Thomayerova nemocnice
Vídeňská 800, Praha 4, 140 59

Informační bezpečnost v praxi velké nemocnice

Ing. Vladimír Rous, MBA
CIO
Mgr Vladimír Vocetka

Toky v nemocnici

Hmotný tok

- přemisťováním věcí, materiálů nebo osob

Procházejí branami po

- Inženýrských sítích
- Do skladů a na pracoviště

Informační tok

- předávání informací od zdroje k cíli

firewally do

- Počítačových sítí
- Do úložišť a PC

Zabezpečení toků:

Hmotný tok

- Hmotná odpovědnost
- Klíčové systémy a identifikační karty
- Chráněná pracoviště

Informační tok

- Odpovědnost za informace
- Přístupová oprávnění a hesla
- Antivirové programy na PC

- **Smluvní vztahy s dodavateli**
- **Školení uživatelů**

Jak připravit uživatele ICT na obranu proti klasickým hrozbám ?

- Uživatelské desatero
- Základní uživatelské postupy údržby a ochrany
- Zabezpečení dokumentů MS Office
- Rizika elektronické komunikace
- Co je antivir a antispam
- Bezpečnost užívání internetu
- Rizika na sociálních sítích
  - **Na učebně i v e-kurzech**

Ošetření krizových situací

Hmotný tok

- Živelná pohroma
- Hromadná havárie
- Teroristický útok

- Krizový plán v rámci IZS

Informační tok

- Kybernetický útok

- Krizový plán v rámci ISMS

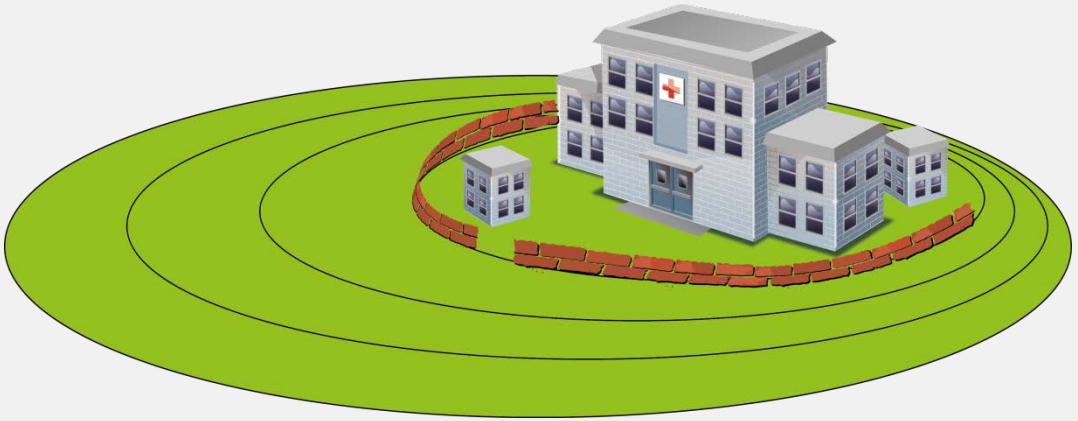
Jsou reálné kybernetické hrozby vně nemocnice?

Útok na poskytovatele služeb

- **Státní instituce**
  - datové schránky, e-preskripce
- **Provozovatele aplikací**
  - e-PACS, REDIMED, dodavatele ICT služeb
- **Zdravotní pojišťovny**
- **Telekomunikační operátory**
- **Banky a** další

Vznik kybernetických hrozeb uvnitř perimetru nemocnice

- Nevzdělaný, nevšímavý uživatel
- Nedisciplinovaný - podle zkušeností ze světa 80% dat odcizili zaměstnanci
- Záškodník - **více než 70% útoků přichází z vnitřní sítě LAN / WAN**



Jak tyto hrozby v perimetru eliminovat?

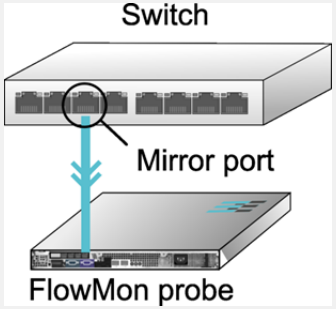
Hmotný tok

Kamery

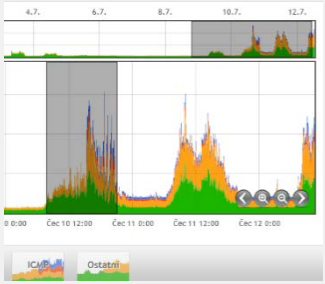
Analýza chování

Informační tok

Sonda



Analýza chování

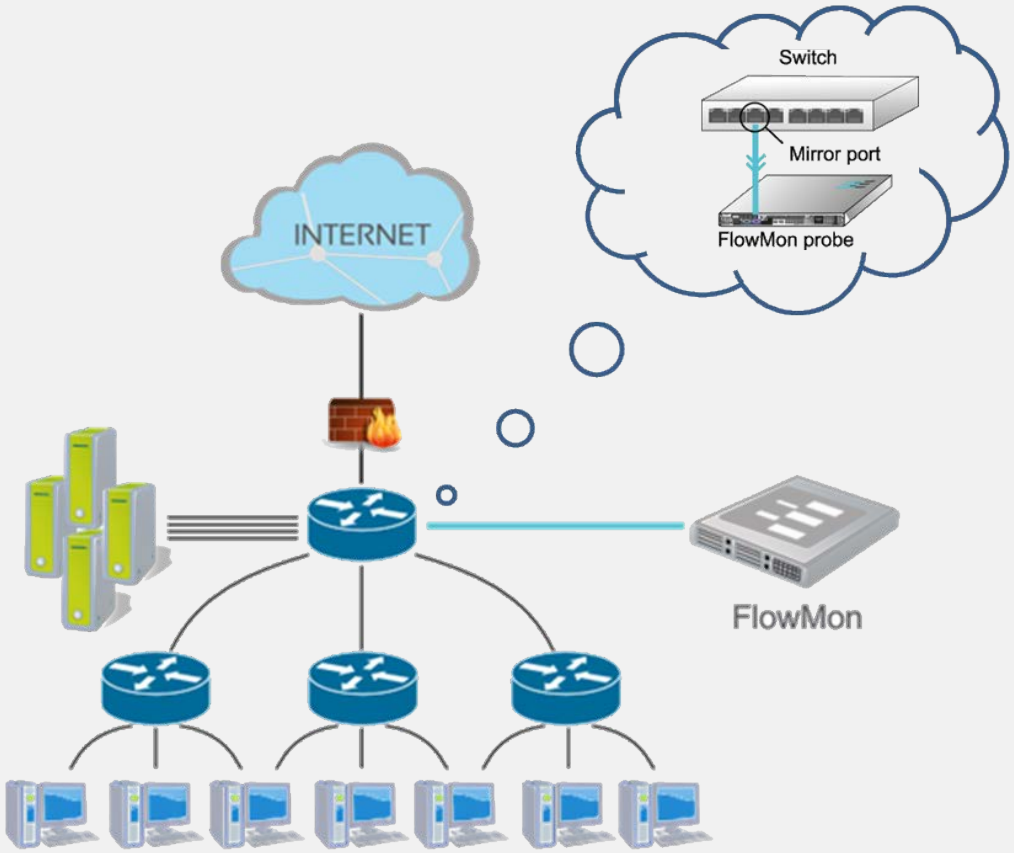


Česká (moravská) invence snoubená s technologií InterSystems z USA vytvořila chytrého „nastražušáka“

- TIL – transparentní intenzionální logika - teoretický základ prof. Tichého
- Umělá inteligence Mycroft Mind – Staníček, Procházka – MU Brno
- Behaviorální analýza sítí pro potřeby Pentagonu – výrobek spin-off MU Brno
- FlowMon sonda – produkt fy INVEA-TECH

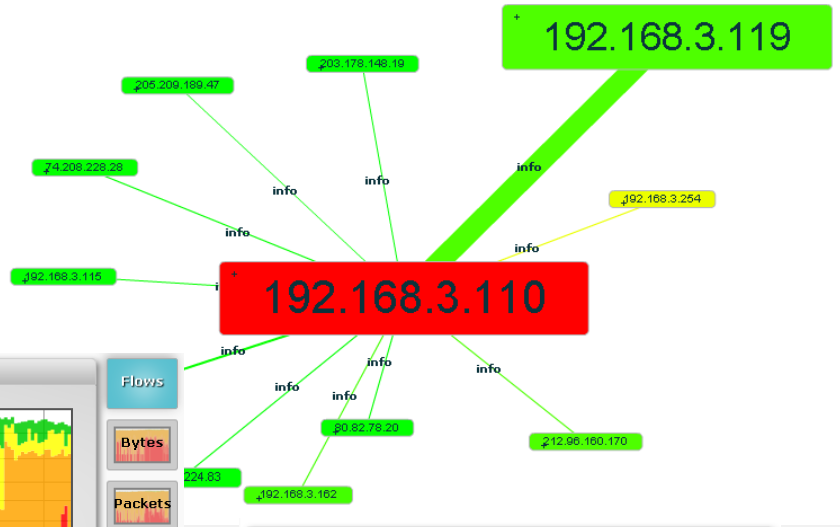
Co se skrývá uvnitř informačních toků v TN?

To sleduje pasivní a „neviditelná“ sonda Flowmon



Co vidíme, jaké jsou výstupy ?

- Vizuální analýza
  - Interaktivní vizualizace
  - Dashboardy a reporty

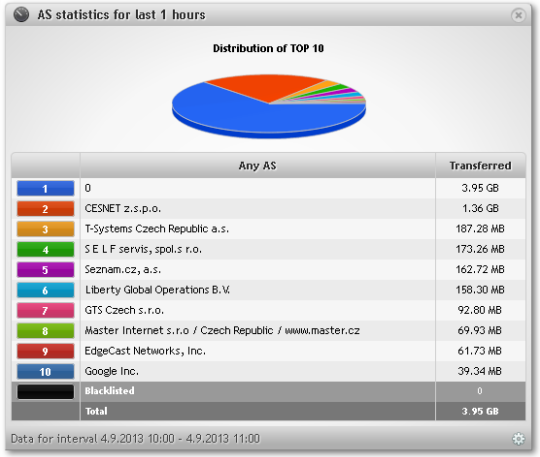


Traffic statistics (2013-05-06 10:35 - 2013-05-06 11:25)

Priority	Flows	Average flows	Bytes	Average bytes	Packets	Average packets
High priority	10.9 k flows	3.623 flows/s	295.2 MiB	100.8 KiB/s	456.1 k packets	152.0 packets/s
Medium priority	15.9 k flows	5.284 flows/s	24.1 GiB	8.2 MiB/s	45.0 M packets	15.0 k packets/s
Low priority	168.3 k flows	56.098 flows/s	1.7 GiB	578.1 KiB/s	3.2 M packets	1.1 k packets/s
Legitimate traffic	264.3 k flows	88.102 flows/s	3.5 GiB	1.2 MiB/s	5.8 M packets	1.9 k packets/s
Total traffic	459.3 k flows	153.107 flows/s	29.5 GiB	10.1 MiB/s	54.4 M packets	18.1 k packets/s

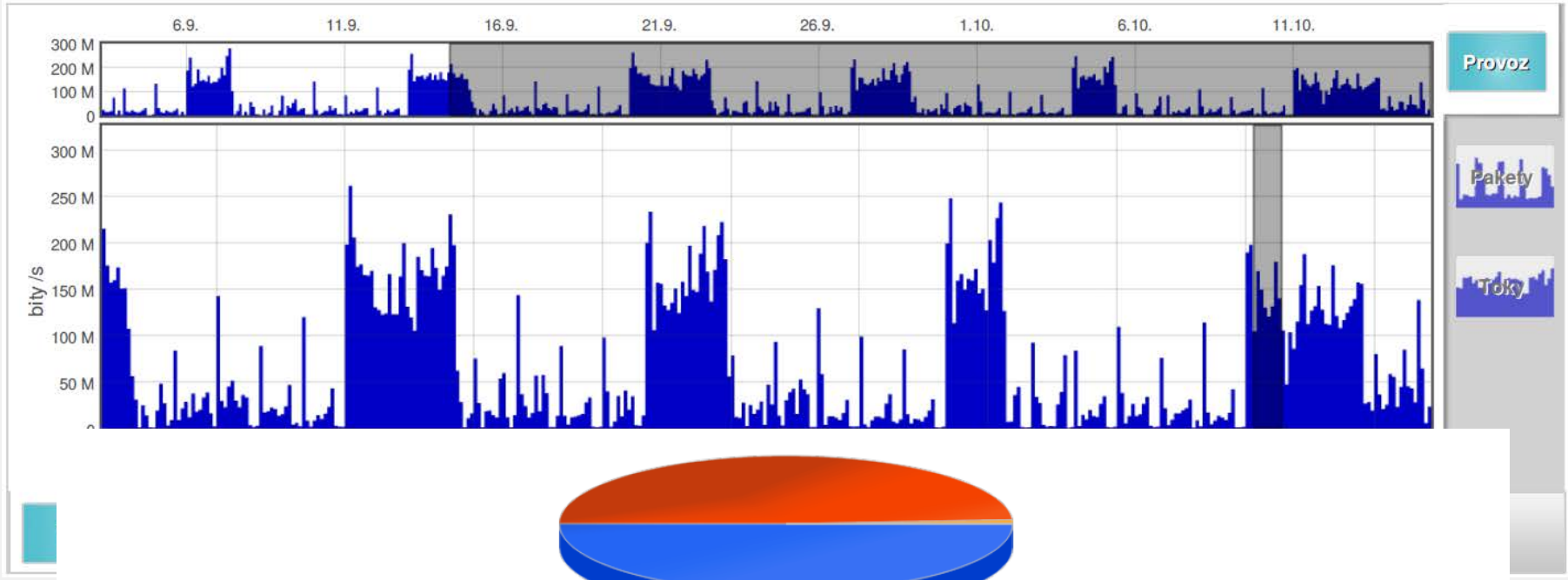
Top 10 event types by priority (2013-05-06 10:35 - 2013-05-06 11:25)

SMTP anomaly (OUTSPAM)	**57** events
SSH attack (SSHDICT)	**9** events
RDP attack (RDPDICT)	**1** events



Co můžeme rozpoznat?

- Špatná odezva sítě v důsledku přetížení



Barva	Počáteční čas	Trvání	IP protokol	IP adresa	Toky	Pakety na vstupu	Bajty na vstupu	Paketů za sekundu	Bitů za sekundu	Bajtů na paket
1	11.10.2013 4:29:56	15h, 37m, 12s	všechny	10.[redacted]	6.07 K (100.0%)	598.8 M (100.0%)	834.11 GB (100.0%)	10648	127415809	1495
2	11.10.2013 4:29:56	15h, 37m, 12s	všechny	10.[redacted]	4.91 K (80.9%)	587.07 M (98.0%)	817.95 GB (98.1%)	10440	124948302	1496
3	11.10.2013 4:31:14	12m, 17s	všechny	10.[redacted]	472 (7.8%)	11.73 M (2.0%)	16.15 GB (1.9%)	15896	188115446	1479
4	11.10.2013 13:14:15	6h, 45m, 59s	všechny	10.[redacted]	330 (5.4%)	578 (0.0%)	43.19 KB (0.0%)	0	14	76

Systémové řešení: Zavedení ISMS Information Security Management System

- **Identifikovat**
- **Kategorizovat** – přiřadit váhy
- **Vytvářet havarijní plány** pro eliminaci různých útoků
- **Aktualizovat legislativu** (směrnice) a důsledně kontrolovat její dodržování
- **Školit uživatele** ICT systémů

Školení nového zaměstnance: „Akčního nastražušáka“

- Reakce ve zlomku sekundy
- Schopnost učit se z historie
- Vnímat Národní (evropské) centrum kybernetické bezpečnosti

URNA nepřispěchá !

Ochrana informací vyžaduje alokaci zdrojů

- **Personální** – manažer kybernetické bezpečnosti
  - Hlídání a dozor nad systémy
  - Styk s Národním centrem kybernetické bezpečnosti
  - Zavedení programů školení a zvyšování informovanosti
- **Finanční**
  - Hw + Sw
  - Služby

Jednejme bez otálení !

Kybernetické útoky jsou realitou

Začínají být cenově dostupné pro širokou zločineckou veřejnost a magory všech druhů!

Otázky?

Děkuji za pozornost