cesnet

HSOC – technická skupina

- představa o fungování
- výchozí návrh tématických okruhů

Tomáš Košňar
CESNET

2020/11/27
VC, hsoc-tech

- *vybudování komunitního HSOC týmu/pracoviště → společná péče o "bezpečnost" komunitní infrastruktury zdravotnických pracovišť*
- technické a organizační prostředky, podpora
  - logicky oddělená modelová infrastruktura na bázi e-infrastruktury CESNET
  - optimalizace vnitřní infrastruktury zdravotnických zařízení
  - vytvoření a postupné uvedení do praxe modelového CSIRT komunitního týmu
- postup v rámci hsoc-tech
  - **nosná témata → společné semináře-workshopy, sdílení zkušeností**
  - **diskuze → shoda → formulace "doporučení" → implementace**
    - + technické oblasti, synergie s dalšími aktivitami ~ NÚKIB, NAKIT, MVČR, MZČR,..
  - **praktická stránka věci** (reálný svět, cvičení-testování) → vyšší odolnost, efektivnější IH, „infrastruktura pod kontrolou“

hsoc-tech – návrh tématických okruhů

- **architektura sítě organizace** (vnitřní síť)
- fyzická infrastruktura, strukturovana kabelaz, opticka infrastruktura, technologie , kategorie kabelů, topologie
- struktura – L2, L3, IPv4, IPv6, velikost dílčích celků
- souvislosti a adaptivita architektury na provozní potřeby vyvíjející se v čase
- typické dílčí celky
  - síťové prvky, DC, výpočetní a úložná infrastruktura, přístroje, zaměstnanecká síť, síť pro připojení pacientů, pevná infrastruktura, WiFi
  - přístup k, vzájemné propojení/oddělení dílčích celků
    - politika
    - řízení provozu
  - obecný přístup zařízení do sítě
    - MAC/port based security, 802.1x apod.

hsoc-tech – návrh tématických okruhů

- **vnější síťový perimetr**
- architektura (FW, DMZ apod.)
  - průchodnost
  - specifická řešení (potřeba vysokých kapacit, dedikované propojení s partnerskou sítí, službou apod.)
- strategie/politika nastavení
  - služby pro vnější svět
  - přístupy pro zástupce dodavatelů
  - přístupy zaměstnanců z vnějších sítí
  - přístupy z vnitřní sítě (politika, techniká opatření ~ *ošetření „reakce“ na phishing apod.*)

hsoc-tech – návrh tématických okruhů

- **správa výpočetních prostředků**
  - servery, úložiště, pracovní stanice, osobní uživatelské prostředky (organizace/soukromé)
  - auto-konfigurace, síťová nastavení, hromadná konfigurace, automatická správa OS, aplikací, zálohování
  - přístupová práva, oprávnění ke správě, soukromé prostředky, organizační a technická opatření
  - on-host FW, antiviry, ...
- **podpůrné infrastrukturní služby**
  - DNS, mail (antispam), distribuce konfigurací, AAI, hromadná správa, ...

hsoc-tech – návrh tématických okruhů

- **monitoring, regulace provozu**
  - vhodná/nezbytná místa (topologie, vrstvy)
  - detekce anomálií, regulace provozu (na základě architektury/přednastavení, ručně, adaptivně, nástroje)
  - logy, hlášení, zpracování informací o událostech, sdílení informací (uvnitř, vně)
- **testování odolnosti**
  - externí, interní
- *operativa, dohled, CSIRT, ...HSOC*
  - *workflow řešení událostí, incidentů*
  - *konstituence CSIRT, HSOC, rozdělení činností, způsoby komunikace,...*
- *další na základě diskuze..*

hsoc-tech – návrh postupu

- **diskuze**
  - upřesnění, doplnění
  - volba témat pro první semináře
    - architektura sítě + vnější perimetr sítě ?
  - přibližný termín prvního semináře (vzhledem k dalším navazujícím informacím návrh na leden 2021)