Memorandum

Iniciativy pro koordinaci kybernetické bezpečnosti resortu zdravotnictví – hSOC

Září 2020

Aktuální stav, důvody pro vznik iniciativy:

- Zdravotnictví v ČR čelí rostoucímu riziku kybernetických útoků.
- Jsou velké rozdíly v úrovni IT podpory a potřebami jednotlivých nemocnic.
- Existují velké rozdíly ve vnímání kybernetické bezpečnosti jako priority ze strany managementu nemocnic popř. zřizovatelů.
- Chybí systémové a koncepční pojetí zajišťování kybernetické bezpečnosti jak jednotlivých nemocnic, tak resortu jako celku.
- Chybí sdílená vize, jak využít výhody digitálních technologií k transformaci zdravotnictví.
- Chybí diskuze jak využít sdílenou infrastrukturu (e-infrastruktura Cesnetu, datová centra nemocnic, státní a regionální sítě, technologická centra krajů…).
- Problematika kybernetické bezpečnosti je ve zdravotnictví zásadně personálně a finančně podhodnocena
- Existuje možnost čerpání značných finančních prostředků (typicky investičních, EU fondy) a je riziko jejich neefektivního použití.
- Využití výsledků dotazníkového šetření MZdr ke kybernetické bezpečnosti v nemocnicích (zpětná vazba není) k možné realizaci nápravných opatření a odůvodnění peněz z fondů.
- Reálná hrozba kybernetického napadení jednotlivých nemocnic i většího počtu zdravotnických zařízení současně roste den ze dne.

Vize – Cílový stav

Poskytovatelé zdravotních služeb provozující bezpečné informační technologie s dostatečným technickým a personálním zázemím s podporou centralizované ochrany typu SOC.

Návrh kroků pro dosažení cílového stavu

- Vytvoření zájmové platformy pro podporu koordinace kybernetické bezpečnosti v rezortu Ministerstva zdravotnictví.
- Vznik pozice koordinátora kybernetické bezpečnosti ministerstva zdravotnictví, přímo podřízeného ministru.
- Níže podepsaní signatáři iniciativy navrhují do této pozice Ing. Petra Pavlince.
- Vznik komunitního týmu kybernetické bezpečnosti zdravotnictví vedeného koordinátorem kybernetické bezpečnosti MZdr.
- Mezi očekávanými výstupy tohoto týmu jsou:

    - Vytvoření základních jednotných pravidel bezpečnosti informací (metodiky pro analýzu rizik, hodnocení aktiv, hodnocení informací atd.) s maximálním využitím existující dobré praxe (metodiky NUKIB, NAKIT, ZoKB, VoKB, ČSN 2700X).
    - Definice základní podmínek personálních a finančních zdrojů pro realizaci navrhovaných opatření.
    - Návrh účelu, cílů a právní formy subjektu, prostřednictvím kterého by bylo možné realizovat společné aktivity důležitých aktérů v oblasti kybernetické bezpečnosti zdravotnictví (státní a krajské nemocnice, stát, kraje, akademický sektor/školství, Cesnet,…) – subjektu typu SOC (Security Operation Center).
- Sdílení dobré praxe v oblasti kybernetické bezpečnosti.
- Sdílení dobré praxe při pořizování a zavádění nových technologií.
- Ustanovení komunikačních kanálů pro efektivní předávání informací a varování v oblasti kybernetických hrozeb ve zdravotnictví.
- Iniciace vzniku bezpečné uzavřené datové sítě a sdílených služeb státem zřizovaných nemocnic na bázi služeb sdružení CESNET.
- Vznik společného výzkumného pracoviště MZdr a CIIRC ČVUT pro kybernetickou bezpečnost.

Mezi možné činnosti navrhovaného subjektu (SOC) by mělo patřit například:

- Bezpečnostní aspekty provozu a monitoringu bezpečné síťové infrastruktury.
- Koordinace systému včasné výstrahy před hrozbami.
- Bezpečnostní aspekty provozu vybraných sdílených informačních systémů resortu zdravotnictví (např. Národní kontaktní místo elektronického zdravotnictví).
- Příprava vzdělávacích programů zaměstnanců (včetně manažerů) poskytovatelů zdravotních služeb v oblasti kybernetické bezpečnosti. Možnost centrálního vzdělávání (e-learning) + místní odlišnosti (školení). Minimálně povinná položka plánu vzdělávání.
- Poskytování služeb laboratoře pro bezpečnostní testování a certifikaci.
- Vznik sdíleného akreditovaného CSIRT/response týmu.

Signatáři iniciativy

Jméno	**Instituce**	**Podpis**
Petr Pavlinec	Kraj Vysočina	Ing. Petr Pavlinec Digitálně podepsal Ing. Petr Pavlinec Datum: 2020.09.22 22:05:21 +02'00'

