HEALTHCARE &
LIFE SCIENCES

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

linkedin.com/in/janvasa/

Trusted partner for your **Digital Journey**

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

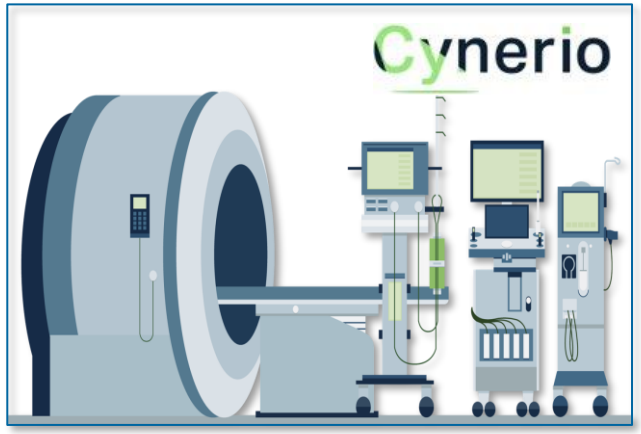
“Tradiční” typy útoků > na IT

Nová hrozba

Phishing
(zcizení přístupových kódů)

Malware
(vir v komunikaci a webu)

Ransomware
(zaheslování IT)



Útok na medicínská zařízení

Atos

Nemocnice Benešov po kyberútoku

Nemocnice Rudolfa a Stefanie Benešov, a.s.,
nemocnice Středočeského kraje
Středočeský kraj

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

Atos

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

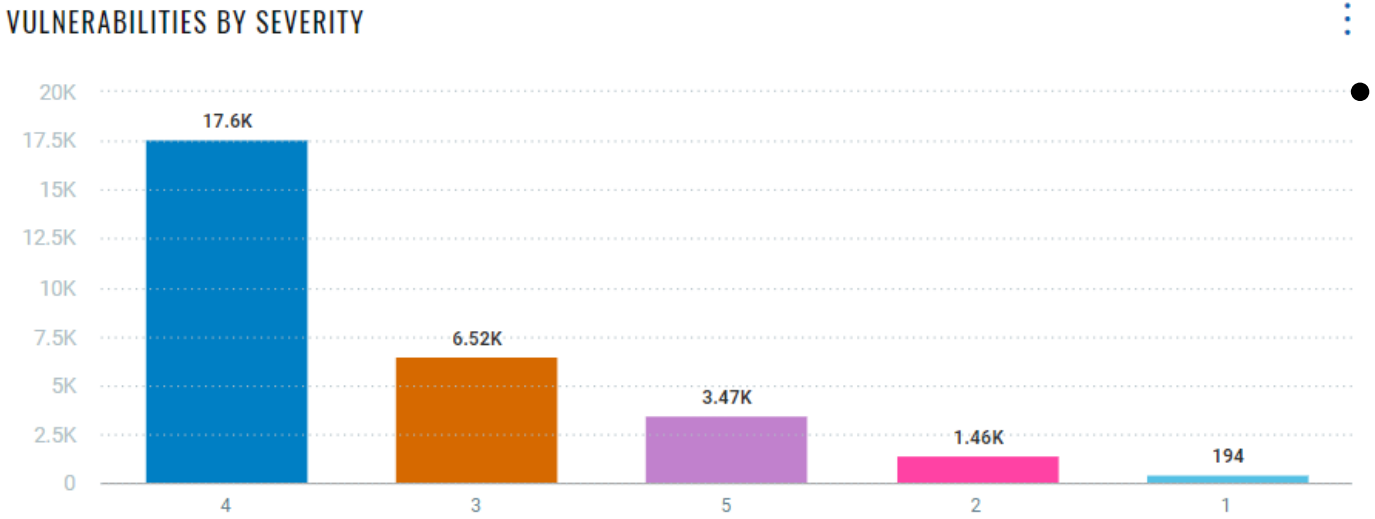
- ve 3 hlavních budovách
- v dalších externích klinikách

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)



- **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

Jan Váša
Cyber Security Sales Engineer

+420 722 446 644
jan.vasa@atos.net
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

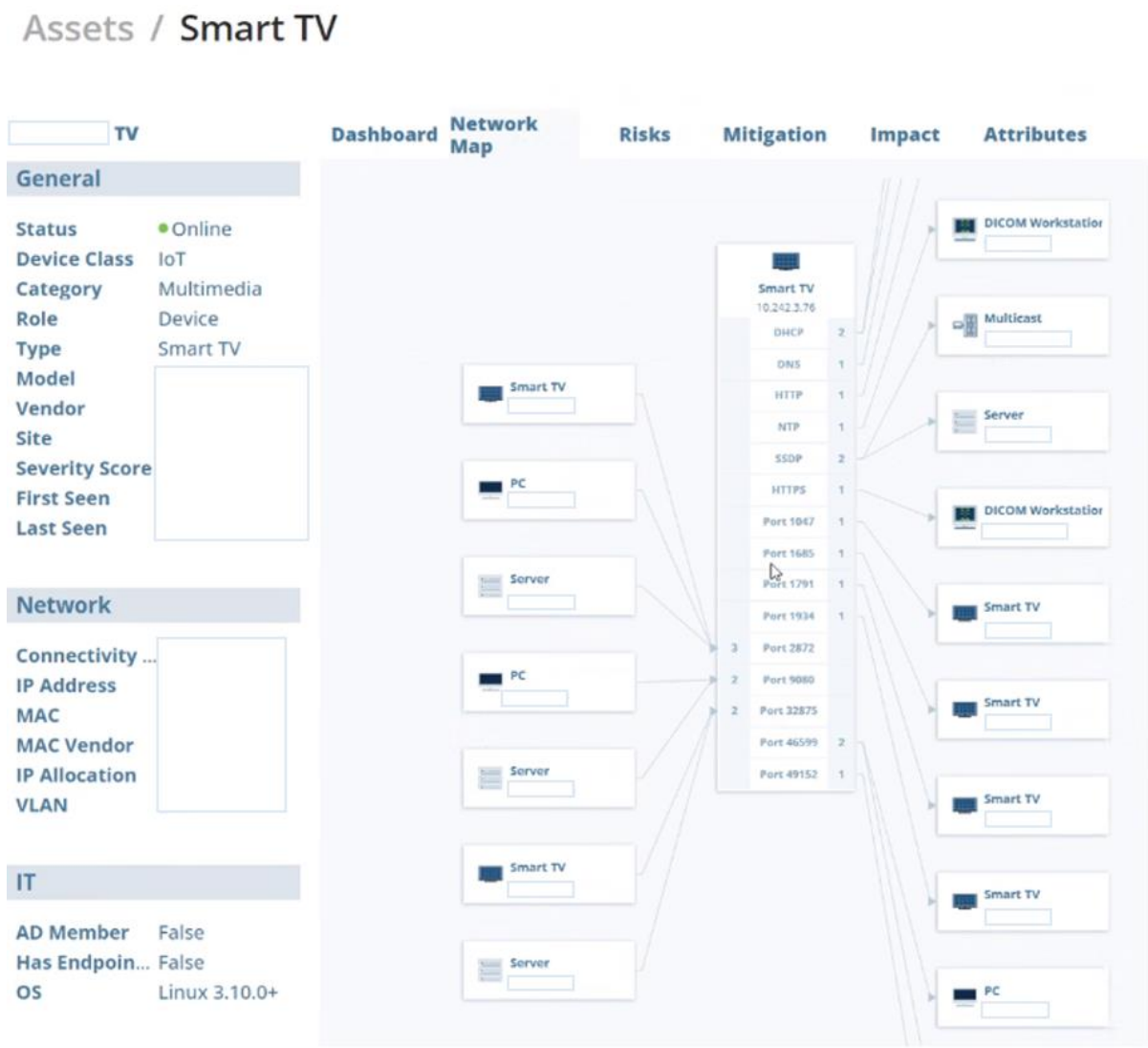
Příklady nálezů bezpečnostních děr (1/4)

Kritická zranitelnost drahého přístroje

Příklady nálezů bezpečnostních děr (2/4)

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

Proč?



Příklady nálezů bezpečnostních děr (3/4)

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

Login: ***

Password: ***

Hacker může odpojit od proudu celou nemocnici za pár sekund…

Atos

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	Dekováno 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