Příloha č. 1 výzvy

Technická dokumentace

I. Úvod

Tato technická dokumentace slouží jako podklad k veřejné zakázce - Odborné konzultace při realizaci projektu „Soubor bezpečnostních opatření proti nežádoucím aktivitám v síťovém prostředí Nemocnice Tábor, a.s.“

Technická dokumentace obsahuje popis současného stavu a zároveň také návrh řešení v jednotlivých oblastech, které budou řešeny v samostatné veřejné zakázce na jednotlivé dodavatele pro každou nadefinovanou oblast.

II. Popis současného stavu

LAN Nemta

Současná LAN NEMTA je topologická skoro hvězda s částečným kruhem vedení tras optických kabelů. Centrálním agregačním prvkem je modulární přepínač, který je umístěný v datovém centru společně s několika přepínači.

Topologie hvězda je následně tvořena cca dvěma desítkami DR, které jsou rozmístěny v rámci celého areálu NEMTA. Datové centrum a všechny podružné přepínače jsou napájeny ze zálohovaných okruhů a jištěny systémy UPS, a to buď centrálním nebo v některých případech lokální UPS. Fyzická kabeláž odpovídá historickému vývoji budování LAN v NEMTA. Horizontální kabeláž je tvořena především kabely CAT 5E, dále CAT 6 a v některých částech sítě také CAT 5. Optická kabeláž propojuje podružné rozvaděče s datovým centrem dle obrázku uvedeného níže.

LAN NEMTA je postavena na cca 30 aktivních prvcích převážně značky HP.
Součástí LAN NEMTA je také bezdrátová síť, která je tvořena centrální řídící jednotkou (kontrolér) a 40 Access Pointy. Tato bezdrátová infrastruktura je primárně určena pro pacienty a návštěvníky NEMTA. Pro některá technologická zařízení a vybrané zaměstnance existují dedikované autonomní access pointy, kterými je realizován přístup do interní sítě NEMTA.
Ke správě aktivních prvků je používán centralizovaný management sítě HP Intelligent Management Center.
Jednotlivé aktivní prvky jsou jednoduše propojeny jedním přípojem na úrovni rychlosti 1Gb. V současné době není nasazeno řešení typu NAC, nejsou dostatečně segmentovány jednotlivé zóny LAN NEMTA do vícenásobných demilitarizovaných zón a také nejsou definovány jednotlivé bezpečnostní profily, které by mohly být aplikovány v rámci zabezpečeného provozu KS NEMTA.

Serverová a backup infrastruktura
Síť NEMTA je postavená na technologické platformě MS Windows. Autentifikace a autorizace probíhá vůči doménovým kontrolerům MS Active Directory s řízením koncových stanic přes Group Policy (GPO). Primárním operačním systémem koncových stanic i serverového vybavení je MS Windows.
Serverové zázemí je tvořeno především 10 fyzickými servery. Na 4 těchto fyzických serverech je ve virtuálním prostředí Hyper-V provozováno dalších 13 virtuálních serverů.
V současné době se realizují zálohy prostřednictvím zálohovacího software Veeam Backup Essentials na omezené možnosti diskových úložišť jednotlivých serverů a diskového pole SYNOLOGY. Replikace virtuálních serverů na jiné servery nyní neprobíhá. NEMTA v současné době nedisponuje páskovou zálohovací mechanikou.

III. Řešené oblasti

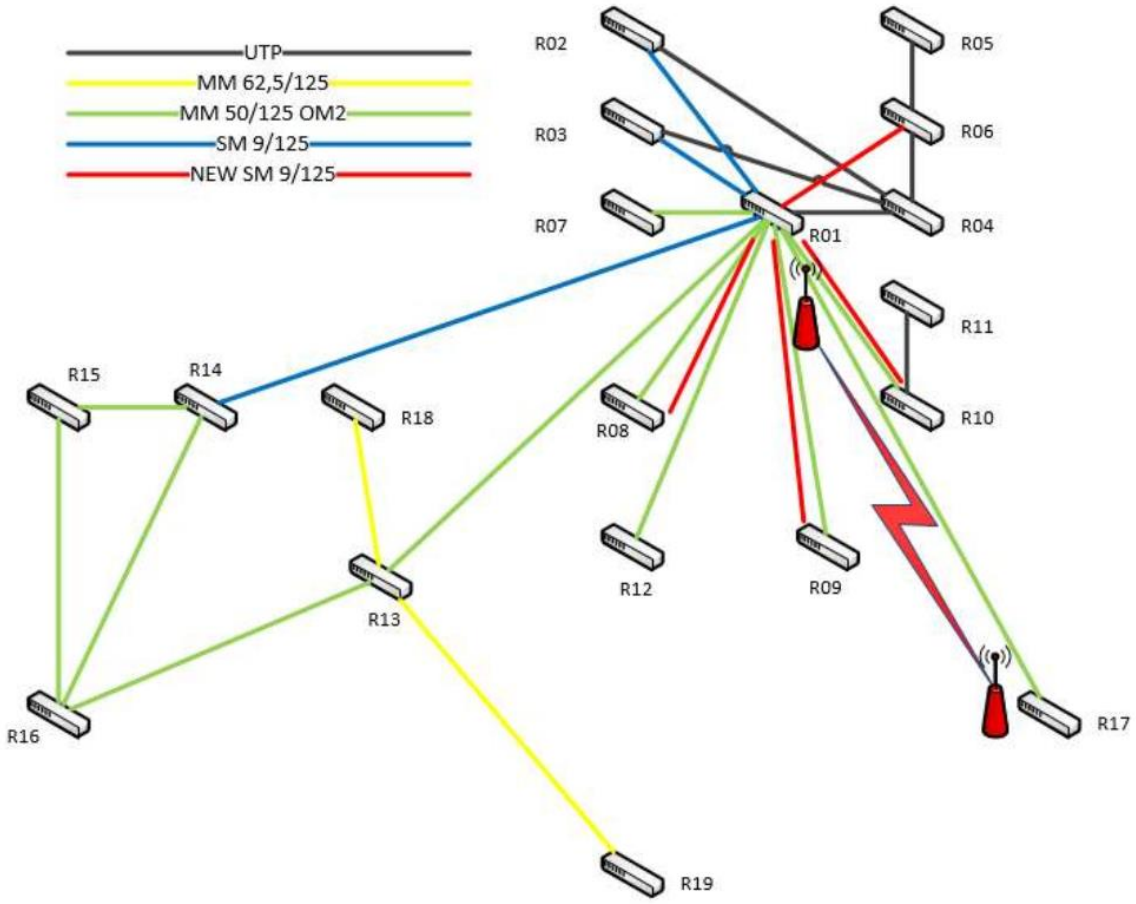
V této části technické dokumentace jsou uvedeny jednotlivé oblasti, které je nutné řešit. Všechny níže uvedené oblasti budou realizovány na základě samostatné veřejné zakázky na jednotlivé dodavatele příslušných níže vymezených oblastí. Odborné konzultační služby budou poskytovány ve všech těchto oblastech.

1. Vybudování 4 tras optického kabelu včetně zakončení, proměření a dokumentace

Za účelem minimalizace rizika výpadku LAN infrastruktury NEMTA je i s ohledem na potřebu garance dostupnosti provozu KS NEMTA plánováno redundantního propojení jednotlivých DR. Plánuje se duplicitně propojit z pohledu významnosti některých DR tyto komunikační body:

- optický kabel SM 9/125 s 12 vlákny mezi R01 a R08
- optický kabel SM 9/125 s 12 vlákny mezi R01 a R09
- optický kabel SM 9/125 s 12 vlákny mezi R01 a R10
- optický kabel SM 9/125 s 12 vlákny mezi R01 a R06
- bezdrátové spojení s rychlostí min. 1Gb na frekvenci 60-80GHz mezi R01 a R17

Topologie by tedy měla respektovat hrubý principiální návrh schéma propojení viz. obrázek níže.



2. Dovybavení síťového prostředí LAN

Pro potřebu úplné stabilní komunikace prostřednictvím KS NEMTA se plánuje dokoupení moderních bezpečnostních prvků LAN NEMTA (FW) a nasazení vícenásobné segmentace počítačové sítě s tvorbou vícenásobných demilitarizovaných zón.

NEMTA v rámci dokončení implementace komplexní finální redundance a zabezpečení provozu počítačové sítě plánuje LAN NEMTA doplnit stávající síťovou infrastrukturu o vybrané komponenty, mezi které patří zejména:

- modernizace a dovybavení LAN dalšími aktivními prvky (viz. Tabulka)

Počet	Typ
2	CORE switch 48x1Gb+4xSFP+
2	CORE switch 24xSFP+2xSFP+
8	Access switch 48x1Gb+2xSFP+
6	modul SFP SM
58	modul SFP MM
32	modul SFP+ SM

- aplikační firewally v clusteru
- rozdělení a segmentace počítačové sítě NEMTA na jednotlivé demilitarizované zóny prezentované jednotlivými VLANami (směrování, limitace, prioritizace, filtrace provozu paketů, monitorování provozu).

To vše bude organizováno prostřednictvím Active Directory na bázi přiřazených profilů k zařízení nebo k profilu oprávněného uživatele počítačové sítě NEMTA. V plánovaném řešení se počítá s instalací a konfigurací dodávaného zboží tak, že bude zajištěn cílový stav v tomto rozsahu požadovaných činností:

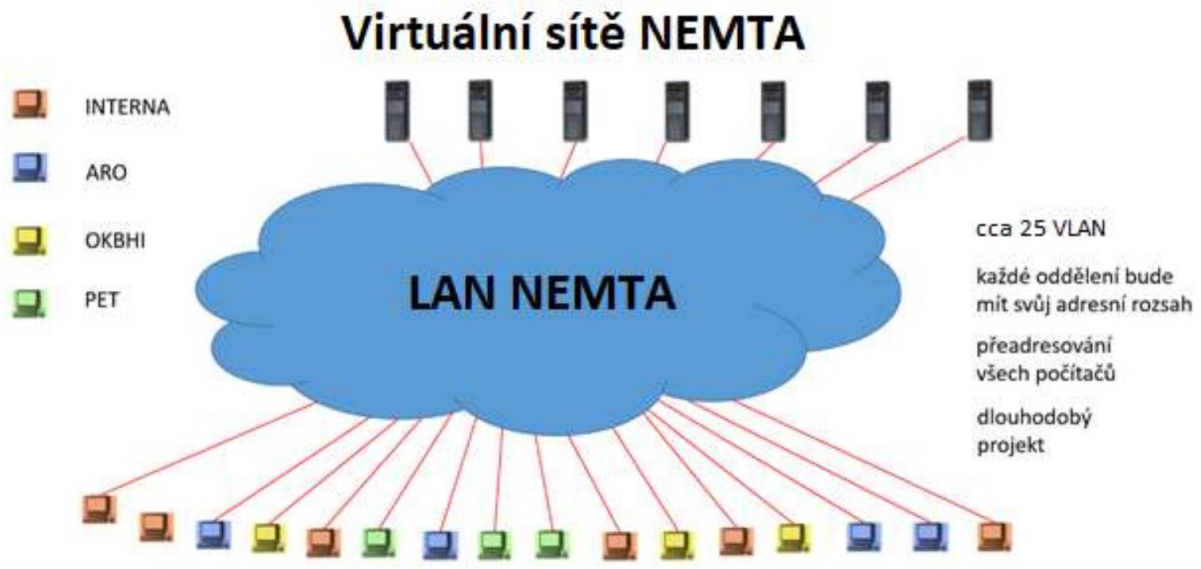
- Instalace, konfigurace a nastavení dodávaných Firewallů do cluster spojení. Následná aktualizace na nejnovější platné verze provozních SW. Následně bude aplikována definice segmentace VLAN (v počtu cca 25 nezávislých VLAN) s požadovanými vlastnostmi, kdy v rámci jedné VLANy vzniká izolovaná demilitarizovaná zóna s povolenou vybranou komunikací.

- Mezi typizované VLANy budou patřit VLANy oddělující zařízení typu management karty a aktivní prvky, servery, tiskárny, WiFi dle SSID, ostatní ICT zařízení (např. teplotní čidla), PC a NTB dle oddělení a typu přístupu uživatele, pacienti a ostatní uživatelé.

- Součástí instalace bude i integrace s AD, možnost napojení na RADIUS server a duplicitní/paralelní připojení pro více jak dva poskytovatele Internetu.

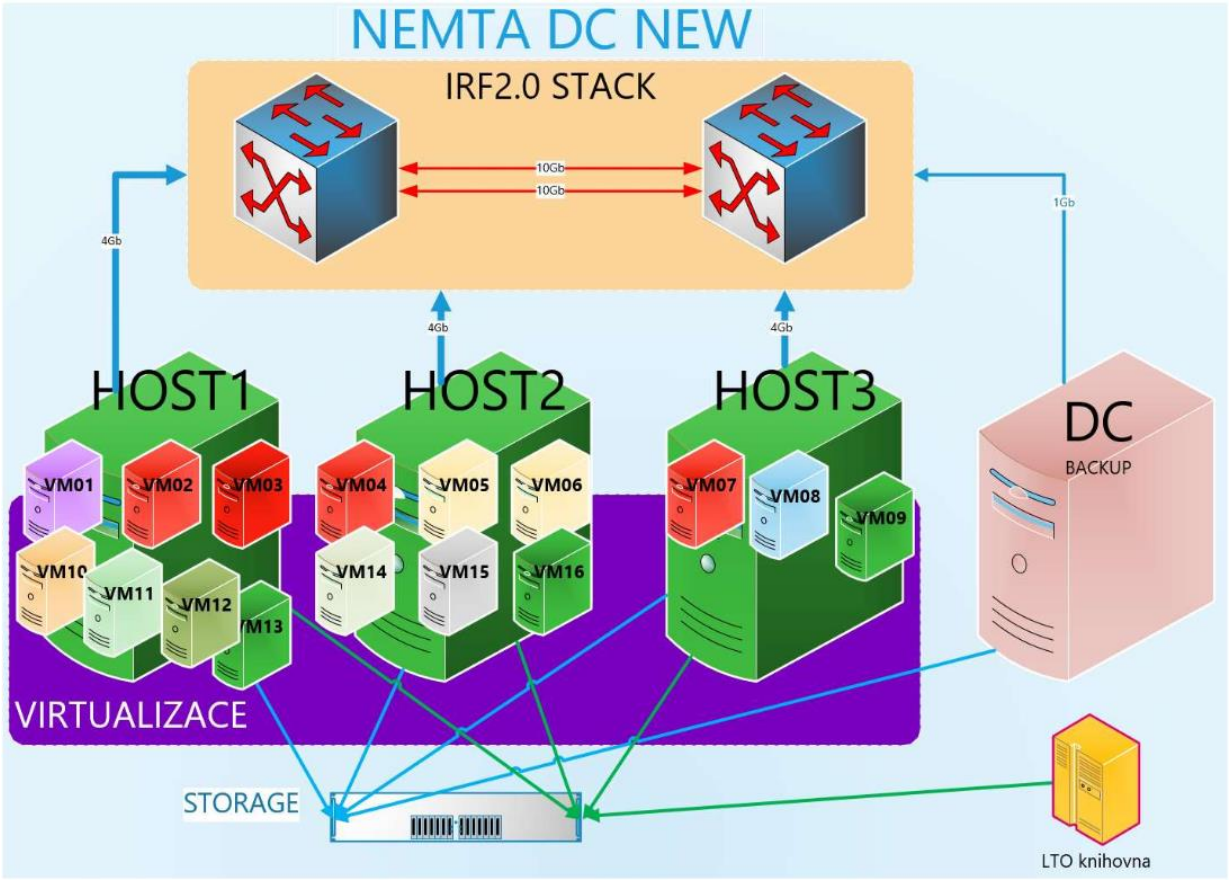
- Vlastní konfigurace, definice VLAN a parametrů provozu bude sepsáno v dokumentaci zrealizovaného stavu a spolu s povinnými pravidly pro změnu a údržbu tohoto nového bezpečnostního řešení bude definováno jak a proč dané parametry jsou popsány a nastaveny.

Předpokládaný principiální stav segmentace počítačové sítě NEMTA je uveden níže.



3. Dovybavení datového centra vybudováním Hyper –V cluster a vyřešení zálohování

Pro zajištění bezpečného a pokud možno nepřerušovaného provozu IS NEMTA je plánována realizace zajištění provozu IS NEMTA v cluster režimu (redundantní provoz) na virtuální platformě. Řešení je koncipováno tak, aby byl možný provoz aplikací IS NEMTA i při výpadku HW serveru, jednotlivého páteřního propojení či při lokálním výpadku elektrické energie. Cílový plánovaný stav clusteru provozu virtuální platformy je plánován na základě architektury uspořádání jednotlivých ICT zařízení v KS NEMTA tak, jak je principiálně uvedeno na následujícím obrázku.



Součástí řešení je i doplnění záložních zdrojů napájení a dodání příslušného počtu SW licencí pro obnovu operačních systémů a databází.

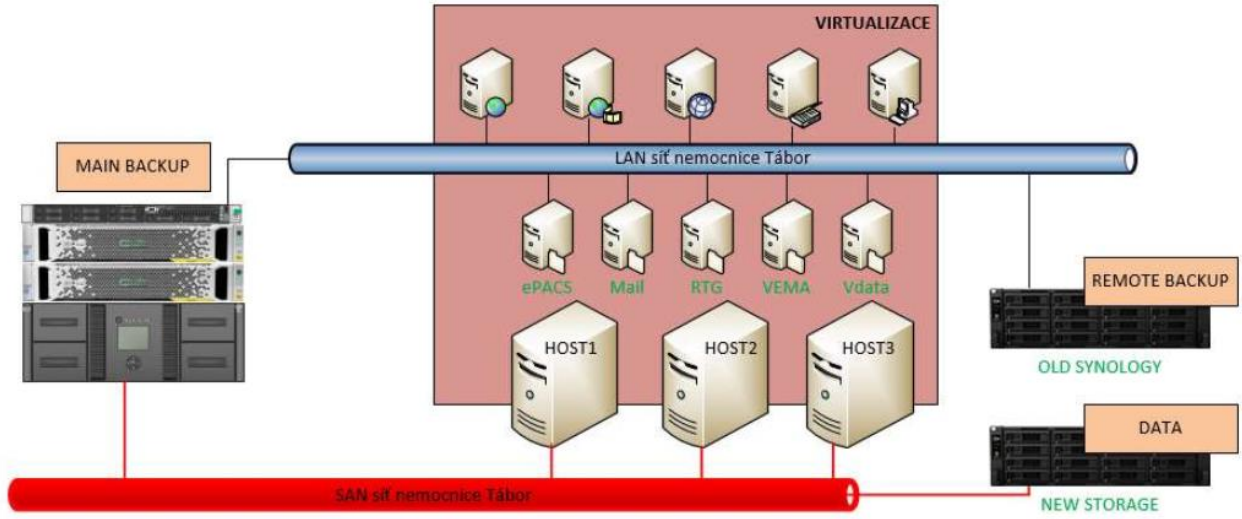
V plánovaném řešení se počítá s instalací a konfigurací dodávaného zboží tak, že bude zajištěn cílový stav v tomto rozsahu požadovaných činností:

- Instalace, konfigurace a nastavení serverů v clusteru a jejich napojení na SAN diskové úložiště s nastavením managementu UPS pro automatizované vypínání při nízkém stavu baterií.
- Instalace a oživení UPS s instalací managementu viz předchozí bod.
- Instalace a konfigurace diskového pole v rozložení a typu zapojení disků dle dispozic žadatele. Dále bude provedena konfigurace a nastavení pro potřeby zprovozněni virtuální platformy . Součástí řešení bude úplná aktualizace všech HW komponent na poslední platné verze SW patchů a firmwarů.

Dále se počítá s řešením pro vícenásobný BACKUP, a tedy možnost obnovy i z fyzicky nezávislého média (LTO pásky).

Nový systém zálohování by měl zajistit zejména:

- zálohovací SW podporuje zálohování kompletní infrastruktury žadatele (virtuální i fyzické servery, všechny typy diskových úložišť)
- záloha zabezpečí jak obnovení části infrastruktury, tak obnovení kompletní celé infrastruktury
- zachování pravidla zálohování 3-2-1 (3 kopie dat na 2 různých médiích, 1 kopie se nachází mimo hlavní lokalitu)
- systém bude schopen bezpečně ukládat zálohy s delší časovou retencí (archiv záloh i několik let zpět).



Popis navrhovaného stavu SAN sítě Nemocnice Tábor, a.s. (provozní a zálohovací úložiště)

V plánovaném řešení se počítá s instalací a konfigurací dodávaného zboží tak, že bude zajištěn cílový stav v tomto rozsahu požadovaných činností:

- Instalace, konfigurace a nastavení stávajícího BACKUP serveru pro potřeby připojení do SAN prostředí a provozu BACKUP SW. Dále instalace a konfigurace NAS dle požadavků žadatele, tedy ve smyslu konfigurace disků a jejich členění. Dále nastavení a konfigurace pro vzdálený přístup (síťové vícenásobné připojení a vystavení přístupu pro příslušné oprávnění).

- Instalace a konfigurace BACKUP SW, který umožní efektivně a garantované provozovat zálohování a případnou obnovu dat ve vazbě na virtuální platformu Hyper-V. Součástí je i konfigurace páskové knihovny, načtení a kategorizace médií, přístup k NAS (funkce RemoteDisk).

- Vytvoření zálohovacích politik pro režim zálohování First2Disk, Second2RemoteDisk, Thierd2DoubleTape.

- Definice a nastavení organizace provozu zálohovacích politik ve vazbě na potřeby a definice potřeb provozu důležitých IS NEMTA dle požadavků žadatele.

- Demonstrace procesu zálohy a obnovy na 5 vybraných fyzických a virtuálních serverech. Následně zadokumentování všech pravidel, politik, časových organigramů a přibližných časových náročností pro jednotlivé úkony zálohování.

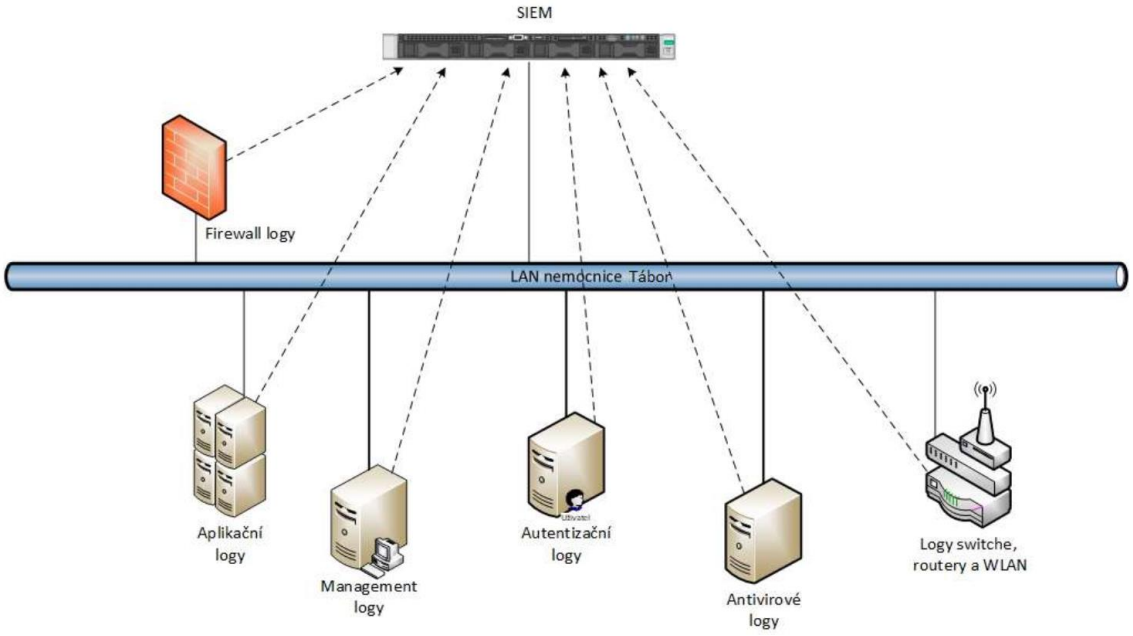
4. Software SIEM – nástroj pro integrovaný sběr a detekci kybernetických bezpečnostních událostí

Pro potřebu sledovat, vyhodnocovat a konsolidovat informace o potenciálních bezpečnostních hrozbách na úrovni jak KS NEMTA, tak i IS NEMTA se plánuje nasazení řešení SIEM, které by mělo všechny požadované vlastnosti zastřešit jedním centralizovaným řešením bez významného vlivu potřeby lidské práce.
NEMTA hodlá zlepšit ochranu před hrozbami a naplnit zákonné požadavky s využitím integrovaného analytického a reportingového systému. Cílem je implementovat v rámci organizace řešení SIEM (Security Intelligence and Event Management), které sdružuje záznamy o událostech ze všech klíčových zařízeních, rozmístěných napříč celou sítí NEMTA. NEMTA hodlá v rámci podpory stabilního provozu KS NEMTA a IS NEMTA zabezpečit SIEMem tyto oblasti:

- Firewally - komplexní UTM řešení s aplikační kontrolou paketů
- Centrální síťové switche
- WIFI kontroléry pro sledování jednotlivých AP
- NIS
- PACS
- LIS
- HR systémy
- Lékárenský systém
- Ostatní technologické prostředí, jako jsou např. MS Active Directory, MS SQL, MS SharePoint, Hyper-V.

Předmětem bude dodávka a implementace systému pro řízení bezpečnostních informací a událostí – dále „SIEM“ (Security Information and Event Management). Kromě ochrany dat včetně osobních údajů je jedním z důvodů realizace SIEM také to, aby v návaznosti na zákon č. 181/2014 Sb., O kybernetické bezpečnosti, organizace zavedla bezpečnostní opatření (Systém řízení bezpečnosti informací(ISMS)), hlášení kybernetických bezpečnostních incidentů a provádění protiopatření– organizačních a technických.

Nabízený systém by měl respektovat navrhovanou strukturu zdrojů informací:



5. **Software na monitoring a sběr dat z koncových zařízení včetně následné analýzy dat**

Pro potřebu monitoringu a sběru dat z PC s následnou pokročilou analýzu je plánován upgrade stávajícího řešení zastaralé verze Optim Access. Celé řešení se požaduje v rozsahu nasazení pro 450 PC, kdy bude možné sledovat tyto monitorované činnosti PC:

- Informace o provozu PC;
- Hardwarový a softwarový audit
- Podrobné informace o přihlášení uživatele na PC
- Způsob využívání aplikací
- Záznamy o nečinnosti uživatele (pauzy
- Přístupy na webové stránky
- Download a upload souborů v rámci internetu i intranetu
- Odchozí a příchozí trafik na síti
- Podrobné informace o tisku
- Pohyb externích zařízení v organizaci
- Informace o pohybu dat na externích zařízeních
- Informace o přístupu k vybraným datům na pevných discích a síti

Požadují se následné výstupy informací v tomto rozsahu:

- Behaviorální analýza chování uživatelů: Systém vyhodnocuje aktivitu uživatele z pohledu bezpečnostního (datový tok, pohyb souborů) a ekonomického (efektivní využití PC). Stavebním kamenem celého řešení je využití moderních technologií strojového učení a behaviorální analýzy chování uživatele. Pomocí těchto metod systém detekuje anomálie v chování zaměstnanců a na tento fakt upozorňuje odpovědné osoby.

- „Near time“ vyhodnocení: Velmi rychlé vyhodnocení monitorovaných dat. Na monitorovaná data jsou v desetiminutových intervalech centralizována a ihned předávána ke zpracování. Díky rychlému vyhodnocení je dramaticky snížena odezva na potenciální hrozbu.
- Přehled o pohybu dat: Díky sledování a vyhodnocení pohybu dat prostřednictvím periferních zařízení, internetu a emailu, ale i lokálních a sdílených disků, máte okamžitý přehled o tom, jaká data organizaci opouští, nebo naopak jaká data jsou zaměstnanci přinášena.
- Snadný přístup k vyhodnocení: Pro prezentaci monitorovaných dat je využíváno webového rozhraní, ke kterému lze snadno přistoupit z libovolného počítače nebo mobilního zařízení v organizaci. Není tak nutné instalovat jakoukoliv aplikaci v rámci koncové stanice.
- Důležité informace na jednom místě: Všechny podstatné informace jsou zobrazovány na jednom místě, tzv. dashboardu. Máte tak rychlý přehled o tom, co se ve vaší organizaci děje. Mezi zobrazované informace patří vyhodnocení chování uživatele (detekce anomálií), souhrnné informace o pohybu dat, využívání externích zařízení, přístupy k webovým stránkám, využívání aplikací a další.

6. Software Antivir

Pro potřeby ochrany před škodlivým kódem NEMTA plánuje nasazení soudobého ANTI SW řešení,které dokáže pomoci ochránit provoz jak na serverové úrovni, tak i desktopové a v rámci mobilních zařízení.
NEMTA v této souvislosti stanovil tyto obecné požadavky na nový ANTI SW pro 500 desktop zařízení a 15 serverů:

- centrální správa, možnost sledovat stav jednotlivých komponent na stanicích,
- víceúrovňová architektura ochrany prostřednictvím navzájem propojených a samostatně konfigurovatelných komponent (ochranu e-mailu, web, firewall, souborový systém apod.),
- definice nastavení systému na jednotlivých stanicích
- automatické řešení bezpečnostních incidentů bez potřeby dialogu s uživatelem, reportování incidentu správci,
- vzdálené prohlížení výsledků kontrol a řešení jednotlivých incidentů, možnost „ručního“ zásahu do nastavených pravidel
- vzdálené spouštění testů na stanicích
- distribuce aktualizačních soborů v rámci lokální sítě
- vzdálený přístup do „virového trezoru“ stanic
- agregace dat o provozu, centralizované úložiště, snadná možnost připojení celku do SIEM
- minimální nároky na prostředky stanice

Cílem nasazení nového systému je plně automatizovaná antivirová a antispamová ochrana hardwarových prostředků NEMTA s centrální správou, napojením do SIEM a minimální potřebou dohledu administrátora. V plánovaném řešení se počítá s instalací a konfigurací dodávaného zboží tak, že bude zajištěn cílový stav v tomto rozsahu požadovaných činností:

- Instalace, konfigurace a nastavení centrální administrátorské konzole s definicí alespoň 3 bezpečnostních setů pro aplikaci na zařízení typu Server, Desktop a Notebook

- Zavedení a implementace ANTI SW řešení pro minimálně 5 Serverů, 20 Desktopů a 5 Notebooků, demonstrace aktualizace a vzdálené kontroly s výstupem do centrálního reportu.

Seznam použitých zkratek:

V seznamu zkratek nejsou uvedeny ty , které jsou obecně známé a používané.

Zkratka	Význam zkratky
AP	Access point
DR	Distribuční rozvaděč
FW	Firewall
HR	Human Resources
HW	Hardware
ICT	Information and Communication Technologies
KS	Komunikační infrastruktura
LAN	Local Area Network
LIS	Laboratorní informační systém
LTO	Linear Tape Open
NAC	Network Access Control
MM	Multimode
NAC	Network Access Conntrol
NAS	Network Area Storage
NEMTA	Nemocnice Tábor a. s.
NIS	Nemocniční informační systém
PACS	Picture Archiving and Communication System. Technologie umožňující správu, ukládání a zobrazení obrazové dokumentace v medicíně.
SAN	Storage Area Network
SFP	Small form-factor pluggable
SIEM	Security Information and Event Management
SM	Singlemode
SSID	Service Set Identifier
UPS	Uninterruptible Power Supply
UTM	Unified Threat Management