WEBINÁŘ AFCEA

17. března 2021

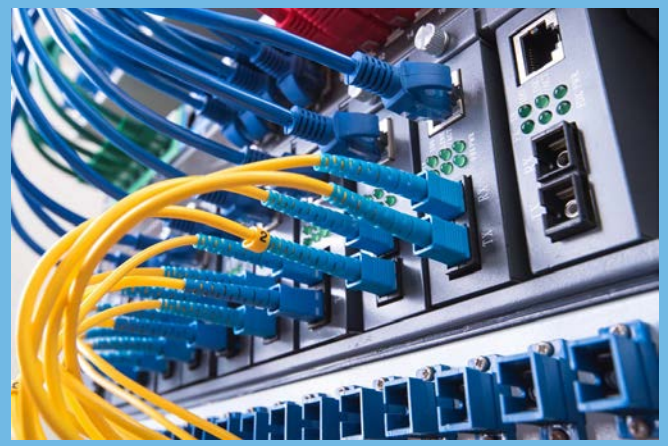
KYBERNETICKÁ BEZPEČNOST VE ZDRAVOTNICTVÍ

Jsou nemocnice snadný terč pro kybernetické útoky?

Rostislav Frys

Vojenský technický ústav

AGENDA

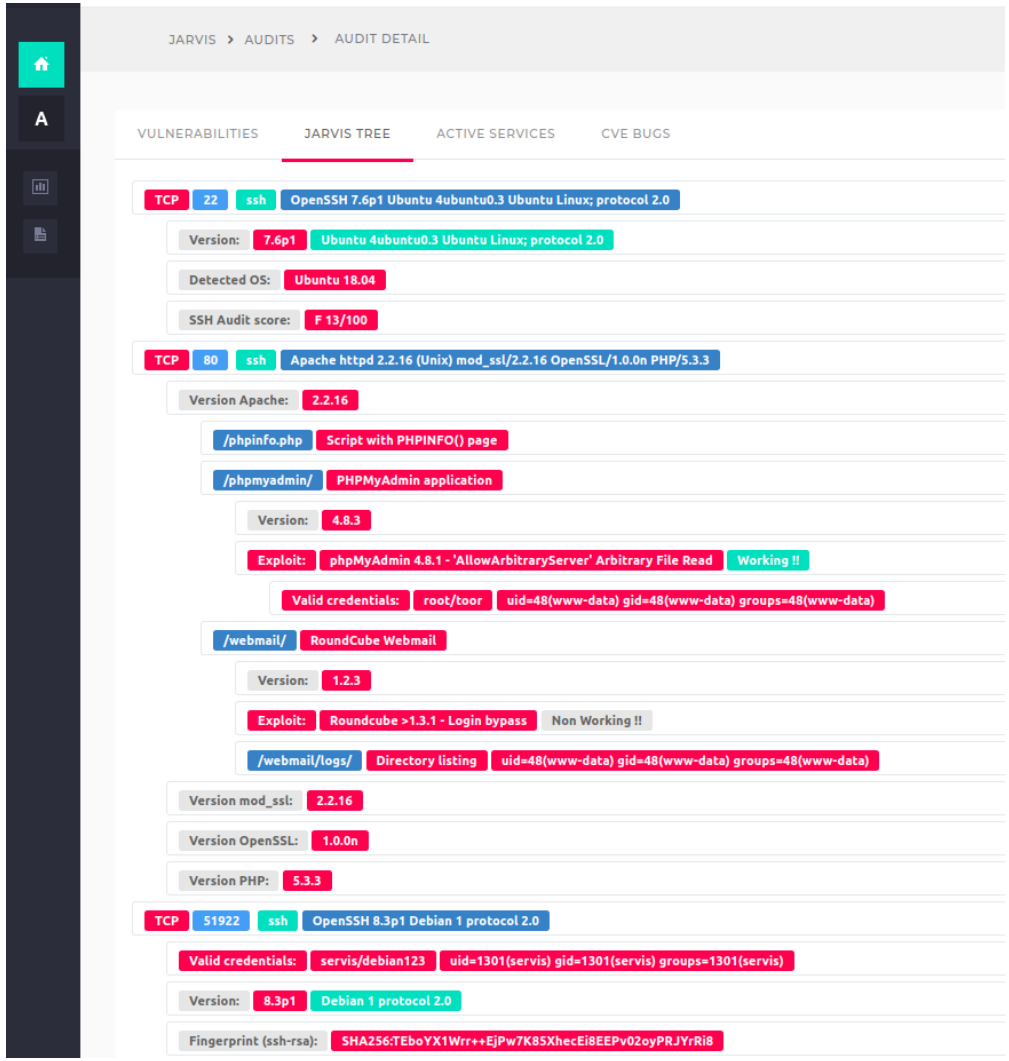


- Data z monitorování a testování ICT nemocnic – analýza, příklady
- Jsou nemocnice opravdu snadným cílem pro kybernetické útoky?
- Některé specifické požadavky pro zajištění bezpečnosti nemocnic

VSTUPNÍ ANALÝZA STAVU KB VYBRANÝCH NEMOCNIC

Zdroje dat pro analýzu současného stavu kybernetické bezpečnosti vybraných nemocnic

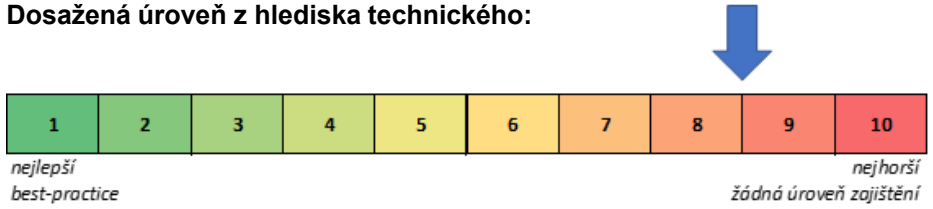
- **bezpečnostní audit** (pokryto cca 40 oblastí v šesti kategoriích)
- **analýza provozu ICT vybraných nemocnic**
  - hloubková analýza síťového provozu
  - automatizované zmapování topologie sítí a identifikace IT aktiv
  - bezpečnostní profiling IT aktiv
  - detekce moderních hrozeb v reálném čase (i v historii v průběhu monitoringu)
  - rekognoskace a analýza proprietárních komunikačních protokolů
- **blackhat penetrační testy s využitím umělé inteligence**



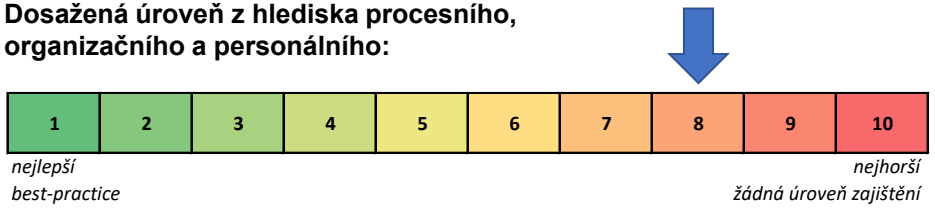
VÝSLEDKY BEZPEČNOSTNÍHO AUDITU

Kategorie opatření	Hodnocení
Detekce a vyšetřování bezpečnostních událostí	Základní úroveň pokrytí a bez schopnosti reagovat na generické i moderní hrozby.
Preventivní činnosti a technologie	Základní úroveň pokrytí a bez schopnosti reagovat na moderní hrozby.
Schopnost reakce na bezpečnostní události	Zcela nepokryto
Procesní řízení kybernetické bezpečnosti	Základní úroveň pokrytí a bez schopnosti reagovat na generické i moderní hrozby.
Testování a ověřování stavu ochrany	Zcela nepokryto
Vzdělávání uživatelů a odborníků	Zcela nepokryto

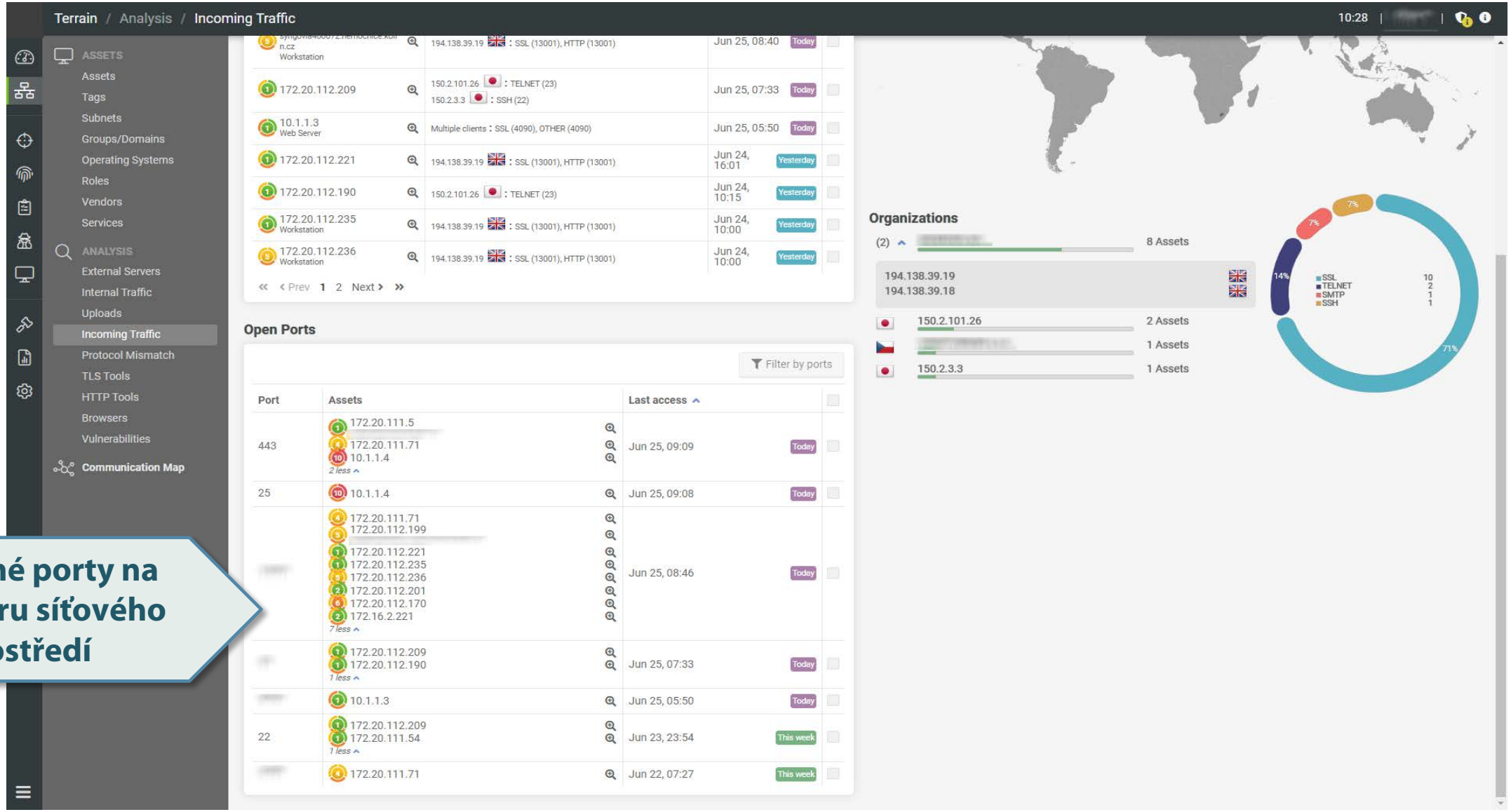
Dosažená úroveň z hlediska technického:



Dosažená úroveň z hlediska procesního, organizačního a personálního:



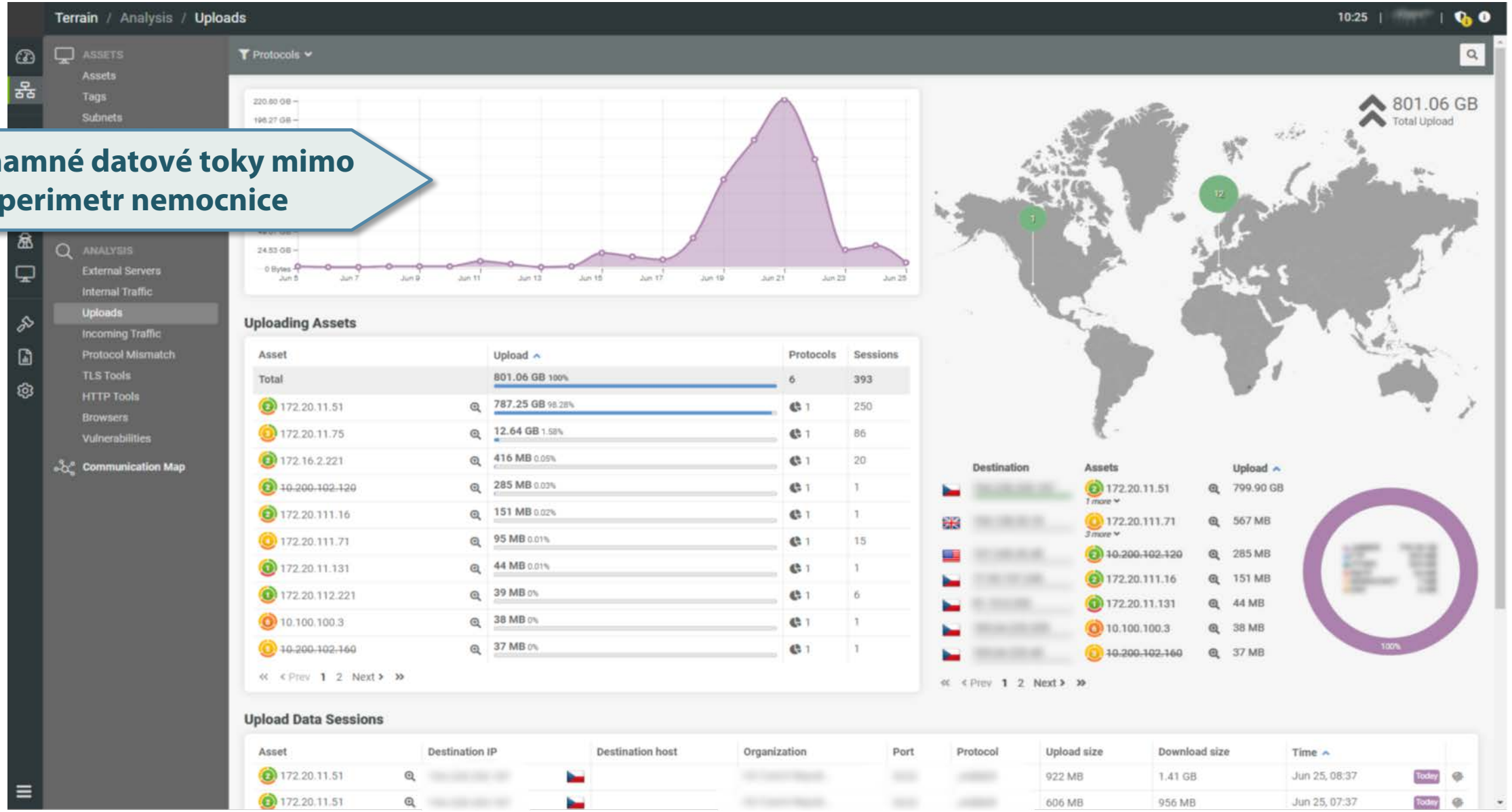
SOUČASNÝ STAV – ZJIŠTĚNÉ SKUTEČNOSTI / PŘÍKLADY



Otevřené porty na perimetru síťového prostředí

SOUČASNÝ STAV – ZJIŠTĚNÉ SKUTEČNOSTI / PŘÍKLADY

Významné datové toky mimo perimetr nemocnice



AGENDA

- Data z monitorování a testování ICT nemocnic – analýza, příklady
- Jsou nemocnice opravdu snadným cílem pro kybernetické útoky?
- Některé specifické požadavky pro zajištění bezpečnosti nemocnic

SOUČASNÝ STAV – ZJIŠTĚNÉ SKUTEČNOSTI

Výsledek analýzy není nijak překvapující a odpovídá i (bohužel) běžné situaci i v jiných oborech…

- prověření organizačního, procesního a technologického stavu kybernetické bezpečnosti zapojených nemocnic

→

- většina analyzovaných oblastí má jen základní nebo vůbec žádné pokrytí v oblasti kyb. bezpečnosti
- personálně i zdrojově podceněná oblast

- hloubkové zmapování a testování prostředí ICT vybraných nemocnic
  - počty a typ IT aktiv, role, síťová topologie..
  - bezpečnostní profiling IT aktiv, seznamy zranitelností
  - hloubková analýza síťového provozu (úroveň DPI i DSI)

→

- nízká míra segmenatce sítí
- tisíce IT aktiv bez potřebných aktualizací, násobně víc aktivních zranitelností
- otevřené porty do internetu, přímý vnější přístup k aktivům, pohyby malware po síti i koncových bodech

…. atd.

… s některými oborovými specifikami:

- esenciální **nutnost provozu nezabezpečených zařízení** (typicky medicínské přístroje) .. dlouhodobý problém nákupu těchto zařízení bez vazby na bezpečnost
- obvykle i nutnost nechat **přímý vnější přístup** k části přístrojového vybavení z prostoru mimo chráněný perimetr
- **proprietární protokoly** (komunikace mezi přístroji)

SOUČASNÝ STAV – KLÍČOVÁ ZJIŠTĚNÍ*

- Z hlediska technického, procesního i organizačního je **úroveň zajištění** kybernetické bezpečnosti zúčastněných nemocnic **velmi nízká (kritická).**
- Současná úroveň zajištění kybernetické bezpečnosti **nedokáže ochránit provoz a data nemocnic ani před** (náhodnými) **automatizovanými** (robotickými) **útoky**, natož pak před cílenými a připravenými útoky zkušených hackerů.
- **Není tedy otázka zda, ale kdy k takovému útoku dojde** a v současnosti nemají nemocnice účinné nástroje podobný útok včas detekovat a účinně se bránit

*) *vztaženo ke vzorku analyzovaných organizací*

AGENDA

- Data z monitorování a testování ICT nemocnic – analýza, příklady
- Jsou nemocnice opravdu snadným cílem pro kybernetické útoky?
- Specifické požadavky pro zajištění bezpečnosti nemocnic

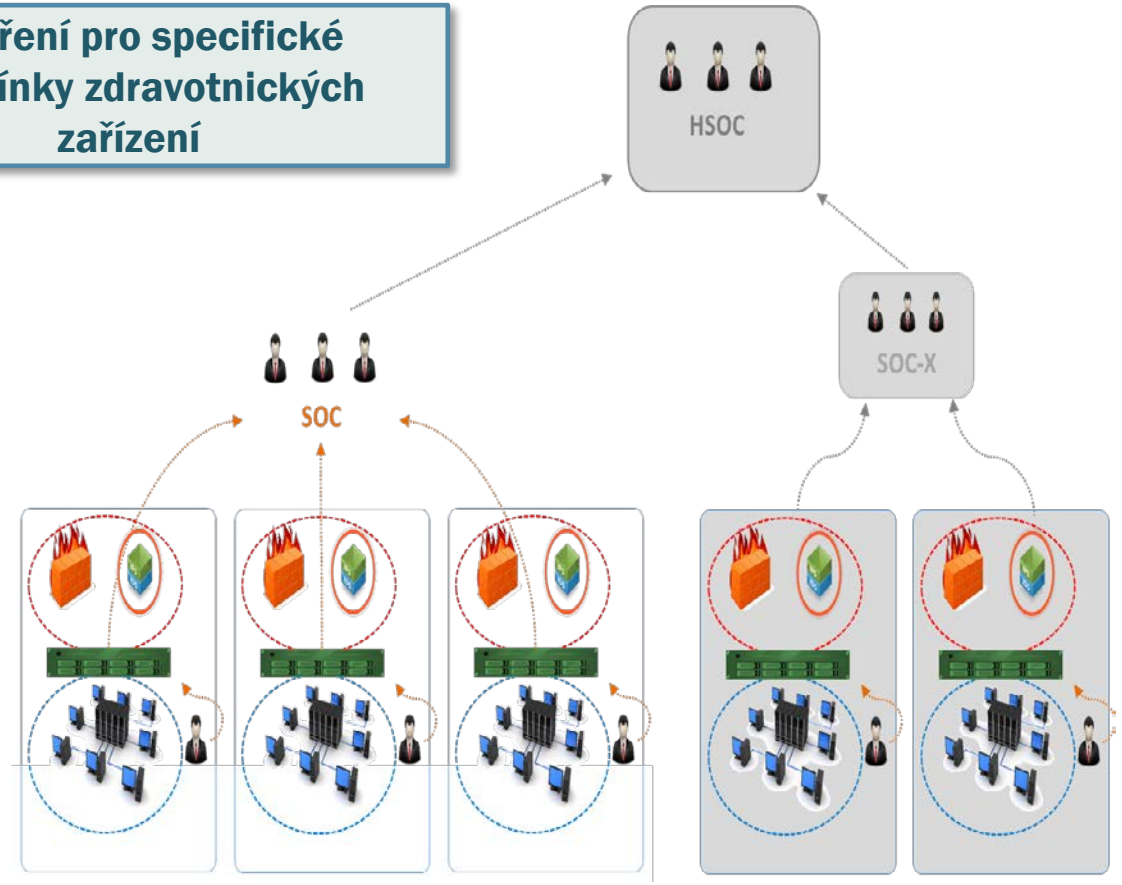
ŘEŠENÍ KB VE ZDRAVOTNICTVÍ - SPECIFIKA

Standardní opatření (v plné míře platná i pro zdravotnická zařízení)

analýza rizik, plán zvládání rizik, nastavení procesů a odpovědnosti, nastavení řízení přístupů a politik, segmentace sítí, revize prostupů do internetu, implementace XDR systémů, školení a vzdělávání, aktualizace systémů, vytvoření DR a BC plánů... atd.;

- kromě implementace systémů KB je třeba **revidovat celkovou ICT architekturu** ... a promítnout do podmínek případných dotačních titulů
- **spolupráce/kooperace** zejména při budování služeb externích SOC - efektivita, (ne)dostupnost pracovníků, sdílení informací, případně hierarchická struktura SOC
- implementace **rozpoznání a analýzy proprietárních protokolů** do XDR systémů
- **izolace neošetřitelných/neaktualizovatelných systémů** (do budoucna snižovat jejich množství)
- **definování standardů kybernetické bezpečnosti přístrojového vybavení** a jejich vyžadování/prosazování při nákupu nových přístrojů
- **definování bezpečnostních standardů služeb** podpory a servisu medicínských přístrojů, zpracování dat + důsledné vyžadování plnění standardů při nákupu služeb

opatření pro specifické podmínky zdravotnických zařízení



Rostislav Frys
rostislav.frys@quantien.eu

DĚKUJI ZA POZORNOST

Poděkování za spolupráci: