cesnet

# HSOC
## HOSPITAL SECURITY OPERATION CENTER

**Jan Kolouch, Radovan Igliar**
**CESNET**

**25. 4. 2022**
**Hospital Management 2022**

cesnet

HSOC
HOSPITAL SECURITY OPERATION CENTER

cesnet

HSOC
HOSPITAL
SECURITY
OPERATION
CENTER

hSOC

- 61 zdravotnických zařízení
- 8 zřizovatelů
- 1 ministerstvo
- 3 univerzity
- 5 dalších institucí

cesnet

# ZAČÁTEK?

cesnet

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

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".

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

KLATOVSKÝ
deník.cz

VYBRAT REGION

VYBRAT MĚSTO | ZPRÁVY | SPORT | ČERNÁ KRONIKA | KULTURA | PODNIKÁNÍ | MIMINKA | NAŠI PRVŇÁČCI | TIPY DENÍKU | DALŠÍ

# Horažďovickou nemocnici napadl hacker, zmizely rentgeny

**Horažďovice – Počítačový systém nemocnice v Horažďovicích nejspíše napadl hacker.**

30.1.2018 1 SDÍLEJ:

DALŠÍ ČLÁNKY Z RUBRIKY


OBRAZEM: Horažďovický kulturní dům patřil dětem


Domov pro seniory v Horažďovicích stavět nezačnou


VIDEO: Lyžaři mají na Šumavě ideální podmínky

ŠÍP


Co má Vendula Svobodová raději než SEX S MANŽELEM? Tomu snad nikdo nebude věřit


Celebrity, které si k dokonalému vzhledu pomohly novým nosem


Martina Navrátilová EXKLUZIVNĚ o rakovině: ANI PENÍZE VÁM ŽIVOT NEZACHRÁNÍ

Syn Ivety Bartošové VZDAL své hudební SNY? Hodlá zcela změnit obor!

https://klatovsky.denik.cz/zpravy_region/horazdovickou-nemocnici-napadl-hacker-zmizely-rentgeny-20180130.html

cesnet

# WANNACRY

cesnet


Wana Decrypt0r 2.0
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/15/2017 16:32:52
Time Left
02:23:59:49
Your files will be lost on
5/19/2017 16:32:52
Time Left
06:23:59:49
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt

cesnet

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.

| 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 2021 | Phishing | **(ransomware)** | Neoprávněné použití, poškození a smazání dat | 150 000 Kč |
| **Českolipská nemocnice** | Únor 2022 | - | **-** | - | - |

cesnet


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

cesnet

# BUZZWORDS

cesnet

# BUZZWORDS?

CLOUD

NIS2

ZKB

SOC

ISMS

SIEM

DRP

MDS2

cesnet

# HSOC

## HOSPITAL SECURITY OPERATION CENTER

cesnet

# NENÍ

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

cesnet

# ONE BOX SOLUTION

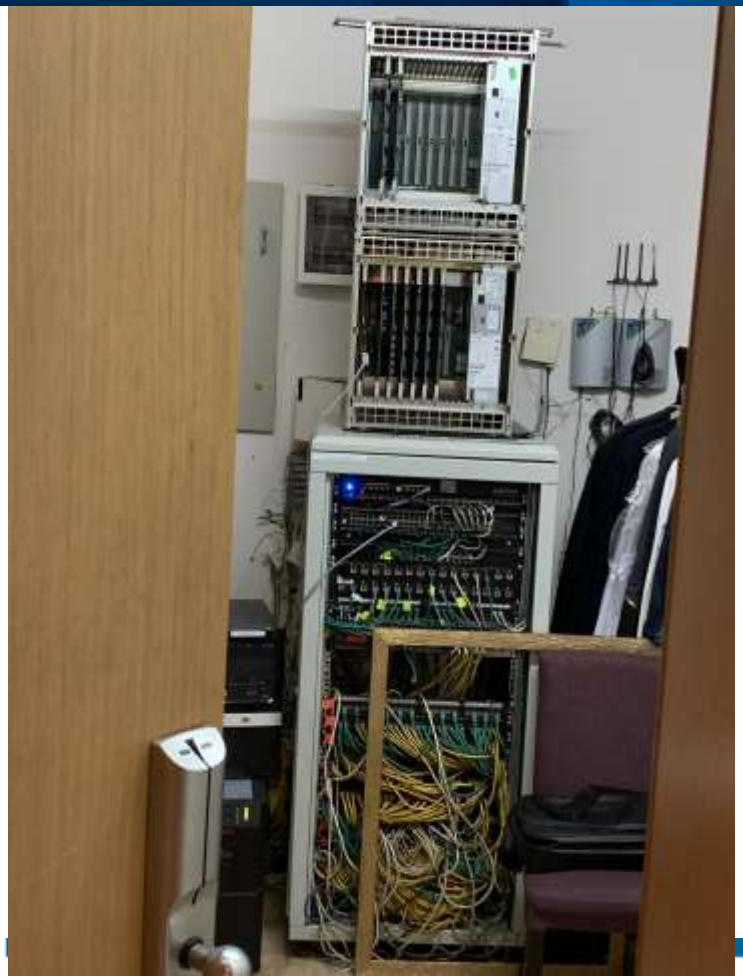
https://knowyourmeme.com/photos/1032935


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


IN CASE OF
CYBERATTACK
BREAK GLASS
AND PULL CABLES

cesnet

# FYZICKOU BEZPEČNOSTÍ

cesnet

# 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**

# 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 je**

**personálně ~~a finančně~~ podhodnocena**

# CÍL hSOC

- **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/**

cesnet

# KOMUNITNÍ ŘÍZENÍ, TRANSPARENTNOST

cesnet

# Přehled aktivit HSOC

**Do aktivity je aktuálně zapojeno 56 zdravotnických organizací, 8 zřizovatelů, 3 univerzity, 1 ministerstvo a dalších 5 instituce.** /15. 2. 2022/

- 13. 4. 2022 - jednání s MZČR
- 11. 4. 2022 - prezentace **Bezpečnostní aspekty digitální medicíny** na konferenci Czech digital medicine summit 2022
- 23. 3. 2022 - workshop: Architektura - kybernetická bezpečnost nemocnice
- 2. 3. 2022 - školení Monitorovací a bezpečnostní nástroje
- 28. 2. 2022 - jednání HSOC na Ministerstvu zdravotnictví
- 23. 2. 2022 - workshop Zdravotechnika a vzdálený přístup
- 22. 2. 2022- **Oblastní nemocnice Mladá Boleslav, a.s.** přepojena do **sítě HSOC**.
- 22. 2. 2022 - prezentace na ICT ve Zdravotnictví
- 02/2022 - Informace o detekci a eliminaci anomálního provozu v hSOC-VRF - 02/2022
- 3. 2. 2022- **Krajská nemocnice T. Bati ve Zlíně** přepojena do **sítě HSOC**.
- 2. 2. 2022 - jednání **hSOC s MZ a NUKIB**
- 15. 11. 2021 - prezentace na setkání Metamorfosa 2021 - bezpečné zdravotnictví
- 4. 11. 2021 - prezentace na eGovernment - Setkání informatiků krajů, Plzeň
- 6. - 7. 10. 2021 - **Seminář Ransomware + výjezdní jednání HSOC**, Jihlava
- 4. - 5. 10. 2021 - **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
- 22. 7. 2021 - jednání MZČR
- 22. 7. 2021 - Workshop: best-practices #3 - SIEM
- 15. 7. 2021 - založení **pracovní skupiny MZČR k Bezpečnostním standardům ve zdravotnictví**
- 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

## Best-practices workshop: Zdravotechnika a vzdálené přístupy

| | |
|---|---|
| Termín: | **23. 2. 2022, 10:00 - cca 12:00** |
| Místo: | online, pozvánka zaslána do listu HSOC-WG, HSOC-MAN, HSOC-TECH |
| Účastníci: | náměstci a vedoucí, architekti systémů a bezpečnosti, správci ICT systémů |

Cílem workshopu je sdílení dobré praxe (best-practices) a know-how mezi nemocnicemi.

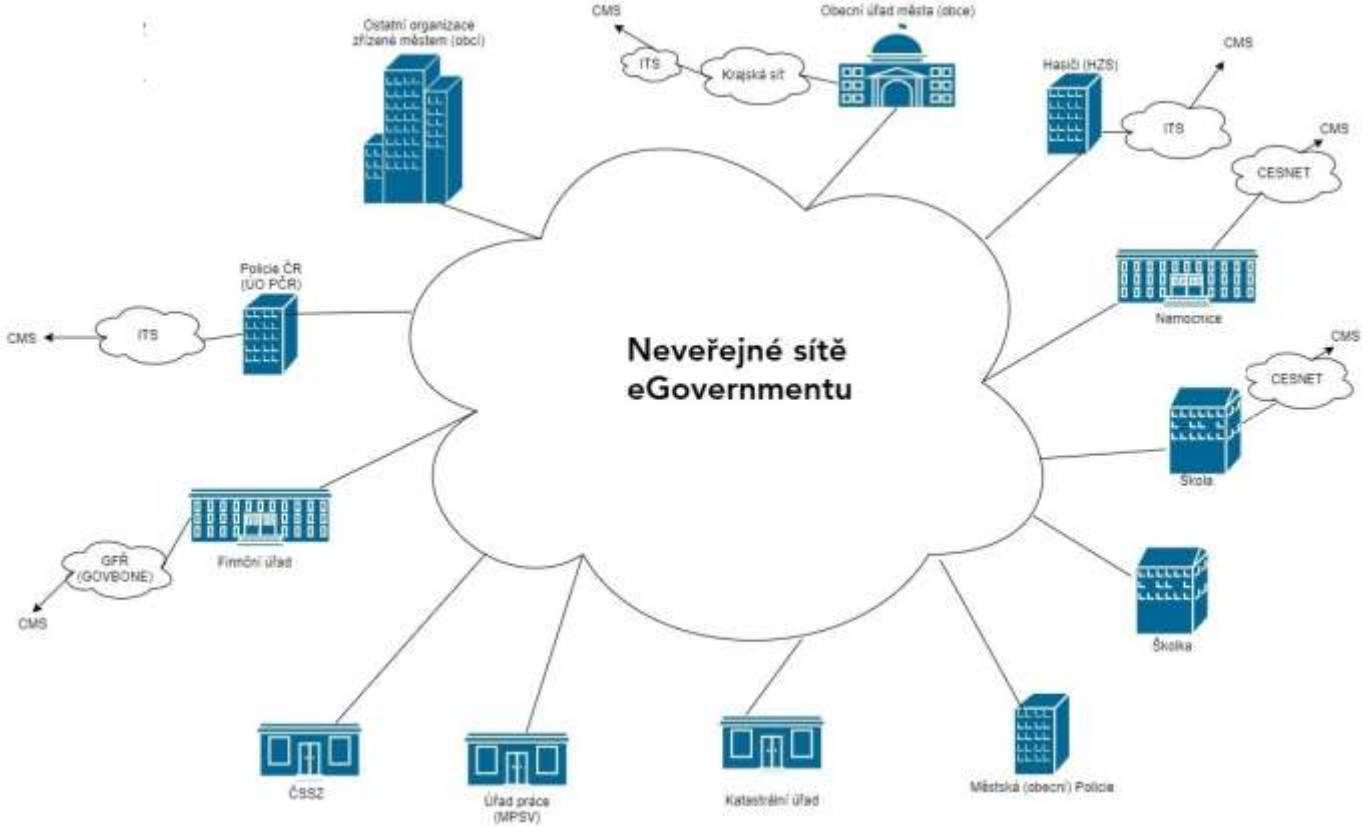

cesnet
KONKRÉTNÍ AKTIVITY?

https://knowyourmeme.com/photos/1032935

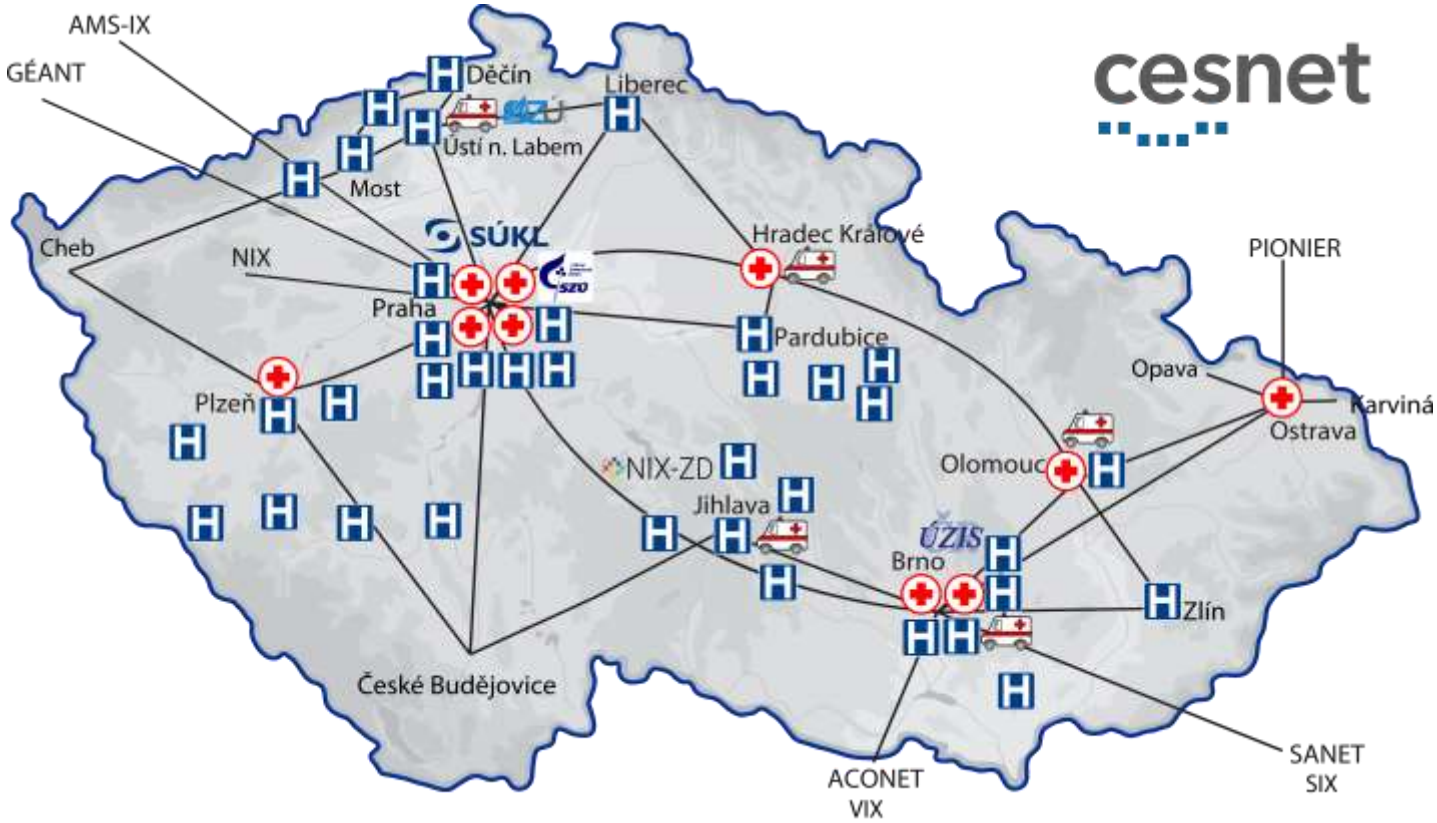
# POC: KOMUNITNÍ DISTRIBUOVANÝ SOC/CSIRT TÝM

| | Project month | | | | | |
|---|---|---|---|---|---|---|
| Activity | 1 | 2 | 3 | 4 | 5 | 6 |
| **1. Distributed community SOC** | | | | | | |
| - establishment of the SOC/CSIRT team | X | | | | | |
| - setting the internal team rules and processes | | X | | | | |
| - setting the external rules and processes for cooperation with other CSIRT teams | | | X | | | |
| - hSOC team operation | | | X | X | X | X |
| | | | | | | |
| **2. Define cybersecurity standards and best-practices for health sector** | | | X | X | X | |
| | | | | | | |
| **3. Education and training (workshops)** | | X | | X | | X |
| | | | | | | |
| **4. Conclusions and recommendations (case study)** | | | | | | X |

## Neveřejné sítě eGovernmetu



## Sdílené služby – sdílené kapacity



# DALŠÍ AKTIVITY

- **Podpora a zapojení NUKIB, NAKIT, OHA MVČR, …**
- **Standardy a architektura**
- **PoC: komunitní distribuovaný SOC/CSIRT tým**
- **Neveřejné sítě eGovernmentu**
- **Služby**
  - Zálohované připojení
  - hSOC-VRF
  - Monitoring a bezpečnostní nástroje
  - Disaster recovery
  - SOC CESNET
- **Best-practice sharing**
- **Emergency komunikační kanál**

- **9 nemocnic zapojeno**
- **další v procesu připojování**













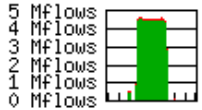
- **Monitorovací a bezpečnostní nástroje**
  - Společné politiky a pravidla

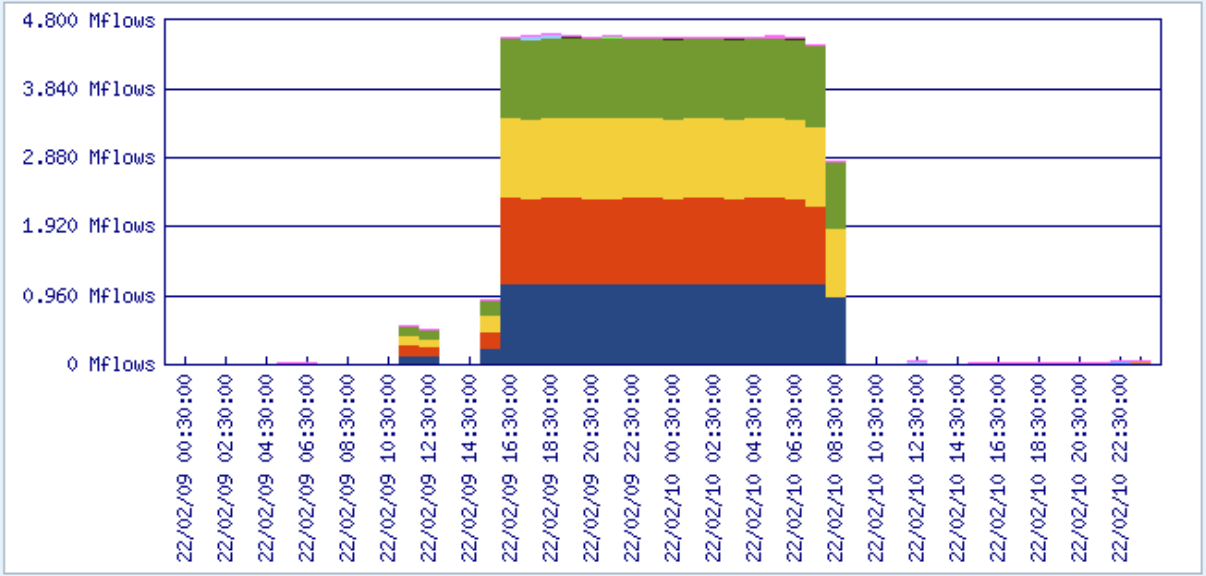

- **Striktnější pravidla a politiky**


**Flow-Cnt-Drop:** *sums/time steps, 22/02/09 00:00:00-22/02/11 00:00:00, value per 1 hour, cumulative*

*Summary*

| | | |
|---|---|---|
| **In graph** | 78.051 Mflows | 99.58% |
| **Rest of results** | 0.328 Mflows | 0.42% |
| **Total** | 78.379 Mflows | 100.00% |




| o | > | Src-IP | Src-GeoIP | Flow-Start | Flow-End | Bytes-measured | Bytes-estimated | Pkts-measured | Pkts-estimated | Flow-Cnt | Flow-Cnt-Drop |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1. | > | [redacted] | | 22/02/09 11:31:00.000 | 22/02/10 08:50:48.000 | 794.470 MB | 794.470 MB | 19.597 Mp | 19.597 Mp | 19589981 | 19502770 |
| 2. | > | | | 22/02/09 11:29:52.000 | 22/02/10 07:54:28.000 | 791.902 MB | 791.902 MB | 19.691 Mp | 19.691 Mp | 19684338 | 19599917 |
| 3. | > | | | 22/02/09 11:32:20.000 | 22/02/10 08:50:48.000 | 781.825 MB | 781.825 MB | 19.283 Mp | 19.283 Mp | 19276531 | 19190849 |
| 4. | > | | | 22/02/09 11:31:30.000 | 22/02/10 08:50:42.000 | 780.890 MB | 780.890 MB | 19.257 Mp | 19.257 Mp | 19250179 | 19163519 |

cesnet

# GENEZE?

cesnet

MINISTERSTVO ZDRAVOTNICTVÍ
ČESKÉ REPUBLIKY

Milan BLAHA
náměstek ministra pro informační a komunikační technologie

Praha 4. března 2022

Č. j.: MZDR 8118/2022-1/IKT

*MZDRX01JPHTT*

MZDRX01JPHTT

Vážená paní ředitelko, vážený pane řediteli,

obracím se na Vás v souvislosti s činností komunitní platformy hSOC, která má za cíl zvýšit počet poskytovatelů zdravotních služeb provozujících bezpečné informační technologie s dostatečným technickým a personálním zázemím v oblasti kybernetické bezpečnosti.

Ministerstvo zdravotnictví zapojení dalších poskytovatelů zdravotních služeb do komunitní platformy hSOC podporuje a sdílí vizi spočívající ve využití sdílených vědomostí, znalostí a infrastruktury směřující k zvýšení kybernetické bezpečnosti poskytovatelů zdravotních služeb.

Informace o této platformě jsou k dispozici na webové stránce https://hsoc.cesnet.cz. Hlavní myšlenkou je vytvoření bezpečné komunikační infrastruktury mezi nemocnicemi, lepší zabezpečení připojení k veřejném internetu, nastavení bezpečnostního monitoringu provozu, sdílení know-how a poskytování sdílených (distribuovaných) služeb pro včasné varování. Platforma hSOC propojuje poskytovatele zdravotních služeb s cílem zvýšení kybernetické bezpečnosti zejména:

- organizováním komunity odborníků na IT a kybernetickou bezpečnost,
- poskytováním sdílených (distribuovaných) služeb,
- sdílením informací o incidentech a koordinací systému včasné výstrahy před kybernetickými hrozbami,
- společným budováním bezpečné ICT infrastruktury (např. hSOC VRF aj.),

https://hsoc.cesnet.cz/_media/cs/2022-03-04-mzcr-hsoc-letter_of_support.pdf

Návrh

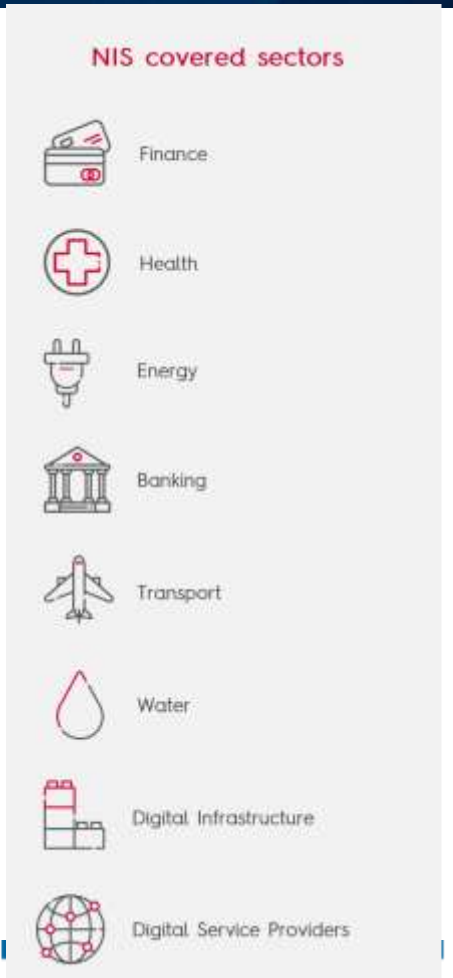
SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY

o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o zrušení směrnice (EU) 2016/1148

https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52020PC0823&from=EN

# NIS A NIS2

- **NIS předpokládal, že některé organizace nejsou závislé na ICT**
- Současná odvětví jsou zachována a jsou **přidána odvětví další**
- **Identifikace a regulace dopadne na organizaci jako celek**, nikoli na systém, na němž je závislé fungování základní služby

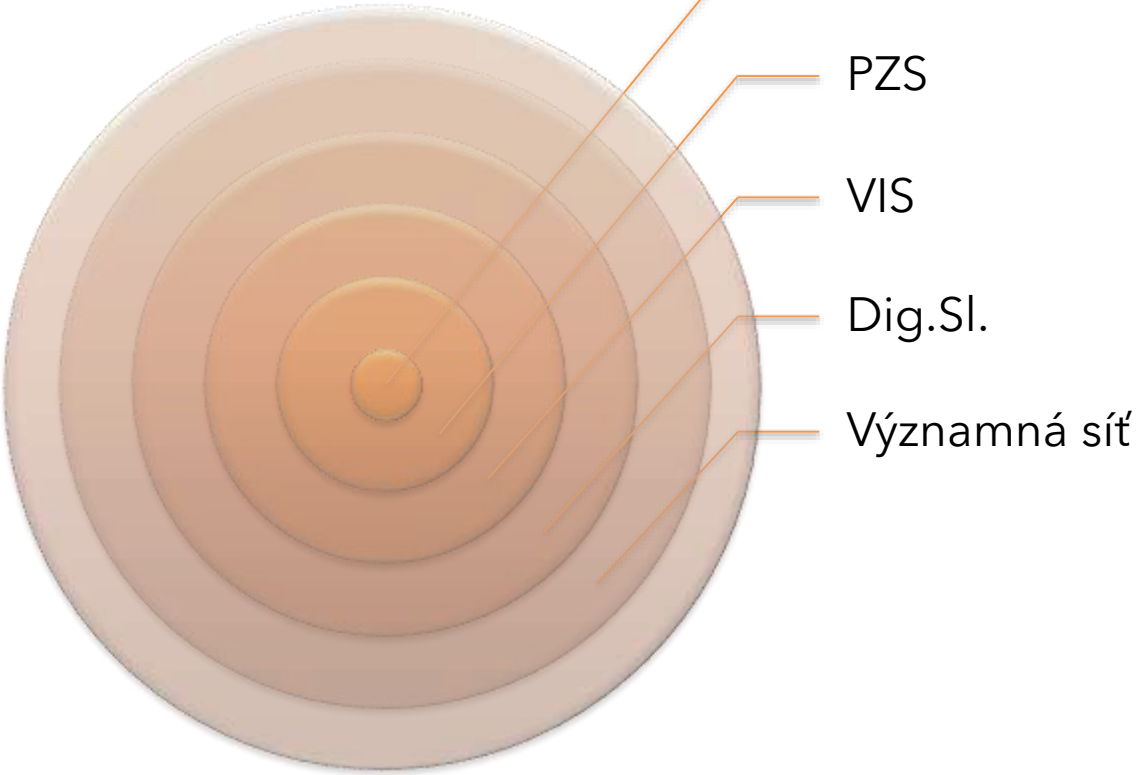


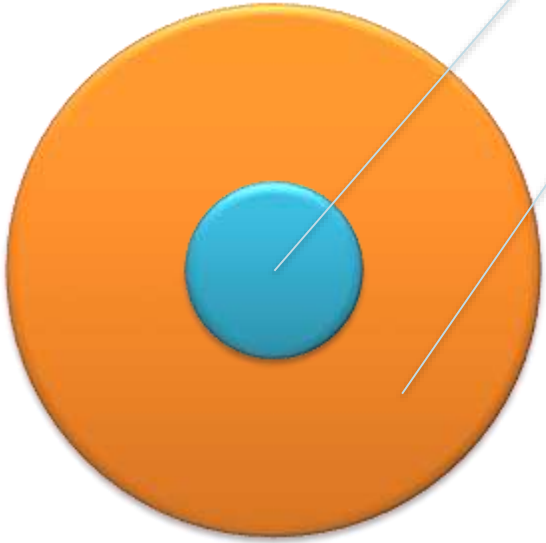

| Sectors covered by NIS 1 | Sectors covered by NIS 2 proposal |
|---|---|
| "Operators of essential services" category | "Essential entities" |
| | ***All sectors from NIS 1*** |
| Healthcare providers | Additional health-related services - including pharma, some medical device manufacturers, researchers |
| Digital infrastructure - IXPs, DNS services, TLD registries) | Additional digital infrastructure services - cloud computing services, data centers, CDNs, network providers |
| Drinking water | Waste water |
| Transport | Space |
| Financial market infrastructure | Public Administration |
| Energy | |
| Banking | |
| "Digital service providers" category | "Important entities" |
| Online marketplaces | Online marketplaces |
| Online search services | Online search services |
| Cloud services | Social networking services |
| | Food production & distribution |
| | Postal services |
| | Waste management |
| | Chemical manufacturers |
| | Manufacturing - medical devices, electronic products and equipment, machinery, vehicles and transport equipment |

https://www.rapid7.com/blog/post/2021/04/20/overview-of-the-eus-draft-nis-2-directive/

cesnet

# CO SE STANE?



cesnet

HSOC
HOSPITAL SECURITY OPERATION CENTER

cesnet

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

hsoc@cesnet.cz


cesnet
DĚKUJI ZA POZORNOST