**Příloha č. 3. Popis stávajícího stavu**

**k Zadávací dokumentaci**

**ve veřejné zakázce**

**„Kybernetická bezpečnost Nemocnice Pelhřimov“**

Obsah

[1. Organizační struktura Nemocnice Pelhřimov a počty pracovníků 3](#_Toc142044104)

[2. Aplikační vybavení 3](#_Toc142044105)

[3. ICT prostředky 4](#_Toc142044106)

[4. Lokální technické prostředky 5](#_Toc142044107)

# **Organizační struktura Nemocnice Pelhřimov a počty pracovníků**

Organizační struktura Nemocnice Pelhřimov a počty pracovníků je uvedeno v následující tabulce

|  |  |
| --- | --- |
| **Položka** | **Popis** |
| Všeobecní informace | Nemocnice Pelhřimov, příspěvková organizace, je hlavním poskytovatelem zdravotních a sociálních služeb v okrese Pelhřimov a nejbližším okolí. V současné době Nemocnice Pelhřimov zaměstnává cca 700 zaměstnanců. Nemocnice provozuje 294 lůžek akutní a 46 lůžek následné péče. V roce 2021 nemocnice ošetřila 11278 pacientů na 10lůžkových odděleních 60404 pacientů v 56 odborných ambulancích. Základem ICT infrastruktury je datové centrum v hlavní serverovně ICT. Technickou infrastrukturu Nemocnice, lze v krátkosti popsat jako plochou, lokální počítačovou síť s cca 350 počítači, 20 hardwarovými, 30 virtuálními servery a 37 datových switchů. Celá síť slouží jak všem interním uživatelům, tak zároveň nemocnice poskytuje svým klientům a návštěvníkům služby spojené s přístupem na veřejný internet. |
| Celkový počet zaměstnanců využívající IS | cca 700 |

# **Aplikační vybavení**

Nemocnice Pelhřimov provozuje informační a komunikační systémy, které budou dotčeny realizací bezpečnostních opatření, která jsou předmětem této veřejné zakázky:

| **Název** | **Popis** |
| --- | --- |
| Vmware vSphere 7 | Virtualizační platforma použitá pro provoz všech kritických serverů Nemocnice Pelhřimov |
| FONS –  Enterprise -Stapro | KIS – klinický informační systém – centrální databázový systém klinických informací o pacientech. Včetně importů výsledků vyšetření z laboratorních systémů a výsledků obrazové dokumentace (PACS). KIS komunikuje s zdravotnickými přístroji. Jeho integrální součástí je modul RIS – radiologický informační systém pro řízení oddělení zobrazovacích metod (RDG). Modul řeší systém žádanek, popisů a výsledků vyšetření pacientů RDG oddělení včetně napojení na worklisty jednotlivých modalit |
| Stravovací systém – Stapro | Stravovací informační systém, objednávání zaměstnanecké stravy |
| OpenLIMS | LIS – laboratorní informační systém centrální biochemické, mikrobiologické, hematologické a transfuzní laboratoře, které řeší výsledky vyšetření pacientů Nemocnice Pelhřimov i externích partnerů. Výsledky jsou importovány z analyzátorů nebo zadávány ručně a poté vyhodnocovány. Systém výsledky exportuje žadatelům elektronickou cestou vlastním systémem. |
| Mediox | Informační systém lékárny a SZM – sklad a výdej léčivých přípravků (recepty, vnitřní zásobování), evidence a vykazování ředění cytostatik |
| Vema | Mzdový systém a personalistika – cloudové řešení. |
| MEDIX | Informační systém centrálních operačních sálů a centrální sterilizace |
| Marie PACS | Informační systém zpracování, archivace, distribuce obrazových dat RDG |
| DMS-Software 602 | Informační systém pro řízení dokumentů, smluv a uložiště dokumentů (DDA) |
| Amadeus | Informační systém pro transfuzní službu |
| eMEDOCS | Odesílání a přijímání zdravotnické dokumentace |
| Microsoft AD | Správa identit, uživatelů, skupin a počítačů |
| AC identita – IDM | Primární správa identit, uživatelů, skupin a počítačů |
| QI | Ekonomický informační systém – účetnictví, cashflow, majetek, sklady, žádanky |
| Kernun UTM FW | Systém zabezpečení perimetru, centrální firewall, VPN |
| ShiftMaster – Ivar | Docházka a plánovaní služeb |
| Fama+ | Správa zdravotnických přístrojů, facility managment, správa budov. |
| PRTG | Monitoring stavu sítě |
| ESET Protect | Centrální správa antivirové kontroly koncových stanic |
| Epacs,Redimed | Systémy pro výměnu obrazové digitální dokumentace |
| IceWarp - Apptocloud | Mailový systém, správa a sdílení kontaktů a kalendářů |
| LAN infrastruktura | Komunikační infrastruktura Nemocnice Pelhřimov |

# **ICT prostředky**

Infrastruktura ICT nemocnice je tvořena interní sítí využívanou zaměstnanci a klienty nemocnice. Je provozován nemocniční informační systém a několik dalších informačních systémů, které slouží pro celkový chod nemocnice. O celkovou správu, provoz a bezpečnost informační a komunikační infrastruktury nemocnice se stará oddělení informačních a komunikačních technologií, spolu s externími smluvními partnery.

Firewall Nemocnice Pelhřimov – přístup zařízení ve vnitřní síti a internetu je řízen firewallem Kernun UTM.

Vzdálený přístup interních a externích uživatelů do vnitřní sítě je řešen pomocí OpenVPN serveru, který je součástí nedostačujícího FIREWALLu.

Při přístupu zařízení do sítě nemocnice není ověřena identita.

Připojení zařízení do KS není dostatečně na L2 vrstvě monitorováno.

Ve stávající sítí Nemocnice Pelhřimov jsou zapojeny switche Cisco, HP,3Com a Avaya různého typového označení a data pořízení, které nedisponují dostatečnými bezpečnostními funkcemi pro zabezpečení LAN provozu (dynamická ARP inspekce, IP source guard atd.) a plně nepodporují ověřování koncových uživatelských zařízení pomocí protokolu 802.1x.

V současné době je provoz zajištěn ze dvou datových center (technologických místností), které jsou vzájemně propojeny na úrovni CORE switchů, ale nejsou pokryta rizika spojená výpadkem a zajištěním vysoké dostupnosti dat.

V současně době nemá Nemocnice Pelhřimov možnost dohledat informace o aplikacích, které nejvíce vytěžují síť.

Nemocnice postrádá nástroj, který by na základě chování uživatelů v síti byl schopný identifikovat možná bezpečnostní rizika.

Datové propojení mezi přístupovými přepínači a distribuční vrstvou či páteří sítě jsou ve většině případů realizovány pouze jedním datovým spojem. Není zde k dispozici záložní trasa, takže ani nelze zajistit vysokou dostupnost pro přístup k primárním aktivům v LAN síti.

Stávající antivirová řešení, na uživatelských zařízeních nejsou schopna řešit problematiku „zero day“ útoků a hrozeb.

Není implementována technologie DLP pro ochranu citlivých dat, a to jak na koncových stanicích, serverech nebo perimetru.

Nemocnice Pelhřimov nerealizuje dvou faktorovou autentizaci

Způsob zálohování je na minimální úrovni a neodpovídá požadavkům ZKB (off-line zálohování a ochrana proti ransomware).

Neexistuje žádný centrální LOG MANAGEMENT.

Nemocnice Pelhřimov nedisponuje efektivním nástrojem na odhalení a zastavení malwaru, který je připraven hackery na míru.

# **Lokální technické prostředky**

Správa lokálních technických prostředků je uvedena v následující tabulce.

|  |  |
| --- | --- |
| **Položka** | **Popis** |
| **Lokální pracovní stanice** | |
| Monitor – rozlišení | LCD s LED podsvícením o min. konfiguraci:  úhlopříčka min. 19” wide, rozlišení 1920x1080. |
| Typ lokální pracovní stanice | Běžné kancelářské PC s min. konfigurací:  CPU Intel i3 (i5), RAM 4 GB (max. 32 GB), disk 128 GB SSD (500 GB HDD), grafická karta integrovaná |
| Operační systém | Windows 10 Professional 32 a 64-bit |
| Správa lokálních stanic | Je řešena centrální správa politik (nastavení práv lokálních uživatelů k operačnímu systému pracovní stanice) pomocí politik a rolí.  Ochrana proti škodlivému kódu (viry, malware apod.) je centralizovaná, pravidelné aktualizace probíhají na stanicích včetně systémových záplat centrálně. |
| **Periferie lokálních stanic** | |
| Typy tiskáren | Standardní laserové tiskárny převážně formátu A4, podporující oboustranný tisk s PCL 6, doplněné multifunkčními stroji formátu A3 |