
Radovan Igliar, Jan Kolouch

cesnet


NEMOCNICE NA HOMOLCE
FAKULTNÍ NEMOCNICE OLOMOUC
FAKULTNÍ NEMOCNICE BULOVKA
FAKULTNÍ NEMOCNICE U SV. ANNY V BRNĚ
ÚVN
ÚSTŘEDNÍ VOJENSKÁ NEMOCNICE
Vojenská fakultní nemocnice Praha
ODBORNÝ LÉČEBNÝ ÚSTAV PASEKA
OBLASTNÍ NEMOCNICE PŘÍBRAM, a. s.
ZZS KVK
ZÁCHRANNÁ SLUŽBA OLOMOUCKÉHO KRAJE
Zdravotnická záchranná služba
Královéhradeckého kraje
VFN PRAHA
VŠEOBECNÁ FAKULTNÍ NEMOCNICE
OBLASTNÍ NEMOCNICE KOLÍN
akciová společnost
NEMOCNICE TOMÁŠE BATI VE ZLÍNĚ
uhkt
Ústav hematologie a krevní transfuze
NEMOCNICE HAVLÍČKŮV BROD
ZDRAVOTNICKÁ ZÁCHRANNÁ SLUŽBA KRAJE VYSOČINA
FAKULTNÍ NEMOCNICE BRNO
NEMOCNICE JIHLAVA
Krajská nemocnice Liberec, a.s.
Liberec a Turnov
HSOC
HOSPITAL SECURITY OPERATION CENTER
ZZS ÚK
NEMOCNICE PARDUBICKÉHO KRAJE
PARDUBICKÁ NEMOCNICE
FN MOTOL
ZDRAVOTNICKÁ ZÁCHRANNÁ SLUŽBA MS KRAJE
NEMOCNICE NOVÉ MĚSTO NA MORAVĚ
příspěvková organizace
Rodinné nemocnice v Plzeňském kraji
Klatovská nemocnice
MO Masarykův onkologický ústav
NEMOCNICE HAVÍŘOV
SLEZSKÁ NEMOCNICE V OPAVĚ
Krajská zdravotní, a.s.
Masarykova nemocnice v Ústí nad Labem, o.z.
NAKIT
Národní agentura pro komunikační a informační technologie, s. p.
REHABILITAČNÍ NEMOCNICE BEROUN
FAKULTNÍ NEMOCNICE HRADEC KRÁLOVÉ
KLAUDIÁNOVA NEMOCNICE
NEMOCNICE VE FRÝDKU-MÍSTKU
MINISTERSTVO VNITRA ČESKÉ REPUBLIKY
Kraj Vysočina
ČVUT
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE
Spolek pro ochranu osobních údajů
cesnet

# ZAČÁTEK?

# V Benešově udeřil virus, který vydírá nemocnice i města po celém světě

https://www.idnes.cz/technet/software/benesov-nemocnice-ransomware-paralyzovana-kryptovirus.A191211_085601_software_kuz

11. prosince 2019 10:46, aktualizováno 11:35

V benešovské nemocnici pravděpodobně zaútočil typ počítačového viru, který dokáže z provozu vyřadit policii, úřady i celá města. V Česku novinka, jinde už běžná praxe.


ilustrační snímek | foto: @k3r3n3, Jan Kužník, Technet.cz

Provoz benešovské nemocnice zcela narušil počítačový virus, který v noci napadl nemocniční počítačový systém. Nelze spustit žádný přístroj včetně počítačové sítě. Nemocnice musí rušit i plánované operace. Lékaři odbavují pacienty postaru, jako „před příchodem počítačů".

| Cíl útoku | Zjištění útoku | Vektor úroku | Nástroj útoku | Dopad útoku | Odhadované škody |
|---|---|---|---|---|---|
| **Nemocnice Rudolfa a Stefanie v Benešově (444 lůžek)** | 11. 12. 2019 | Phishing | EMOTET-TRICKBOT-RYUK **(ransomware)** | Odstavení nemocnice z provozu. Nefunkčnost některých ICT služeb. | 59 milionů Kč |
| **FN Brno (1889 lůžek)** | 12. 3. 2020 | Phishing | DEFRAY **(ransomware)** | Odstavení z provozu. Nedostupnost dat pacientů. | Řádově stovky milionů Kč |
| **Psychiatrická léčebna Kosmonosy (cca 600 lůžek)** | 27. 3. 2020 | Phishing | DEWAR **(ransomware)** | Zašifrování sdílených úložišť, doménových a aplikačních disků. Ztráta části záloh. | Není známo |
| **FN Ostrava (1200 lůžek)** | 17. 4. 2020 | Spear phishing | Není znám | Neuvedeno | Není známo |
| **FN Olomouc (1198 lůžek)** | 17. 4. 2020 | Scanování sítě | Není znám | Neuvedeno | Není známo |
| **Nemocnice následné péče LDN Horažďovice (140 lůžek)** | Leden 2020 | Phishing | **(ransomware)** | Neoprávněné použití, poškození a smazání dat | 150 000 Kč |

# REAKCE?

# Hrozí hackerské útoky na nemocnice, varuje kyberúřad. Očekává je v příštích dnech

https://zpravy.aktualne.cz/domaci/hrozi-hackerske-utoky-na-nemocnice-varuje-kyberurad-ocekava/r~98267f407fcf11eaa6f6ac1f6b220ee8/

ČTK, Domácí

*Aktualizováno 16. 4. 2020 13:50*

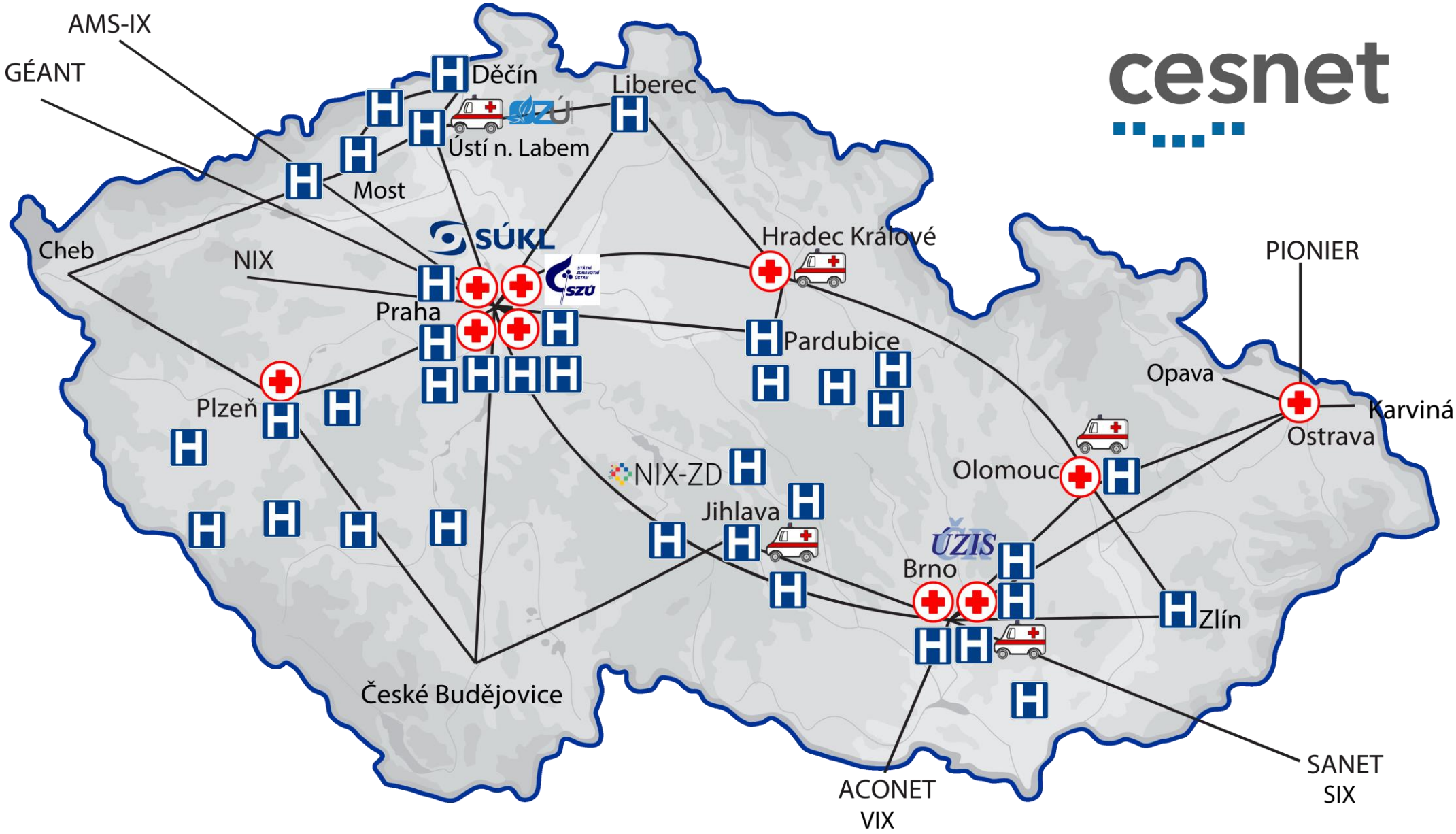
Národní úřad pro kybernetickou a informační bezpečnost varuje před hrozbou kyberútoků na nemocnice a jiné cíle. Lze je podle něj očekávat v nejbližších dnech.

- **v březnu 2020 vydal NÚKIB reaktivní opatření,**

  https://www.nukib.cz/cs/infoservis/aktuality/1418-nukib-vydal-reaktivni-opatreni-pro-vybrane-subjekty-ve-zdravotnictvi/

- **v dubnu 2020 vydal NÚKIB varování** https://www.nukib.cz/cs/infoservis/aktuality/1425-hrozba-kybernetickych-utoku-na-nemocnice-a-jine-vyznamne-cile-cr/


https://www.nukib.cz/download/publikace/podpurne_materialy/2020-07-17_Minimalni-bezpecnostni-standard_v1.0.pdf


AMS-IX
GÉANT
Děčín
Liberec
Ústí n. Labem
Most
SÚKL
Cheb
NIX
Praha
Hradec Králové
PIONIER
Pardubice
Opava
Karviná
Ostrava
Plzeň
NIX-ZD
Olomouc
Jihlava
ÚZIS
Brno
Zlín
České Budějovice
ACONET
VIX
SANET
SIX


HSOC
HOSPITAL
SECURITY
OPERATION
CENTER

NENÍ

https://allcore.ca/blog/what-does-managed-it-services-mean-to-you/

# NEUDĚLÁ ZA VÁS

Strategie


MULTI-MILLION CORPORATE
CYBER SECURITY SPENDING
USER WITH LOCAL ADMIN
RIGHTS OPENS EMAIL ATTACHMENT
imgflip.com

Disaster recovery plány, zálohování,…

Personální kapacity, rozvoj znalostí …

# KOOPERACE, KOMUNIKACE

https://jagwire.augusta.edu/free-virtual-cybersecurity-camps-offered-this-summer/

# DŮVODY VZNIKU

- **Výrazný nárůst** kybernetických útoků na zdravotnická zařízení.
- **Velké rozdíly** v úrovni IT podpory a potřebami jednotlivých zdravotnických zařízení.
- **Chybí sdílená vize**, jak využít výhody digitálních technologií k transformaci zdravotnictví.

Problematika kybernetické bezpečnosti je ve zdravotnictví zásadně

**personálně a finančně podhodnocena**

# CÍL INICIATIVY

- **vznik komunity**, která zvýší počet poskytovatelů zdravotních služeb provozujících bezpečné informační technologie s dostatečným technickým a personálním zázemím.

- **Kooperace na budování kybernetické bezpečnosti ve zdravotnictví**

- Cíle a aktivity iniciativy jsou shrnuty v **memorandu** - https://hsoc.cesnet.cz/

# Memorandum

# Iniciativy pro koordinaci kybernetické bezpečnosti resortu zdravotnictví – hSOC

Září 2020

**Aktuální stav, důvody pro vznik iniciativy:**

- Zdravotnictví v ČR čelí rostoucímu riziku kybernetických útoků.
- Jsou velké rozdíly v úrovni IT podpory a potřebami jednotlivých nemocnic.
- Existují velké rozdíly ve vnímání kybernetické bezpečnosti jako priority ze strany managementu nemocnic popř. zřizovatelů.
- Chybí systémové a koncepční pojetí zajišťování kybernetické bezpečnosti jak jednotlivých nemocnic, tak resortu jako celku.

# Memorandum

## Iniciativy pro koordinaci kybernetické bezpečnosti v resortu zdravotnictví – hSOC

## v.2

## Srpen 2021

### Důvody vzniku iniciativy hSOC:

- Zdravotnictví v ČR čelí dlouhodobě tlaku kybernetických hrozeb a v poslední době proběhla řada významných kybernetických útoků.
- Mezi jednotlivými poskytovateli zdravotních služeb existují velké rozdíly v úrovni zabezpečení, vnitřní i vnější ICT podpory a ve vnímání kybernetické bezpečnosti, jako priority ze strany managementu; toto se týká jak poskytovatelů zdravotních služeb, tak i jejich zřizovatelů.
- Chybí systémové a koncepční pojetí zajišťování kybernetické bezpečnosti jak jednotlivých poskytovatelů zdravotních služeb, tak resortu jako celku.
- Systémově chybí sdílená vize transformace směrem k digitálnímu zdravotnictví

# CO JE A NENÍ CÍLEM

## hSOC je…

- **Platforma** pro výměnu informací a dobré praxe
- **Varovný a koordinační komunikační kanál**
- Platforma pro **provoz sdílených služeb a technologií**
- Komunita IT a bezpečnostních profesionálů a nadšenců
- **Prostor pro vzdělávání**

## hSOC není…

- **Univerzální řešení bezpečnosti zdravotnického zařízení**
- Subjekt
- Dohledové bezpečnostní centrum

# PRACOVNÍ SKUPINY

https://hsoc.cesnet.cz/cs/skupiny

**hSOC - Working group -> RADA**

- **Hlavní komunikační kanál řídícího výboru hSOC**
- účel: koordinace hSOC a signatářů iniciativy

**hSOC – Board**

- **Operativa, koordinace, řízení**
- účel: koordinace hSOC a signatářů iniciativy

**hSOC - EMERGENCY**

- **Emergency komunikační kanál hSOC**
- účel: předávání varování o aktuálních bezpečnostních hrozbách

**hSOC - TECH**

- technická pracovní skupina pro **řešení technických aspektů (síť, infrastruktura, zdravotnické systémy – modality)**
- účel: technické aspekty a standardy.

**hSOC – Management -> Governance CIOS**

- pracovní skupina pro **Governance hSOC**
- účel~~: řešící právní, legislativní, finanční a institucionálních aspektů hSOC~~
- účel: směrování architektury, financování a strategií IT ve zdravotnictví
- sdílení best-practices

**hSOC – MKB**

- pracovní skupina Manažerů kybernetické bezpečnosti
- účel: sdílení informací a dobré praxe manažerů kybernetické bezpečnosti

**hSOC – Education a HR**

- pracovní skupina **Human resources / Education**
- účel: rozvoj lidských zdrojů a vzdělávání v oblasti kybernetické bezpečnosti, sdílení lidských zdrojů

# KOMUNITNÍ ŘÍZENÍ, TRANSPARENTNOST

# Přehled aktivit HSOC

**Do aktivity je aktuálně zapojeno 42 zdravotnických organizací, 7 zřizovatelů a dalších 8 institucí.** /4. 10. 2021/

- 6. - 7. 10. - **Seminář Ransomware + výjezdní jednání HSOC**, Jihlava
- 4. - 5. 10. - **Health Czech 2021**, NUKIB, Brno
- 1. 10. 2021 - účast na jednání skupiny Manažerů kybernetické bezpečnosti nemocnic (iniciované NUKIBem)
- 30. 9. 2021 - Jednání pracovní skupiny MZ pro Standardy kybernetické bezpečnosti ve zdravotnictví
- 2. 9. 2021 a 9. 9. 2021 - Workshop: best-practice eGOV SOC
- 8. 9. 2021 - Prezentace Petr Pavlinec na akci e-government 20:10, Mikulov
- 11. 8. 2021 - Jednání signatářů HSOC
- 22. 7. 2021 - jednání MZČR
- 22. 7. 2021 - Workshop: best-practices #3 - SIEM
- 15. 7. 2021 - založ[illegible] **ezpečnostním standardům ve zdravotnictví**

cs:dokumenty:man:workshop-2021-07-22

- 30. 6. 2021 - zapojení nemocnic Středočeského kraje do HSOC
- 30. 6. 2021 - Prezentace HSOC na setkání Nemocnic Pardubického kraje
- 29. 6. 2021 - Metamorfosa 2021 - Nutné kroky k bezpečnému zdravotnictví - X dní po kyberútocích na nemocnice
- 23. 6. 2021 - Workshop: best-practices #2 - audity
- 18. 6. 2021 - Prezentace HSOC pro ředitele nemocnic Středočeského kraje na setkání PS **Kyberbezpečnost nemocnic Středočeského kraje**
- 14. 6. 2021 - **Všeobecná fakultní nemocnice v Praze** přepojena do **sítě HSOC**.
- 2. 6. 2021 - **Workshop: best-practices** - cybermanagement
- 12. 5. 2021 - ihned.cz / Hospodářské noviny - Nemocnice prosí stát o pomoc v boji s hackery: Víme, jak odrazit tisíce útoků, podělte se s námi o miliardy z Evropy
- 10. 5. 2021 - Computerworld.cz - Cesnet rozšiřuje zabezpečení infrastruktury

# AKTIVITY

# ZAPOJENO: 55+

- Podpora a zapojení NUKIB, NAKIT, OHA MVČR, …
- **Vyhrazená síťová infrastruktura (HSOC-VRF)**
- **Sdílení know-how a lidských kapacit**
  - best-practice, koncepce a design architektury
  - školení, semináře a workshopy
  - technologické standardy
  - **plán vzniku společného distribuovaného CSIRT týmu, SOC**
- **Nastavení workflow a procesů u zapojených subjektů**
- **Emergency komunikační kanály**
  - mailing-listy, videokonferenční systém, datové úložiště

# UZAVŘENÁ BEZPEČNÁ SÍŤ hSOC

- **7 nemocnic zapojeno**




- **další v procesu připojování**


  - **Monitorovací a bezpečnostní nástroje**
    - Společné politiky a pravidla

  - **Striktnější pravidla a politiky**

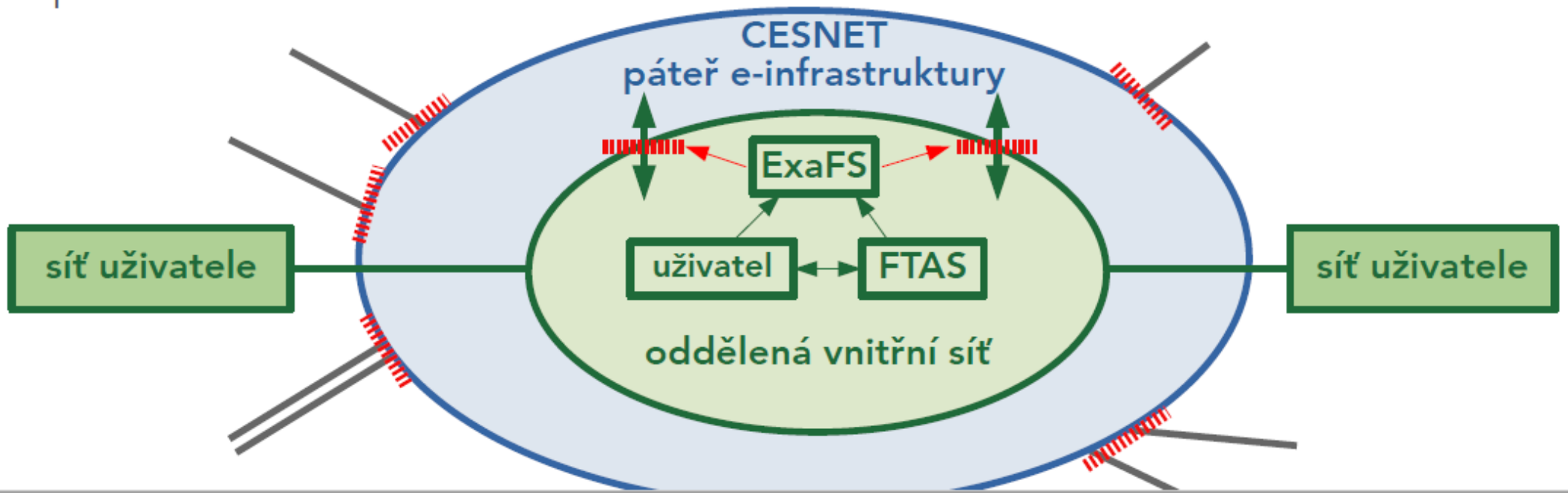
dalsi opevneni a striktnejsimi politikami

# hSOC VRF

- **Geografická redundance přepojení do Internetu ve dvou lokalitách**
- **Ochrana**
  - proti podvržení IP adres (IP spoofing),
  - proti podvržení oznamovaných prefixů od peering-partnerú,
  - proti amplifikačním (volumetrickým) DDoS útokům,
  - proti agresivním i pomalým scanům,
  - nástroji pro uživatele pro analýzu a regulaci svého provozu v síti e-infrastruktury CESNET,
  - automatickým přesměrováním provozu k vyčištění v jádru globálního internetu (celosvětová mitigace vůči detekovaným zdrojům nežádoucího provozu.
- **Tvrději nastavené limity a politiky**
  - Možnost omezení, zahození útoku ještě na páteřní síti

**V současnosti denně cca 80 – 90 tis. detekovaných a automaticky mitigovaných hrozeb na perimetru sítě**

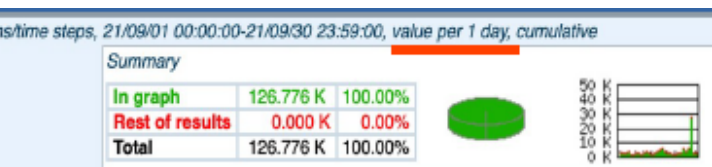
- **oddělená infrastruktura pro specifickou komunitu** ~ síť v síti
  - automaticky sdílí prvky obrany a zabezpečení vnější sítě – e-infrastruktury CESNET
    - ACL, BCP-38, policing provozu, RTBH, BGP FlowSpec, externí čištění, monitoring, dohled, sdílení bezpečnostních informací, CSIRT, ...
  - + samostatné instance nástrojů pro regulaci provozu, monitoring a detekci anomálií
    - specifická nastavení pro komunitu, automatická regulace, přístup správců k nástrojům pro řízení provozu

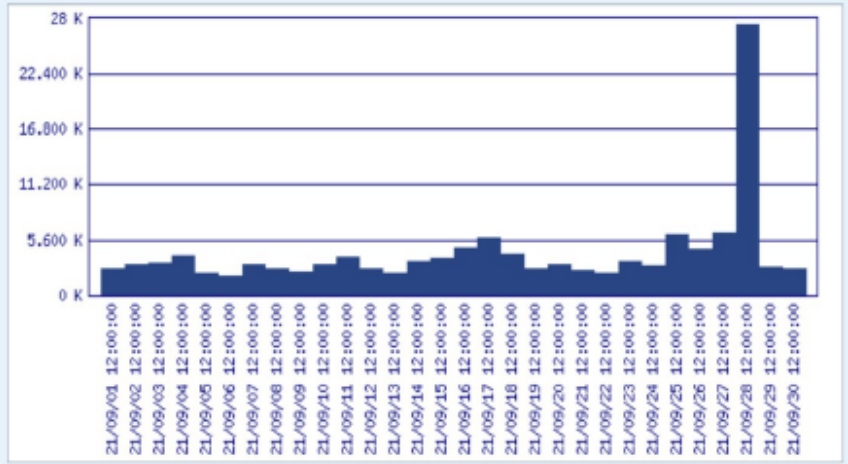


*nt-Cnt:* sums/time steps, 21/09/01 00:00:00-21/09/30 23:59:00, value per 1 day, cumulative

Summary

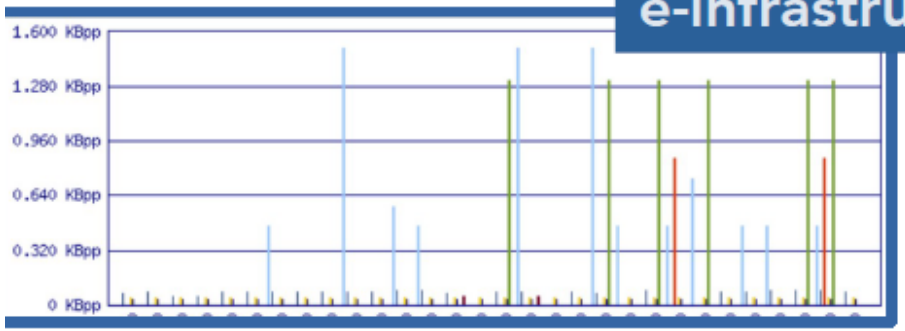
| | | |
|---|---|---|
| In graph | 126.776 K | 100.00% |
| Rest of results | 0.000 K | 0.00% |
| Total | 126.776 K | 100.00% |




| Flow-Start | Flow-End | Bytes-estimated | Pkts-estimated | Src-IP-Cnt | Avr-Pkt-Length | Flow-Cnt | Flow-Cnt-Drop | Detected-Event-Cnt |
|---|---|---|---|---|---|---|---|---|
| 09/01 00:01:55.000 | 21/09/30 23:57:20.000 | 2.987 TB | 31.680 Gp | 4616 | 94.29 | 68531679 | 2722920 | 126776 |

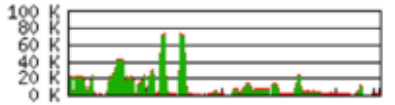
e-infrastruktura

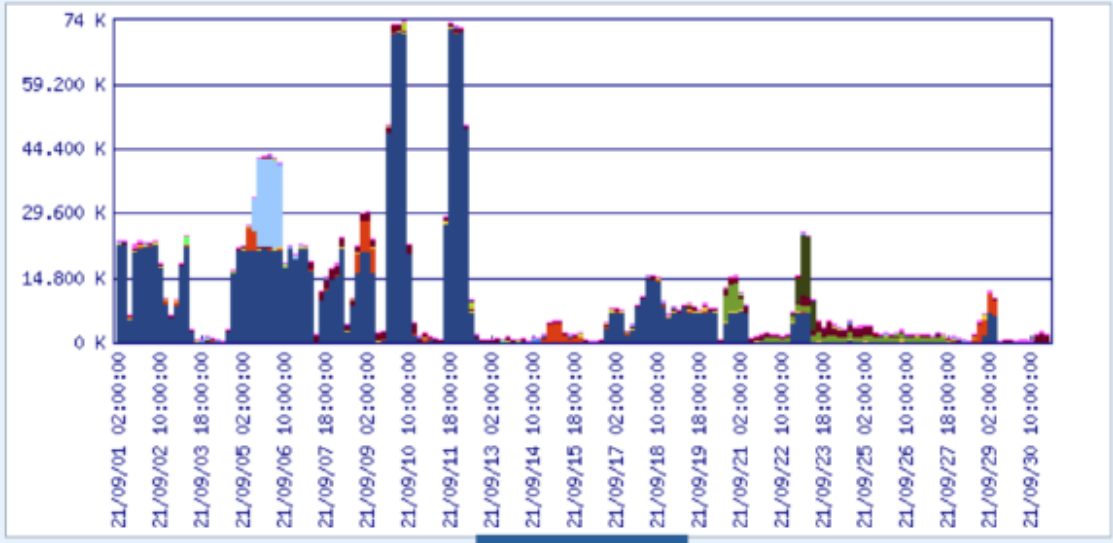



***Detected-Event-Cnt:*** *sums/time steps, 21/09/01 00:00:00-21/09/30 23:59:00, value per 4 hours, cumulative*

Summary

| | | |
|---|---|---|
| In graph | 2.071 M | 98.93% |
| Rest of results | 0.022 M | 1.07% |
| Total | 2.093 M | 100.00% |




hSOC

| | | Bytes-estimated | Pkts-estimated | Src-IP-Cnt | Avr-Pkt-Length | Flow-Cnt | Flow-Cnt-Drop | Detected-Event-Cnt |
|---|---|---|---|---|---|---|---|---|
| 1. | > | 25.054 GB | 613.014 Mp | 8324 | 40.87 | 612676912 | 598686837 | 2093241 |

- **Pracovní skupiny**
- **Podpis memoranda**
- https://hsoc.cesnet.cz/_media/cs/memorandum_hsoc_2021.pdf
- **Standardy - Minimální a doporučující standardy vs. ZKB -> NIS2 ☺**
  - **Identifikace aktiv**
  - **Disaster recovery**
- **Komunitní emergency platforma a komunikační postupy**
- **Technické zapojení:**
  - Zálohované připojení
  - HSOC-VRF
  - Monitorovací a bezpečnostní nástroje
  - Technické standardy
  - Service desk - procesy
- **Best-practice sharing**
- **Sdílené služby**
  - **Distribuovaný CSIRT, SOC tým**
- **CESNET SOC**


Fosa 2021

https://hsoc.cesnet.cz/

**https://hsoc.cesnet.cz/cs/join**

hsoc@cesnet.cz

# DĚKUJI ZA POZORNOST

**Radovan Igliar**
radovan.Igliar@cesnet.cz

**doc. JUDr. Jan Kolouch, Ph.D.**
jan.kolouch@cesnet.cz