

# PRÍNOSY A RIZIKÁ DIGITALIZÁCIE NEMOCNÍC ZAOSTRENÉ NA KYBERBEZPEČNOSŤ

ITAPA HEALTH & CARE 2023

16. 03. 2023 | Hotel IMPOZANT, Valčianska dolina



**Jan Váša**

*Cyber Security Sales Engineer*

**Atos IT Solutions and Services s.r.o.**

+420 722 446 644, [jan.vasa@atos.net](mailto:jan.vasa@atos.net)  
[linkedin.com/in/janvasa/](https://www.linkedin.com/in/janvasa/)



# Digitalizace zdravotnictví

... má jednoznačné přínosy:

- úspora času
- efektivnější komunikace
- lepší organizaci činností
- lepší využití zdrojů
- transparentnost

Cíle digitalizace:

- Dostupnost a kvalita péče
- Ekonomicky dostupná péče
- Zapojení pacienta

” Pokud chceme udržet kvalitu péče, není jiné cesty než důsledná a promyšlená digitalizace, která povede k zefektivnění práce zdravotnického personálu.

MARTIN KOČÍ, PŘEDSEDA SPOLKU MLADÍ LÉKAŘI, RADIOLOG FN MOTOL

<https://www.seznamzpravy.cz/clanek/lecit-budou-dal-doktori-bez-digitalizace-to-ale-zdravotnictvi-nezvladne-177634>

# Agenda

## Rizika digitalizace

- Typy útoků
- Následky útoku na nemocnici
- Tradiční a nové hrozby
- Zabezpečte se

# Kyberútoky na nemocnice

“Tradiční” typy útoků > na IT

Nová hrozba



**Phishing**

(zčizení přístupových kódů)



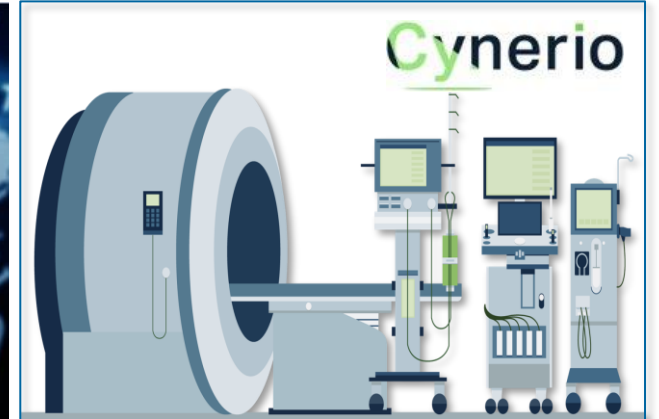
**Malware**

(vir v komunikaci a webu)



**Ransomware**

(zaheslování IT)



**Útok na medicínská  
zařzení**



## Průběh útoku

- 11.12.19 2:17 chirurgická ambulance
- 11.12.19 2:50 už nešlo nic
- Výpadek provozu 20 dní
- Obnova systémů cca ½ roku

## Finanční ztráta

- **60 mio Kč (~ 2.5 mio EUR)**

## Vyřazení provozu

- Na 600 serverů a pracovních stanic
- Laboratoře
- Systém dárců krve



## Ztráta dat

- administrativních
- ekonomických



## Kyberútok 5.3.23 ochromil nemocnici v Barceloně

# Hospital Clínic de Barcelona

Zdravotnické zařízení s 819 lůžky, ve spádové oblasti více než půl milionu obyvatel.

### Bezprostřední následky

- zrušení 150 plánovaných operací
- zrušení na 3000 vyšetření
- nedostupná data o pacientech
- nemožnost komunikace mezi odděleními

### Vyřazení počítačů z provozu

- v nemocničních laboratořích
- na urgentním příjmu
- v nemocničních lékárnách
- ve 3 hlavních budovách
- v dalších externích klinikách

<https://www.sme.sk/minuta/23143536/jednu-z-najvaecsich-nemocnic-v-barcelone-ochromil-kyberneticky-utok>

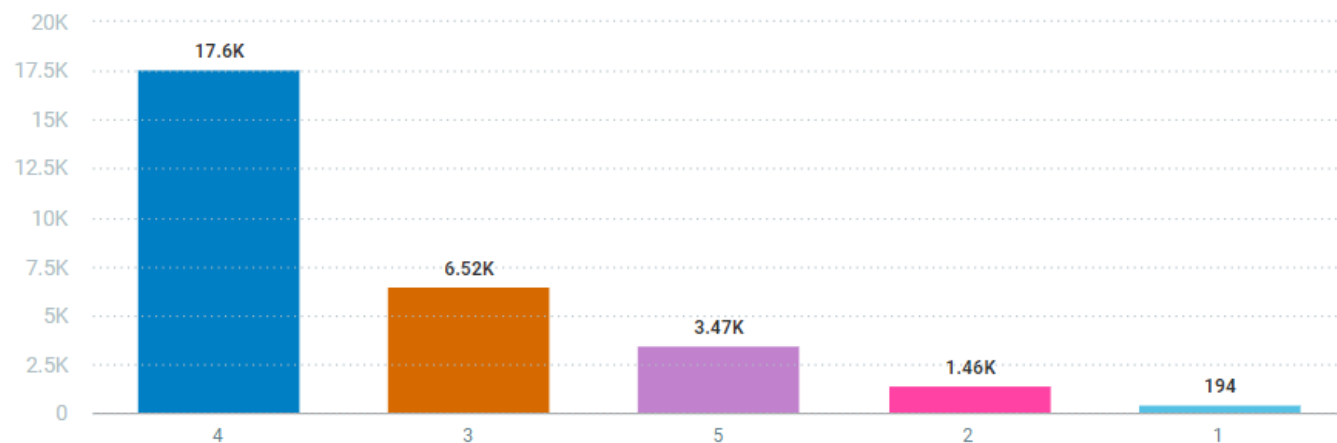
**Jsou slovenské (a české)  
nemocnice připraveny  
na kyberútoky?**



# Vulnerability Scan IT prostředí nemocnice (sk)

- Počet monitorovaných IT assetů **1 000**
- Počet detekovaných zranitelností **29 244** (detekováno ihned v první vlně implementace)
- Z toho celkově Public Exploit zranitelností **4 437**
- Kritické zranitelnosti s veřejnou IP adresou **37** (monitorováno 10 IP Adres)

VULNERABILITIES BY SEVERITY



## Možné útoky na infrastrukturu:

- High Data Lose **11 208**
- Privilege Escalation **8 098**
- Denial of Service **11 141**

aktivních zranitelností



# Zranitelnosti medicínské techniky nemocnice (cz)



# Co pro vás můžeme udělat

- Zmapování assetů
- Ověření zranitelností a jejich zneužitelnosti
- Doporučení ke zmírnění nalezených nedostatků
- Návrh opatření
- Detekce kyberútoků na medicínskou techniku a reakce na ně

# Kontakty pro zvýšení kyberbochrany nemocnic



**Vladimír Brenkuš**

*Digital Workplace Architect*

+421 911 054027

[vladimir.brenkus@atos.net](mailto:vladimir.brenkus@atos.net)



**Jan Váša**

*Cyber Security Sales Engineer*

+420 722 446 644

[jan.vasa@atos.net](mailto:jan.vasa@atos.net)

[linkedin.com/in/janvasa/](https://www.linkedin.com/in/janvasa/)



# Poznatky z nemocnic v SR a v Evropě

Co je podobné a v čem se lišíme?

## PODOBNÉ

- Podobné bezpečnostní skóre
- Podobné bezpečností problémy

## ROZDÍL

- Vyšší počet připojených zařízení do sítě  
*(nemocnice v SR začínají tento trend kopírovat)*
- Rychlejší nákup bezpečnostních produktů
- Silnější potřeba posílit automatizaci pomocí nástrojů a odlehčit IT oddělení

 Security Posture Score

**57.8**

Score

**88,5**

Benchmark

Medical

**56.9**

Score

**88**

Benchmark

Non-Medical

**58.9**

Score

**89**


Benchmark

# Příklady nálezů bezpečnostních děr (1/4)

## Kritická zranitelnost drahého přístroje

Dashboard Network Map Risks Mitigation Impact Utilization MDS2 FDA Attributes

Name Legacy OS Risk Group End of Life OS ... IDENTIFY



Impact (environmental score)	
Confidentiality	Medium
Patient Safety	Medium
Service Disruption	High

Base Score 10	
Confidentiality	Complete
Integrity	Complete
Availability	Complete

Type	Vulnerability
Vendor	N/A
CVE	N/A
CWE	Use of Unmaintained T...
Publish Date	16/03/2017

**Description**  
Device is running an OS which is not supported by the OS manufacturer and does not receive security updates. Legacy OS can be a potential liability which can weaken or compromise an otherwise well maintained network

**More Details**  
[Microsoft product lifecycle search](#)

**Mitigation**  
1 . Apply East-West Segmentation: Unsupported OS can't be patched and the only compensating control that can be applied is East-West segmentation. Configure East-West segmentation policy to mitigate risk and reduce the attack vector by limiting the devices' communications to authorized network entities.  
2 . Apply North-South Segmentation: Devices running an unsupported OS are vulnerable to many remotely exploitable vulnerabilities. Use North-South Segmentation to make sure they are not accessible via internet to threat actors

# Příklady nálezů bezpečnostních děr (2/4)

Jedna konkrétní „čiperná“  
nemocniční televize  
intenzivně komunikuje  
uvnitř nemocniční sítě

Proč?

Assets / Smart TV

TV	
<b>General</b>	
Status	Online
Device Class	IoT
Category	Multimedia
Role	Device
Type	Smart TV
Model	
Vendor	
Site	
Severity Score	
First Seen	
Last Seen	
<b>Network</b>	
Connectivity ...	
IP Address	
MAC	
MAC Vendor	
IP Allocation	
VLAN	
<b>IT</b>	
AD Member	False
Has Endpoin...	False
OS	Linux 3.10.0+



# Příklady nálezů bezpečnostních děr (3/4)

Záložní zdroje mají stejně heslo a navíc přednastavené v továrně.  
Heslo je veřejně známé.

Login: \*\*\*

Password: \*\*\*

Hacker může odpojit od proudu celou nemocnici za pár sekund...

# Příklady nálezů bezpečnostních děr (4/4)

Pravidelná komunikace z/do zemí s nedemokratickým režimem





# Vulnerability Scan IT prostředí nemocnice (sk)

- Počet monitorovaných IT assetů v nemocnici v první vlně 300
- po měsíci celkem implementováno celkem 3 000
- Počet detekovaných aktivních zranitelností v první vlně 27 584
- Z toho celkově detekovaných Public Exploit zranitelností 3 552
- Kritické zranitelnosti detekované na zařízeních s public IP adresou 45 (monitorováno 15 IP Adres)
- Na základě informací z první vlny jsme byli schopni efektivně nasadit opravné balíčky na kritické zranitelnosti a během prvního týdne, opravit 10 517 zranitelností

Postup	Počet IT Assetů	Vyhodnocení
Fáze 1 – Implementace a reporting	300	Detkováno 27 584 zranitelností
Fáze 2 – Spuštěn patchovací proces – na základě doporučení spol. Atos	300	Eliminace 10 517 zranitelností
Fáze 3 – Finální implementace	3000	Automatizace procesu remediace