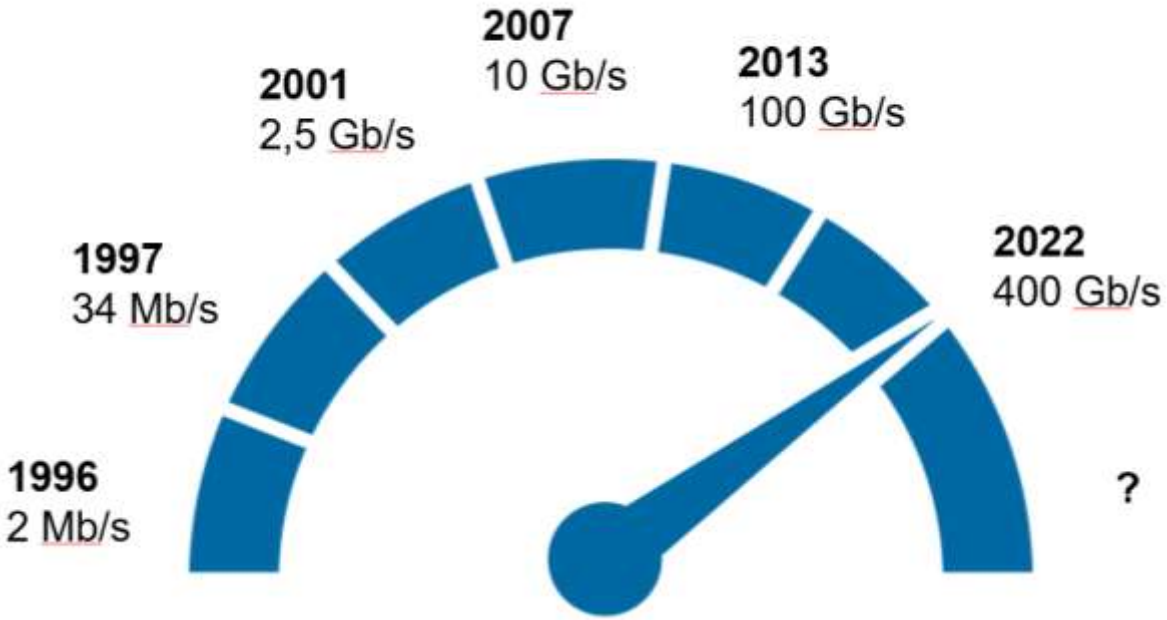
cesnet

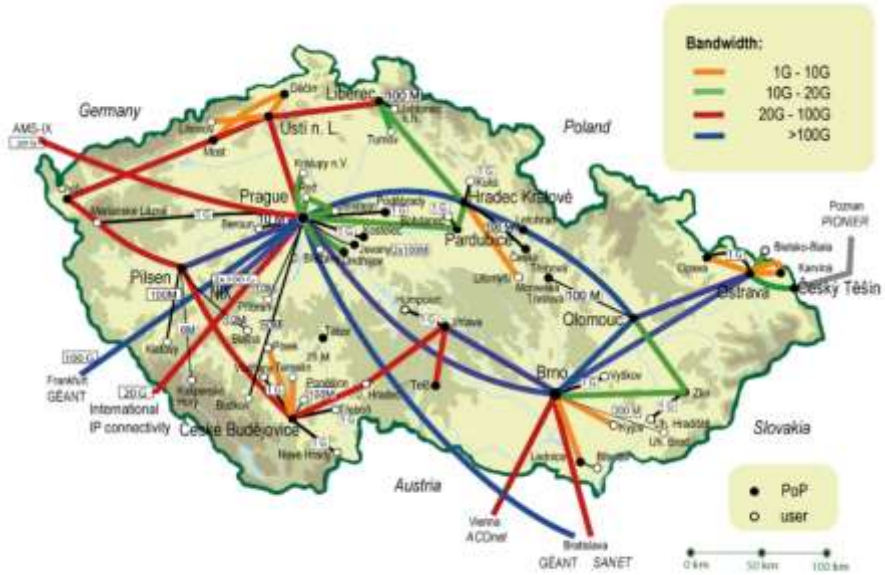
SLUŽBY CESNET PRO ZDRAVOTNICTVÍ

Jan Kolouch
CESNET z. s. p. o.

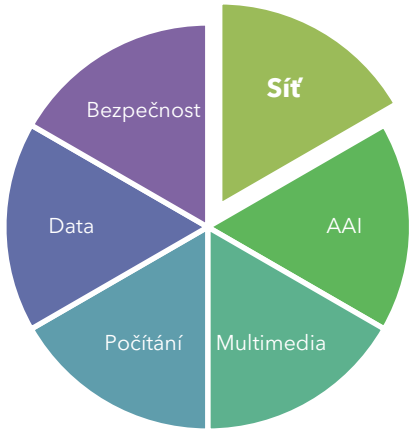
13.5.2024
isss

Z 2 Mb/s na 400 Gb/s





cesnet



1996

1

služba

2000

14 služeb

2005

24 služeb

2010

27 služeb

2015

38 služeb

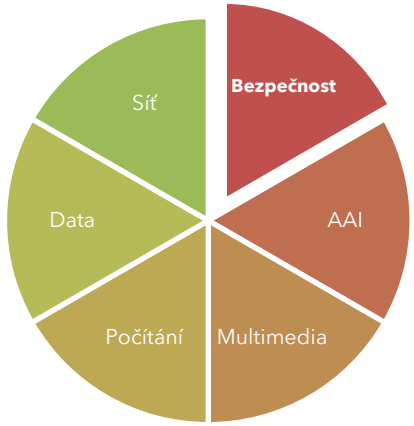
2020

57 services

2023

60+

služeb



cesnet

SPOLU PRO VĚDU

- Jsme součástí konsorcia e-INFRA CZ

- páteřní síť **400 Gb/s**
- datová úložiště **103 PB**
- výpočetní výkon **37 628 CPU**

NAŠI UŽIVATELÉ

500.000 individuálních uživatelů

300 připojených organizací

VŠ a univerzity

Výzkumné organizace,
zdravotnická zařízení

Veřejná správa a samospráva

ZŠ, SŠ a VOŠ

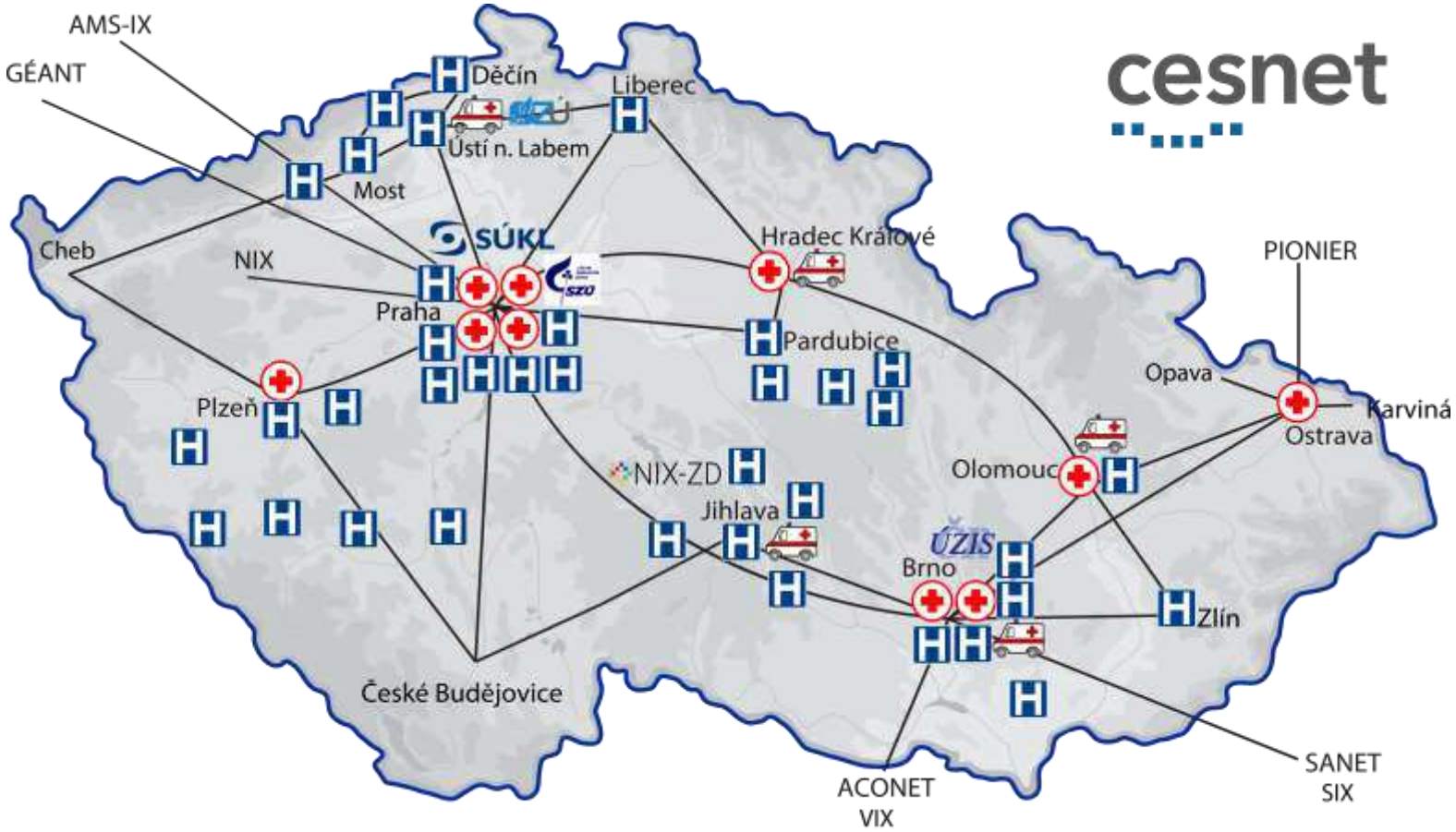
Ústavy Akademie věd

Knihovny, muzea, galerie

cesnet

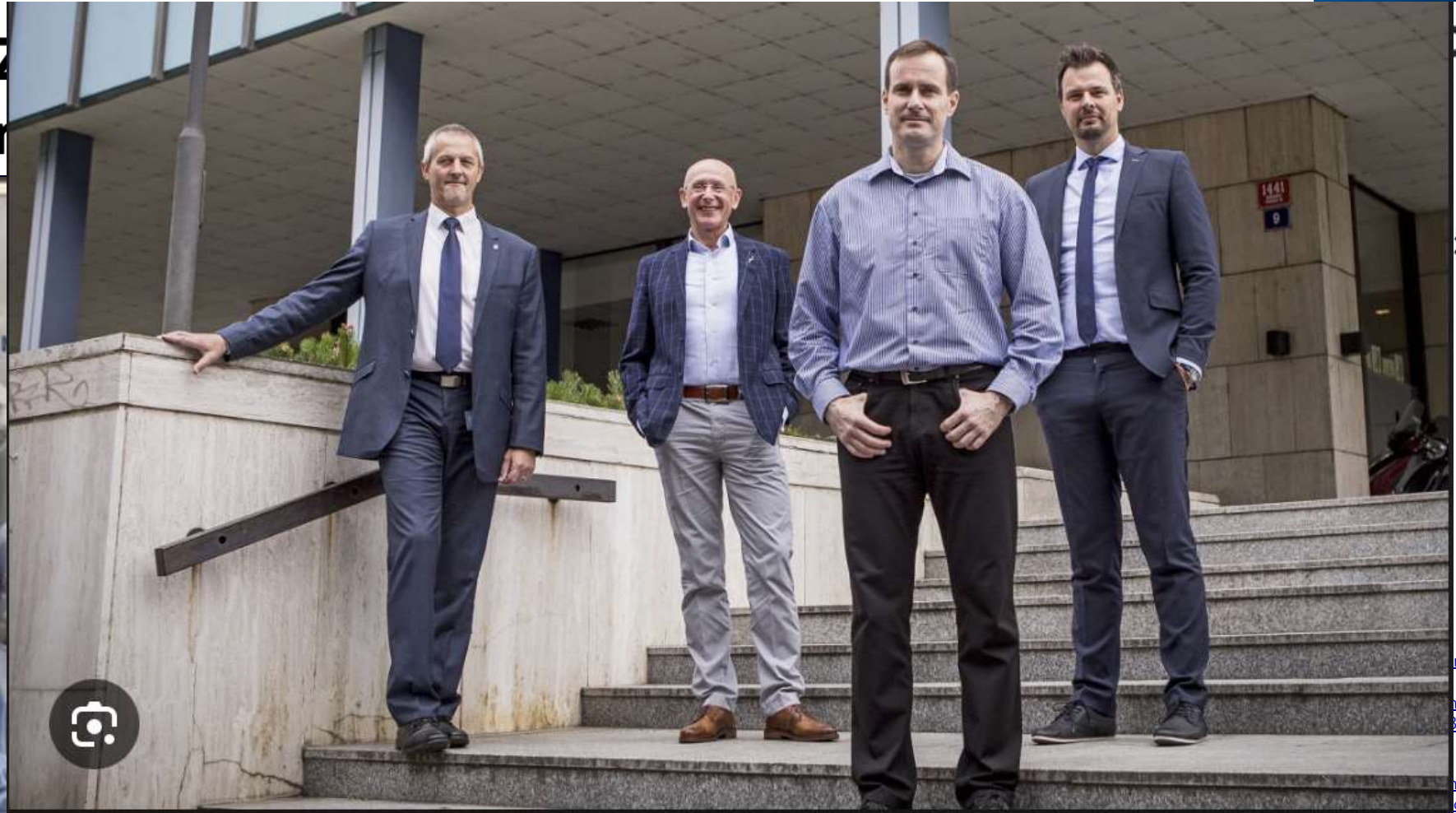
CESNET & zdravotnictví?

KONEKTIVITA - 57



cesnet

BEZPEČNOST

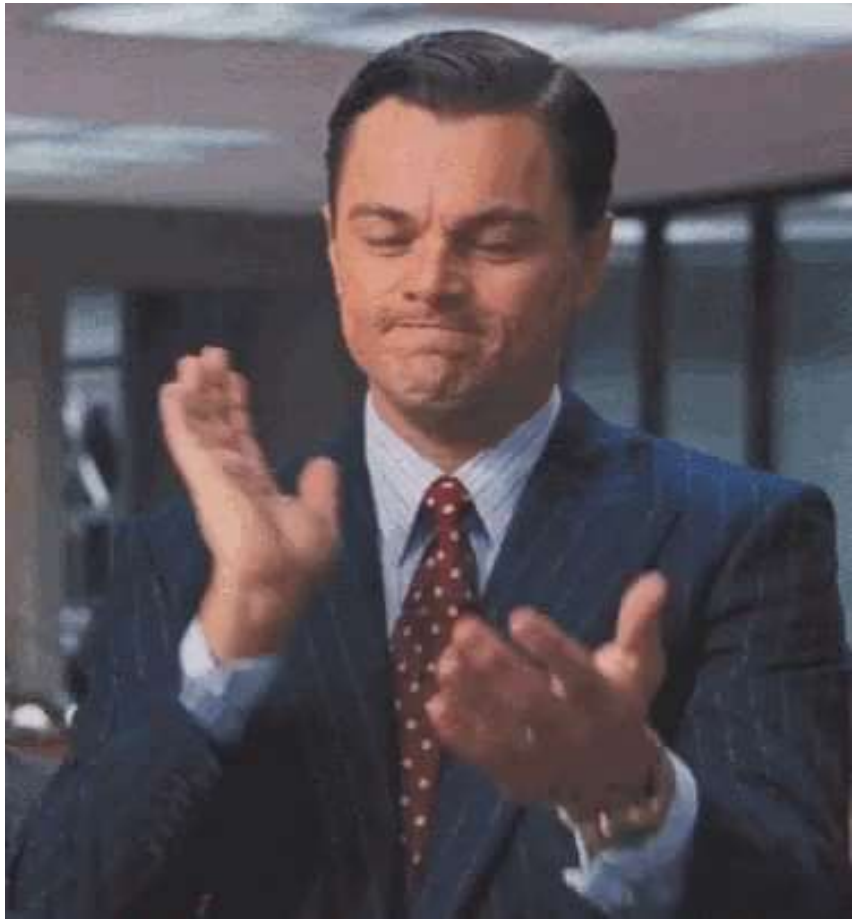


Nejvyšší muži českého IT se spojili, chtějí založit kyberochranku pro nemocnice. Vojtěch to...

Navštívit

cesnet

GREAT IDEA



cesnet

cesnet

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.

Léčebnu v Horažďovicích už podruhé napadli hackeři, vymazali některá data

na scéně. Masivně útočí

ažďovicích na Klatovsku napadli na konci
i se jim podařilo vymazat některá data
ckému útoku čelilo toto krajské zdravotnické

WannaCry. Tento škodlivý kód
něj však nepodařilo zcela vyzrát,
nce v letošním roce tento

vý červ, který
infikování
a za jejich
Peter

ic a další cíle ve čtvrtek varoval
ční bezpečnost (NÚKIB).

Fakultní nemocnice v Ostravě. | Foto: ikatudiné.cz

cesnet

hSOC

cesnet

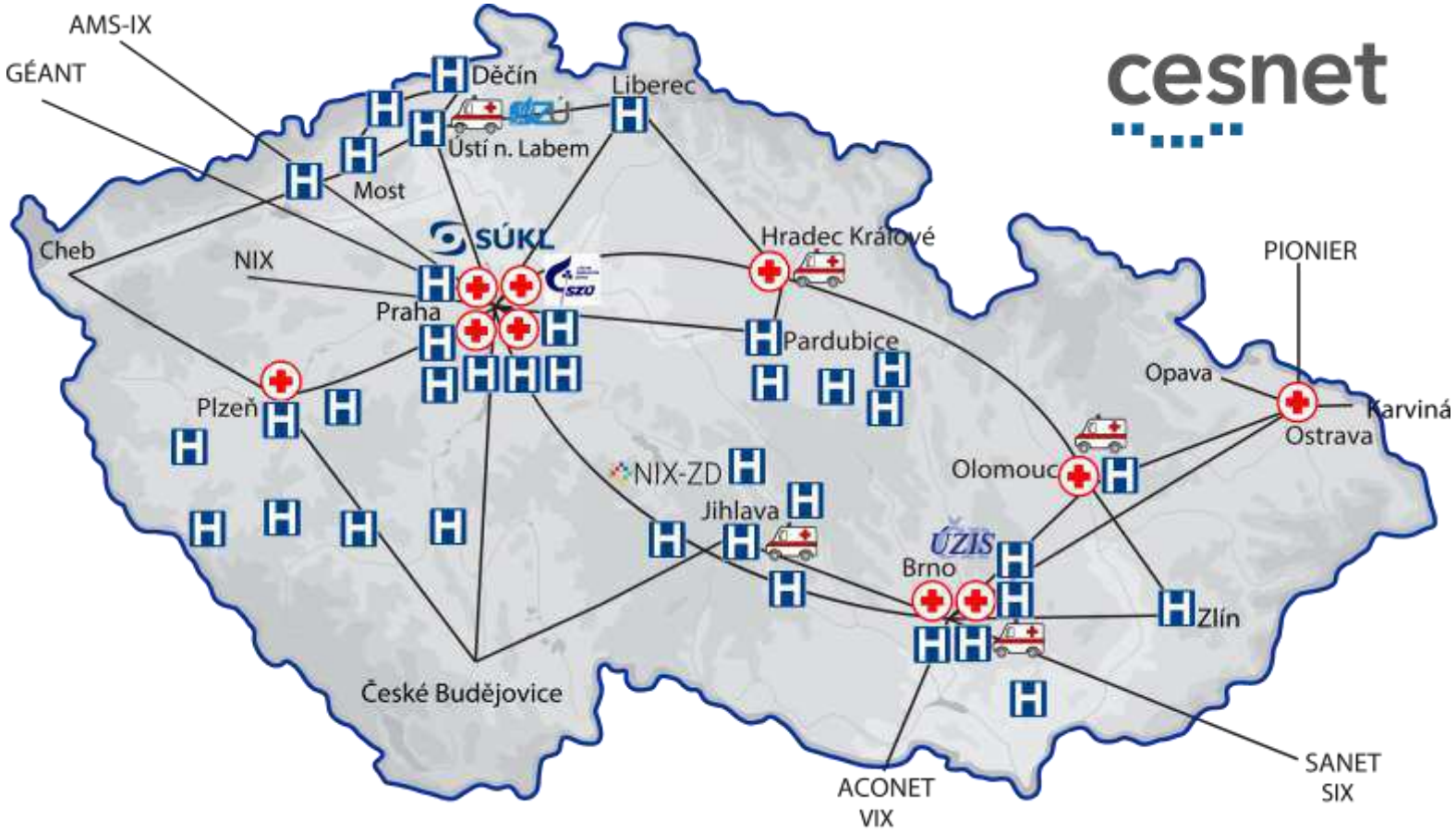
HSOC
HOSPITAL SECURITY OPERATION CENTER

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

cesnet

CESNET & hSOC?

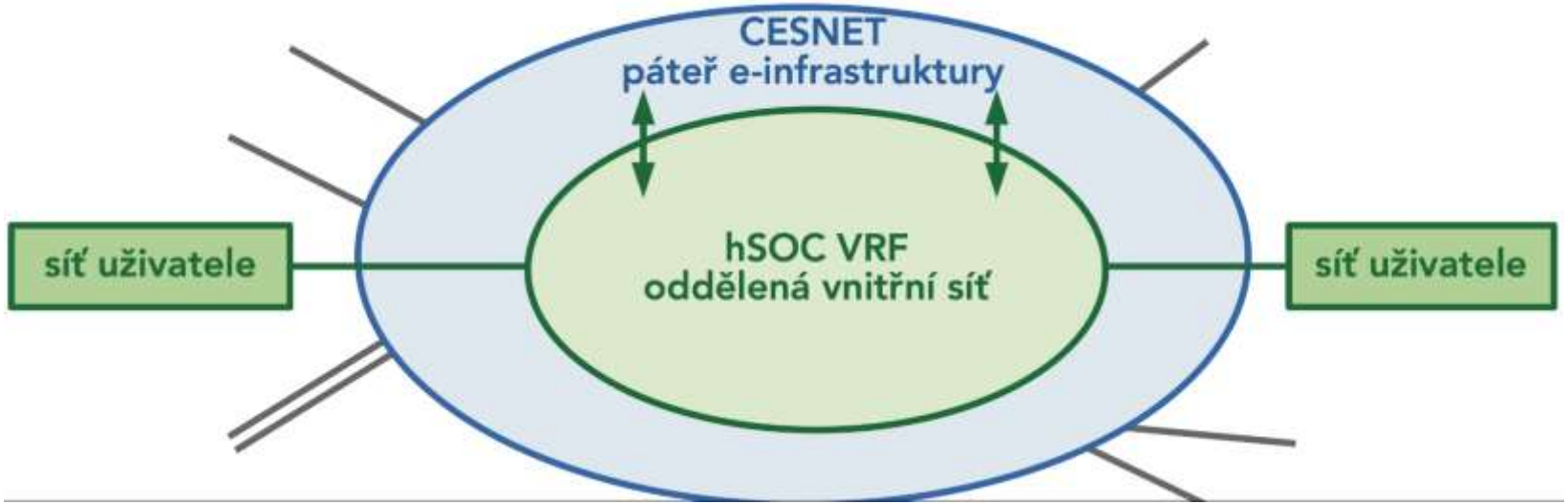
cesnet


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

cesnet

hSOC VRF

- **hSOC VRF → oddělená infrastruktura pro specifickou komunitu ~ síť v síti**
  - propojení do „velké“ sítě v geograficky různých lokalitách
  - proč oddělená síť ?
  - připojení do VRF z pohledu uživatele ?



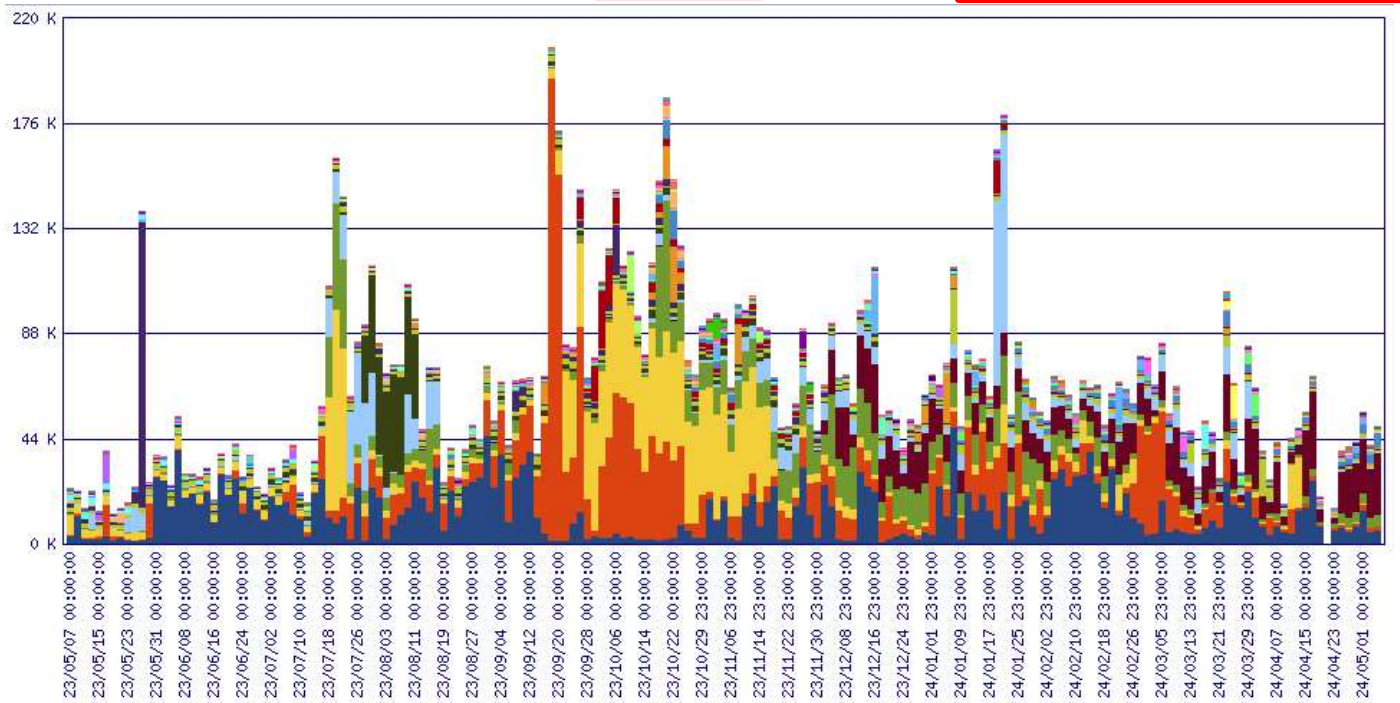
hSOC VRF – detected events (1 year)

o	Flow-Start [CEST]	Flow-End [CEST]	Bytes-estimated	Src-IP-Cnt	Flow-Cnt	Flow-Cnt-Drop	Detected-Event-Cnt	Detector-Type
1.	23/05/05 23:19:30.000	24/05/06 00:22:58.000	120.099 GB	67129	1962329448	1807462296	12182741	Src-IP

exklusivní adresy

92%

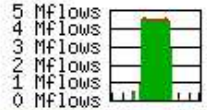
0.38/s

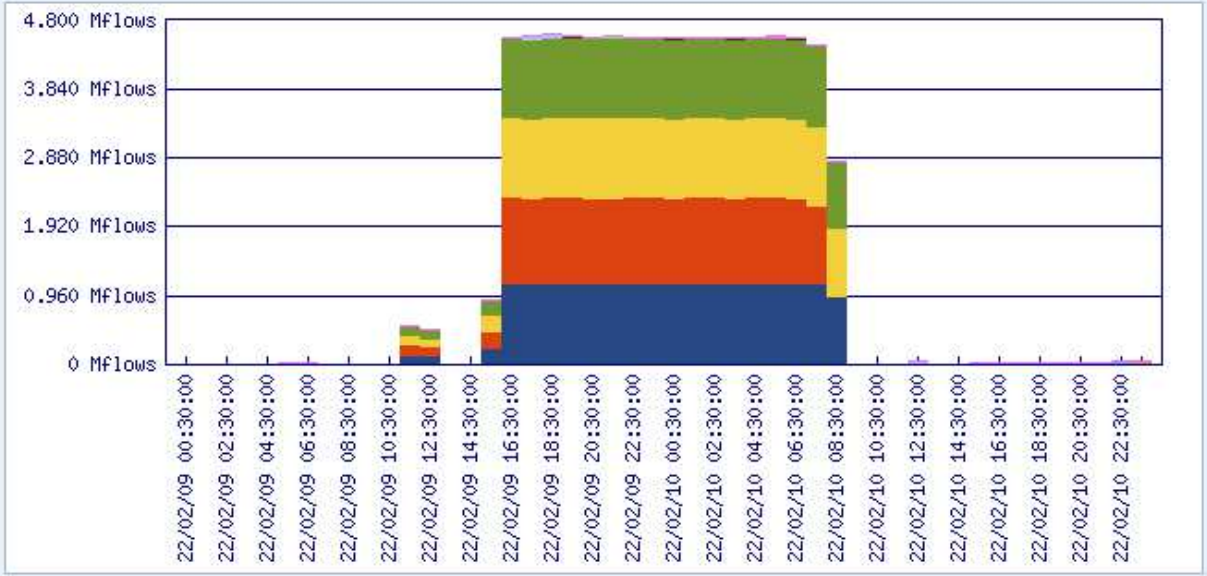


Flow-Cnt-Drop: *sums/time steps, 22/02/09 00:00:00-22/02/11 00:00:00, value per 1 hour, cumulative*

Summary

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



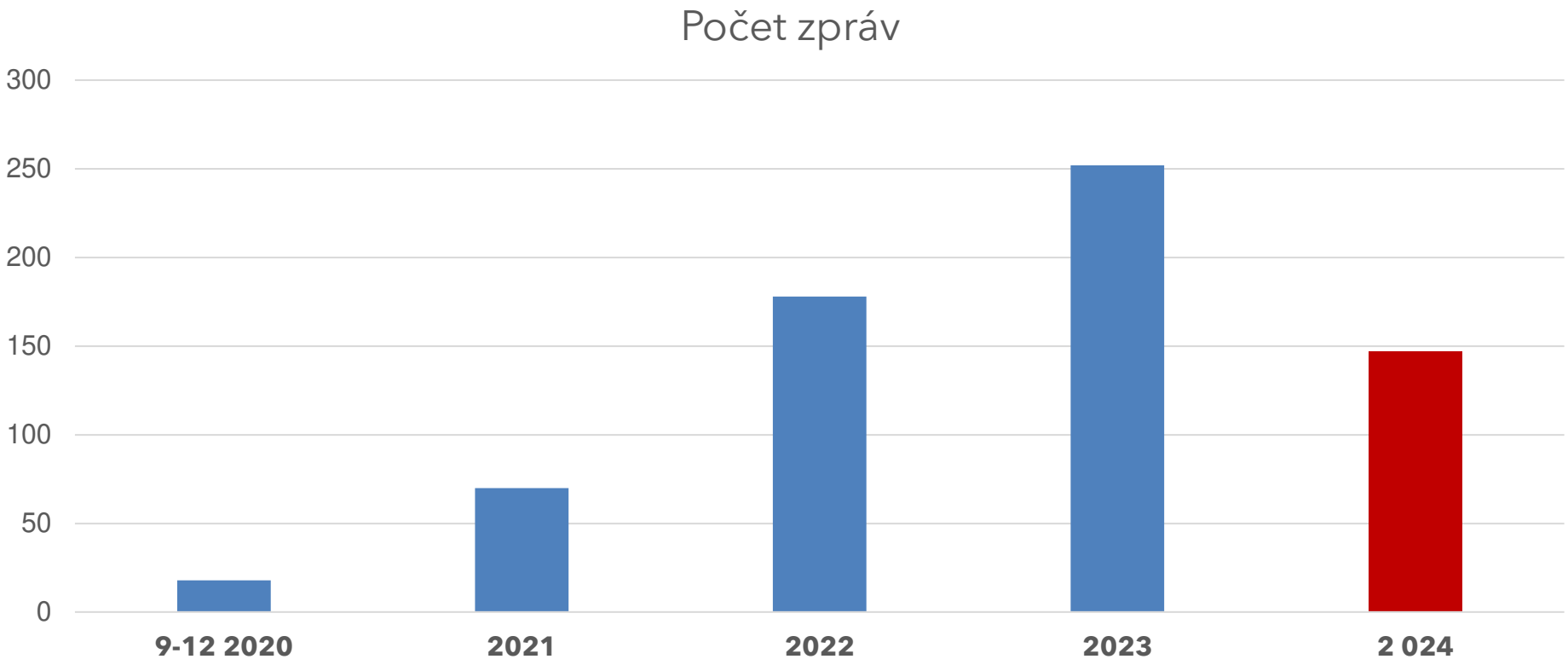


o	>	Src-IP	Src-GeoIP	Flow-Start	Flow-End	Bytes-measured	Bytes-estimated	Pkts-measured	Pkts-estimated	Flow-Cnt	Flow-Cnt-Drop
1.	>	[redacted]		22/02/09 11:31:00.000	22/02/10 08:50:48.000	794.470 MB	794.470 MB	19.597 Mp	19.597 Mp	19589981	19502770
2.	>			22/02/09 11:29:52.000	22/02/10 07:54:28.000	791.902 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

- 15 nemocnic zapojeno
- další v procesu připojování

cesnet

SITUATIONAL AWARENESS


Počet zpráv
300
250
200
150
100
50
0
9-12 2020
2021
2022
2023
2 024

cesnet

HYBRIDNÍ MODEL SOC?

cesnet

cesnet

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

Externí zdroje

bezpečnostní události, NÚKIB, partneři aj.

hSOC

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

- **Příjem**
- **Zpracování**
- **Obohacení**
- **Analýza**
- **aj.**

DATA

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

cesnet certs

(incident handling)

FTAS a síťová analytika

Situational Awareness analytika

Analytik Analytik Analytik Analytik

Zásahy
(filtry, blokace aj.)

konzultace, spolupráce

Incident reports, event reports, vulnerability reports.

konzultace, spolupráce

cesnet flab

Připojená organizace
(univerzita, nemocnice aj.)

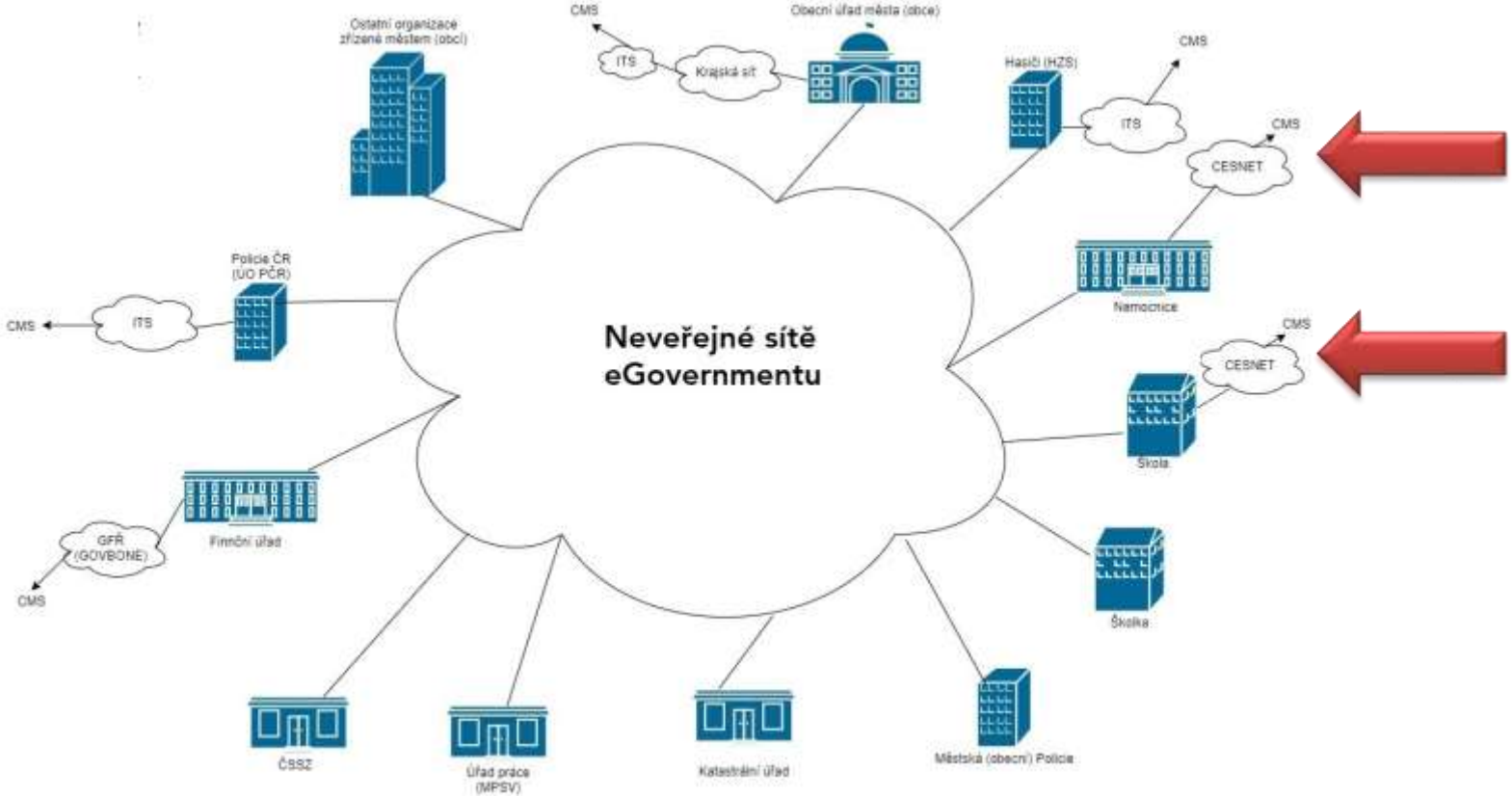
Response
Disaster recovery

- Postupy
- Asset management
- DRP
- Analýza rizik
- Dopady aj.

cesnet

CMS 2.0

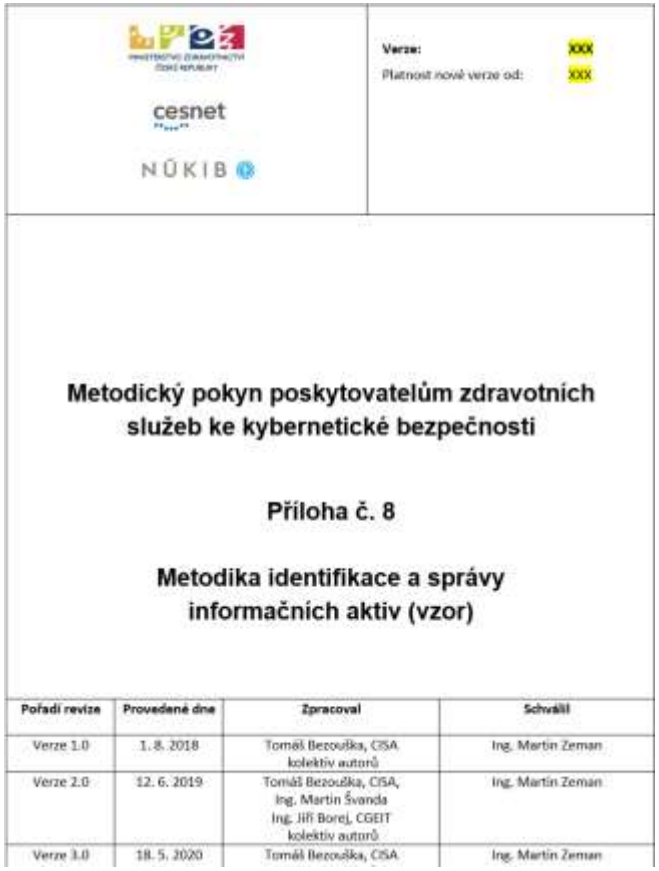
Neveřejné sítě eGovernmetu



cesnet

METODIKA A LEGISLATIVA

cesnet



Verze: XXX
Platnost nové verze od: XXX

cesnet

NÚKIB

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

Verze: XXX
Platnost nové verze od: XXX

cesnet

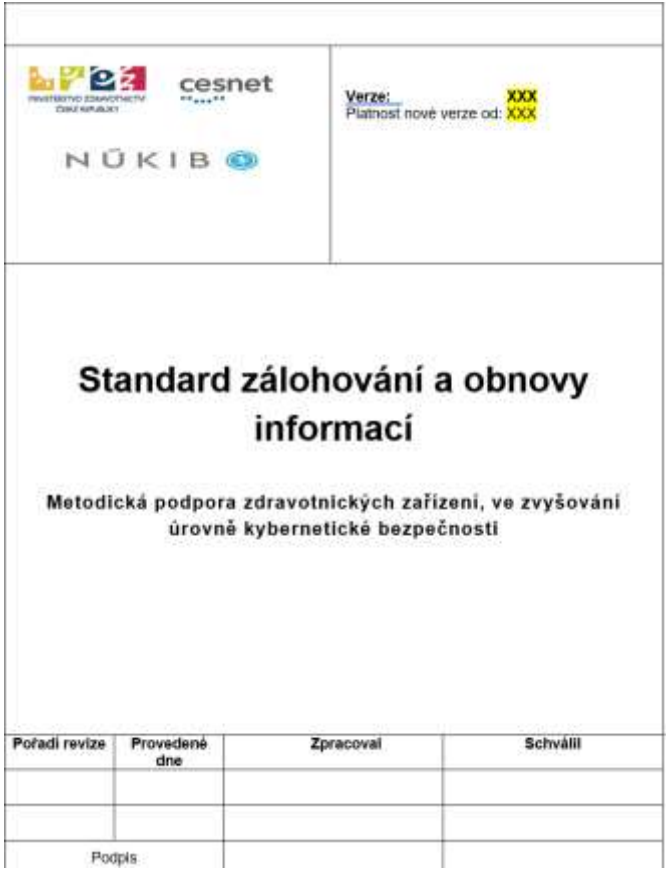
NÚKIB

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	



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

KOOPERACE A KOMUNIKACE

cesnet

PŘÍLEŽITOSTI

- **Podpora a zapojení dalších subjektů**
- **Sdílení know-how a lidských kapacit**
  - best-practice, koncepce a design architektury
  - školení, semináře a workshopy
  - technologické standardy
- **Nastavení workflow a procesů u zapojených subjektů**
- **Emergency komunikační kanály**
  - mailing-listy, videokonferenční systém, datové úložiště

cesnet

https://hsoc.cesnet.cz

hsoc@cesnet.cz

cesnet

JSOU NEMOCNICE BEZPEČNÉ?

cesnet

cesnet

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

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.

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

10. 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

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.

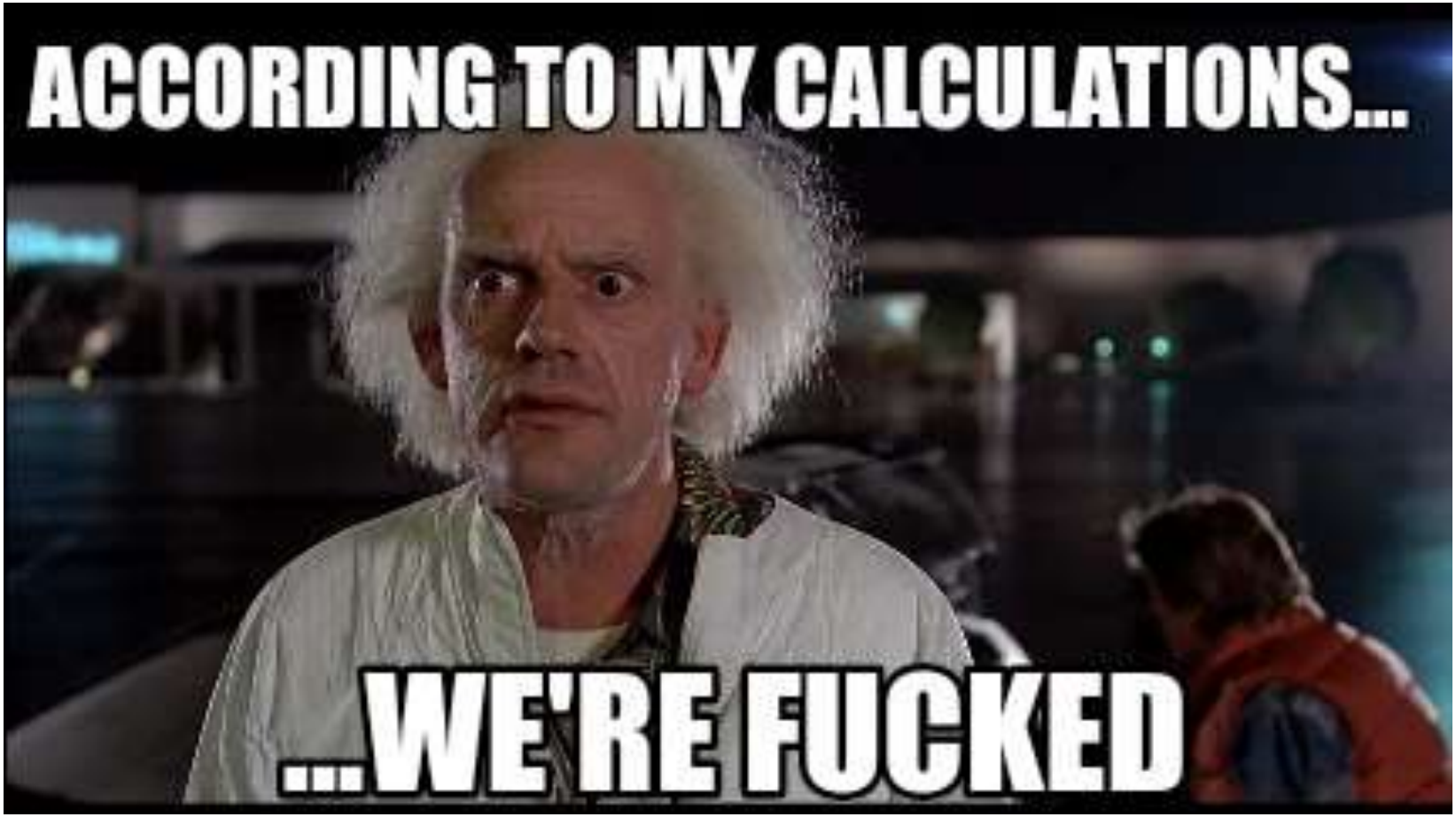
„WannaCry bohužel opět masivně útočí. WannaCry je ransomwarový červ, který se v květnu 2017 rychle šířil počítačovými sítěmi po celém světě. Po infikování počítačů se systémem Windows zašifruje soubory na pevném disku a za jejich zpřístupnění a dešifrování požaduje výkupné v bitcoinech," varoval Peter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

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

ČTK, Domácí

…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 …mační bezpečnost.

cesnet



cesnet

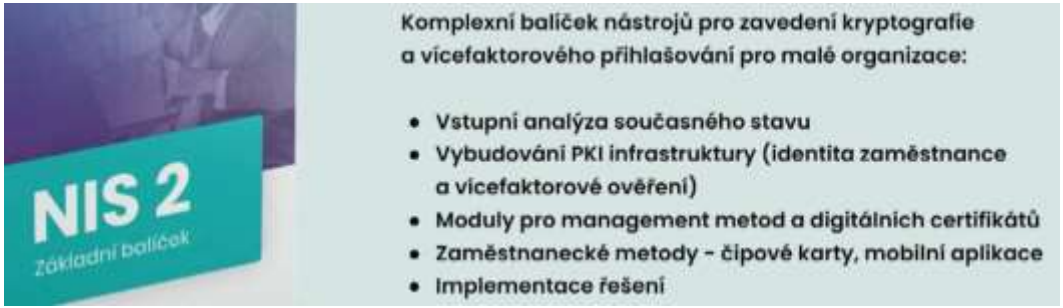
ŘEŠENÍ?

cesnet

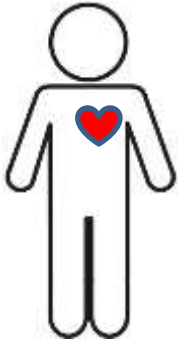
No. 1

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

Celé si to koupím!



- Capacity building
- Lidé na straně koncové organizace
- Nečekat, až…
  - se to stane znovu
  - bude ZoKB v 2.0
- Komunitní spolupráce



cesnet

DĚKUJI ZA POZORNOST

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