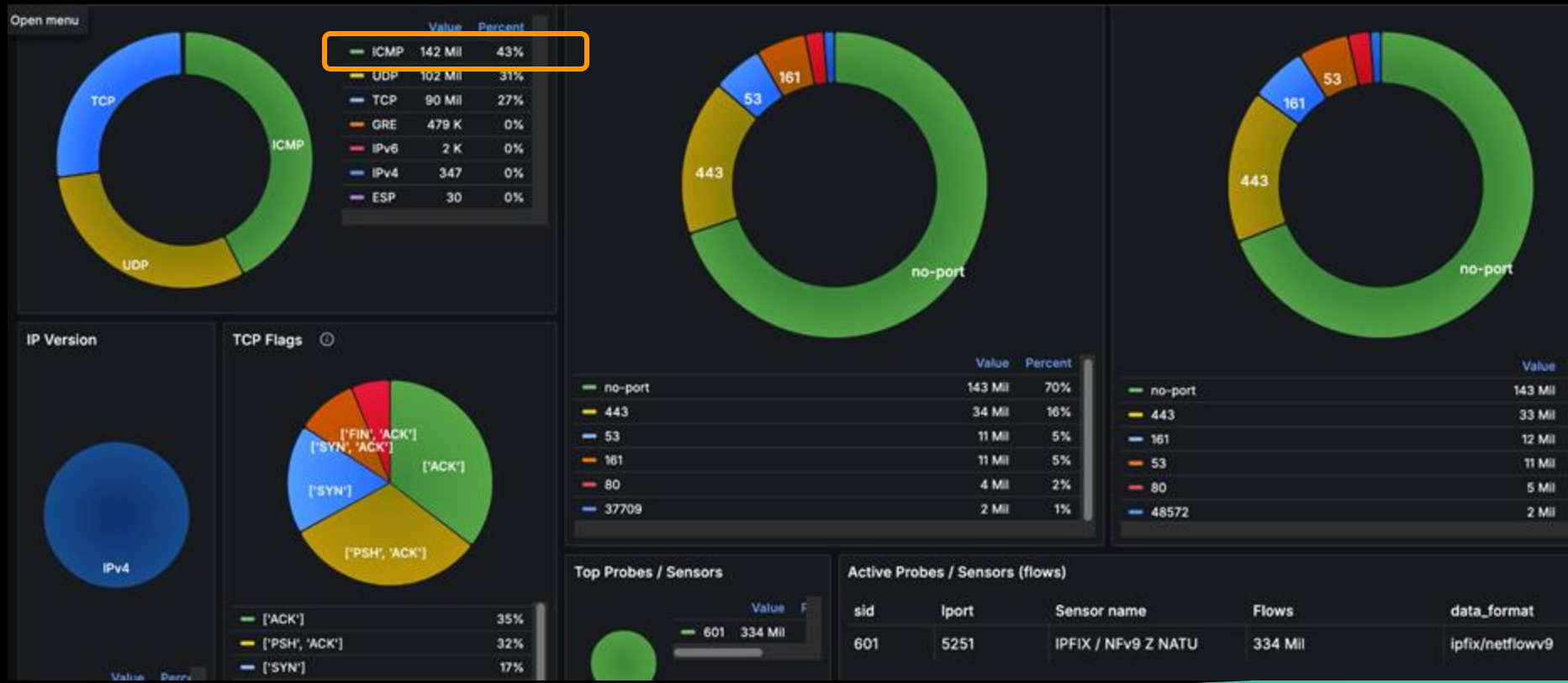
Adaptive detection

Different attacks behave differently (DNS reflection vs TCP SYN flood)

ASN & Country


Country & ASN & IP adresses
Source Country
High
1755
Top Source Country
China 687 K
United States 172 K
India 113 K
South Korea 58 K
Brazil 41 K
Taiwan 38 K
Russia 31 K
Japan 29 K
Ukraine 29 K
Top Source AS
Chinanet
CHINA UNICOM China169 Backbone
National Internet Backbone
Korea Telecom
Hangzhou Alibaba Advertising Co.,Ltd.

IP adress, protocol, s/d port, TCP flags



Opatření: DDoS

- On-prem Detekce z flows, řeknou i jak mitigovat
- Není tak časté, aby vyžadovalo automatický response
- Dle velikosti ISP: strategie při mitigaci útoku

  Podpora: RTBH, BGP Flowspec

  nebo mít možnost komunikovat s upstream

Riziko

Zranitelnosti služeb a systémů na perimetru

Příklady zranitelností

- **Ubiquity (CVE-2017-0938)** discovery on UDP -p 10001
- **Mikrotik (CVE-2024-54772)** winbox enumeration + bruteforce

  CVE-2019-3978) nepotřebují servisní porty ani API
- **OpenSSH (CVE-2024-6387)** “regreSSHion”

Databáze zranitelností

FLOWCUTTER

Vulnerability Scan

- Databáze zranitelností cílí na unix/networking
- 11.000 CVEs
- 60.000 NVTs

Statistika útoků

Studie *FlowCutter* z roku 2025:

- Selected ISPs, bez outliers
- 3 dny, celkem ~84 mld. flows
- GDPR compliant

54.000 skenů každých 5 minut!

- **Ne, většina nejsou univerzity, apod. - Top ASN**
- Talkers (5 min) 3500 Telnet / 3800 SSH / 1000 Mikrotik
- **Avg. 18 / 38 pokusů každou sekundu** (Telnet/SSH)
- **Jaká je strategie?**

Scan > list cílů > cílený útok > {spam, botnet, c2}

Top scanning ASN

Telnet

SSH

Statistika útoků

Studie *FlowCutter* z roku 2025:

- Selected ISPs, bez outliers
- 3 dny, celkem ~84 mld. flows
- GDPR compliant

54.000 skenů každých 5 minut!

- **Ne, většina nejsou univerzity, apod.**
- Talkers (5 min) 3500 Telnet / 3800 SSH / 1000 Mikrotik
- **Avg. 18 / 38 pokusů každou sekundu** (Telnet/SSH)
- **Jaká je strategie?**

Scan > list cílů > cílený útok > {spam, botnet, c2}

Zranitelnosti sw služeb a zařízení

- SW zranitelnosti, miskonfigurace
- Čím rozšířenější vendor, tím lákavější cíl
- Nyní bezpečné, za měsíc vyjde nová zranitelnost
- Které služby / zařízení (BGP/NAT router, hosting)
- Hodnocení rizika pro CORE

Hodnocení rizika pro CORE

- Před a po opatření?
- Jak často jsme zranitelní?
- **Hodnocení rizika**

dů 3, int 2, dost 2, hrzb 3, zrn 4

max(d,i,d) * HH * HZ

3 * 3 * 4 = 36 bez opatření

3 * 3 * 1 = 9 po opatření

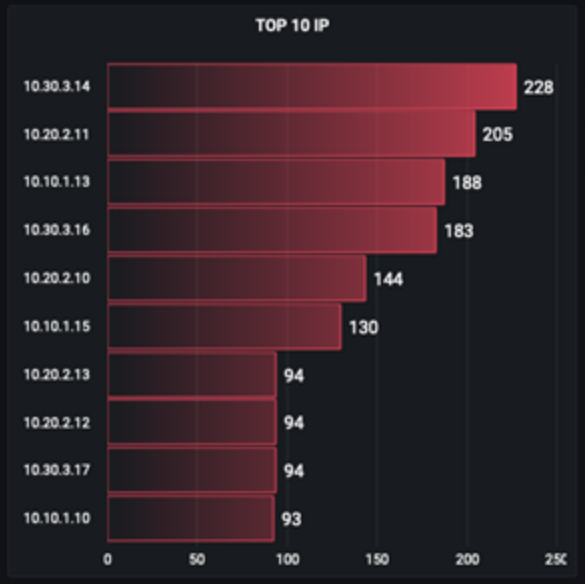
Úroveň
Nízká
1
Střední
2
Vysoká
3

Hodnocení rizika

Hodnocení rizik			Hodnocení rizik
Úroveň		Popis	Proces zvládání rizika
Nízká	**< 7**	Riziko je považováno za akceptovatelné.	Riziko akceptuje MKB. Dále jej monituruje.
Střední	**8 <= HR < 15**	Riziko může být sníženo méně náročnými opatřeními nebo v případě vyšší náročnosti opatření je riziko akceptovatelné.	Riziko může akceptovat MKB ve spolupráci s garantem aktiva. Opatření navrhuje architekt kybernetické bezpečnosti ve spolupráci s MKB.
Vysoká	**16 <= HR < 31**	Riziko je dlouhodobě nepřípustné a musí být zahájeny systematické kroky k jeho odstranění.	Způsob zvládání rizika schvaluje Výbor pro kybernetickou bezpečnost, kterému rizika a opatření prezentuje MKB. Opatření pro snížení rizika navrhuje architekt kybernetické bezpečnosti ve spolupráci s MKB.
Kritická	**>= 32**	Riziko je nepřípustné a musí být neprodleně zahájeny kroky k jeho odstranění.	Způsob zvládání rizika schvaluje Výbor pro kybernetickou bezpečnost, kterému rizika a opatření prezentuje MKB. Opatření pro snížení rizika navrhuje architekt kybernetické bezpečnosti ve spolupráci s MKB.

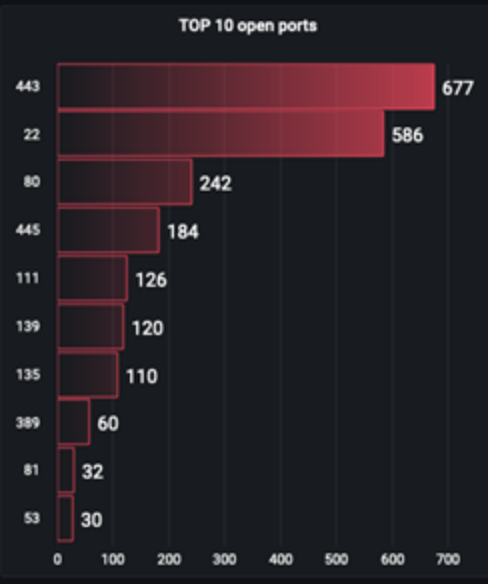
Vulnerabilities

Number of findings	High severity	Medium severity	Low severity	Log severity	Most of the findings:	Most visited CVE
2.19 K	3	36	40	25	10.30.3.14	CVE-1999-0632



TOP 10 CVEs

CVEs	Description
CVE-1999-0632	RPC Portmapper Service Detection (TCP)
CVE-2020-25073	Apache HTTP Server /server-status accessible (HTTP)
CVE-2011-3389,CVE...	SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detec
CVE-2017-0143,CVE...	Microsoft Windows SMB Server Multiple Vulnerabilities-Re
CVE-2010-0020,CVE...	Microsoft Windows SMB Server NTLM Multiple Vulnerabili



Opatření: sw zranitelnosti

- Pravidelný auditovatelný Sken zranitelností
- Hluboký sken “default credentials”
- Update latest firmware
- Monitor versions (in Zabbix)
- Ve skladu předkonfigurovaná náhrada
- *Optional: ročně penetrační testy*

Riziko

Otevřené servisní porty

Servisní porty

- Infra operátora vyžaduje vzdálenou konfiguraci
- SSH, Telnet, Mikrotik winbox, API, …
- Častý cíl zranitelností

Opatření: servisní porty

- Pravidelný auditovatelný Sken otevřených portů
- Hluboký sken “default credentials”
- Segmentace sítě - separátní vlan na servis
- Přístup pouze přes jump host
- Fail to ban
- Detekce brute force útoku

Hrozby vnitřní

Hrozby, které mají původ u zákazníků poskytovatele

Hrozby z vnitřní sítě

Od zákazníků operátora

- Otevřený DNS port do internetu
- Hacknutá kamera u zákazníka poškodila /22 prefix
- …

Riziko

Otevřený DNS port

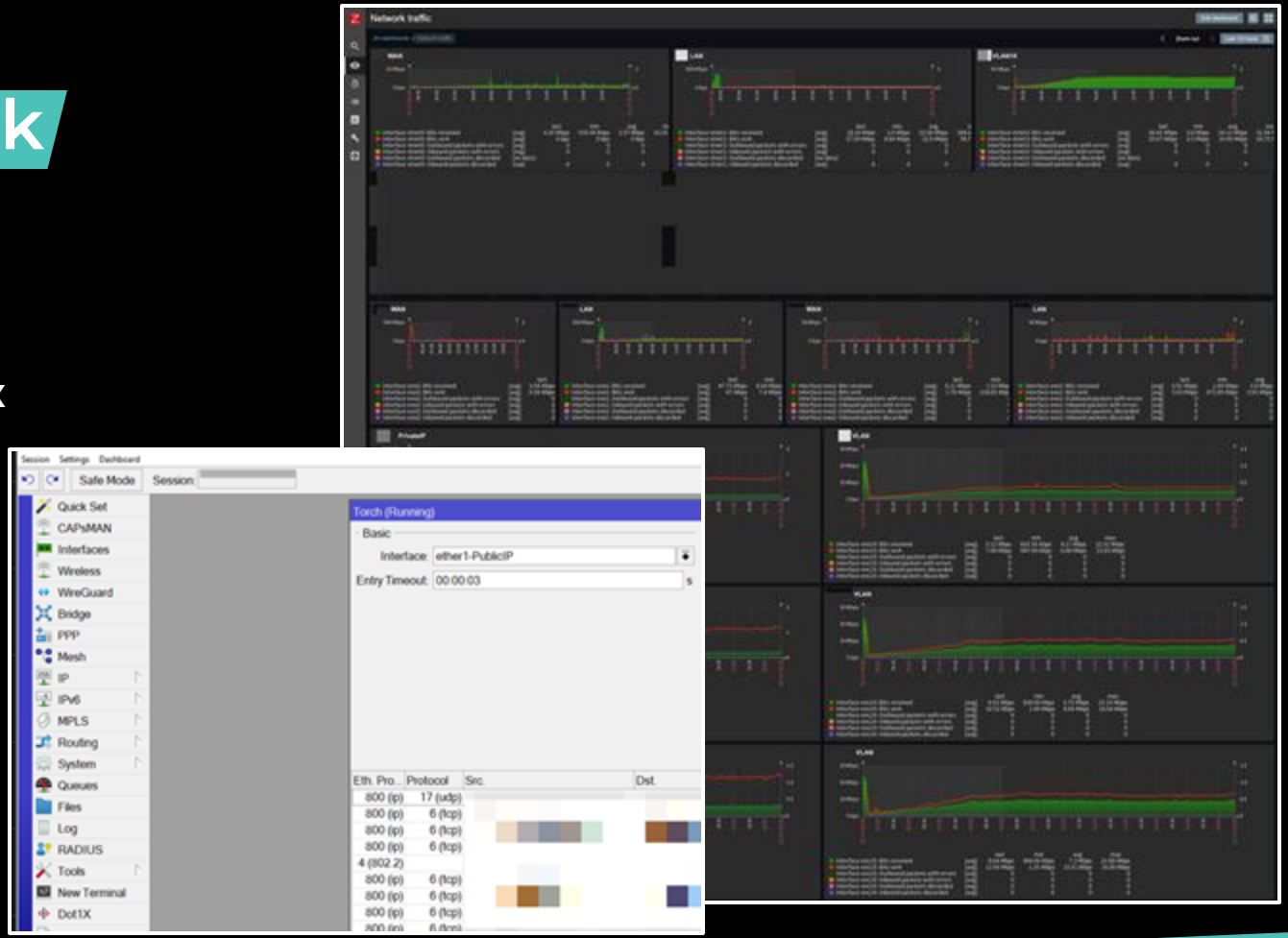
Statistika útoků

Alespoň 1x měsíčně

- Nemáme přesnou statistiku
- Vždy vede k odchozímu reflexivnímu útoku

Typical stack

- Zabbix
- Mikrotik winbox



Before / after

During anomaly

Before anomaly

Drill down

- Source port = 53

Reflection attack

- Distributed attack using open DNS ports
- Mitigated using BGP FlowSpec: Src/Dest ports = 53/24335

Open ports

- **Automated scan** (every night)
- **DNS port open** on SME customer's public IP

Example screenshot (not the actual case)

Opatření: Otevřené DNS porty

- Zakázat 53 ven - těžší pro zákazníky s veřejnou IP
- Pravidelný sken otevřených portů - if (+1) than alert
- Detekce z flows, řeknou i jak mitigovat

Riziko

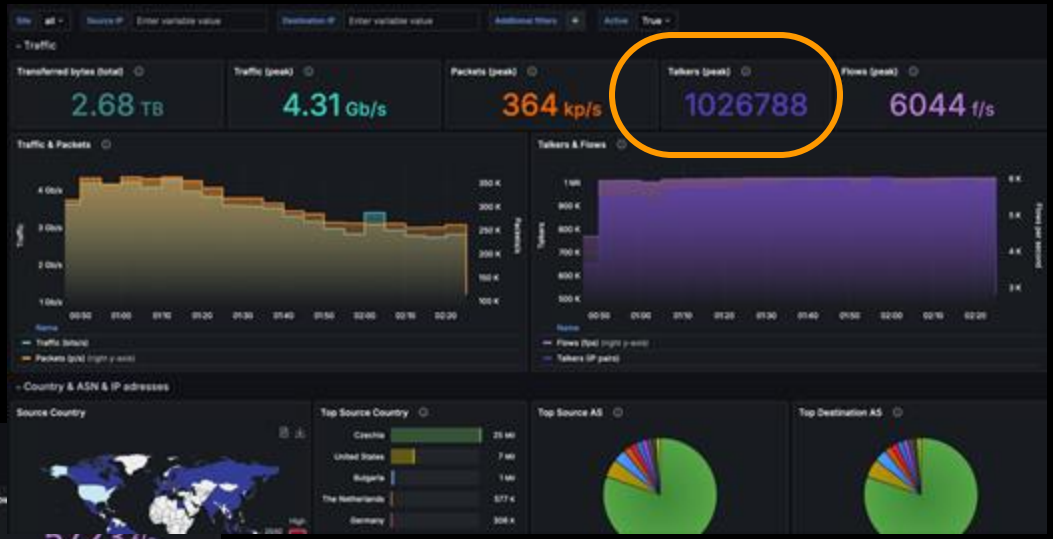
Hacknutá kameru u zákazníka

Anomaly on talkers

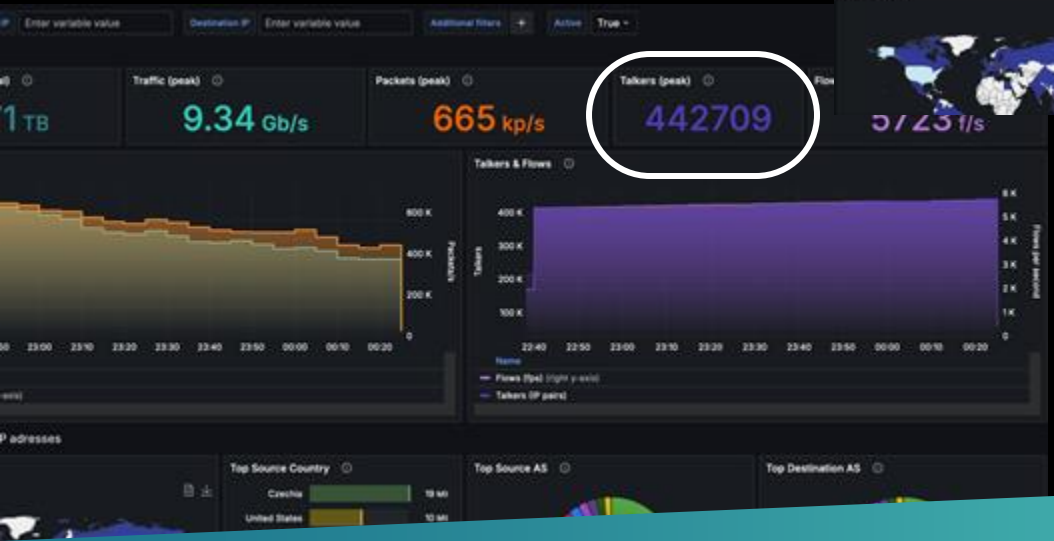
- Calculated on 10s interval

Before / after

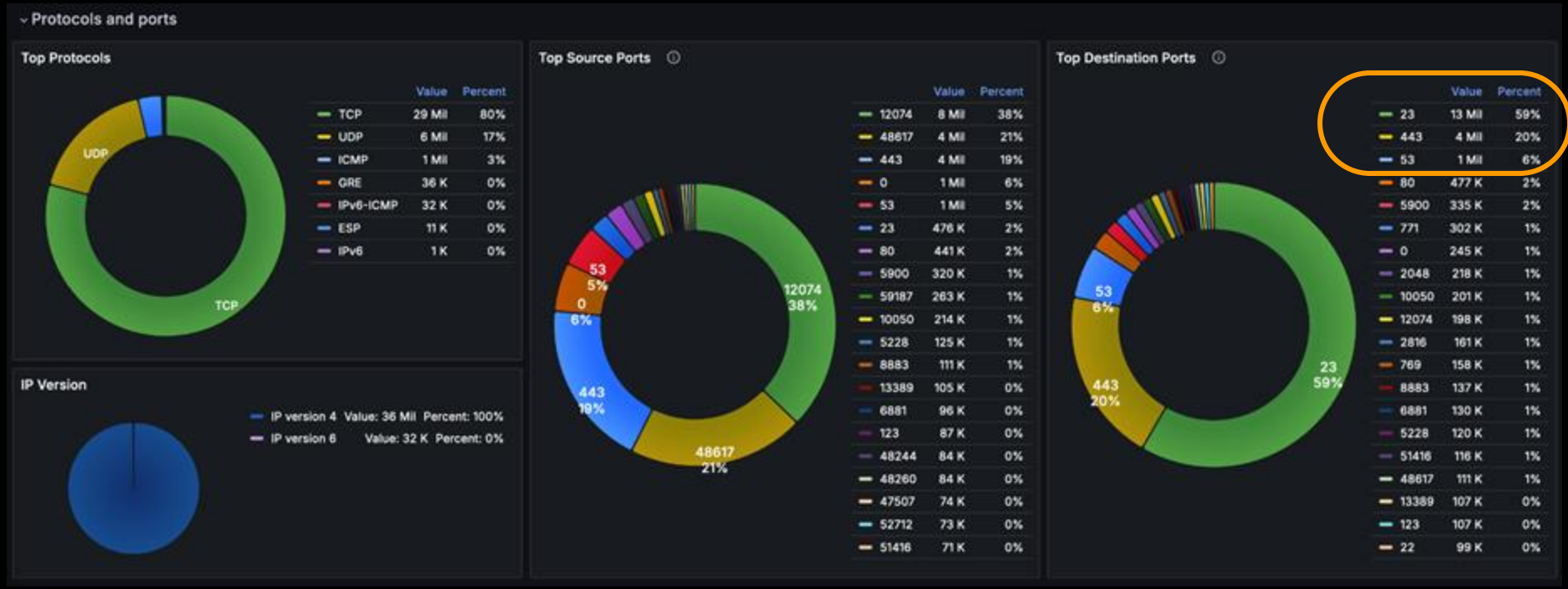
During anomaly



Before anomaly



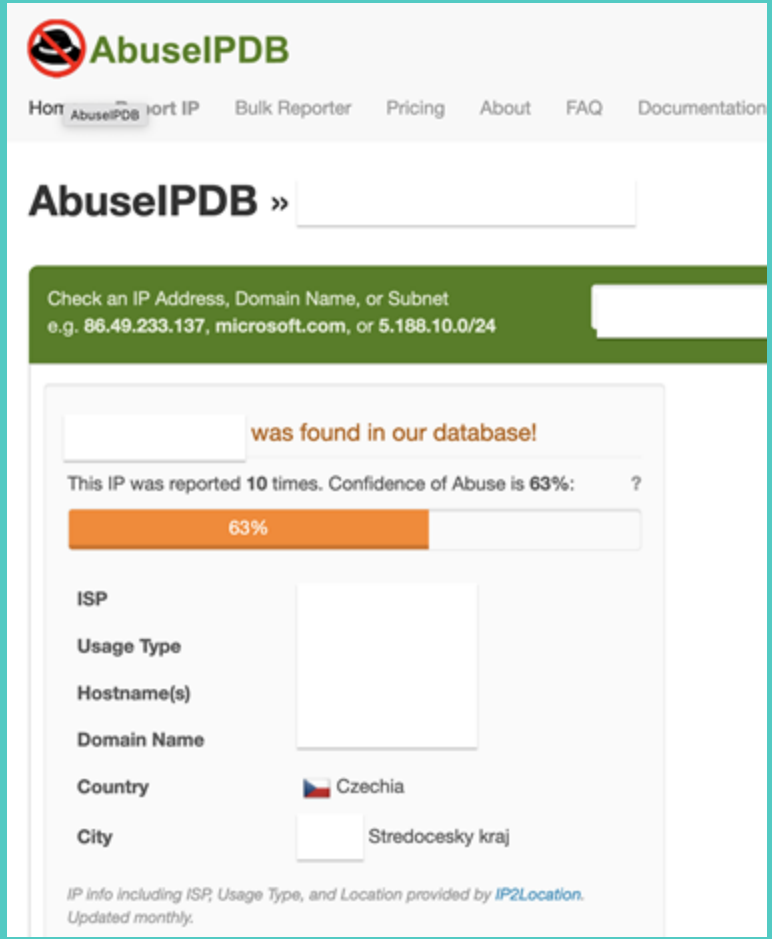
Anomaly on port 23



Single host traffic

Impact

- Home camera on botnet
- IP on blacklist
- /22 IP Prefix on blacklist
- 30+ emails from ASNs
- Clean up



Statistika útoků

Studie *FlowCutter* z roku 2025:

- Selected ISPs, bez outliers
- 3 dny, celkem ~84 mld. flows
- GDPR compliant

Jak se chovají zákazníci?

- 29% ISP má útočícího zákazníka via Telnet
- **71% ISP** má útočícího zákazníka via SSH
- **Avg. 35 pokusů každou sekundu**

(tvoří jen 0.17% z flows a ~0.008% z trafficu)

Ze SNMP tento jev nevidíte! Shaping také ne.

Opatření: Hacknutý zákazník

- Dopad není kritický, ale je častý
- Sledovat anomálie z dohledových systémů (flows)
- Zahrnout IP reputaci (blacklisty) do dohledu
- Mít připravený postup

Hrozby vnitřní

Hrozby, které mají původ u zaměstnanců

Hrozby od zaměstnanců

- Pomsta od bývalého zaměstnance
- Hacknutý laptop v kanceláři
- Malware odkazy, phishing
- Miskofigurace po zásahu technika / resetu routeru
- …

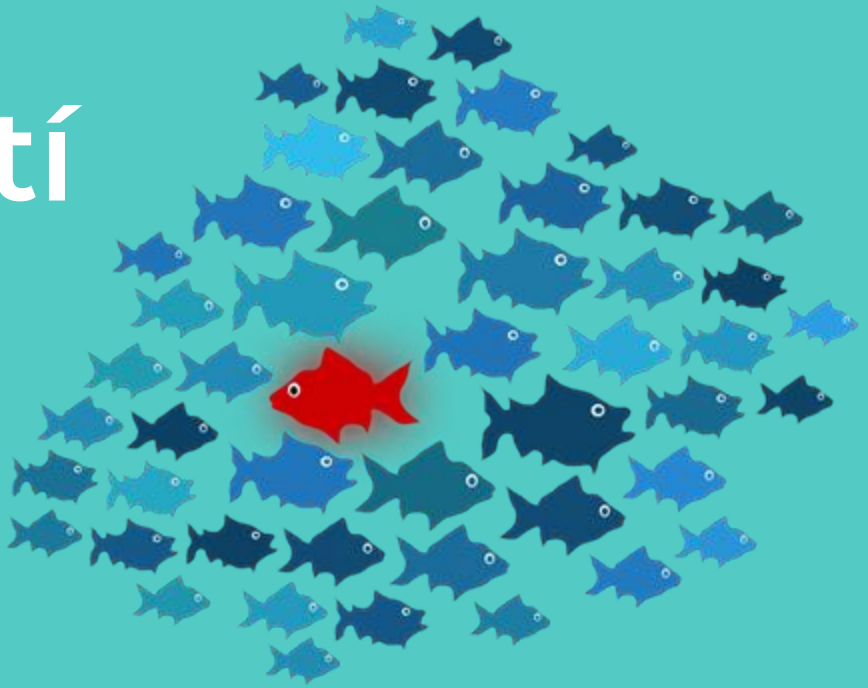
Opatření

- Žádné defaultní nebo sdílené hesla, 2FA
- Přístup k infra vždy identifikovatelná osoba + log
- Vzdálený přístup přes jump host s logováním
- Jasný proces na “offboarding” zaměstnance
- Optional: centrální sběr logů

Shrnutí

Photo from thedatascientist.com/

Bezpečností opatření



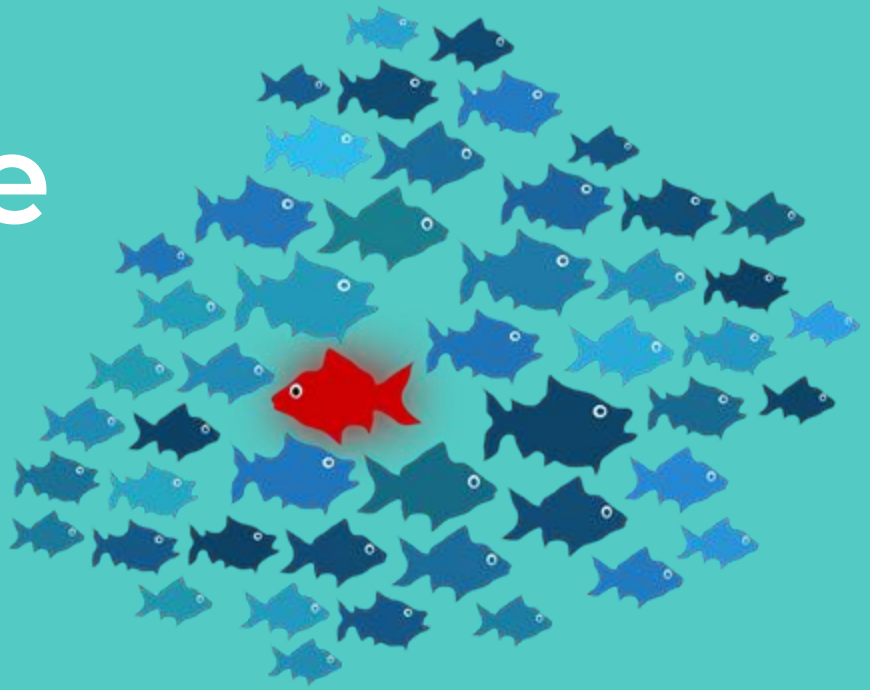
Závěr

- Kyberbezpečnost = preventivní přístup k rizikům

  kt je levnější řešit hned a nečekat na důsledky
- Preventivní protiopatření
- Dohled na ty rizika, kt mají velký dopad

Photo from thedatascientist.com/

Děkujeme



FLOWCUTTER

Mgr. Matej Pavelka PhD.
Ing. Filip Sklenár