MUNI
CSIRT-MU

Kyberbezpečnost v roce 2021

Setkání IT komunity, 2. 9. 2021

Tomáš Plesník et al.
CSIRT-MU

DDoS útoky

- V roce 2020 univerzita nečelila **žádnému DDoS útoku**
  - Nebyl detekován, hlášen, ani zaznamenán v podobě nedostupnosti služeb
  - Ohlášen pouze vyděračský DDoS na CESNET
- Během 2021 již **několik útoků s významnými dopady** na infrastrukturu MUNI
- V jednom případě útok způsobil **výpadek VIS dle ZoKB/VoVIS**
  - Zákonná povinnost incident nahlásit na NÚKIB a přijmout opatření

Přehled DDoS útoků

- DDoS útok proti **community.csirt.muni.cz**
  - 2021-03-23 port UDP/1900 protokolu UPnP/SSDP
  - Datový tok **1,2 Gb/s** a 0,4 Mpps
  - **Bez omezení dostupnosti**

Přehled DDoS útoků

- DDoS útok proti **webcentrum-c.ics.muni.cz**
  - 2021-03-23 port UDP/111 ONC RPC (Portmapper)
  - Datový tok **3,4 Gb/s** a 0,77 Mpps
  - Útok **zahltil ochranný síťový prvek (firewall)**, který je předřazen výpočetnímu clusteru serverů poskytující webové služby univerzity
  - Následkem bylo **zhoršení dostupnosti služeb různých webových systémů** hostovaných na tomto clusteru, včetně jednoho z nahlášených VIS

Přehled DDoS útoků

- DDoS proti **webcentrum-c.ics.muni.cz**
  - 2021-07-26 port UDP/123 protokolu NTP
  - Datový tok **0,85 Gb/s** a 0,22 Mpps
  - V době DDoS útoku bylo **nedostupných celkem 6 serverů**, nefungovala Icinga, byly zaznamenány **výpadky VPN** a krátce indikován i **výpadek Jednotného Přihlášení**

Přehled DDoS útoků

- DDoS proti **csirt.muni.cz** na **webcentrum-c.ics.muni.cz**
  - 2021-07-27 port TCP/80 a TCP/443 protokolu HTTP(S)
  - Datový tok **15 Mb/s** a 12 kpps
  - V době útoku byly **nedostupné všechny weby v Umbraco** hostované na webcentrum-c.ics.muni.cz

DDoS z „naší“ sítě

- Zneužití reflektoru v **připojené organizaci** (Dětská nemocnice)
- Probíhalo na portu UDP/11211 protokolu Memcached
- Datový tok **0,213 Gb/s** a 0,02 Mpps (213 Mb/s, 21 kpps)
- Potřeba zabránit útokům z obou směrů (z/do MUNI)

Jak nás chrání CESNET?

- Quality of Service (QoS) rate limit na vybrané známé DDoS amplifikátory
  - Mezi nimi ovšem **nebyl žádný ze zneužitých** pro útoky
  - Na základě analýzy útoků nově zavedli **limit UDP/111 5x 20 Mb/s** na vstupu do páteřní sítě CESNET (5 linek „do světa“)
- CESNET má nasmlouvaná scrubbing centra (tzv. „čističky provozu“)
  - Schopni přesměrovávat bloky provozu na **základě 24 bitového CIDR prefixu** (/24)
  - DDoS detektor CESNETu zde má **nastaven limit 400 Mb/s**
  - Zatím v beta verzi, **funguje na základě explicitně vyjmenovaných portů**
  - **CESNET nezná detaily, co se uvnitř děje** (komerční řešení nechce sdílet cenné know-how)

Jak nás chrání CESNET?

- Nasazen **BGP Flowspec,** umožňuje zadávat pravidla připojeným organizacím přes systém ExaFS

Active IPv4 rules that you can modify

Source addr. ▲	S port ▲	Dest. addr. ▲	D port ▲	Proto ▲	Packet len ▲	Expires ▲	Action ▲	Flags ▲	User ▲	Edit	
	111	147.251.0.0/16		udp		2025/08/08 10:30	QoS 10 Mbps		Martin Laštovička		
147.251.0.0/16	111			udp		2025/08/18 09:50	QoS 10 Mbps		Martin Laštovička		
	11211	147.251.0.0/16		udp		2025/08/08 10:30	QoS 10 Mbps		Martin Laštovička		
147.251.0.0/16	11211			udp		2025/08/18 10:00	QoS 10 Mbps		Martin Laštovička		
	123	147.251.0.0/16		udp		2025/08/08 08:50	QoS 100 Mbps		Martin Laštovička		
147.251.0.0/16	123			udp		2025/08/18 10:00	QoS 100 Mbps		Martin Laštovička		
	137	147.251.0.0/16		udp		2025/08/08 10:30	QoS 10 Mbps		Martin Laštovička		
147.251.0.0/16	137			udp		2025/08/18 10:00	QoS 10 Mbps		Martin Laštovička		
	161	147.251.0.0/16		udp		2025/08/08 10:30	QoS 10 Mbps		Martin Laštovička		
147.251.0.0/16	161			udp		2025/08/18 09:50	QoS 10 Mbps		Martin Laštovička		
	17	147.251.0.0/16		udp		2025/08/08 10:30	QoS 10 Mbps		Martin Laštovička		
147.251.0.0/16	17			udp		2025/08/18 10:00	QoS 10 Mbps		Martin Laštovička		

Analýza DDoS amplifikačních protokolů

- Výběr 16 nejčastěji zneužívaných protokolů
- Dlouhodobá analýza jejich provozu na MUNI
  - Průměrný datový tok v běžném provozu a ve špičce
  - Maximální datový tok v provozu (mimo útoky)
- **Většina protokolů se prakticky nevyužívá**, jejich datové toky jsou řádově desítky kb/s, ve špičce jednotky Mb/s

Nasazení QoS do Cesnet BGP Flowspec

Protokol	Port UDP	Navržený limit
~~DNS~~	~~53~~	~~100 Mb/s~~
NTP	123	100 Mb/s
Memcached	11211	10 Mb/s
SSDP/UPnP	1900	10 Mb/s
QotD	17	10 Mb/s
CharGen	19	10 Mb/s
cLDAP	389	10 Mb/s
NetBIOS	137	10 Mb/s
WS-Discovery	3702	10 Mb/s
CoAP	5683	10 Mb/s
ARMS	3283	10 Mb/s
TFTP	69	10 Mb/s
SNMP	161	10 Mb/s
Portmapper	111	10 Mb/s
mDNS	5353	10 Mb/s
Kad	751	10 Mb/s

- Na úrovni tranzitní sítě CESNET2
  - **Vnitřní provoz univerzity není nijak omezen**
  - Limitovaný provoz vůbec nedorazí do sítě MUNI
- Limity dle možností poskytovaných QoS, prakticky u všech protokolů **více než 5-10x vyšší než maximální** zaznamenaný provoz
- Nastaveno pro **oba směry**, tedy např. pro NTP je limit 2x 100 Mb/s
- **DNS zatím nelimitován** (mohlo by mít zásadní dopady, potřeba více zkušeností s Flowspec)

MUNI CSIRT-MU

Změna procesu blokace (na základě automatizovaných detekcí)

- Na základě zpětné vazby z Komun{ IT}
- Nově IP adresu útočící „zvenku“ na rozsahy MUNI blokujeme následovně:
  - První detekce za posledních 30 dní - **blokace na dvě hodiny**.
  - Druhá detekce za posledních 30 dní - **blokace na jeden den**.
  - Třetí a každá další detekce za posledních 30 dní - **blokace na 14 dní**.

Změna procesu blokace (na základě automatizovaných detekcí)

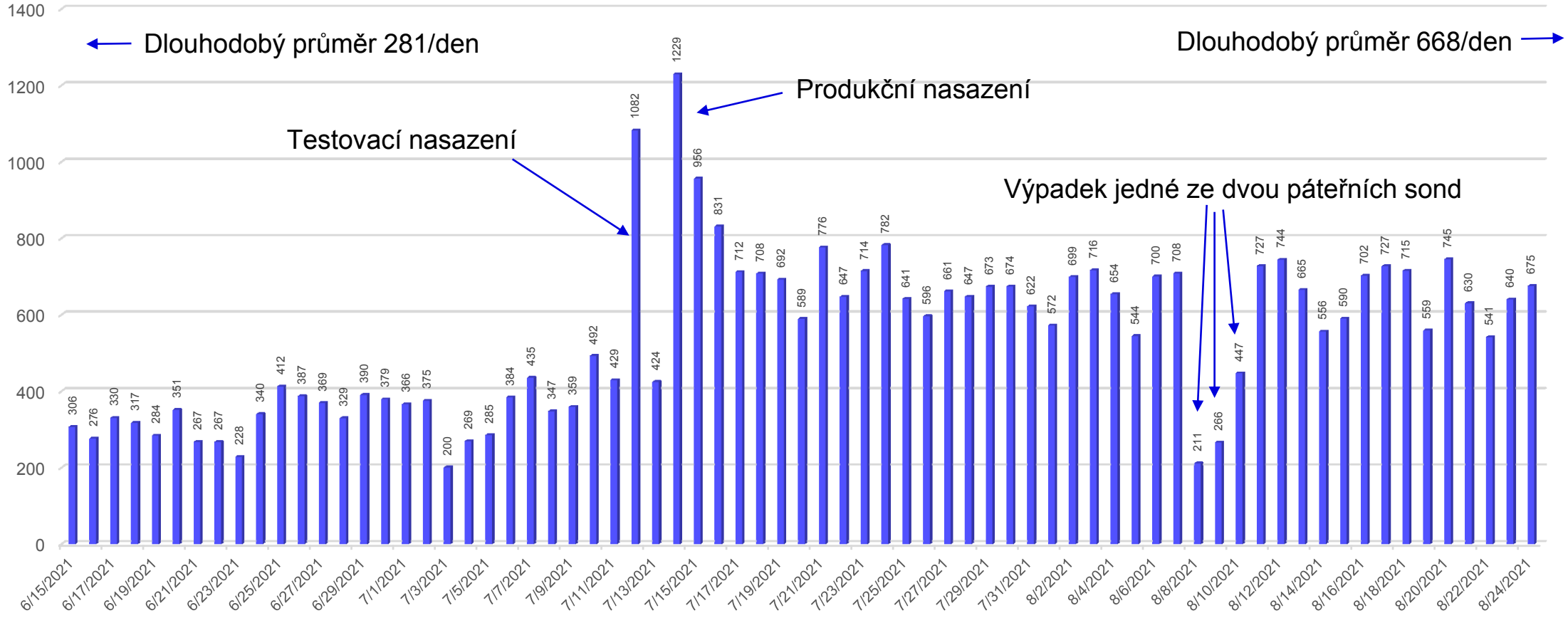
- Všechny detekce útoků **zevnitř sítě MUNI nejprve manuálně ověřujeme**.
- Stroje z MUNI tedy nikdy **automatizovaně neblokujeme**, ani správcům **nerozesíláme automatizovaná hlášení**.
- Jako stroje MUNI identifikujeme naše rozsahy + rozsahy **Metacentra** a **CESNETu**:
  - 147.251.0.0/16
  - 147.230.0.0/15
  - 147.228.0.0/16
  - 195.113.0.0/16
  - 78.128.128.0/17

MUNI CSIRT-MU

Nasazení distribuovaného zpracování flow dat

- Dříve nasazené řešení od Flowmon mělo **tvrdý limit** zpracování 1,5 milionu toků za 5 minut pro detekci pokusů o útok.
- Všechny toky nad limit byly **zahazovány**. Reálně tak detekce fungovaly s (náhodným) **vzorkováním cca 1:2.**
- Nové řešení založené na distribuovaném výpočetním clusteru (DA) zvládá **zpracovat kompletní provoz univerzity.**
- To má za důsledek zvýšení **počtu i kvality** automatizovaných detekcí.

Počet automaticky detekovaných a zpracovaných incidentů



MUNI CSIRT-MU

Penetrační testování – doporučení DPO

- Pro potřebu (ne)udělení **doporučení od Pověřenkyně MUNI (ochrana OÚ)**
- Rozhodnutí na základě provedeného **auditu IS/ICT**
  - Test zranitelností (automatizovaný)
  - Penetrační testování (manuální)
- Výstupem auditu **report z penetračního testování**
- Aktuální čekací doba **cca 2-3 měsíce**
- Testované systémy:
  - Jednotné přihlášení, Fidentis, MUNI pomáhá, JobCheckIN, BIOSKOP,…

Penetrační testování – identifikované problémy

- Problém s provozováním **spousty webových serverů** na MUNI
  - Často zapomenuté, nespravované či nezabezpečené
  - Obsahující osobní údaje
- **Doporučované řešení** CSIRT-MU:
  - Umbraco – statický obsah
  - cPanel – dynamický obsah
- Umbraco i cPanel **provozovány ÚVT MUNI**
- **Přijatelná úroveň** míry rizika zneužití a jeho dopadu

Zvýšení úrovně kyberbezpečnosti v prostředí VVŠ

- Projekt **CRP MŠMT** (CRP-KYBER21)
- Nastavení **základní úrovně KB** v prostředí VVŠ
- Adresace **problematiky (VIS)** dle ZoKB
  - IS MUNI, ESIS MUNI (INET + Magios)
  - Přijetí zákonných opatření, Manažer KB, Rada KB
- **Osvěta a vzdělávání** uživatelů (institucionální školení)
- Zabezpečení kolaborativních platforem pro **distanční výuku**
- V přípravě kyberbezpečnostní **CRP na rok 2022**

MUNI CSIRT-MU

Osvěta a vzdělávání

- Univerzita třetího věku (U3V)
  - **2 kurzy z oblasti kyberbezpečnosti** (Kyberhygiena a kybernetické útoky)
  - Realizace v jarním semestru 2021
  - **Kladná zpětná vazba od absolventů – pokračování i nadále**
  - Navrhovaný výstup – **odborný článek** (výuka KB na U3V)
- Školení sekretariátu rektora
  - Delší a složitější domluva, ale povedlo se!
  - Poděkování **Ondrovi Kulíškovi** za zprostředkování

Osvěta a vzdělávání

- CORE020 Digitální svět: technologie, potenciál i rizika
  - Předmět univerzitního základu
  - Primární zaměření na studenty neIT oborů
  - HPC, ukládání dat, počítačové sítě, AV přenosy, **kyberbezpečnost**, atd.

Příběhy sociálního inženýrství

- https://security.muni.cz/socialni_inzenyrstvi
- Nový kurz zaměřený na **techniky útoků proti uživatelům**
- Na názorných příbězích prezentuje, **v čem útok spočívá** a jak se mu bránit z pohledu běžného uživatele

MUNI CSIRT-MU

Budoucnost inforeportů

- Příliš **nákladné na údržbu**
  - Technologicky, lidsky i finančně
- Přesun do **on-line podoby** v Security Dashboardu
  - Potřeba dořešit autorizaci, kdo bude mít přístup k jakým datům
- **Připravujeme dotazník**, kterým získáme přehled o tom, co:
  - Vám v inforeportech (ne)přišlo užitečné
  - Co Vám na nich vadilo
  - Co dalšího byste si představovali zahrnout do budoucí náhrady

MASARYKOVA
UNIVERZITA