cesnet

HSOC
HOSPITAL SECURITY OPERATION CENTER

Jan Kolouch, Radovan Igliar
CESNET

8. března 2022
Seminář o bezpečnosti sítí a služeb

cesnet

HSOC
HOSPITAL SECURITY OPERATION CENTER

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

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/

cesnet


MINIMÁLNÍ BEZPEČNOSTNÍ STANDARD

podpůrný materiál pro subjekty, které nespadají pod zákon o kybernetické bezpečnosti

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

NAKIT

Národní agentura pro komunikační a informační technologie, s. p.

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

Verze 1.0, platná ke dni 17. července 2020

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

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

HSOC

HOSPITAL SECURITY OPERATION CENTER

cesnet

NENÍ

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

cesnet

ONE BOX SOLUTION

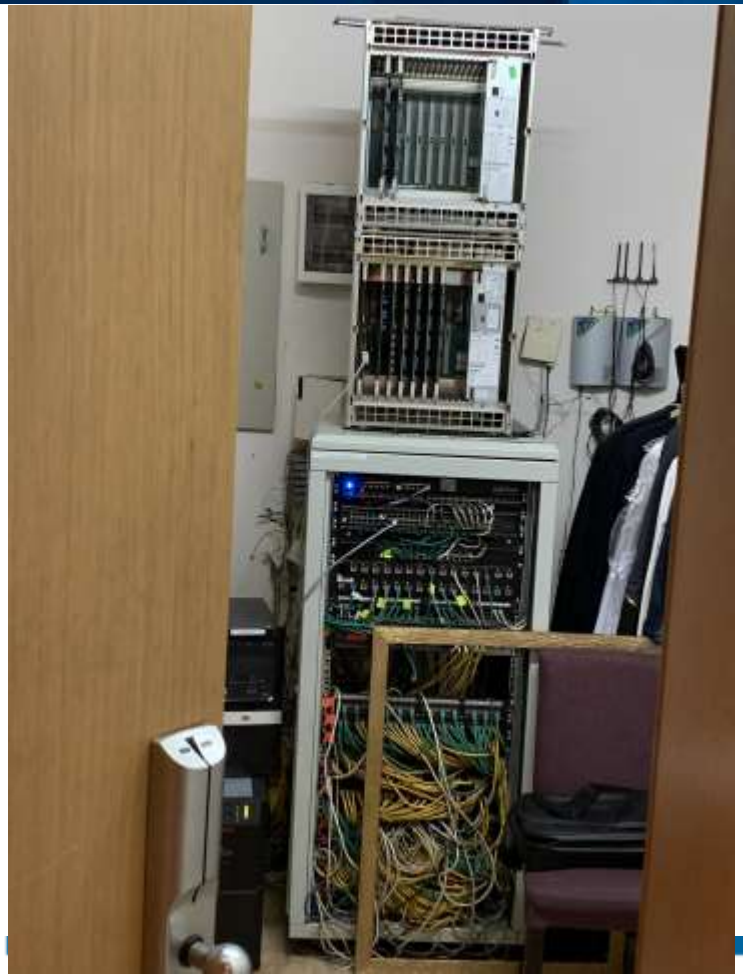
https://knowyourmeme.com/photos/1032935


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

KOOPERACE A KOMUNIKACE

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

Memorandum

Iniciativy pro koordinaci kybernetické bezpečnosti resortu zdravotnictví – hSOC

Září 2020

Vize – Cílový stav

Poskytovatelé zdravotních služeb provozující bezpečné informační technologie s dostatečným technickým a personálním zázemím s podporou centralizované ochrany typu SOC.

- Chybí systémové a koncepční pojetí zajišťování kybernetické bezpečnosti jak jednotlivých nemocnic, tak resortu jako celku.

cesnet

Memorandum

Iniciativy pro koordinaci kybernetické bezpečnosti v resortu zdravotnictví – hSOC

v.2

Srpen 2021

Vize – Cílový stav

Poskytovatelé zdravotních služeb provozující bezpečné informační technologie s dostatečným technickým a personálním zázemím s podporou CSIRT (Computer Security Incident Response Team) a SOC (Security Operation Center) v rezortu zdravotnictví.

PRACOVNÍ KUPINY

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

hSOC - Working group -> RADA

- **Hlavní komunikační kanál řídícího výboru hSOC**

hSOC – Board

- **Operativa, koordinace, řízení**

hSOC - EMERGENCY

- **Emergency komunikační kanál hSOC**

hSOC - TECH

- technická pracovní skupina pro **řešení technických aspektů (síť, infrastruktura, zdravotnické systémy – modality)**

hSOC – Management -> Governance CIOs

- 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

- účel: rozvoj lidských zdrojů a vzdělávání v oblasti kybernetické bezpečnosti, sdílení lidských zdrojů


cesnet
KOMUNITNÍ ŘÍZENÍ,
TRANSPARENTNOST

Přehled aktivit HSOC

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

- 2. 3. - školení Monitorovací a bezpečnostní nástroje
- 28. 2. proběhlo jednání HSOC na Ministerstvo zdravotnictví
- 23. 2. workshop Zdravotechnika a vzdálený přístup
- 22.2. - **Oblastní nemocnice Mladá Boleslav, a.s.** přepojena do **sítě HSOC**.
- 22.2. - prezentace na ICT ve Zdravotnictví
- 3.2. - **Krajská nemocnice T. Bati ve Zlíně** přepojena do **sítě HSOC**.
- 2.2. - jednání **hSOC s MZ a NUKIB**
- 15.11. - prezentace na setkání Metamorfosa 2021 - bezpečné zdravotnictví
- zentace na eGovernment - Setkání informatiků krajů, Plzeň
- **Seminář Ransomware + výjezdní jednání HSOC**, Jihlava
- **Health Czech 2021**, NUKIB, Brno
- 1 - účast na jednání skupiny Manažerů kybernetické bezpečnosti nemocnic NUKIBem)
- 1 - Jednání pracovní skupiny MZ pro Standardy kybernetické bezpečnosti ve ví
- a 9. 9. 2021 - Workshop: best-practice eGOV SOC
- Prezentace Petr Pavlinec na akci e-government 20:10, Mikulov
- - jednání MZČR
- - 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

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.

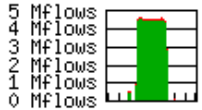
- **7 nemocnic zapojeno**
- **další v procesu připojování**
  - **Monitorovací a bezpečnostní nástroje**
    - Společné politiky a pravidla
  - **Striktnější pravidla a politiky**

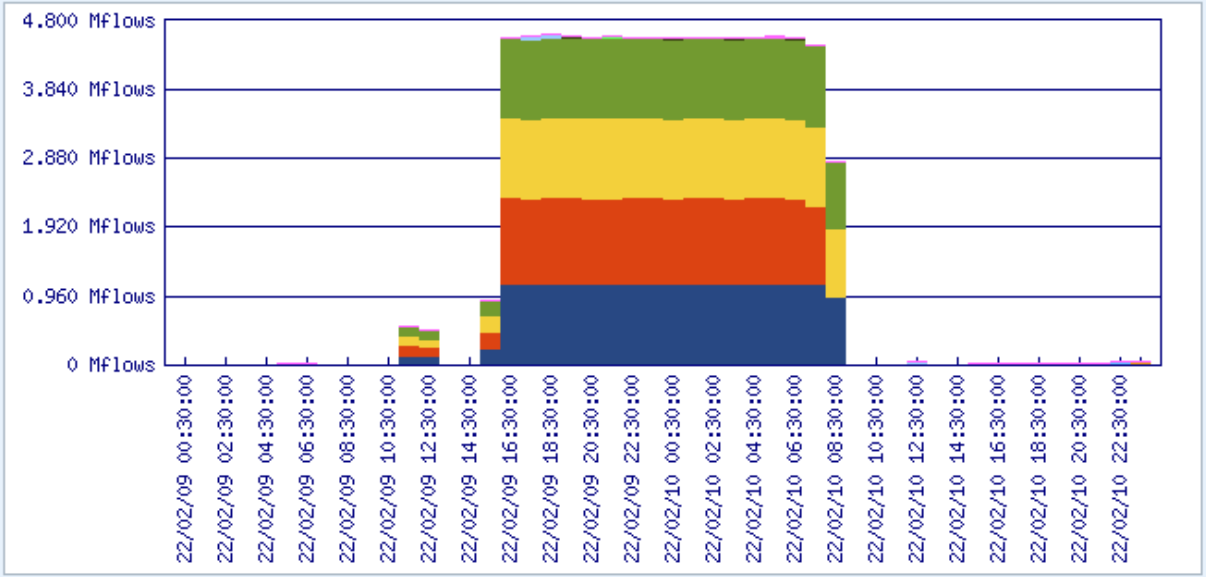
- **Geografická redundance přepojení do Internetu ve dvou lokalitách**
- **Ochrana**
  - proti podvržení IP adres (IP spoofing),
  - proti podvržení oznamovaných prefixů od peering-partnerů,
  - proti amplifikačním (volumetrickým) DDoS útokům,
  - proti agresivním i pomalým scanům,
  - nástroji pro uživatele 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

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

DISTRIBUCE, SDÍLENÉ SLUŽBY

DALŠÍ AKTIVITY

- **Pracovní skupiny**
- **Standardy (Minimální a doporučující standardy vs. ZKB...NIS2)**
  - Identifikace aktiv
  - DRP
- **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 a SOC tým
- **CESNET SOC**

cesnet

HSOC
HOSPITAL SECURITY OPERATION CENTER

cesnet

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

hsoc@cesnet.cz


cesnet
DĚKUJI ZA POZORNOST