cesnet

NREN's role in co-assuring the cybersecurity of critical entities

Jan Kolouch, Andrea Kropáčová
CESNET

13th June 2024
TNC24

TLP:AMBER

- Backbone network **400 Gb/s**
- Data repositories **103 PB**
- Computing power **37 628 CPU**

From 2 Mb/s to 400 Gb/s

1996
2 Mb/s

1997
34 Mb/s

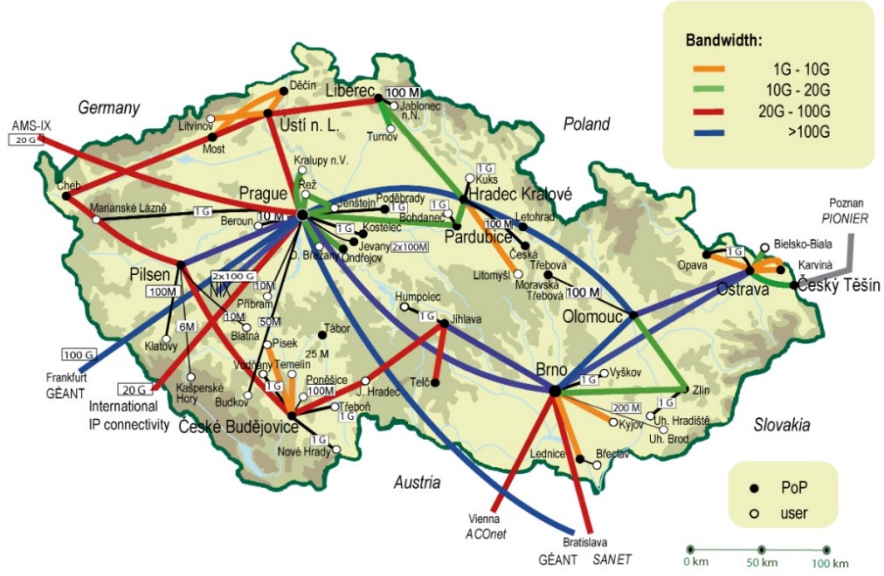
2001
2,5 Gb/s

2007
10 Gb/s

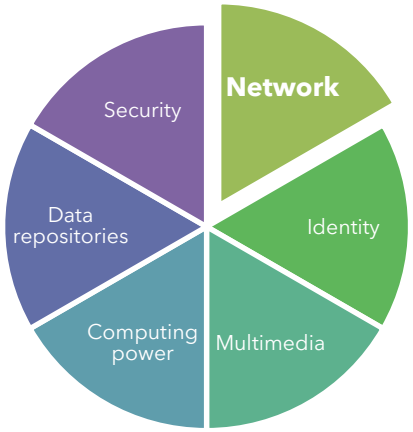
2013
100 Gb/s

2022
400 Gb/s

?



cesnet



1996

1

service

2000

14

services

2005

24 services

2010

27 services

2015

38 services

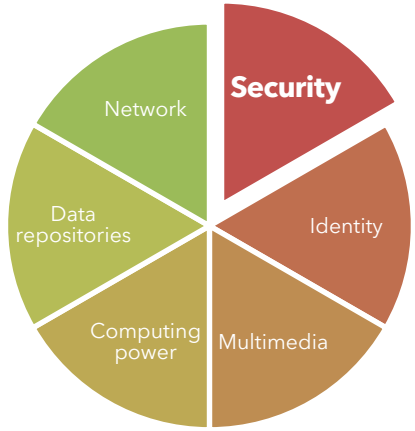
2020

57 services

2023

60+

services



Users

500.000 users/day

300 connected institutions

Universities

Research organisations and **hospitals**

Public administration and local government

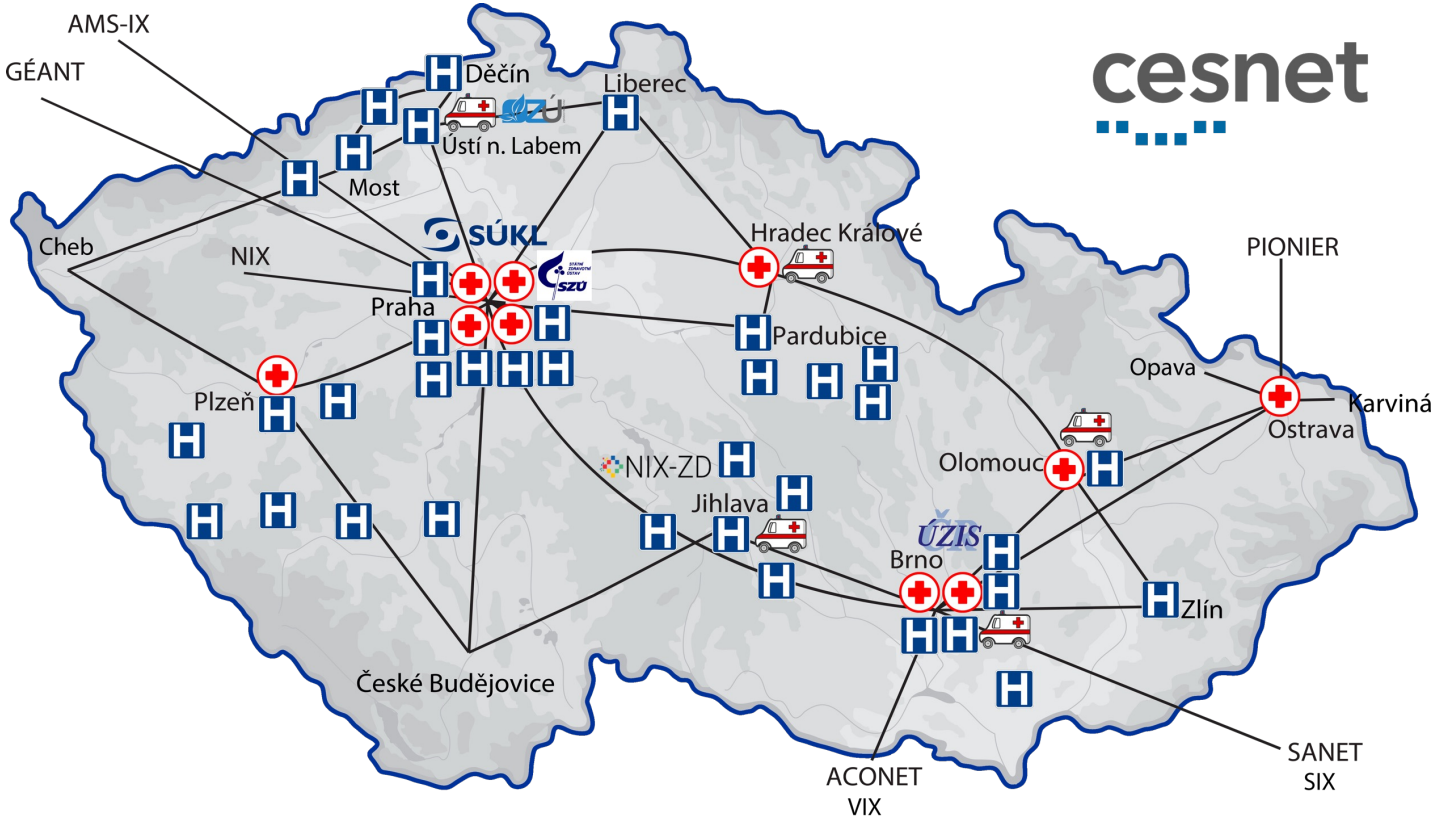
Schools

Institutes of the Academy of Sciences

Libraries, museums and galleries

cesnet

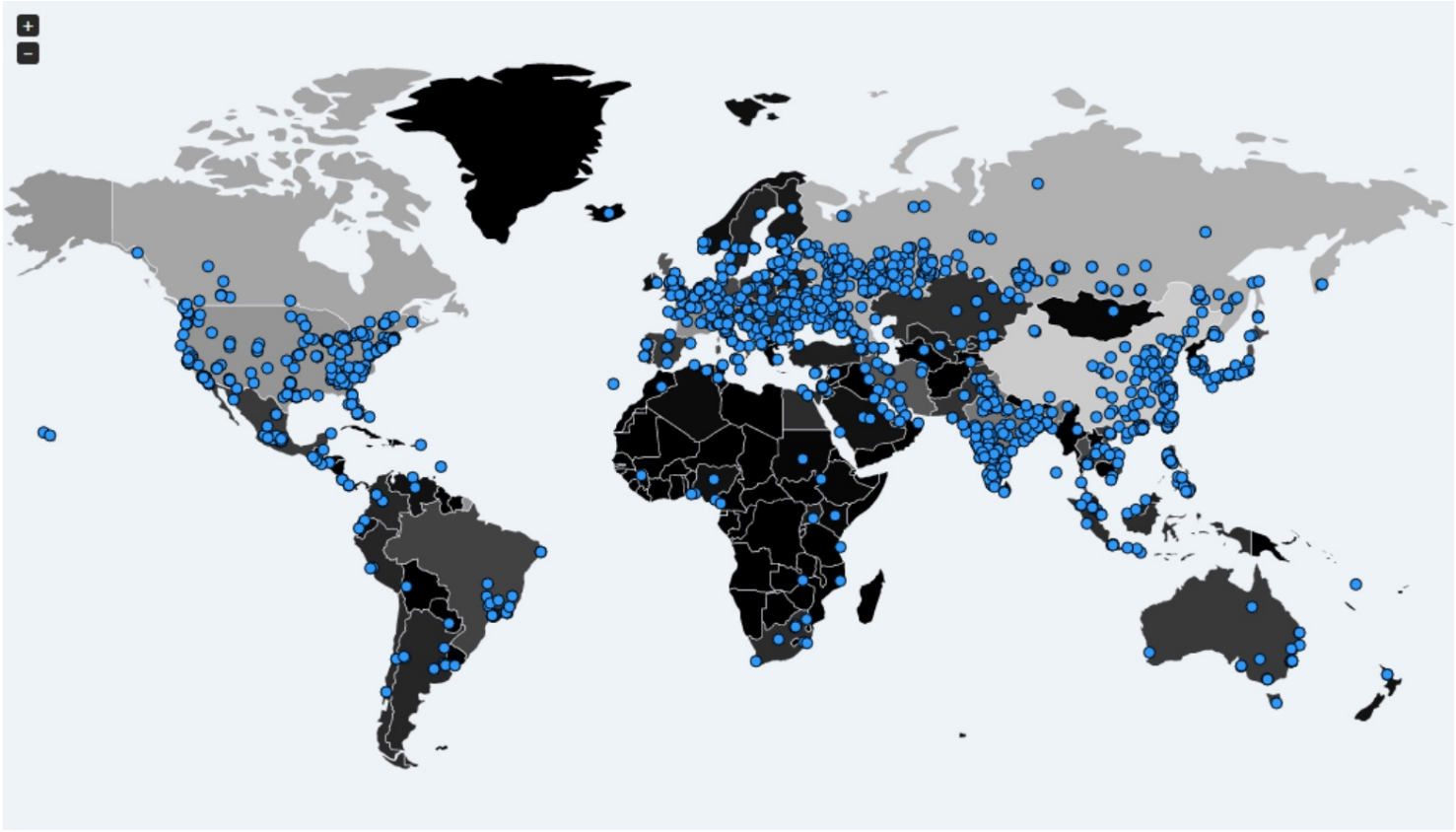
HEALTHCARE SECTOR




cesnet
Cyber sec in hospitals?

cesnet

WANNACRY?



https://www.cnet.com/news/watch-wannacry-attack-geography-in-real-time/

cesnet

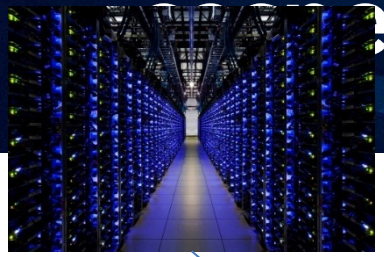

Wana Decrypt0r 2.0
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. 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

WANNACRY

- On March 14, 2017, Microsoft released a security update that addresses a critical vulnerability in the operating system.
- The update mainly affects Windows XP, Windows Server 2003, and Windows 8


cesnet
LAZINESS?

EXPECTATIONS



Gmail

MINISTERSTVO ZDRAVOTNICTVÍ
ČESKÉ REPUBLIKY

https://www.agilus.ai/difference-between-vendor-and-supplier/

TEČKA

Microsoft
Active Directory

https://www.irozhlas.cz/zpravy-domov/konci-moznost-rychle-zmeny-zdravotni-pojistovny_201111301143_mkopp

SÚKL
Státní ústav pro kontrolu léčiv

TYPICAL CONDITION

IT/ICT?

- 3-5 IT staff
- Mostly without experience from elsewhere
- Maintain systems often older than 15 years
- Poorly paid and compensated
- No substitutability
- No training

Cyber security?

Compliance?

ZDRAVOTNICKÉ ZAŘÍZENÍ	Celkový počet zaměstnanců (SM)	Počet zaměstnanců IT (SM)	% z celkem
Fakultní nemocnice 1	5 433	73,6	1,35%
Fakultní nemocnice 2	4 500	32	0,71%
Fakultní nemocnice 3	3 000	31	1,03%
Fakultní nemocnice 4	3 902	31	0,79%
Fakultní nemocnice 5	4 668	27	0,58%
Fakultní nemocnice 6	3 396	32	0,94%
Fakultní nemocnice 7	3 100	42	1,35%
Fakultní nemocnice 8	5667	98	1,73%
Fakultní nemocnice 9	2409	28	1,16%
Fakultní nemocnice 10	4 000	43	1,08%
Pzn.: Data z roku 2019		Průměr	1,07%

ZDRAVOTNICKÉ ZAŘÍZENÍ	Celkový počet zaměstnanců (SM)	Počet zaměstnanců IT (SM)	% z celkem
Okresní nemocnice 1	1485	7	0,47%
Krajská nemocnice	3600	16	0,44%
Okresní nemocnice 2	742	5	0,67%
Okresní nemocncie 3	843	5	0,59%
Pzn.: Data z roku 2022		Průměr	0,55%

16	1,08%
36	1,00%
8	1,08%
9	1,07%

Nárůst o 109 % !

KLATOVSKÝ
deník.cz

VYBRAT REGION

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

DALŠÍ ČLÁNKY Z RUBRIKY

Horaždovický
m patřil dětem

o seniory v
cích staveb
nezačnou

VIDEO: Lyžaři mají na Šumavě ideální podmínky

KOMERČNÍ SDĚLENÍ

ŠÍP

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

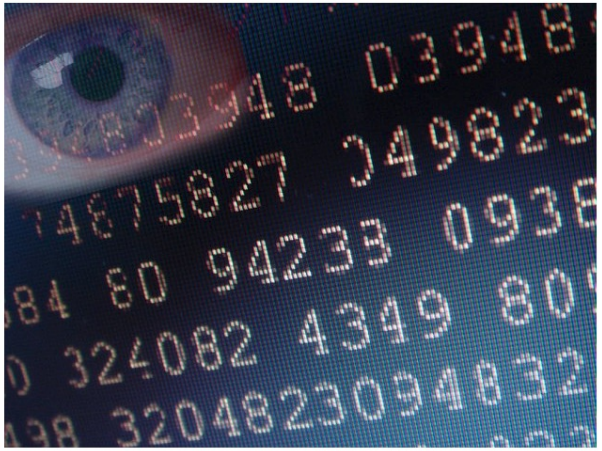
Celebrity, které si k dokonalému vzhledu pomohly novým nosem!

Martina Navrátilová EXKLUZIVNĚ o rakovině: ANI PENÍZE VÁM ŽIVOT NEZACHRÁNÍ

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

Horaždovice **hospital was attacked** by a hacker, **X-rays disappeared**

30.1.2018 1 SDÍLEJ:



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

A virus has struck Benesov, blackmailing hospitals and cities around the world

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

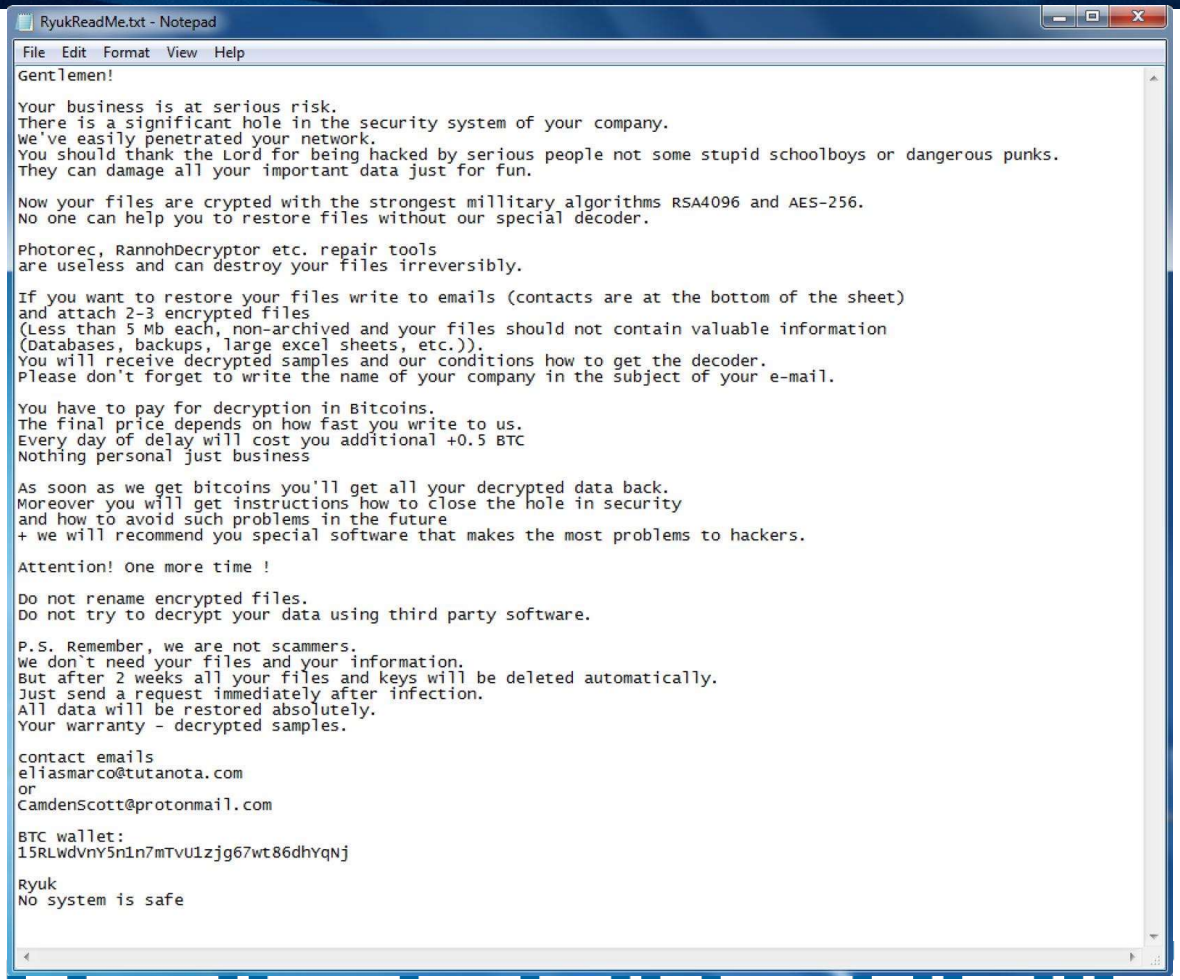
V benešovské nemocnici pravděpodobně zaútočil typ počítačového viru, který dokáže z provozu vyřadit policii, úřady i celá města. V Česku novinka, jinde už běžná praxe.

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

cesnet



RyukReadMe.txt - Notepad

File Edit Format View Help

```
Gentlemen!

Your business is at serious risk.
There is a significant hole in the security system of your company.
We've easily penetrated your network.
You should thank the Lord for being hacked by serious people not some stupid schoolboys or dangerous punks.
They can damage all your important data just for fun.

Now your files are crypted with the strongest millitary algorithms RSA4096 and AES-256.
No one can help you to restore files without our special decoder.

Photorec, RannohDecryptor etc. repair tools
are useless and can destroy your files irreversibly.

If you want to restore your files write to emails (contacts are at the bottom of the sheet)
and attach 2-3 encrypted files
(Less than 5 Mb each, non-archived and your files should not contain valuable information
(Databases, backups, large excel sheets, etc.)).
You will receive decrypted samples and our conditions how to get the decoder.
Please don't forget to write the name of your company in the subject of your e-mail.

You have to pay for decryption in Bitcoins.
The final price depends on how fast you write to us.
Every day of delay will cost you additional +0.5 BTC
Nothing personal just business

As soon as we get bitcoins you'll get all your decrypted data back.
Moreover you will get instructions how to close the hole in security
and how to avoid such problems in the future
+ we will recommend you special software that makes the most problems to hackers.

Attention! One more time !

Do not rename encrypted files.
Do not try to decrypt your data using third party software.

P.S. Remember, we are not scammers.
We don`t need your files and your information.
But after 2 weeks all your files and keys will be deleted automatically.
Just send a request immediately after infection.
All data will be restored absolutely.
Your warranty - decrypted samples.

contact emails
eliasmarco@tutanota.com
or
CamdenScott@protonmail.com

BTC wallet:
15RLWdVnY5n1n7mTvU1zjg67wt86dhYqNj

Ryuk
No system is safe
```

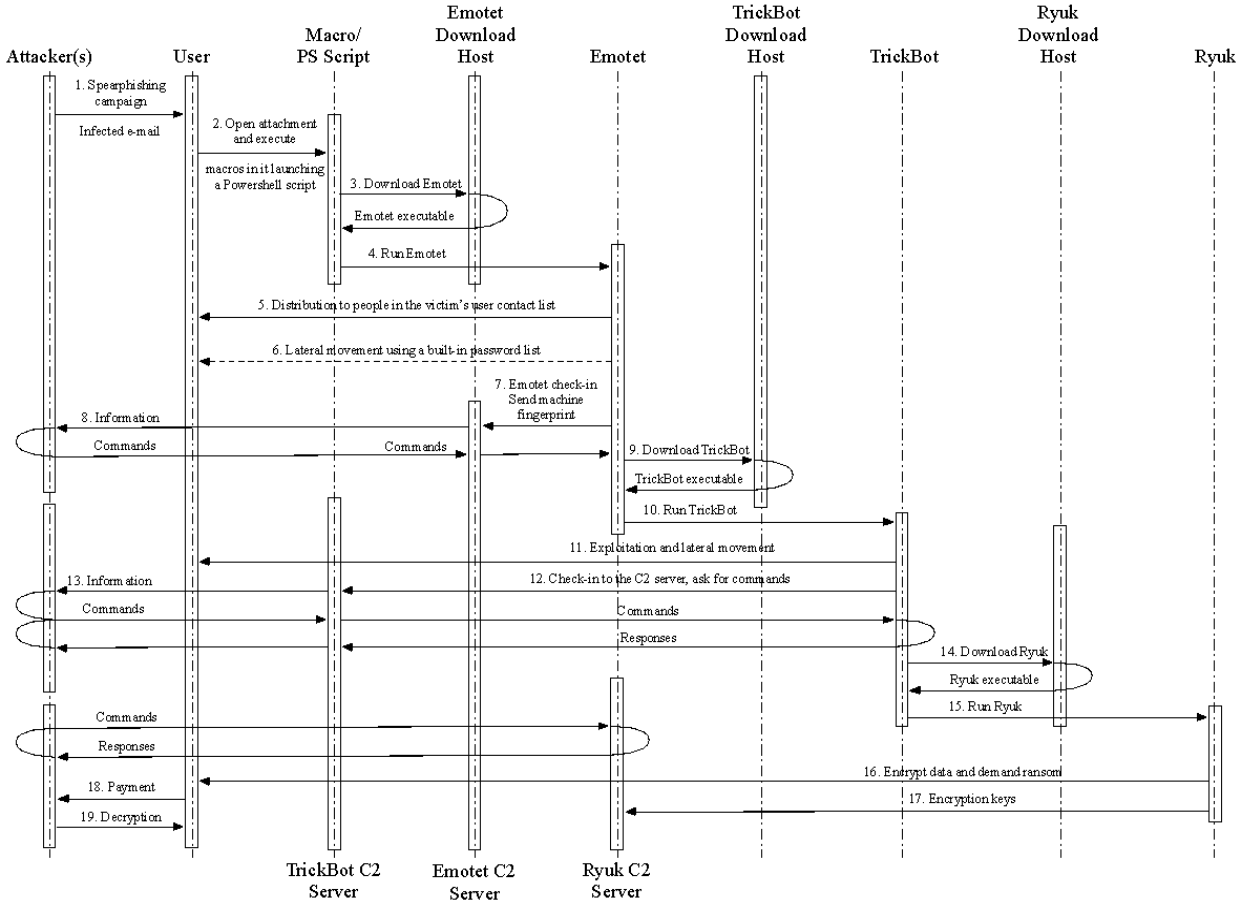
cesnet

VECTOR OF THE ATTACK
COMBINATION & COOPERATION

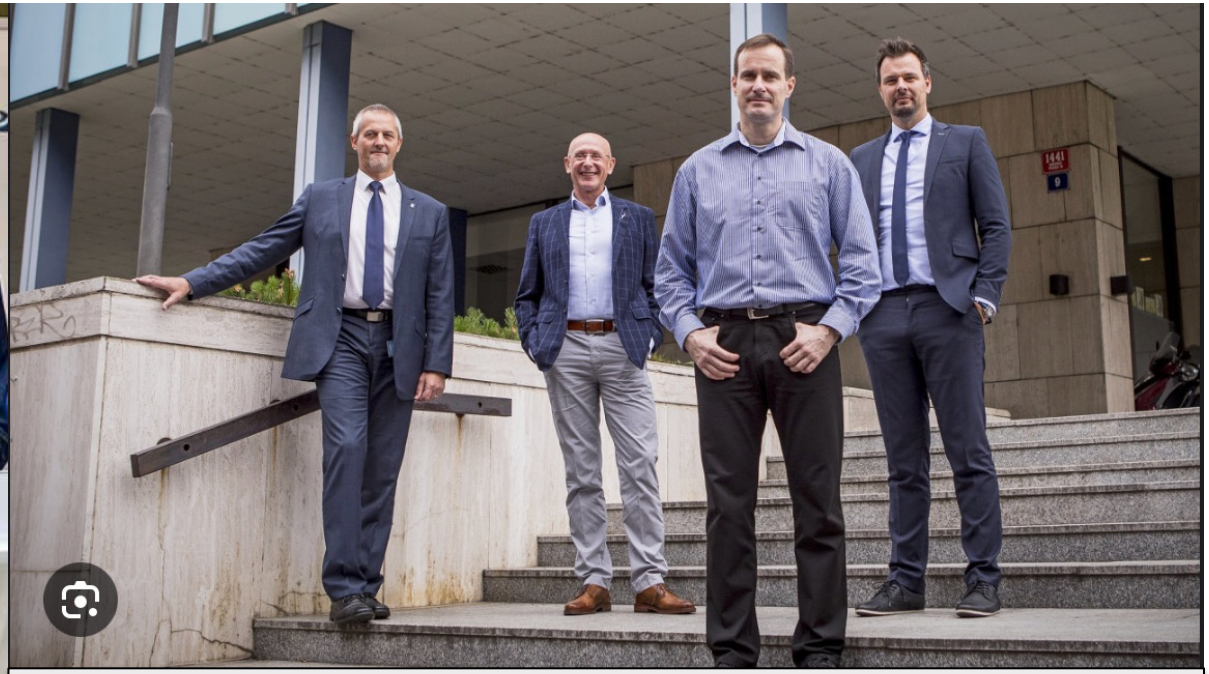
Emotet

Trickbot

Ryuk


Attacker(s)
User
Macro/ PS Script
Emotet Download Host
Emotet
TrickBot Download Host
TrickBot
Ryuk Download Host
Ryuk
1. Spearphishing campaign
Infected e-mail
2. Open attachment and execute
macros in it launching a Powershell script
3. Download Emotet
Emotet executable
4. Run Emotet
5. Distribution to people in the victim's user contact list
6. Lateral movement using a built-in password list
7. Emotet check-in Send machine fingerprint
8. Information
Commands
Commands
9. Download TrickBot
TrickBot executable
10. Run TrickBot
11. Exploitation and lateral movement
12. Check-in to the C2 server, ask for commands
13. Information
Commands
Commands
Responses
14. Download Ryuk
Ryuk executable
15. Run Ryuk
Commands
Responses
16. Encrypt data and demand ransom
17. Encryption keys
18. Payment
19. Decryption
TrickBot C2 Server
Emotet C2 Server
Ryuk C2 Server

The whole republic should learn from the mess at Benešov Hospital



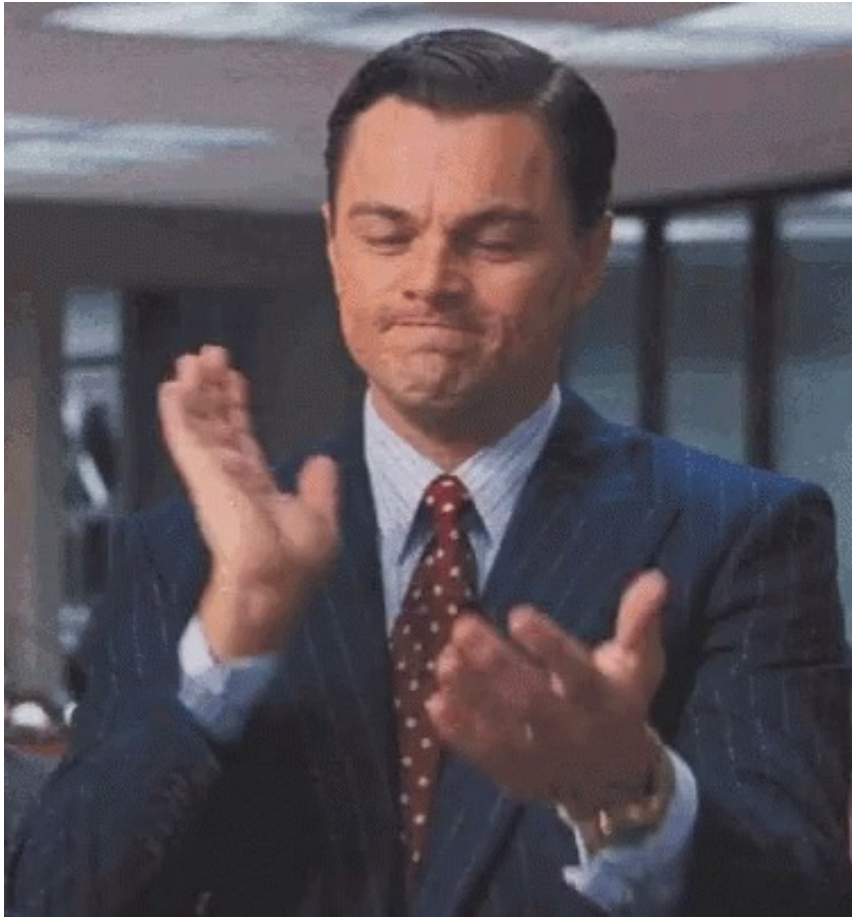
The top men of Czech IT have teamed up to establish a **cyber-guard for hospitals**.

https://www.denik.cz/galerie/ministr-adam-vojtech.html?photo=1&back=3052085763-48-1

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

cesnet

GREAT IDEA

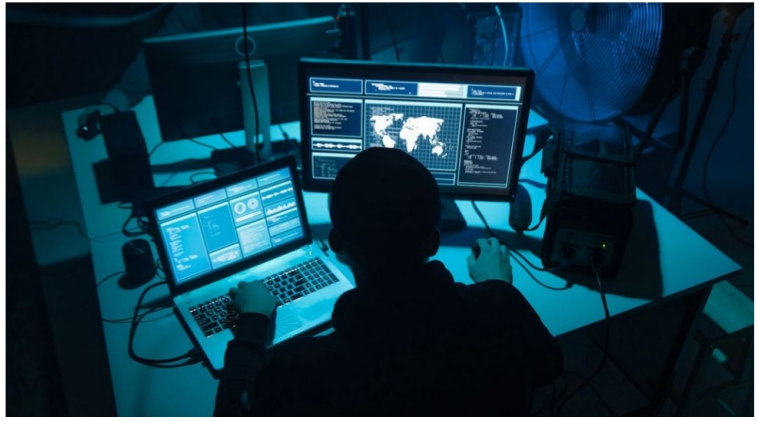


cesnet

The hospital in Brno was attacked by a blackmailer, the hospital called a crisis IT manager

Jan Horák
20. 3. 2020 17:15

Je to přesně týden, co provoz Fakultní nemocnice Brno ochromil kybernetický útok. Podle zjištění deníku Aktuálně.cz útočník vnikl do IT systému nemocnice prostřednictvím kryptoviru Defray, který je typický při požadování výkupného. Nemocnice kvůli obnově systému povolala specialistu ze Všeobecné fakultní nemocnice v Praze Vlastimila Černého, na místě zůstávají experti z NÚKIB a NCOZ.



https://zpravy.aktualne.cz/domaci/na-nemocnici-v-brne-zautocil-vyderacsky-virus-spital-povolal/r~ff91a02c6aa011eab1110cc47ab5f122/

Vector of the attack

13 March 2020

- **Dafray 777 (2017)**
- focused mainly on health, education
- "Authentic email" typically sent from hospital management
- Attachment: "invoice" or "patient"
- encrypts all data on the target computer system. Displays the message: “ransom demand”.

Olomouc faculty hospital was attacked by hackers, the attack was repelled

Daniela Tauberová

Fakultní nemocnice Olomouc zaznamenala útok na počítačové systémy. Jak v pátek informovala, hackerskému útoku odolala a funguje bez omezení.

Fakultní nemocnice Olomouc. Ilustrační foto | *Foto: DENÍK*

Před útoky na počítačové systémy nemocnic a další cíle ve čtvrtek varoval Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB).

https://olomoucky.denik.cz/zpravy_region/fakutni-nemocnice-olomouc-hackersky-utok-2020.html

Ostrava and Olomouc hospitals attacked by hackers, Prague airport also fought off attacks

ČTK, Domácí
Aktualizováno 17. 4. 2020 18:27

Fakultní nemocnice Ostrava se v noci na pátek stala terčem kybernetického útoku. Cílem byl jeden z jejích serverů. Podobný útok zaznamenala i Fakultní nemocnice v Olomouci. Obě jej odrazily. Několik kybernetických útoků zaznamenalo i Letiště Praha, hackeři se pokoušeli získat především přístupové údaje do systémů. Před útoky varoval Národní úřad pro kybernetickou a informační bezpečnost.

Fakultní nemocnice v Ostravě. | Foto: Aktuálně.cz

https://zpravy.aktualne.cz/domaci/ostravskou-fakultni-nemocnici-v-noci-napadli-hackeri/r~fd5f7078808e11eab1110cc47ab5f122/

The hospital in Horažďovice was attacked by hackers for the second time, some data were deleted

13. 1. 2021, 17:43 – Horažďovice – pab, Právo

Léčebnu dlouhodobě nemocných (LDN) v Horažďovicích na Klatovsku napadli na konci minulého týdne hackeři. Podle informací Práva se jim podařilo vymazat některá data z počítačového systému. Podobnému kybernetickému útoku čelilo toto krajské zdravotnické zařízení i v lednu 2018.

https://www.novinky.cz/krimi/clanek/lecebnu-v-horazdovicich-uz-podruhe-napadli-hackeri-vymazali-nektera-data-40347750

Three polyclinics in Prague attacked by hackers, mail and orders not working

16. března 2021 16:42

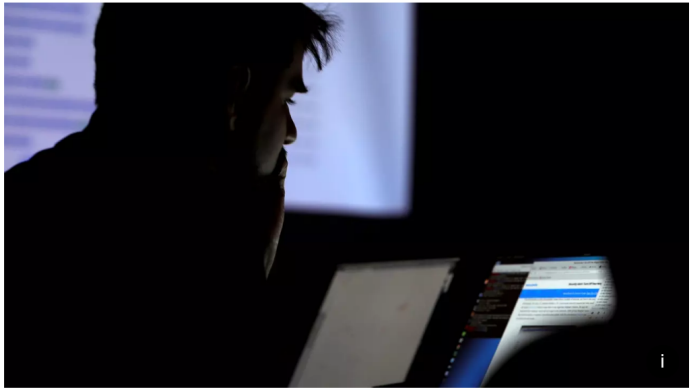
Hackeři zaútočili na tři soukromé polikliniky v centru Prahy, uvedl v úterý server Deník N. Poliklinikám v Legerově, Kartouzské a Myslíkově ulici nefunguje e-mailová pošta ani objednávkový systém. Lékaři přišli o přístup do databází laboratoří. Internetový útok potvrdil Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB).

https://www.idnes.cz/zpravy/domaci/hacker-poliklinika-praha-narodni-urad-pro-kybernetickou-a-informacni-bezpecnost.A210316_162241_domaci_flo

The insidious WannaCry virus is on the scene again. Massively attacking computers

Dnes 13:02 – Ondřej Husák, Novinky

Jako lavina se internetem šířil před třemi roky vyděračský virus WannaCry. Tento škodlivý kód způsobil kolaps drah, benzínek i nemocnic. Ani po letech se na něj však nepodařilo zcela vyzrát, podle analýzy kyberbezpečnostní společnosti Check Point dokonce v letošním roce tento nezvaný návštěvník opět masivně útočí.



„WannaCry bohužel opět masivně útočí. WannaCry je ransomwarový červ, který se v květnu 2017 rychle šířil počítačovými sítěmi po celém světě. Po infikování počítačů se systémem Windows zašifruje soubory na pevném disku a za jejich zpřístupnění a dešifrování požaduje výkupné v bitcoinech," varoval Peter Kovalčík, bezpečnostní expert Check Pointu.

https://www.novinky.cz/internet-a-pc/bezpecnost/clanek/zakerny-virus-wannacry-opet-na-scene-masivne-utoci-na-pocitace-40356244#dop_ab_variant=0&dop_source_zone_name=novinky.sznhp.box&dop_req_id=ECS3Cf9o0Go-202104071752&dop_id=40356244&source=hp&seq_no=5&utm_campaign=&utm_medium=z-boxiku&utm_source=www.seznam.cz

The hospital in Horažďovice fell for a scammer, sent him 1.3 million crowns

14. 9. 2022, 9:55 – Horažďovice
Patrik Biskup

Klatovští kriminalisté pátrají po neznámém podvodníkovi, kterému se podařilo vylákat z horažďovické léčebny dlouhodobě nemocných téměř 1,3 milionu korun. Podle informací Práva poslal koncem srpna na e-mailovou adresu ekonomického oddělení zprávu, ve které se vydával za ředitele léčebny Martina Grolmuse, s pokynem provést platbu ve výši bezmála 49 tisíc eur na konkrétní bankovní konto.

https://www.novinky.cz/clanek/krimi-lecebna-v-horazdovicich-naletela-podvodnikovi-poslala-mu-13-milionu-korun-40408639

cesnet

cesnet

hSOC

Protect yourself

Protect others


cesnet
HSOC
HOSPITAL SECURITY OPERATION CENTER
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.
Vsetínská nemocnice
NEMOCNICE!!! MĚSTSKÁ NEMOCNICE OSTRAVA
VFN PRAHA
OBLASTNÍ NEMOCNICE KOLÍN akciová společnost
NEMOCNICE TOMÁŠE BATI VE ZLÍNĚ
NEMOCNICE ŠUMPERK
Nemocnice Pelhřimov
NEMOCNICE TŘEBÍČ
KLAUDIÁNOVA NEMOCNICE
Krajská zdravotní, a.s.
Masarykova nemocnice v Ústí nad Labem, o.z.
Nemocnice Břeclav
Revmatologický ústav
FAKULTNÍ NEMOCNICE BRNO
ÚPMD
Oblastní Nemocnice Kladno, a.s.
Nemocnice České Budějovice a.s.
KARLOVA STUDÁNKA
uh+ Uherskohradišťská nemocnice a.s.
Nemocnice Kyjov
NEMOCNICE PARDUBICKÉHO KRAJE PARDUBICKÁ NEMOCNICE
CKTCH
AGEL
Rodinné nemocnice v Plzeňském kraji
Nemocnice Rudolfa a Stefanie Benešov, a.s., nemocnice Středočeského kraje
Středočeský kraj
jihočeské nemocnice
ZZS ÚK
NEMOCNICE JIHLAVA
Masarykův onkologický ústav
NEMOCNICE VE FRÝDKU-MÍSTKU
NEMOCNICE HAVLÍČKŮV BROD
REHABILITAČNÍ NEMOCNICE BEROUN
FAKULTNÍ NEMOCNICE OSTRAVA
Spolek pro ochranu osobních údajů
Klatovská nemocnice
FAKULTNÍ NEMOCNICE HRADEC KRÁLOVÉ
uhkt Ústav hematologie a krevní transfuze
AKESO
NEMOCNICE HAVÍŘOV
NAKIT Národní agentura pro komunikační a informační technologie, s. p.
SLEZSKÁ NEMOCNICE V OPAVĚ
KRNOVSKÁ NEMOCNICE
UNIVERZITA KARLOVA 1. lékařská fakulta
NÚKIB
FAKULTNÍ NEMOCNICE PLZEŇ
město ŠTERNBERK
Městská nemocnice v Odrách
MINISTERSTVO VNITRA ČESKÉ REPUBLIKY
Kraj Vysočina
Pardubický kraj
Jihočeský kraj
Olomoucký kraj
PLZEŇSKÝ KRAJ
Zlínský kraj
Moravskoslezský kraj
ČVUT ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE
msdc
cesnet

cesnet

HSOC
HOSPITAL
SECURITY
OPERATION
CENTER

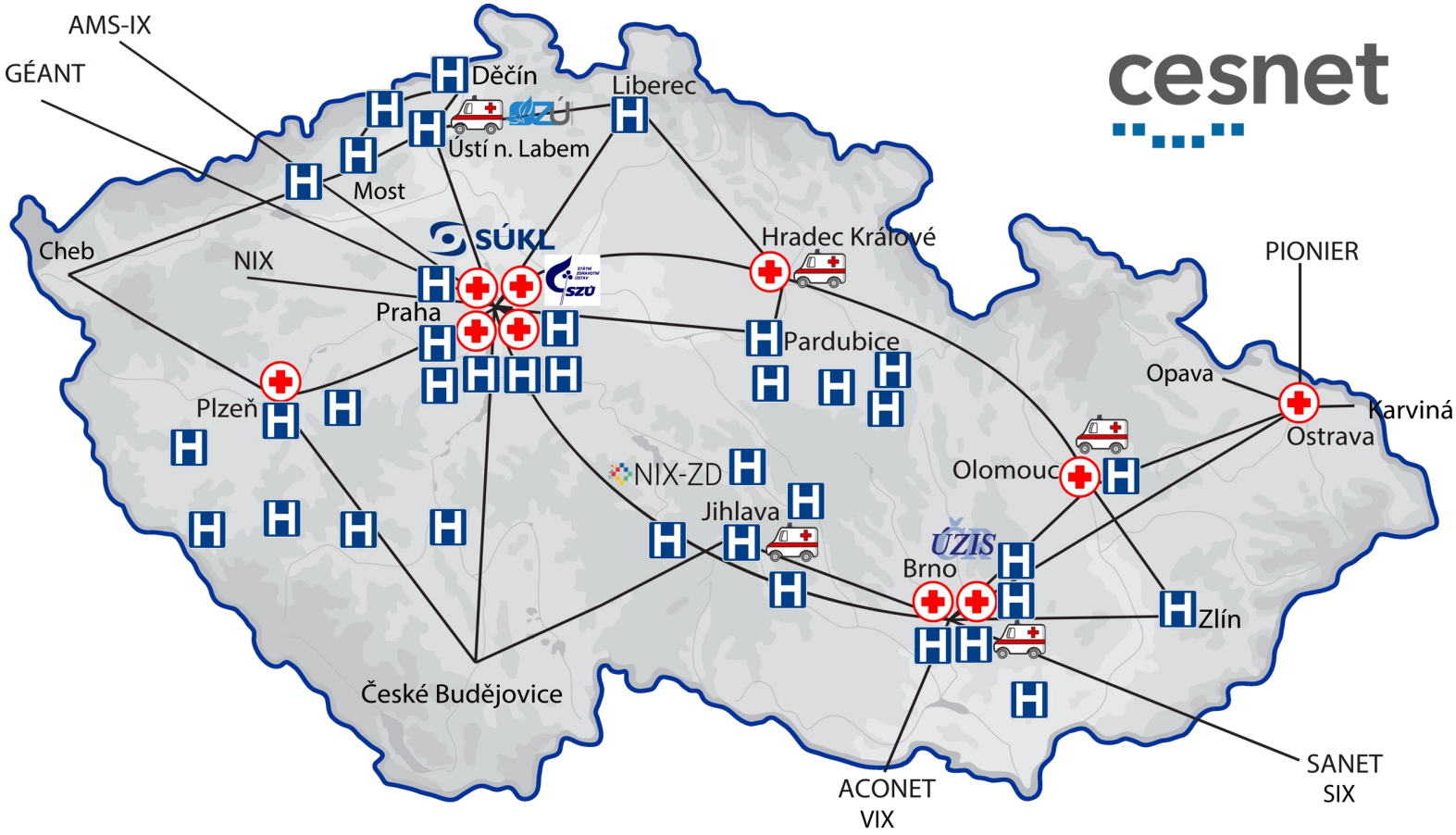
hSOC

- 61 medical facilities
- 8 founders
- 1 ministry
- 3 universities
- 5 other institutions

cesnet

THE ROLE OF CESNET?

cesnet

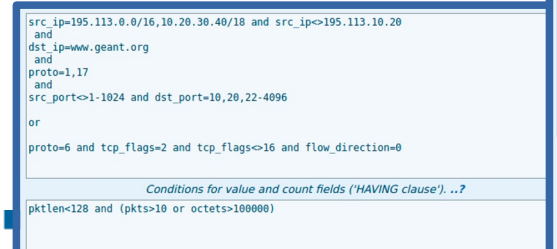

AMS-IX
GÉANT
Děčín
Liberec
Ústí n. Labem
Most
SÚKL
Cheb
NIX
Praha
Hradec Králové
PIONIER
Pardubice
Opava
Karviná
Ostrava
Plzeň
NIX-ZD
Olomouc
Jihlava
ÚZIS
Brno
Zlín
České Budějovice
ACONET
VIX
SANET
SIX

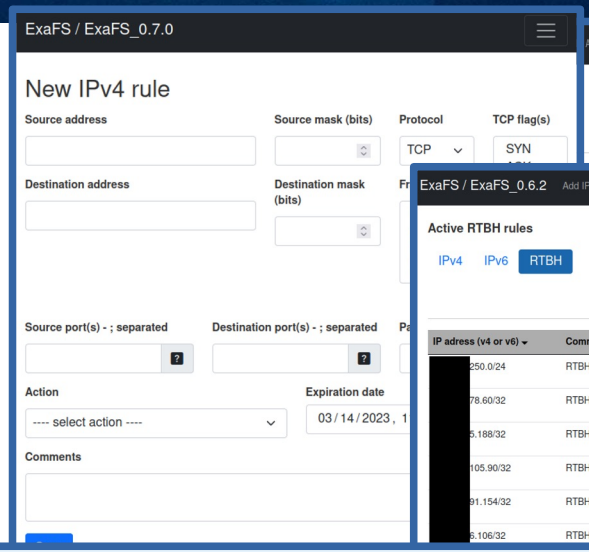
cesnet

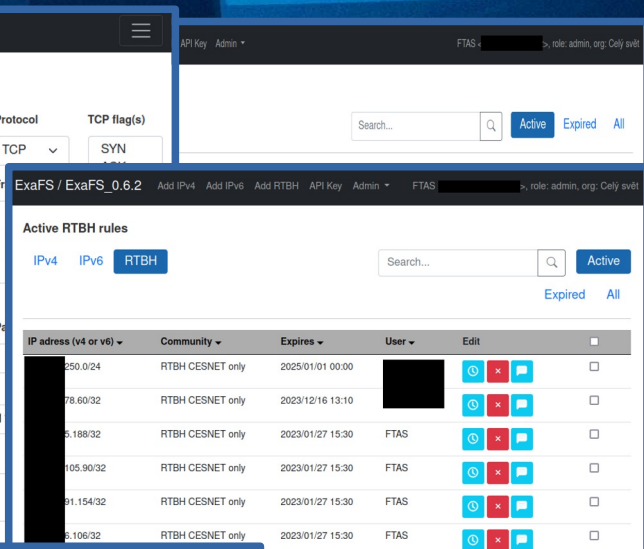
hSOC VRF

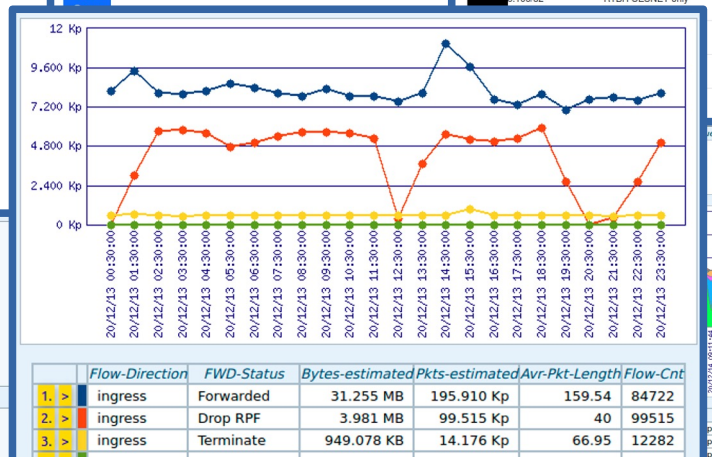
Uniform control of regulation and monitoring of operation

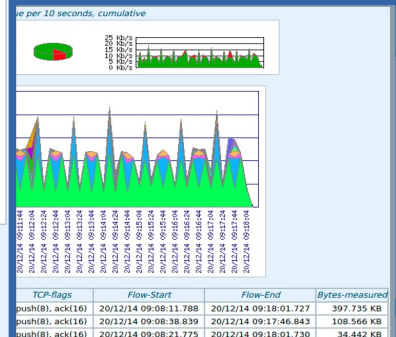
- **unified traffic control management**
- **ExaFS**
  - **unified UI for traffic control ~**
  - “single point of knowledge“
  - transparent API
- **flow-based traffic monitoring**
- **FTAS**
  - collection, processing, storage, visualization of flow-based information
  - configurable **traffic detectors**



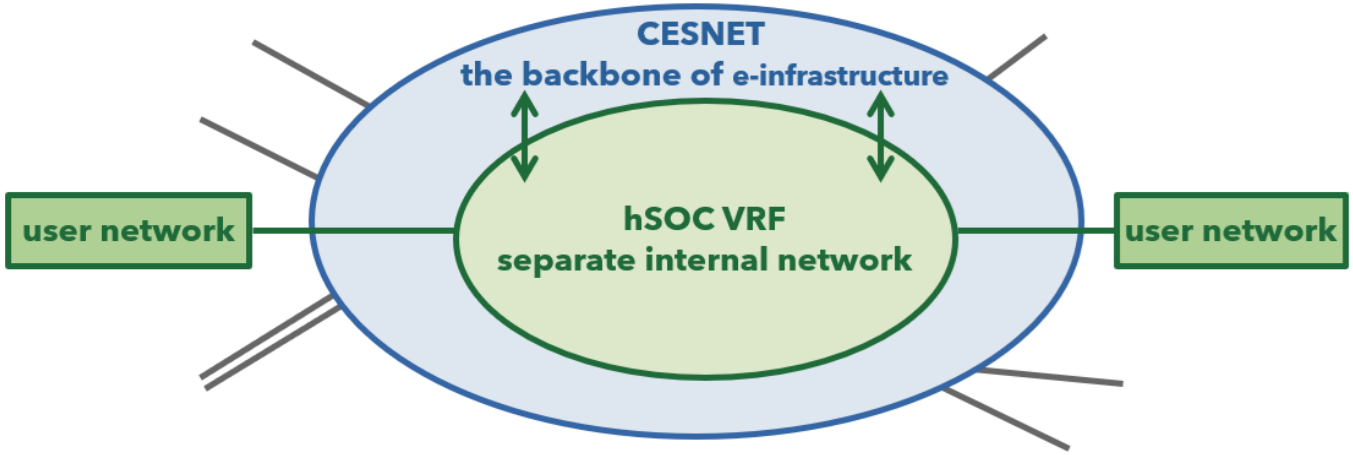






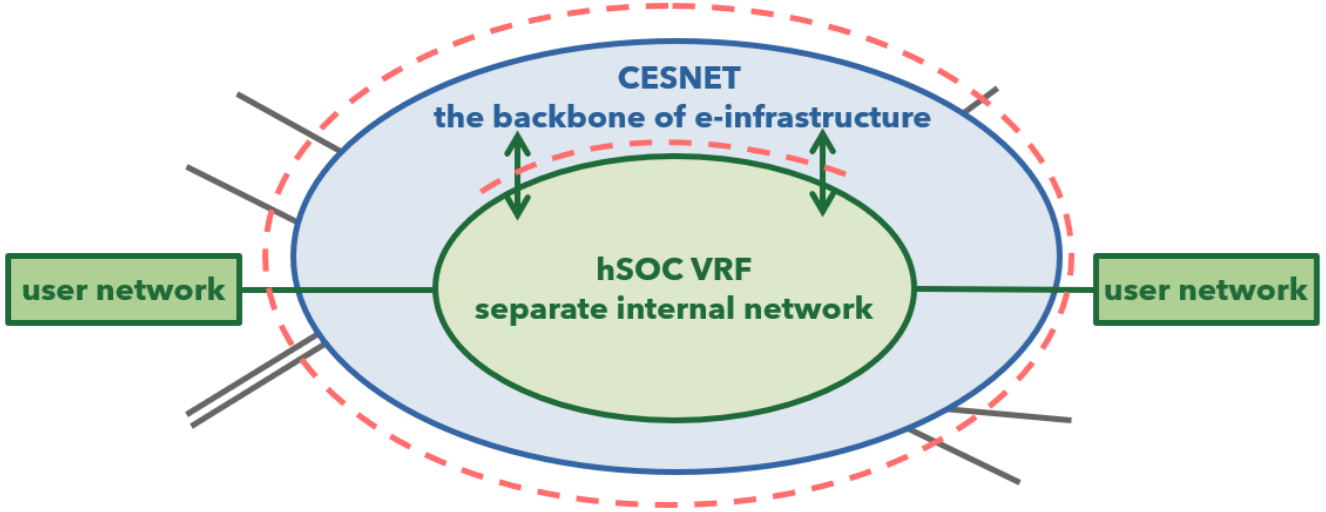


- **hSOC VRF → separate infrastructure for a specific community ~ network within a network**
  - connections to the "big" network in geographically diverse locations
  - why a separate network ?
  - VRF connection from the user's point of view ?



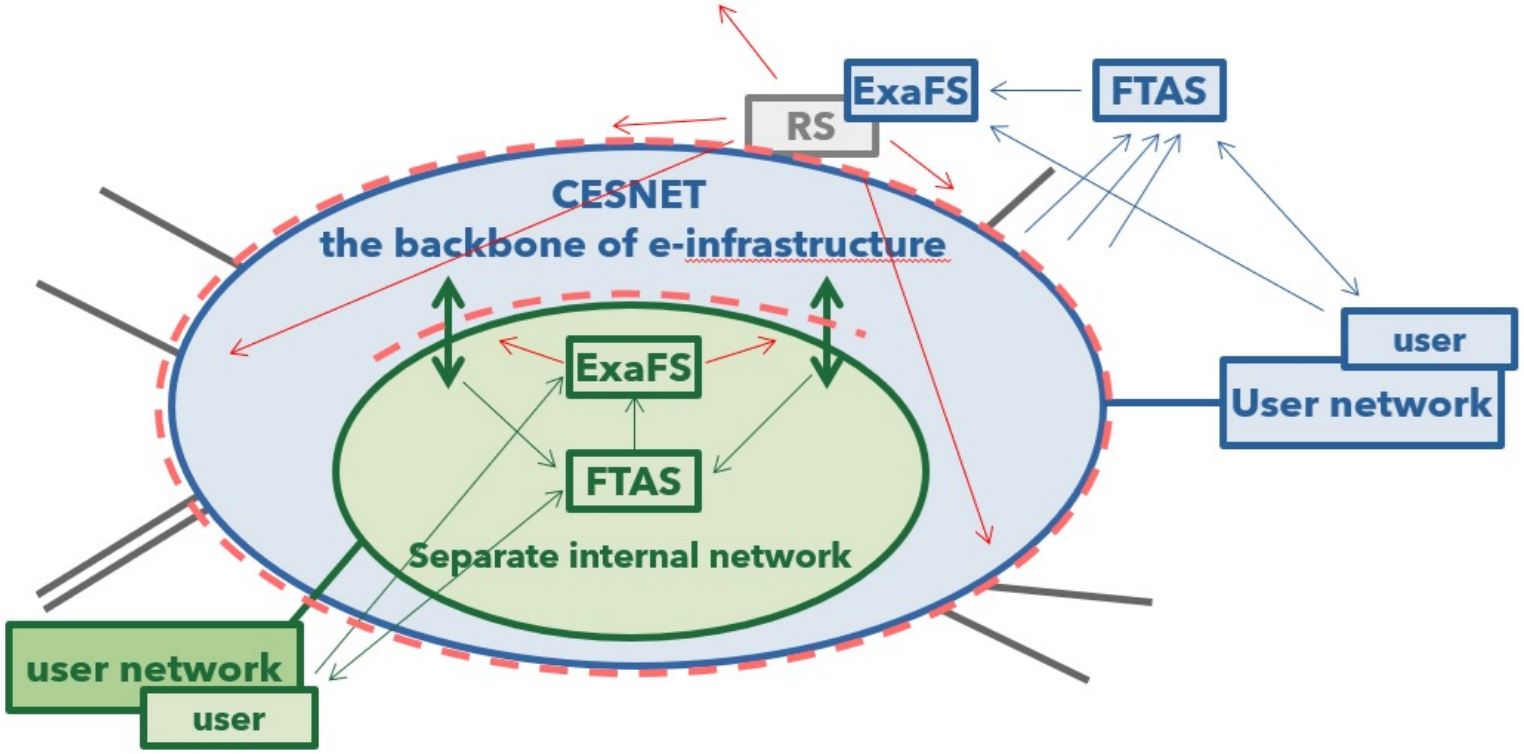
hSOC VRF defence strategy

- **Level 1 - the backbone of e-infrastructure**
  - a set of mechanisms for security and traffic control, unified management
  - control of both directions of operation
- **Level 2 - hSOC VRF**
  - selected set of mechanisms for traffic control, unified control



hSOC VRF - part of a "multi-stage" network defence

- **Each level - dedicated tool instances**
- **detectors in VRF**
  - other policies
  - different sensitivity
  - more specific
- **treatment techniques**
  - RTBH
  - BGP FlowSpec
  - *RPKI, QoS*
  - *AntiDDoS ext.*
  - *DoS Protector*



hSOC VRF - part of a "multi-stage" network defence

- **Automatic traffic treatment**

Level 1

- entire e-infrastructure against typical network attacks, both directions of traffic → compromise basis

Level 2

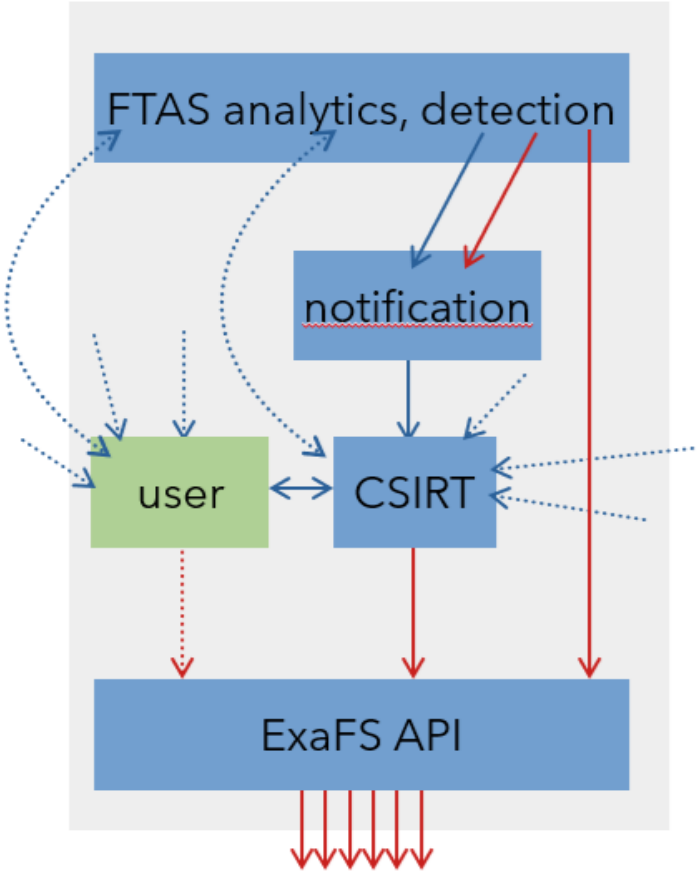
- **hSOC community** → focused on the common nature of traffic

Level 3

- user (end network) → specific needs (vulnerabilities, etc.)

"Manual" traffic treatment

- **CSIRT, backbone administrators**
- **self-service treatment of operation by the user**



hSOC VRF – operatinal experience

- **Under continuous optimization**
  - detectors are configured (not hard-coded)
  - traffic analysis of interesting traffic schemes
  - non-destructive (traffic perspective) testing detectors
  - tuning detection strategy, detection limits, sensitivity
- **Internal cooperation**
  - multi-disciplinary - network admins, security people, developers)
- **Communication with users**
  - applications, network devices, FWs, .. configurations tuning
  - on-demand support (targeted attacks against user resources)
- **False-positives**
  - unpredicted (nothing reported for last year)
  - predicted – in cooperation with users or in extreme situations

- ***Notice:*** *It is* ***flow-based*** *(transport level)* ***detection*** *→ clearly determines range of effective use (observing "packets" not application data)*

Results Examples – hSOC-VRF border – detection & traffic limitation

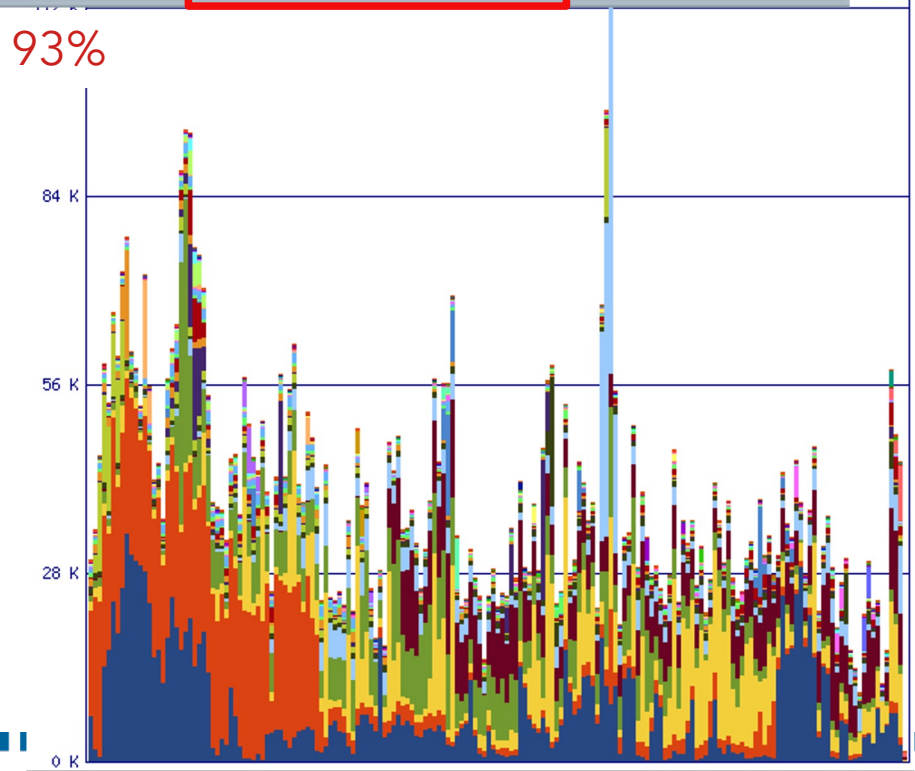
Detected-Event-Cnt: *sums/time steps, 23/09/28 00:00:00-24/03/26 00:00:00, value per 1 day, cumulative*

Bytes-estimated	Pkts-estimated	Src-IP-Cnt	Flow-Cnt	Flow-Cnt-Drop	Detected-Event-Cnt	Detector-Type
81.602 GB	1.363 Gp	32483	1228047744	1147638370	7209300	Src-IP

- 6 months statistics - sources of anomalies
- summaries per day
- 32K unique addresses detected
- 93% of detected flows blocked (automated traffic limitation controlled by monitoring system)
- detection rate ~ 0.4-2 per second

hSOC-VRF

- less than 2% of whole community address space
- participants have similar traffic characteristics – common strategy and detectors can be applied
- it is second level of defense (first level is e-infrastructure perimeter) with much higher sensitivity of detectors

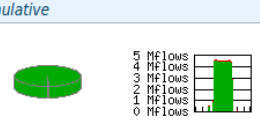


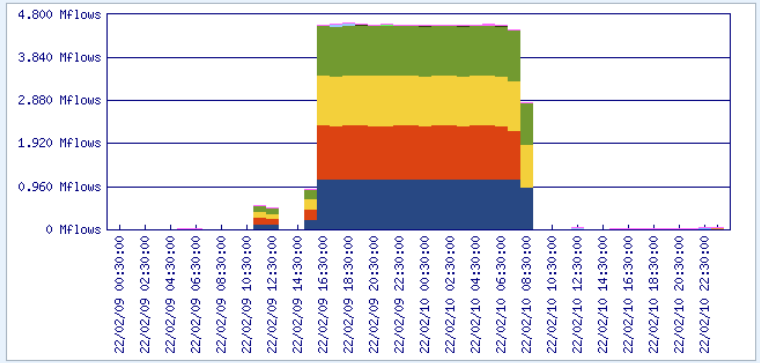
Detected-Event-Cnt: *sums/time steps, 22/02/01 00:00:00-22/02/11 00:00:00, value per 1 hour, cumulative*

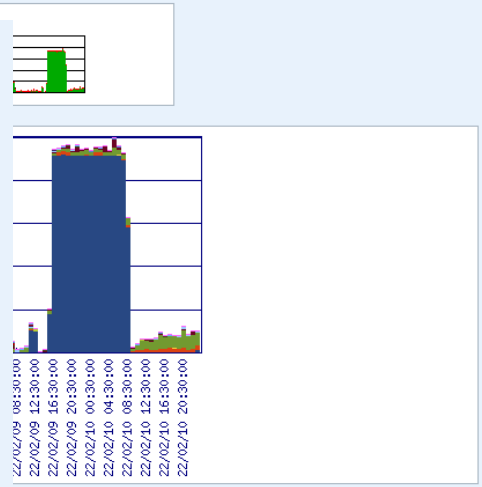
Flow-Cnt-Drop: *sums/time steps, 22/02/09 00:00:00-22/02/11 00:00:00, value per 1 hour, cumulative*

Summary

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





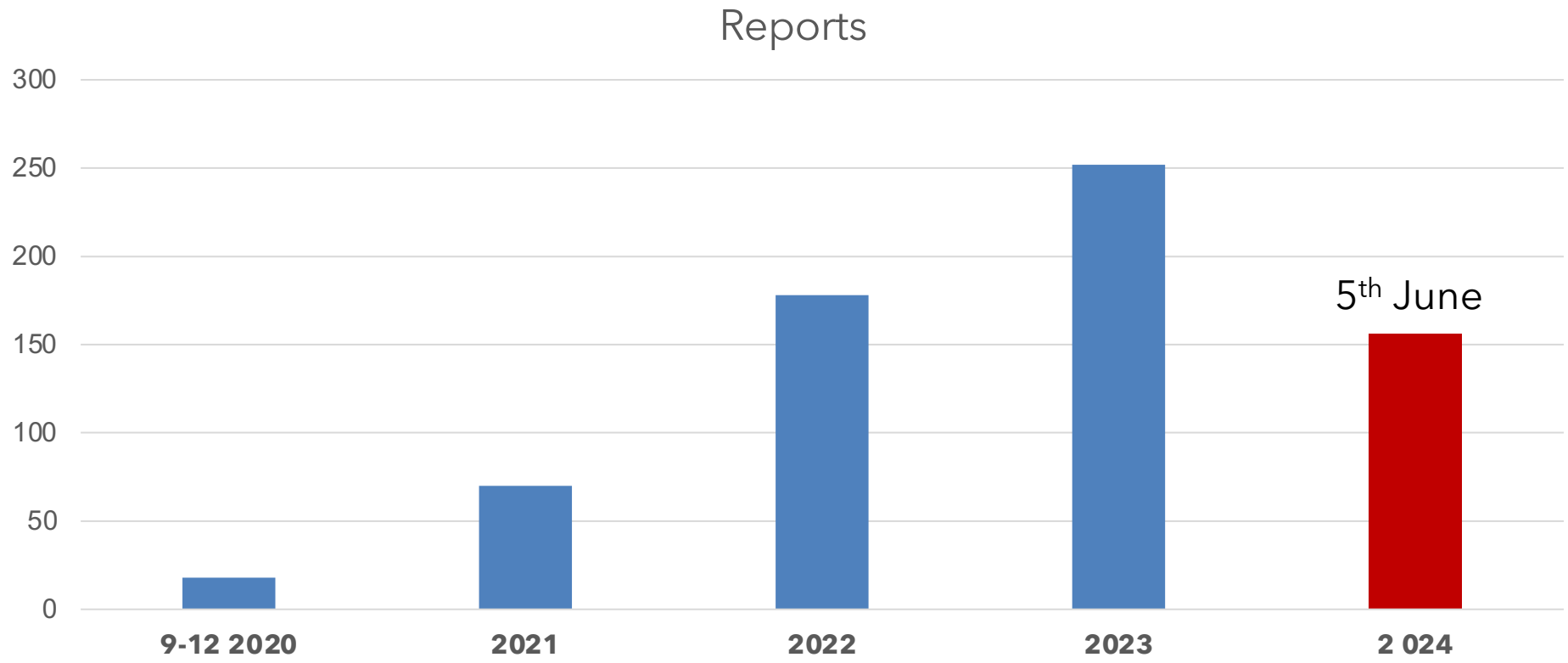


	Src-IP	Src-GeoIP	Flow-Start	Flow-End	Bytes-measured	Bytes-estimated	Pkts-measured	Pkts-estimated	Flow-Cnt	Flow-Cnt-Drop	-IP-Cnt	Flow-Cnt	Flow-Cnt-Drop	Detected-Event-Cnt	Flow-Data-Source
1.	[redacted]		22/02/09 11:31:00.000	22/02/10 08:50:48.000	794.470 MB	794.470 MB	19.597 Mp	19.597 Mp	19589981	19502770	1	78923207 ~ 88.914%	78357447 ~ 91.822%	136284 ~ 60.230%	[redacted]
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	1	2986866 ~ 3.365%	2198664 ~ 2.576%	19559 ~ 8.644%	
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	1	2128058 ~ 2.397%	2024505 ~ 2.372%	10193 ~ 4.505%	
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	1	1726107 ~ 1.945%	1336991 ~ 1.567%	33413 ~ 14.767%	
5.											1	1428017 ~ 1.609%	735103 ~ 0.861%	9871 ~ 4.362%	
6.											1	302496 ~ 0.341%	167108 ~ 0.196%	4098 ~ 1.811%	
7.	[redacted]		22/02/01 02:14:38.000	22/02/10 16:24:08.000	11.020 MB ~ 0.298%	11.020 MB ~ 0.298%	240.331 Kp ~ 0.269%	240.331 Kp ~ 0.269%	51		1	241832 ~ 0.272%	98454 ~ 0.115%	2770 ~ 1.224%	
8.			22/02/01 00:52:44.000	22/02/10 23:41:48.000	10.734 MB ~ 0.290%	10.734 MB ~ 0.290%	231.315 Kp ~ 0.259%	231.315 Kp ~ 0.259%	86		1	224736 ~ 0.253%	107462 ~ 0.126%	3370 ~ 1.489%	
9.			22/02/01 11:12:32.000	22/02/10 18:19:14.000	5.432 MB ~ 0.147%	5.432 MB ~ 0.147%	125.512 Kp ~ 0.140%	125.512 Kp ~ 0.140%	10		1	120540 ~ 0.136%	49195 ~ 0.058%	430 ~ 0.190%	
10.			22/02/01 09:25:38.000	22/02/10 23:36:54.000	5.132 MB ~ 0.139%	5.132 MB ~ 0.139%	71.202 Kp ~ 0.080%	71.202 Kp ~ 0.080%	78		1	33920 ~ 0.038%	9679 ~ 0.011%	306 ~ 0.135%	
11.			22/02/01 07:08:42.000	22/02/10 23:09:34.000	4.662 MB ~ 0.126%	4.662 MB ~ 0.126%	98.208 Kp ~ 0.110%	98.208 Kp ~ 0.110%	53		1	96039 ~ 0.108%	55870 ~ 0.065%	1038 ~ 0.459%	
12.			22/02/01 00:47:58.000	22/02/10 22:14:26.000	3.182 MB ~ 0.086%	3.182 MB ~ 0.086%	78.259 Kp ~ 0.088%	78.259 Kp ~ 0.088%	14		1	76249 ~ 0.086%	35692 ~ 0.042%	1015 ~ 0.449%	
13.			22/02/01 04:23:22.000	22/02/10 13:12:12.000	2.953 MB ~ 0.080%	2.953 MB ~ 0.080%	66.659 Kp ~ 0.075%	66.659 Kp ~ 0.075%	22		1	72765 ~ 0.082%	28650 ~ 0.034%	521 ~ 0.230%	
14.			22/02/01 00:49:00.000	22/02/10 22:56:48.000	2.112 MB ~ 0.057%	2.112 MB ~ 0.057%	45.545 Kp ~ 0.051%	45.545 Kp ~ 0.051%	61		1	36201 ~ 0.041%	6947 ~ 0.008%	521 ~ 0.230%	
15.			22/02/01 10:31:54.000	22/02/10 15:12:40.000	1.784 MB ~ 0.048%	1.784 MB ~ 0.048%	20.357 Kp ~ 0.023%	20.357 Kp ~ 0.023%	15		1	17977 ~ 0.020%	425 ~ 0.000%	65 ~ 0.029%	

- 15 hospitals involved
- next in the connection proces

cesnet

SITUATIONAL AWARENESS


Reports
300
250
200
150
100
50
0
9-12 2020
2021
2022
2023
2 024
5th June

cesnet

HYBRID SOC MODEL?

cesnet

cesnet

FTAS, netflow, ipfix, sFlow, honeypots, IDS, IPS, Logs aj.

Externí zdroje

security events, NÚKIB, partners, etc.

hSOC

Logy - @, NAT, DHCP, FW, dom. controller, radius, IDM…
Scans, vulnerability mgmt…

- **Receiving**
- **Processing**
- **Enrichment**
- **Analysis**
- **etc.**

DATA

- **FTAS**
- **exaFS**
- **NERD**
- **Warden**
- **Mentat**
- **Logmgmt**
- **SIEM**
- **VM**
- **aj.**

cesnet certs

(incident handling)

FTAS and network analytics

Situational Awareness analytics

Analyst Analyst Analyst Analyst

Interventions
(filters, blocking, etc.)

Consultation, cooperation

Incident reports, event reports, vulnerability reports.

consultation, cooperation

cesnet flab

Connected organisation
(university, **hospital** etc.)

Response
Disaster recovery

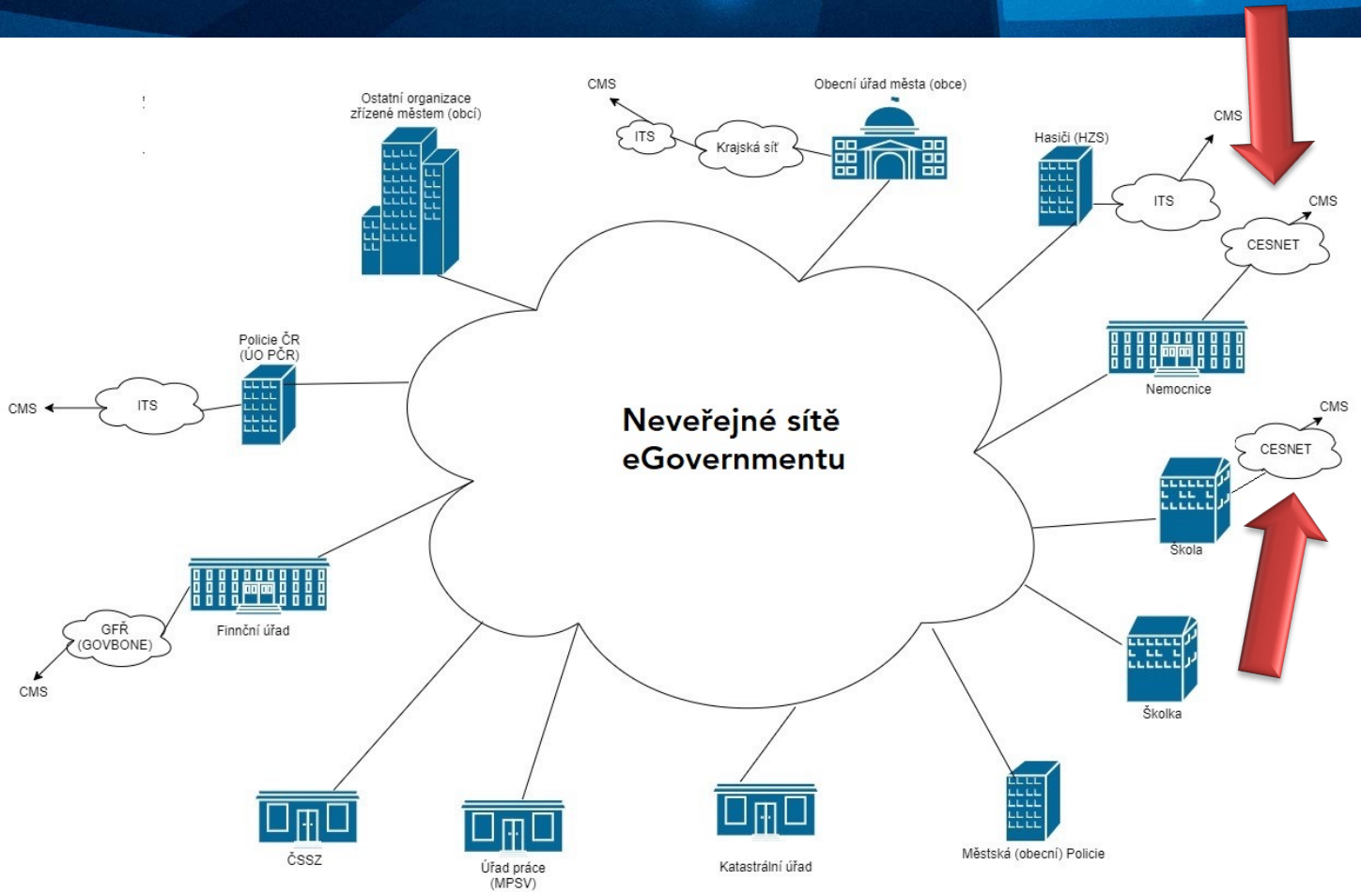
- Procedures
- Asset management
- DRP
- Risk analysis
- Impacts
- Etc.

cesnet

CPoS 2.0

The following describes the variants and method of connecting Metropolitan Networks (MAN) to **Central Point of Service (CMS)** via Regional Networks, Territorial Departments of the Police of the Czech Republic, **Academic Network CESNET** or Financial Offices (GFD network).

https://archi.gov.cz/_media/nap-dokument:metropolitky_1.jpg?cache=



cesnet

METHODOLOGY AND LEGISLATION

cesnet

MINISTERSTVO ZDRAVOTNICTVÍ ČESKÉ REPUBLIKY

cesnet

NÚKIB

Verze:	XXX
Platnost nové verze od:	XXX

Metodický pokyn poskytovatelům zdravotních služeb ke kybernetické bezpečnosti

Příloha č. 8

Metodika identifikace a správy informačních aktiv (vzor)

Pořadí revize	Provedené dne	Zpracoval	Schválil
Verze 1.0	1. 8. 2018	Tomáš Bezouška, CISA kolektiv autorů	Ing. Martin Zeman
Verze 2.0	12. 6. 2019	Tomáš Bezouška, CISA, Ing. Martin Švanda Ing. Jiří Borej, CGEIT kolektiv autorů	Ing. Martin Zeman
Verze 3.0	18. 5. 2020	Tomáš Bezouška, CISA	Ing. Martin Zeman

MINISTERSTVO ZDRAVOTNICTVÍ ČESKÉ REPUBLIKY

cesnet

NÚKIB

Verze:	XXX
Platnost nové verze od:	XXX

METODIKA

HODNOCENÍ DŮLEŽITOSTI INFORMAČNÍCH SYSTÉMŮ POSKYTOVATELŮ ZDRAVOTNÍCH SLUŽEB

Metodická podpora zdravotnických zařízení, ve zvyšování úrovně kybernetické bezpečnosti

Pořadí revize	Provedené dne	Zpracoval	Schválil
Verze 1.0	08. 12. 2021	Tomáš Bezouška, CISA kolektiv autorů MZČR, NÚKIB, CESNET	

MINISTERSTVO ZDRAVOTNICTVÍ ČESKÉ REPUBLIKY

cesnet

NÚKIB

Verze:	XXX
Platnost nové verze od:	XXX

Standard zálohování a obnovy informací

Metodická podpora zdravotnických zařízení, ve zvyšování úrovně kybernetické bezpečnosti

Pořadí revize	Provedené dne	Zpracoval	Schválil
Podpis			


cesnet
COOPERATION AND
COMMUNICATION

cesnet

OPPORTUNITIES

- **Sharing know-how and human capacity**
  - best-practice,
  - concept and design architecture
  - training, seminars and workshops
  - technology standards
  - roadmap for the establishment of a joint distributed CSIRT team, SOC
- **Emergency communication channels**
- **Setting up workflow and processes for the involved entities**

cesnet

https://hsoc.cesnet.cz

cesnet

ARE HOSPITALS SAFE?

cesnet

PATIENT

https://www.alza.cz//withings-wpm04-all-inter-d5694259.htm?kampan=adwsda_domaci-elektro_pla_all_obecna_zdravi_c_21494__WITTL915&gclid=EAIaIQobChMInJmc4KSoqQMVIjIGAB2fEwhVEAkYBiABEgI2p_D_BwE

B BRAUN - INFUSOMAT® SPACE® LARGE VOLUME PUMP

cesnet

DATA SHOULD CIRCULATE, NOT PEOPLE...

cesnet

„AI“...

cesnet

cesnet

Na nemocnici v Brně zaútočil vyděračský virus, špitál povolal krizového IT manažera

Jan Horák
20. 2. 2020 17:15

Je to přesně týden, co provoz Fakultní nemocnice Brno ochromil kybernetický útok. Podle zjištění deníku Aktuálně.cz útočník vnikl do IT systému nemocnice prostřednictvím kryptoviru Defray, který je typický při požadování výkupného. Nemocnice kvůli obnově systému povolala specialistu ze Všeobecné fakultní nemocnice v Praze Vlastimila Černého, na místě zůstávají experti z NÚKIB a NCOZ.

Reklama

Na tři polikliniky v Praze zaútočili hackeři, nefunguje pošta ani objednávky

16. března 2021 16:42

Hackeři zaútočili na tři soukromé polikliniky v centru Prahy, uvedl v úterý server Deník N. Poliklinikám v Legerově, Kartouzské a Myslíkově ulici nefunguje e-mailová pošta ani objednávkový systém. Lékaři přišli o přístup do databází laboratoří. Internetový útok potvrdil Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB).

Léčebnu v Horažďovicích už podruhé napadli hackeři, vymazali některá data

13. 1. 2021, 17:43 – Horažďovice – pab, Právo

Léčebnu dlouhodobě nemocných (LDN) v Horažďovicích na Klatovsku napadli na konci minulého týdne hackeři. Podle informací Práva se jim podařilo vymazat některá data z počítačového systému. Podobnému kybernetickému útoku čelilo toto krajské zdravotnické zařízení i v lednu 2018.

Léčebna v Horažďovicích naletěla podvodníkovi, poslala mu 1,3 milionu korun

14. 9. 2022, 9:55 – Horažďovice
Patrik Biskup

Klatovští kriminalisté pátrají po neznámém podvodníkovi, kterému se podařilo vylákat z horažďovické léčebny dlouhodobě nemocných téměř 1,3 milionu korun. Podle informací Práva poslal koncem srpna na e-mailovou adresu ekonomického oddělení zprávu, ve které se vydával za ředitele léčebny Martina Grolmuse, s pokynem provést platbu ve výši bezmála 49 tisíc eur na konkrétní bankovní konto.

Olomouckou fakultku napadli hackeři, útok se podařilo odrazit

17.4.2020
Daniela Tauberová

Fakultní nemocnice Olomouc zaznamenala útok na počítačové systémy. Jak v pátek informovala, hackerskému útoku odolala a funguje bez omezení.

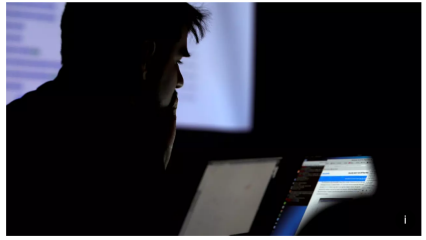
Fakultní nemocnice Olomouc. Ilustrační foto | Foto: DENÍK

Před útoky na počítačové systémy nemocnic a další cíle ve čtvrtek varoval Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB).

Zákeřný virus WannaCry opět na scéně. Masivně útočí na počítače

Dnes 13:02 – Ondřej Husák, Novinky

Jako lavina se internetem šíří před třemi roky vyděračský virus WannaCry. Tento škodlivý kód způsobil kolaps drah, benzínek i nemocnic. Ani po letech se na něj však nepodařilo zcela vyzrát, podle analýzy kyberbezpečnostní společnosti Check Point dokonce v letošním roce tento nezvaný návštěvník opět masivně útočí.



„WannaCry bohužel opět masivně útočí. WannaCry je ransomwarový červ, který se v květnu 2017 rychle šířil počítačovými sítěmi po celém světě. Po infikování počítačů se systémem Windows zašifruje soubory na pevném disku a za jejich zpřístupnění a dešifrování požaduje výkupné v bitcoinech," varoval Peter Kovalčík, bezpečnostní expert Check Pointu.

...travskou i olomouckou nemocnici ...padli hackeři, útoky odvracelo i pražské ...tiště

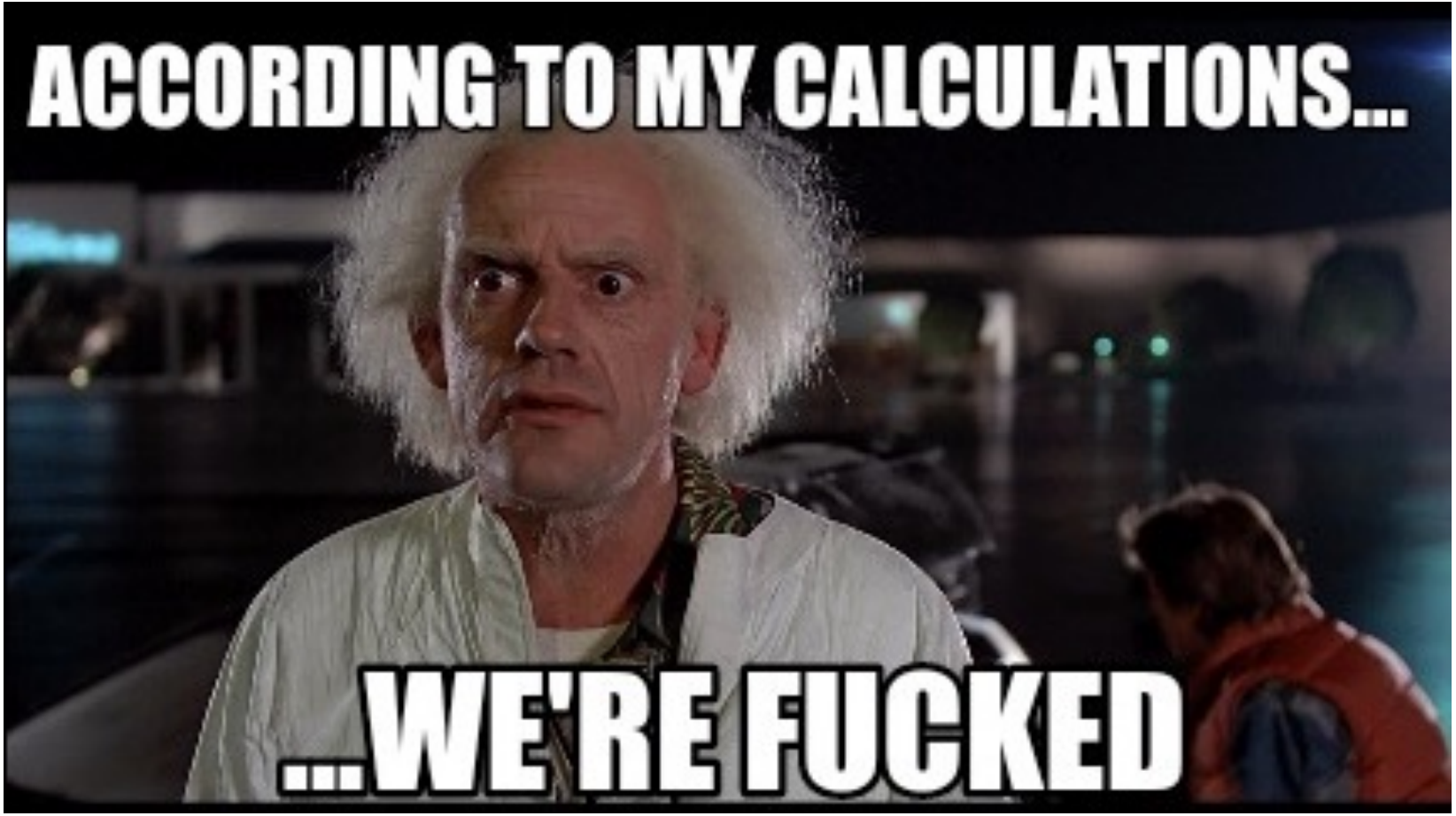
ČTK, Domácí
Aktualizováno 17. 4. 2020 18:27

...ní nemocnice Ostrava se v noci na pátek stala terčem ...netického útoku. Cílem byl jeden z jejích serverů. Podobný ...zaznamenala i Fakultní nemocnice v Olomouci. Obě jej ...ily. Několik kybernetických útoků zaznamenalo i Letiště ..., hackeři se pokoušeli získat především přístupové údaje do ...mů. Před útoky varoval Národní úřad pro kybernetickou a ...ační bezpečnost.

Reklama

Fakultní nemocnice v Ostravě. | Foto: Aktuálně.cz

cesnet



cesnet

SOLUTION No. 1

https://practicalhealthpsychology.com/cz/2020/05/stop-being-an-ostrich-the-benefits-of-helping-people-to-monitor-their-progress/

cesnet

SOLUTION No. 2

cesnet

I'll buy the whole thing!

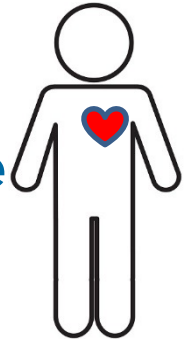
Komplexní balíček nástrojů pro zavedení kryptografie a vícefaktorového přihlašování pro malé organizace:

- Vstupní analýza současného stavu
- Vybudování PKI infrastruktury (identita zaměstnance

cesnet

SOLUTION No. 3

- Capacity building
- People on the end organisation side

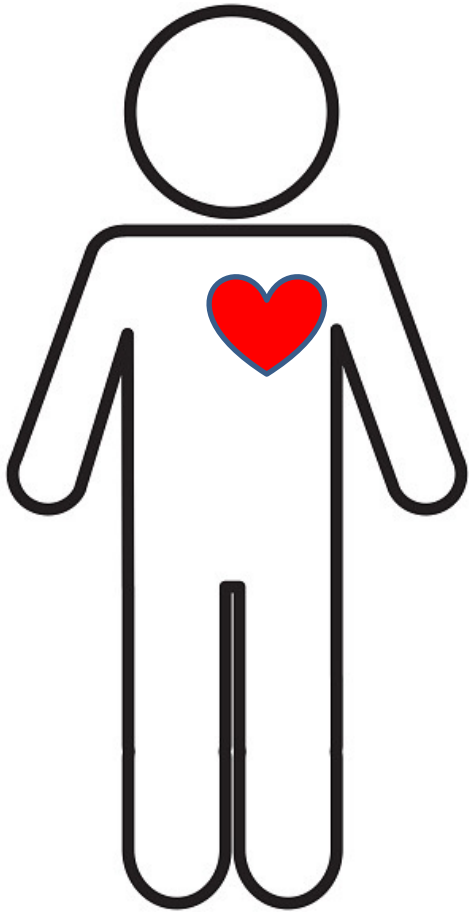


- Don't wait until ...
  - it will happen again
  - Adoption of NIS 2
- Community cooperation


cesnet
Real Challenges?

cesnet

- **Not to succumb to the illusion that buying technology will solve everything**
  - Bottom up approach
  - We **need to know how it works**, to be able to fix it
  - We need **develop skills** and **build capacities**



cesnet

THANK YOU FOR THE ATTENTION

Assoc. Prof. Dr. Jan Kolouch
jan.kolouch@cesnet.cz
Andrea Kropacova
andrea.kropacova@cesnet.cz