

Kybernetická bezpečnost krajského zdravotnictví

Petr Pavlinec, Kraj Vysočina

Klíčové okamžiky kyberbepečnosti na Vysočině

- 2011 – projekt a pracovní skupina eCRIME (PCR, Wales)
- 2012 – technická i metodická spolupráce s CESNETem (FTAS, FLAB)
- 2013 – vznik pozice (kyber)bezpečnostního analytika kraje, GARTNER
- 2014 – strategie elektronické bezpečnosti kraje, vznik projektu KPBI
- 2015 – formální zavedení ISMS do celého úřadu
- 2017 – certifikace ISO27001, hloubkové penetrační testy CESNET FLAB
- 2018 – projekt IROP – TCK – bezpečnost
- 2019 – vznik pozice bezpečnostního analytika pro příspěvkové organizace
- 2020 – spoluzaložení hSOC



Kyberbepečnost v krajském zdravotnictví

- Strategie kyberbezpečnosti kraje – jasná definice prostoru PO a kraje
- Obrana krajské infrastruktury
 - TCK – bezpečný provoz společných aktiv (záloha ERP, eAmbulance...)
 - ROWANet – FTAS (NetFlow), antiDoS FW, monitoring, skenování (Shodan), uzavřené sítě pro citlivou komunikaci
 - Cesnet – ENEM, FENIX (bezpečná VLANa), eIGER (zálohování)
- Pravidelné penetrační testy
- Speciální dotační titul pro metodiky, HW a SW
- Zavedení ISO 27001 v ZZS
- Začlenění krajských nemocnic pod ZKB
- Společný eLearning



Bezpečnost je o spolupráci a sdílení

- Kyberbezpečnost je velmi komplexní téma
- Je nás (ajťáků, bezpečáků) málo
- Bezpečnost je drahá, nekonečně drahá
- Hrozby a útoky jsou mnohdy plošné a týkají se mnoha institucí
- Klíčové je rychlé předávání informací, mnohdy citlivých
- V jednotě je síla
- Druhá strana stále je stále lépe organizovaná
- Stále dokola postupujeme metodou slepých uliček



V čem spolupracovat a sdílet?

- Znalosti – vzdělávání, dobré praxe, metodiky a prevence
- Sdílení kapacit kvalifikovaných profíků (společné SOC a CSIRT týmy)
- Společná obrana perimetru na sdílené infrastruktuře
- Využívání neveřejných sítí
- Integrace IS sdílení dat mimo veřejné sítě
- Křížové auditování a testování bezpečnosti
- Vzájemný monitoring a zálohování
- Společné systémy včasného varování



Co tedy pro to děláme?

- Společně s dalšími subjekty (IKEM, Homolka, krajské nemocnice, CESNET, CVUT a další) jsme iniciovali vznik komunity - **hSOC**
- Společně pořizujeme klíčové bezpečnostní technologie (FW, proxy, IDM, analýza síťového provozu, WAN IPS)
- Budujeme dedikované privátní spoje a virtuální LANky
- Realizujeme projekty prevence a vzdělávání – www.kpbi.cz
- Učíme se od špiček – Cesnet, Taiwan, Estonsko, Evropská komise - a snažíme se nevymýšlet vymyšlené
- **Zapojení do hSOC Taiwanu - MoU**



Stav aktivity hSOC



Spolek pro ochranu osobních údajů



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY



PRACOVNÍ SKUPINY

<https://hsoc.cesnet.cz/cs/skupiny>

hSOC - Working group

- **Hlavní komunikační kanál řídicího výboru hSOC**
- účel: koordinace hSOC a signatářů iniciativy

hSOC - EMERGENCY

- **Emergency komunikační kanál hSOC**
- účel: předávání varování o aktuálních bezpečnostních hrozbách

hSOC - TECH

- **technická pracovní skupina pro řešení technických aspektů**
- účel: technické aspekty a standardy.

hSOC - MANAGEMENT

- pracovní skupina pro **Governance hSOC**
- účel: řeší právní, legislativní, finanční a institucionálních aspektů hSOC
- sdílení **best-practices**

hSOC - HR

- pracovní skupina **Human resources / Education**
- účel: rozvoj lidských zdrojů a vzdělávání v oblasti kybernetické bezpečnosti

CO JE A NENÍ CÍLEM

hSOC je...

- **Platforma** pro výměnu informací a dobré praxe
- **Varovný** a **koordinační komunikační kanál**
- Platforma pro **provoz sdílených služeb a technologií**
- Komunita IT a bezpečnostních profesionálů a nadšenců
- **Prostor pro vzdělávání**

hSOC není...

- **Univerzální řešení bezpečnosti zdravotnického zařízení**
- Subjekt
- Dohledové bezpečnostní centrum

ZAPOJENO: 56

- Podpora a zapojení NUKIB, NAKIT, OHA MVČR, ...
- **Vyhrazená síťová infrastruktura (HSOC-VRF)**
- **Sdílení know-how a lidských kapacit**
 - best-practice, koncepce a design architektury
 - školení, semináře a workshopy
 - technologické standardy
 - **plán vzniku společného distribuovaného CSIRT týmu, SOC**
- **Nastavení workflow a procesů u zapojených subjektů**
- **Emergency komunikační kanály**
 - mailing-listy, videokonferenční systém, datové úložiště

UZAVŘENÁ BEZPEČNÁ SÍŤ hSOC

- 7 nemocnic zapojeno

FAKULTNÍ
NEMOCNICE
U SV. ANNY
V BRNĚ



FAKULTNÍ NEMOCNICE*
OLOMOUC



VFN PRAHA
VŠEOBECNÁ FAKULTNÍ
NEMOCNICE



ÚVN

ÚSTŘEDNÍ VOJENSKÁ NEMOCNICE
Vojenská fakultní nemocnice Praha



NEMOCNICE
JIHLAVA

NEMOCNICE
HAVLÍČKŮV
BROD

- další v procesu připojování

FAKULTNÍ
NEMOCNICE
BRNO

FAKULTNÍ
NEMOCNICE
BULOVKA



- Monitorovací a bezpečnostní nástroje

- Společné politiky a pravidla

- Striktnější pravidla a politiky

hSOC VRF

- **Geografická redundance přepojení do Internetu ve dvou lokalitách**
- **Ochrana**
 - proti podvržení IP adres (IP spoofing),
 - proti podvržení oznamovaných prefixů od peering-partnerů,
 - proti amplifikačním (volumetrickým) DDoS útokům,
 - proti agresivním i pomalým scanům,
 - nástroji pro uživatele pro analýzu a regulaci svého provozu v síti e-infrastruktury CESNET,
 - automatickým přesměrováním provozu k vyčištění v jádru globálního internetu (celosvětová mitigace vůči detekovaným zdrojům nežádoucího provozu.
- **Tvrději nastavené limity a politiky**
 - Možnost omezení, zahazení útoku ještě na páteřní síti

V současnosti denně cca 80 – 90 tis. detekovaných a automaticky mitigovaných hrozeb na perimetru sítě

DALŠÍ AKTIVITY A PLÁNY

- Standardy
- Distribuovaný CSIRT, SOC tým
- Best practice sharing
- Komunitní emergency platforma a komunikační postupy

Podpora a pomoc komunitě

<https://hsoc.cesnet.cz/cs/join>

Děkuji za pozornost....

Petr Pavlinec

<https://hsoc.cesnet.cz/>

www.kr-vysocina.cz/it

www.rowanet.cz