



Obsah

Seznam zkratk a pojmů.....	2
Předmět plnění	4
Vybudování univerzálního kabelážního systému.....	6
Univerzální kabelážní systém (UKS)	6
Instalace datových rozvodů UKS.....	6
UTP kabelové rozvody pro WiFi AP.....	6
Instalace datových rozvaděčů.....	7
Optické datové rozvody	7
Návaznosti, připravenost	7
Specifikace minimálních požadavků technického řešení.....	8
Aktivní Prvky	8
Instalace a konfigurace aktivních síťových prvků LAN	8
Specifikace minimálních požadavků technického řešení.....	10
Bezdrátová infrastruktura (WLAN)	10
Instalace a konfigurace bezdrátové počítačové sítě (WiFi).....	10
Specifikace minimálních požadavků technického řešení.....	11
Řízení přístupu do LAN a WLAN včetně segmentace.....	12
Požadavky na lokální počítačovou síť – drátová (LAN)	12
Požadavky na lokální počítačovou síť – bezdrátová (WLAN)	13
Specifikace minimálních požadavků technického řešení.....	14
Firewall včetně vzdáleného přístupu (VPN).....	14
Řešení ochrany perimetru počítačové sítě – lokalita Kyjov	14
Specifikace minimálních požadavků technického řešení.....	15
Řešení ochrany perimetru počítačové sítě – lokalita Veselí nad Moravou	15
Specifikace minimálních požadavků technického řešení.....	15
Nástroj pro monitoring datových toků (NDR).....	15
Monitoring datových toků a základní reporting.....	15
Specifikace minimálních požadavků technického řešení.....	16
Dvoufaktorová autentizace přes VPN	17
Řešení systému pro dvoufaktorovou (2FA) autentizaci	17
Specifikace minimálních požadavků technického řešení.....	17



Seznam zkratk a pojmů

V následující tabulce je uveden seznam použitých zkratk a pojmů:

Zkratka/pojem	Význam
IT	Informační technologie
ČR	Česká Republika
UKS	Univerzální kabelážní systém
UTP	Unshielded Twisted Pair
TP	Twisted Pair
AP	Aktivní prvky
LAN	Local Area Network
WLAN	Wireless Local Area Network
VPN	Virtual Private Network
NDR	Network Detection and Response
2FA	2-faktorová autentizace
ZoKB	Zákon o kybernetické bezpečnosti
ČSN EN 50173	Česká technická norma Evropská norma EN 50173
CAT6	Technické označení pro síťový kabel – Category 6
CPR: B2ca	Construction Products Regulation – Třída reakce na oheň
CPR	Construction Products Regulation (<i>Nariadení o stavebních výrobcích</i>)
ČSN 342300	Elektrické instalace nízkého napětí
ČSN 332000-5-52	Elektrické instalace nízkého napětí
ČSN EN 50174-2	Česká technická norma stanovující pravidla pro instalaci strukturované kabeláže
RJ45	Standardizovaný konektor (Registered Jack 45)
DC	Datové centrum
PoE	Power over Ethernet (Napájení po ethernetu)
L3 swich	Layer 3 Switch (<i>přepínač vrstvy 3 podle OSI modelu</i>)
VSX	Virtual Switching Extension (<i>Virtuální rozšíření přepínání</i>)
SFP	Small Form-factor Pluggable (<i>zasouvací modul malého formátu</i>)
QSFP	Quad Small Form-factor Pluggable → optický transceiver pro 40/100/200/400 Gbps
DAC	Direct Attach Cable (<i>Přímý připojovací kabel</i>)
SSID	Název bezdrátové Wi-Fi sítě
AAA	Authentication, Authorization, Accounting (<i>Autentizace, Autorizace, Účtování</i>)
HA	High Availability (<i>Vysoká dostupnost</i>)
802.1X	IEEE 802.1X je bezpečnostní standard, který umožňuje ověření uživatele nebo zařízení při připojení k síti ještě než získá přístup k síťovým prostředkům.
CoA	Change of Authorization (<i>Změna oprávnění uživatele během aktivního připojení</i>)
RFC 3576	RFC 3576 je standardizační dokument vydaný organizací IETF, který rozšiřuje funkce RADIUS protokolu o dynamické řízení oprávnění
WebAuth	Webové ověření
EAP	Extensible Authentication Protocol (<i>Rozšiřitelný autentizační protokol</i>)
EAP-TEAP	Extensible Authentication Protocol – Tunnel Extensible Authentication Protocol (<i>Tunelovaný rozšiřitelný autentizační protokol</i>)



Zkratka/pojem	Význam
EAP-PEAP	Extensible Authentication Protocol – Protected Extensible Authentication Protocol (<i>Chráněný rozšiřitelný autentizační protokol</i>)
EAP-TLS	Extensible Authentication Protocol – Transport Layer Security (<i>Rozšiřitelný autentizační protokol s využitím TLS/SSL</i>)
MAC	Jedinečný identifikátor síťového rozhraní zařízení
MAB	MAC Authentication Bypass
PSK	PSK je metoda ověřování, při které mají všechna zařízení stejný předem nastavený klíč (heslo) k přístupu do zabezpečené sítě
TACACS	Terminal Access Controller Access-Control System
AD	Active Directory
OU	Organizational Unit (organizační jednotka)
EAP-FAST	Extensible Authentication Protocol – Flexible Authentication via Secure Tunneling (<i>Rozšiřitelný autentizační protokol – flexibilní autentizace pomocí bezpečného tunelování</i>)
ACL	Access List
IoT	Internet of Things (<i>Internet věcí</i>)
IP	Internet Protocol
DDOS	Distributed Denial of Service (<i>Distribuované odepření služby</i>)
NGFW	Next-Generation Firewall
FW	Firewall
UDP PPS test	UDP PPS test je zátěžový síťový test, který měří, kolik UDP paketů za sekundu dokáže vyslat nebo přijmout síťové zařízení
UDP	Transportní protokol
TCP	Transportní protokol
UDP/64B	UDP paket o velikosti 64 bajtů (Bytes)
MBS	Minimální bezpečnostní standard
TB	Terabyte
NAC	Network Access Control
NUKIB	Národní úřad pro kybernetickou bezpečnost
ISO 27000	Řada mezinárodních standardů pro řízení bezpečnosti informací
ISO 27001	Norma pro řízení bezpečnosti informací
NIS2	Směrnice o bezpečnosti sítí a informací
NO	NIS2 opatření
LACP	Linková agregace
ISZS	Informační systém základní služby



Předmět plnění

Cílem tohoto projektu je zajistit soulad Nemocnice Kyjov, jakožto provozovatele informačních a komunikačních systémů, jenž zpracovává, zprostředkuje a ukládá citlivé údaje, s požadavky ZoKB a s prováděcí vyhláškou. Navržená technická opatření směřují k zajištění souladu s požadavky zákona, čímž přispějí k předcházení hrozbě kybernetických a bezpečnostních incidentů. Výsledkem projektu tedy bude posílení ochrany informačních a komunikačních systémů žadatele před kybernetickými útoky.

Projekt reaguje na potřebu Nemocnice Kyjov řešit neuspokojivý stávající stav v oblasti kybernetické bezpečnosti a závaznou platnost legislativy pro tuto nemocnici (nemocnice je správcem a provozovatelem informačního systému základní služby – ISZS). V nemocnici proběhlo ve 2. kvartálu roku 2022 rozsáhlé šetření a analýza mapující úroveň zabezpečení proti hrozbám kybernetického útoku. Byla identifikována celá řada nedostatků, na jejichž základě lze konstatovat, že prostředí nemocnice je vysoce zranitelné vůči typům útoků, které byly v poslední době cíleny na zdravotnická zařízení.

Projekt zabezpečí dostupnost kvalitních zdravotnických služeb v potřebné kapacitě a v potřebném čase pro své klienty, tj. občany ČR, cizince, a to prostřednictvím ochrany informačního systému nemocnice před kyberútoky. Projekt taktéž zabezpečí stabilní pracovní IT prostředí pro zaměstnance nemocnice.

Cílová situace nemocnice po realizaci projektu přinese významný posun v řízení komplexního systému řízení bezpečnosti informací včetně reakce na kybernetické bezpečnostní události a zajistí tak rychlé řešení případných kybernetických útoků. Dále přinese výrazné ušetření časových možností specialistů, kteří se tak budou moci věnovat dalším rozvojovým aktivitám v oblasti kybernetické bezpečnosti.

Dojde k rozšíření stávajících systémů tak, aby jednak poskytovaly požadavky na danou funkcionalitu v rámci nutných podmínek stanovených příslušnou legislativou, dále aby došlo k vybudování/rozšíření robustnosti stávajících systémů nemocnice v souladu s koncepcí stanovenou analýzou kybernetické bezpečnosti. Dojde k:

- Naplnění požadavků zákona o KB a vyhlášky o KB,
- Naplnění optimálních standardů kybernetické bezpečnosti organizace

Zásadními změnami projektu bude implementace vhodně vybraných bezpečnostních technologií, které jsou podrobně popsány v této dokumentaci. Mezi další změny bude patřit zefektivnění mnoha procesů, které jsou vyžadovány vyhláškou o KB, dobrou praxí a bezpečnostní dokumentací. Dalším výstupem bude úprava nebo vypracování nové provozní a bezpečnostní dokumentace reflektující nové nástroje a procesy. Současně také dojde k důkladnému zavedení těchto procesů a školení všech zainteresovaných stran.

Projekt je zaměřen na zavedení mechanismů, které výrazným způsobem zvyšují bezpečnost síťové infrastruktury a jednotlivých informačních systémů Nemocnice Kyjov. Efektivní realizace bezpečnostních mechanismů si současně s ohledem na stávající stav vyžádá implementaci technologií nebo provedení změn v oblastech:

- Univerzální kabelážní systém
- Aktivní prvky



EVROPSKÁ UNIE
Evropský fond pro regionální rozvoj
Integrovaný regionální operační program



**MINISTERSTVO
PRO MÍSTNÍ
ROZVOJ ČR**

- Bezdrátová infrastruktura
- Řízení přístupů do LAN a WLAN včetně segmentace
- Firewall včetně vzdáleného přístupu (VPN)
- Nástroj pro monitoring datových toků (NDR)
- Dvoufaktorová autentizace přes VPN



Vybudování univerzálního kabelážního systému

Univerzální kabelážní systém (UKS)

Požadavkem je vybudování univerzálního kabelážního systému (strukturovaná kabeláž), která bude v budovách sloužit pro přenášení hlasových a datových služeb. Jedná se o soubor datového rozvaděče, datového kabelu a účastnických (datových) zásuvek.

Všechny komponenty UKS musí být vzájemně kompatibilní a splňovat normy ČSN EN 50173/50174, kabeláž min. CAT6 UTP CPR:B2ca pro datové zásuvky (datové zásuvky budou vybudovány místo stávajících nemanažovatelných switchů) a WiFi AP. Instalace bude provedena v souladu s direktivou CPR.

Rozvody strukturované kabeláže budou vytvořeny s maximálním důrazem na jejich ochranu před případným nežádoucím elektromagnetickým vlivem okolního silového vedení. Je požadováno dodržovat odstupové vzdálenosti, způsob vedení i křížení s ostatními vedeními. Stejně tak je požadováno dbát zvláštní pozornosti na potencionální přiblížení vedení UKS ke svodům vnějšího bleskosvodového systému. V technicky nevyhnutelných případech musí být, při souběhu a křížení, dodrženy minimální vzdálenosti dle ČSN 342300, ČSN 332000-5-52, ČSN EN 50174-2.

Požadovaná záruka na pasivní komponenty UKS je min. 20 let. Zadavatel připouští možnost poskytnutí této záruky formou systémové záruky výrobce nebo rovnocenné záruky dodavatele pojištění u třetí strany.

Instalace datových rozvodů UKS

Montáž a instalace UKS bude rozdělena do dvou vzájemně provázaných celků a to:

- UTP kabelové rozvody pro WiFi přístupové body (AP) a náhrada rozbočených dat. zásuvek, pomocí switchů splňujícími minimální požadavky na porty, propustnost, napájení a hluchost, novými datovými kabely k novým datovým zásuvkám
- páteřní optické kabelové rozvody mezi podružnými dat. rozvaděči dle návrhu viz. „**Nemocnice_Kyjov-navrh_novych_optickych_tras.pdf**“

UTP kabelové rozvody pro WiFi AP

Požadavkem je instalace AP, včetně univerzálního kabelážního systému (UKS) do příslušných datových rozvaděčů v jednotlivých částech budovy, na základě rozmístění jednotlivých AP uvedených v protokolu o měření pokrytí WiFi signálem. Všechny kabelové trasy (datové TP trasy) budou proměřeny certifikovaným měřícím přístrojem a bude vyhotoven měřící protokol prokazující validitu tohoto kabelového spoje.



Dodavatel vybuduje kabelovou trasu mezi AP a RACKem pomocí kabelových žlabů s povrchovou montáží v jednotlivých budovách. Tato trasa bude obsahovat, kromě vlastního UTP kabelu, nosného a montážního materiálu také datovou zásuvku (včetně příslušenství) na straně AP a modulární propojovací pole (včetně příslušenství). Součástí této kabelové trasy, budou také UTP kabely (patch kabel RJ45), příslušné délky, pro aktivaci AP v datové zásuvce a v aktivním prvku.

Rozmístění AP v jednotlivých budovách a místnostech je vyznačeno v protokolu pokrytí WiFi viz „**Návrh umístění AP.pdf**“. Rozmístění jednotlivých AP dle přiložené mapy, v případě ekvivalentního řešení je požadováno prokázání dosaženého pokrytí / kapacity simulací a měření.

Stejným způsobem bude provedena instalace kabelových tras včetně kabelů a všech pasivních komponent, u náhrady rozbočených datových zásuvek pomocí switchů splňujících minimální požadavky.

Požadované zakončení UTP kabelů pro AP a ostatních datových zásuvek, v jednotlivých datových rozvaděcích, je detailně vyznačeno tabulce viz „**Tabulka_datovych_rozvadecu.xlsx**“.

Instalace datových rozvaděčů

V rámci instalace UKS budou ve vyjmenovaných lokalitách podle potřeby přebudovány nebo nainstalovány nové datové rozvaděče.

Při přebudování (výměně) datového rozvaděče musí být všechny prvky a jejich zapojení v původním a funkčním stavu. Ke každému přebudovávanému, nebo novému datovému rozvaděči, dodavatel nainstaluje nový přívod napájení 230V se samostatným jištěním z nejbližšího napájecího silového rozvaděče, včetně samostatného zemního vodiče.

Optické datové rozvody

Součástí dodávky UKS bude montáž a instalace chybějících páteřních optických spojů mezi podružnými datovými rozvaděči v jednotlivých budovách.

Vedení nově navržených optických datových rozvodů, v rámci areálu nemocnice, je zakresleno v situačním plánu „**Nemocnice_Kyjov-navrh_novych_optickych_tras.pdf**“ a tučně vyznačeno v tabulce „**Tabulka_datovych_rozvadecu.xlsx**“.

Návaznosti, připravenost

Dodavatel UKS zajistí:

- montáž všech součástí UKS dle specifikace a výkazu výměr
- montáž zařízení, dodávaných v rámci tohoto projektu, do podružných datových rozvaděčů a do datových rozvaděčů v serverovnách
- drobné stavební úpravy jako např. vrtání příček, zdí a stropů, instalace požárního utěsnění mezi stropy apod.



Specifikace minimálních požadavků technického řešení

Viz. samostatná příloha „Technická specifikace část 1.xlsx“.

Aktivní Prvky

Instalace a konfigurace aktivních síťových prvků LAN

Předmětem této části projektu je specifikace požadavků na vybavení počítačové sítě aktivními síťovými prvky na základě stávající i nově navržené struktury UKS (univerzální kabelážní systém), a které tvoří síťovou LAN infrastrukturu. Návrh designu počítačové sítě je v rámci areálu v Kyjově rozdělen do tří vrstev – přístupová (access), jádro (core) a datacentrová (DC). V rámci Veselí nad Moravou pak chybí vrstva datacentrová, tj. je zde přítomna jen přístupová (access) a jádro (core). Schéma zapojení jednotlivých aktivních prvků viz. příloha „**Topologie řešení počítačové sítě - Kyjov.png**“ pro lokalitu Kyjov a „**Topologie řešení počítačové sítě - Veselí.png**“ pro lokalitu Veselí nad Moravou.

Migrace konfigurace aktivních prvků LAN

Součástí plnění je kompletní převod stávající konfigurace aktivních síťových prvků na nově dodávané zařízení, a to včetně:

- Síťové topologie a VLAN segmentace
- Směrovacích tabulek a L3 rozhraní
- Access-listů, ACL pravidel a bezpečnostních politik (pokud jsou využívány)
- QoS politik, prioritizačních pravidel a VoIP VLAN (pokud jsou využívány)
- Konfigurace trunků, LAG/MLAG/stacking rozhraní a uplinků
- Port security, 802.1X MAC autorizace (pokud jsou aktivní)

Dodavatel je také povinen:

- provést detailní analýzu stávající sítě,
- převést konfiguraci tak, aby byla funkčně ekvivalentní v novém prostředí,
- provést nutné úpravy tak, aby odpovídala nové topologii a bezpečnostnímu návrhu,
- zajistit minimální výpadek provozu během migrace.

Kyjov

Přístupová vrstva (access switch)

Stávající přístupová síť je technicky i morálně zastaralá – nedostačující propustností, heterogenitou a omezenou podporou moderních bezpečnostních protokolů. V rámci tohoto projektu je plánována generační výměna a rozšíření přístupové vrstvy sítě s cílem **sjednotit a modernizovat infrastrukturu**.



Použita bude **kombinace různých typů přístupových switchů**, aby byl ve všech podružných rozvaděčích zajištěn dostatek portů pro připojení koncových zařízení. Pro připojení bezdrátových přístupových bodů (Wi-Fi 7) budou nasazeny switche s **multigigabitovými porty**, umožňujícími vysokou přenosovou kapacitu. Vybrané switche budou navíc podporovat **napájení přes Ethernet (PoE+)**, určené pro připojení IP kamer, senzorů, čteček, IP telefonů a dalších zařízení.

Každý podružný rozvaděč bude **duálně připojen k jádru sítě (core switchům)** – obě linky budou aktivní díky **linkové agregaci (LACP)**. V případě nasazení více switchů v jednom rozvaděči budou tyto propojeny **do stohu** prostřednictvím dedikovaného stohovacího rozhraní.

Jádro sítě (Core switche)

Nové jádro sítě bude tvořeno **dvěma L3 core switchi**, umístěnými v oddělených serverovnách (primární a sekundární). Tyto switche budou fungovat jako jedna logická entita (stoh), zajišťující:

- agregaci přístupové vrstvy,
- směrování datové komunikace,
- konektivitu směrem k datacentrovému prostředí a bezpečnostním prvkům (firewallům)

Datová centra (DC switche)

Z důvodu ochrany investic zůstane stávající datacentrové prostředí zachováno. Nově bude realizováno pouze navýšení kapacity páteřních linek mezi jádrem sítě a datacentry.

Veselí nad Moravou

Přístupová vrstva (access switche)

Obdobně jako v Kyjově jsou stávající prvky přístupové sítě morálně zastaralé, s nevyhovující propustností, heterogenní. Proto je plánovaná generační výměna a rozšíření přístupové vrstvy sítě s cílem homogenizace aktivních prvků zejména s ohledem na podporu a implementaci bezpečnostních protokolů.

Bude použita kombinace několika různých typů switchů tak, aby v každém podružném rozvaděči byl zabezpečen dostatek portů, přičemž pro připojení přístupových bodů bezdrátové sítě (AP) budou, s ohledem na vysokou propustnost WiFi 7, použity **multigigabitové porty**. Vybrané switche pak budou opět podporovat **PoE+** pro napájení IP kamer, senzorů, čteček, IP telefonů a dalších zařízení.

Každý podružný rozvaděč pak bude duálně zapojen do obou páteřních stohů (core) a to tak, že **obě linky budou aktivní** (linková agregace). Pokud bude v daném datovém rozvaděči instalován více jak jeden switch, budou zapojeny do tzv. stohu pomocí dedikovaného stohovacího rozhraní.



Jádro sítě (core switche)

S ohledem na požadavky na síťové prostředí, které jsou ve srovnání s lokalitou Kyjov rámcově nižší, bude nové jádro sítě (core) vybudováno nasazením **dvojice standardních L2 switchů** v konfiguraci jedné logické entity (stohu). Tato logická entita pak bude sloužit k agregaci linek z přístupové vrstvy sítě a poskytovat konektivitu směrem k perimetrovým firewallům.

Přehledové síťové schéma viz. příloha „**Topologie řešení počítačové sítě - Kyjov.png**“ a „**Topologie řešení počítačové sítě - Veselí.png**“ detailně zobrazuje zapojení aktivních prvků po jednotlivých datových rozvaděčích včetně vazby na související technologické části (firewally, kontroléry, externí konektivita). Všechny navrhované switche musí být vybaveny příslušnými moduly pro připojení do počítačové sítě a to včetně připojovacích kabelů a stohovacích modulů, pokud je požadováno jejich stohování v rámci datového rozvaděče viz. příloha „**Tabulka_datovych_rozvadecu.docx**“.

Součástí dodávky musí být i všechny potřebné moduly (SFP, SFP+, QSFP, DAC, atd.) včetně nutného množství optických a metalických patchcordů tak, aby bylo dosaženo požadovaného cílového stavu infrastruktury zachyceném v přílohách „**Topologie řešení počítačové sítě - Kyjov.png**“ a „**Topologie řešení počítačové sítě - Veselí.png**“. Počty aktivních prvků v jednotlivých lokalitách, dle jejich typu, jsou uvedeny v příloze „**Tabulka_rozmisteni_aktivnich_prvku.docx**“.

Na všechny dodávané aktivní prvky je požadována záruka v rozsahu **minimálně 60 měsíců** a po tuto dobu musí být výrobcem garantována podpora dodaných aktivních prvků.

Specifikace minimálních požadavků technického řešení

Viz. samostatná příloha „**Technické specifikace část 2.docx**“.

Bezdrátová infrastruktura (WLAN)

Instalace a konfigurace bezdrátové počítačové sítě (WiFi)

Předmětem této části projektu je pokrytí jednotlivých budov nemocnice bezdrátovým signálem prostřednictvím bezdrátových přístupových bodů (AP) se zajištěním centrálního řízení této WiFi sítě. Je požadována instalace **AP splňující standard 802.11be (WiFi 7)**. Návrh rozmístění AP v rámci jednotlivých budov areálu nemocnice je zanesen v protokolu z měření pokrytí bezdrátovým signálem viz. soubor „**Návrh umístění AP.pdf**“.

Dodávka systému technologie WLAN bude obsahovat vlastní přístupové body a centrální řídicí systém (kontrolér) v redundantním režimu pro řízení a konfigurování bezdrátové sítě.

Dodavatel provede konfiguraci kontrolérů a AP včetně vytvoření **3 SSID** a jejich propagaci pomocí VLAN do LAN. Součástí konfiguračních prací bude implementace segmentace prostřednictvím VLAN a protokolu 802.1x vycházející z bezpečnostních pravidel konfigurovaných VLAN (drátové počítačové sítě) a konfigurace spolupráce s AAA serverem (Radius Server) dodávaným v rámci tohoto projektu.



Dodávka, instalace a konfigurace řešení pro WiFi se bude skládat z následujících částí:

- přístupové body bezdrátové sítě – celkem **299** kusů
- fyzický kontrolér včetně všech připojovacích modulů a kabelů – **2ks**
 - kontroléry budou nainstalovány v režimu vysoké dostupnosti (HA režim) viz. schéma zapojení, příloha „**Topologie řešení počítačové sítě - Kyjov.png**“

Specifikace minimálních požadavků technického řešení

Viz. samostatná příloha „Technické specifikace část 2.docx“.



Řízení přístupu do LAN a WLAN včetně segmentace

Předmětem této části projektu je implementace komplexního řešení pro řízení přístupu zařízení a uživatelů do počítačové sítě nemocnice, a to jak v části LAN, tak i WLAN, včetně centrální autentizace, autorizace a účtování (AAA). Systém zajistí automatické rozpoznání typu zařízení, přiřazení politik a VLAN, a to i pro zařízení, která nepodporují 802.1X. Zabezpečení bude realizováno zejména pomocí protokolu 802.1X, doplněného o náhradní autentizační metody. Součástí bude konfigurace aktivních prvků, kontrolérů a autentizačního, autorizačního a účtovacího serveru (dále jen AAA server) minimálně v rozsahu této kapitoly. Software může být ve formě HW appliance anebo SW image pro virtualizaci v prostředí VMware, Hyper-V nebo KVM.

Zařízení, která nepodporují 802.1X budou autentizována pomocí náhradních metod: ověření - MAB, WebAuth, PSK založené na attributech zařízení (skupina MAC, lokalita, apod.)

Všechny veřejně přístupné porty síťových přepínačů budou nakonfigurované pro ověřování pomocí 802.1X, MAB a případně WebAuth (dle analýzy během implementace). Zařízení bude ověřeno na AAA serveru a dle definované politiky mu budou přiděleny práva na portu switchu. Ověřené zařízení dostane na všech portech stejná práva. V případě, že zařízení je možné připojit do bezdrátové i drátové sítě, pak stejná práva bude mít nezávisle na použité konektivitě.

Součástí řešení řízení přístupu do počítačové sítě bude také řízení přístupu k síťovým zařízením, typicky aktivním prvkům, prostřednictvím protokolu **TACACS** (Terminal Access Controller Access-Control System) s funkcí autentizace, autorizace a účtování (AAA).

Požadavky na lokální počítačovou síť – drátová (LAN)

Switch ověří zařízení prostřednictvím protokolu 802.1X a pokud projde ověřením, přidělí mu příslušná práva dle definovaných politik. Pokud zařízení neumí 802.1X či dojde při ověřování k chybě, pokusí se zařízení ověřit podle MAC adresy (MAB – MAC Authentication Bypass). Pokud je MAB úspěšný, zařízení opět dostane práva dle definovaných politik. Pokud je MAB neúspěšný, budou nakonfigurovány politiky na základě analýzy požadavků zadavatele – např. WebAuth v zasedací místnosti, instalační VLAN na definovaných datových zásuvkách, apod.

Politiky musí být možno definovat minimálně pro tyto dva typy zařízení:

Doménový počítač (typicky zařízení s OS WIN)

- Počítač i přihlášený uživatel MUSÍ být v doméně (AD).
- Počítač v AD bude zařazen v příslušné skupině nebo OU (organizační jednotka).



- Počítač má z AD vygenerovaný certifikát, který použije k přihlášení (počítače odstraněné z domény nesmí být vpuštěny do sítě i v případě platnosti certifikátu).
- Počítač před přihlášením uživatele do domény dostane práva na přihlášení uživatele do domény.
- Po přihlášení uživatele do domény bude počítač reautentizován a dojde k současnému ověření počítače a uživatele (metoda EAP-TEAP nebo EAP-FAST podporující EAP-Chaining).
- Počítači bude přidělena VLAN, pomocí níž se dostane do interní sítě a bude mít přístup na servery.

Tiskárny, scannery apod. (ostatní zařízení, které neumí protokol 802.1x)

- Zařízení bude definováno na AAA serveru (administrátorem nebo pověřeným zaměstnancem s omezenými právy).
- Účet bude mít definovanou skupinu nebo přímo VLAN.
- Tyto zařízení budou mít zpravidla dedikovanou VLAN, případně speciální VLAN s omezením práv pomocí ACL (Access List).

Dále je požadována možnost definovat skupiny návštěvníků a soukromých zařízení, které mohou být ověřovány např. pomocí WebAuth portálu, případně může být jejich přístup omezen např. vyhrazenými porty (při zachování autentizace pro doménové počítače i IoT zařízení), časem přístupu apod.

Požadavky na lokální počítačovou síť – bezdrátová (WLAN)

Bezdrátová síť bude využívat stejný způsob ověřování jako LAN pouze s tím rozdílem, že se uživatel nepřipojuje do ethernetového portu („datové zásuvky“), ale připojuje se prostřednictvím přístupových bodů a ověření probíhá prostřednictvím kontroléru. Bezpečnost musí být jednotná pro LAN i WLAN tzn. způsob autentizace bude pro zaměstnance, pacienty, síťové administrátory a notebooky totožný.

V bezdrátové síti budou nakonfigurovány tyto typy bezdrátových sítí (SSID):

- **Interní SSID** – zařízení používající 802.1X k autentizaci
- **IoT SSID** – zařízení, která nepodporují autentizaci 802.1X, ale využívají nebo jsou využívány prostředky v interní síti. Tyto zařízení budou využívat autentizaci pomocí PSK (PreShared Key), které je unikátní pro zařízení nebo skupinu zařízení.
- **Guest SSID** – autentizace pomocí WebAuth pro uživatele (zpravidla pacienty či hosty) s přístupem pouze do internetu. Tito uživatelé si budou sami založit účet (tzv. self-registration portál) nebo bude možno jim vytvořit účet na AAA serveru.



Součástí dodávky bude kompletní nasazení segmentace počítačové sítě prostřednictvím VLAN, nasazení nového IP plánu a ověřování všech zařízení prostřednictvím AAA serveru.

Specifikace minimálních požadavků technického řešení

Viz. samostatná příloha „Technické specifikace část 2.docx“.

Firewall včetně vzdáleného přístupu (VPN)

Řešení ochrany perimetru počítačové sítě – lokalita Kyjov

Předmětem této části projektu je ochrana perimetru nemocniční počítačové sítě a zároveň zajištění bezpečného vzdáleného přístupu uživatelů a správců do interní sítě prostřednictvím technologie VPN. Řešení musí být postaveno na technologii **Next Generation Firewall (NGFW)** v režimu **vysoké dostupnosti** a musí zahrnovat moderní bezpečnostní funkce, jejichž účinnost bude ověřitelná měřením. Jsou požadovány dva hardwarové boxy běžící v HA clusteru v režimu active/passive. V případě výpadku aktivního člena automaticky plně přebírá jeho funkci člen záložní. Dodavatel zajistí nepřetržitou hardwarovou a softwarovou podporu výrobce v režimu 24/7, včetně dodávek bezpečnostních aktualizací, signatur a reputačních databází, aktualizací IPS/IDS, AV, AntiSpam, Application Control a Web Filtering služeb, a aktualizací systémového firmware, po dobu minimálně 5 let od převzetí díla. Systém bude využívat databázi IP reputation pro blokadu DDoS útoků. Součástí řešení bude redundantní konektivita se zbytkem síťové infrastruktury. NGFW musí podporovat a zahrnovat VPN bránu pro zabezpečený vzdálený přístup uživatelů i správců. VPN musí být integrovanou součástí firewallu, nikoliv externí či doplňkovou službou a musí využívat aktuálně bezpečnostně doporučené protokoly.

Součástí plnění je kompletní převod stávající funkční konfigurace ze současných firewallových řešení (lokalita Kyjov + lokalita Veselí nad Moravou) na dodávané NGFW včetně:

- Bezpečnostních politik (ACL, FW rulesets)
- Objektů sítí, adres a služeb
- NAT pravidel
- Routingových tabulek a statických cest
- Segmentace sítí / VLAN / zónové politiky
- Veškerých pravidel Application Control, IPS, Web Filtering a dalších bezpečnostních funkcí

Dále musí dodavatel provést migraci a znovu-vytvoření existujících VPN přístupů, včetně:

- VPN pro uživatele
- VPN pro správce
- VPN pro externí dodavatele a servisní partnery



Specifikace minimálních požadavků technického řešení

Viz. samostatná příloha „Technické specifikace část 2.docx“.

Řešení ochrany perimetru počítačové sítě – lokalita Veselí nad Moravou

Navržené řešení ochrany perimetru počítačové sítě v lokalitě Veselí nad Moravou se skládá ze dvou hardwarových boxů běžících v HA clusteru v režimu active/passive, kdy v případě výpadku aktivního člena automaticky plně přebírá jeho funkci člen záložní. Redundantní konektivita se zbytkem síťové infrastruktury je samozřejmostí. **Next Generation Firewall** (dále jen NGFW) budou řešeny ve formě hardware appliance.

Tyto NGFW budou sloužit k permanentnímu a šifrovanému propojení lokality Kyjov a Veselí nad Moravou. Budou nakonfigurovány tak, aby všechny síťový provoz, včetně přístupu do internetu, zabezpečovaly NGFW v Kyjově. Tím bude docílený centrální monitoring datových toků v počítačové síti řešením v rámci technologie NDR a centrální ochrana prostřednictvím pokročilých služeb NGFW v lokalitě Kyjov.

Dodavatel zajistí nepřetržitou hardwarovou a softwarovou podporu výrobce v režimu 24/7 po dobu minimálně 5 let od převzetí díla.

Specifikace minimálních požadavků technického řešení

Viz. samostatná příloha „Technické specifikace část 2.docx“.

Nástroj pro monitoring datových toků (NDR)

Monitoring datových toků a základní reporting

Cílem této části projektu je implementace monitoringu datových toků a základního reportingu za účelem zvýšení schopnosti detekce a ochrany před kybernetickými útoky v rámci IT infrastruktury nemocnice. Monitoring umožní detailní sledování síťového provozu a jeho následnou analýzu.

HW- kolektor tokových dat se sondou

Systém pro analýzu síťového provozu a bezpečnostní monitoring, který okamžitě identifikuje bezpečnostní rizika a události a který splňuje klíčové požadavky uvedené v technické specifikaci. Při definici technických požadavků jsou všechny uvedené požadavky závazné. Je-li definice požadavku „umožňuje, lze, je možné, možnost, ...“ je uvedený parametr závazný a požadovaná funkcionalita musí být v rámci systému dodána/naimplementována a případně licencována. Tyto technické požadavky



jsou minimální možné, poskytovatel (dále také „dodavatel“) může nabídnout charakteristiky (funkce) lepší.

Implementační služby

Všechna dodavatelem instalovaná zařízení nebo komponenty musí být dodavatelem profesionálně nainstalována a zprovozněna a po jejich nasazení řádně dokumentována a otestována, vč. prokázání, že tato zařízení plní všechny požadované a výkonnostní parametry.

Všechna dodavatelem instalovaná zařízení budou zabezpečena a nebudou obsahovat zjevná rizika a zranitelnosti, a to po celou dobu provozu služby.

Dodavatel zajistí vyladění a nastavení detekce všech dodávaných systémů tak, aby nebyly detekované nežádoucí a falešně pozitivní události. Tato činnost bude provedena ve spolupráci s kompetentními osobami zadavatele. Dodavatel zajistí integraci nástroje s aktuálním log managementem zadavatele, dále pak nastavení aktivních alertů a reportů dle potřeb zadavatele.

Produktová podpora výrobce

Dodavatel musí zajistit:

- softwarovou produktovou podporu řešení v délce 60 měsíců od podepsání akceptačního protokolu po předání monitorovacího systému
- záruku na veškerá dodaná HW zařízení minimálně v rozsahu 5 let NBD ode dne akceptace (Next-Business Day) On-Site

Administrátorské školení

V rámci realizace je požadováno administrátorské a uživatelské školení pro zaměstnance zadavatele v rozsahu nezbytném pro kvalifikovanou obsluhu včetně videozáznamu pro zpětné použití, který bude dostupný online na zabezpečeném úložišti dodavatele. Dále je požadováno opakované proškolení uživatelů jednou ročně v rozsahu minimálně 1MD, včetně revize analýzy bezpečnostních událostí ve všech lokalitách.

Specifikace minimálních požadavků technického řešení

Viz. samostatná příloha „Technické specifikace část 2.docx“.



Dvoufaktorová autentizace přes VPN

Řešení systému pro dvoufaktorovou (2FA) autentizaci

Cílem této části projektu je dodávka kompletního systému pro dvoufaktorovou autentizaci (2FA). Tato autentizace bude využívána pro přístup do VPN prostřednictvím zařízení řešených v kapitole „**Řešení ochrany perimetru počítačové sítě**“ tohoto projektu. Řešení musí být kompatibilní a integrovatelné se systémem Network Access Control (NAC), který je popsán v kapitole „**Řešení přístupu zařízení a uživatelů do LAN a WLAN včetně segmentace**“.

Součástí integrace musí být minimálně:

- synchronizace uživatelských účtů z Active Directory (AD) nebo ekvivalentní adresářové služby do cloudu (bez přenosu hesel),
- a zároveň lokální ověřování prvního faktoru (např. hesla) vůči AD.

Zadavatel požaduje licencování alespoň pro **300 registrovaných uživatelů**. Pokud je licencování řešení založeno na počtu uživatelů a softwarový token není součástí licence, musí nabídka zahrnovat minimálně **300 licencí pro SW tokeny**.

Jedná-li se o časově omezenou licenci (subscription), musí být tato licence minimálně na 5 let.

V rámci dodávky musí být rovněž zajištěna **kompletní instalace a konfigurace** systému dvoufaktorové autentizace.

Specifikace minimálních požadavků technického řešení

Viz. samostatná příloha „Technické specifikace část 2.docx“.