Veřejná zakázka s názvem

Bezbariérové úpravy ZŠ Komenského 17 Domažlice a vybudování odborných učeben – konektivita a vybavení IT

**Technická dokumentace**

1. Současný stav technické infrastruktury

Školní komplex se skládá z několika vzájemně propojených budov. Hlavní budovy 1. a 2. stupně (historická zástavba) jsou třípodlažní, nová spojovací budova dvoupodlažní. Ve spojovací budově se nachází několik tříd, jídelna, družina a šatny. Součástí komplexu je školní sportovní hala se třemi tělocvičnami, která je podzemním tunelem propojena s hlavními budovami. Celková situace je patrná z následujících obrázků.



Obrázek 1 – celkový pohled na školu (zprava 1. stupeň, jídelna/družina, 2. stupeň)



Obrázek 2 – areál školy

Současná kabeláž školy vznikala nárazově bez dlohodobého konceptu dle momentálních potřeb a i vzhledem k tomu neodpovídá dnešním standardům a předeším potřebám školy a projektu.

Žadatel v současnosti nedisponuje technologickým centrem ani řádnou ICT infrastrukturou pro implementaci a provoz plánovaných řešení. Stav jednotlivých technických zařízení je uveden dále.

1. WAN / Internet

Žadatel – škola - je připojena do metropolitní sítě (MAN) vlastněné a provozované městem Domažlice, které je Zřizovatelem školy. Připojení je provedeno optickým spojem o rychlosti 1 Gb. Prostřednictvím MAN je škola připojena k Internetu rychlostí 100 Mbit. Připojení je symetrické, bez agregace a není uplatňováno žádné omezení. Celková rychlost připojení MAN k Internetu je v současné době 500 Mbit.

Připojení k Internetu zajišťuje společnost United Networks SE.

Rychlost a kvalita současného internetového připojení v současnosti vyhovuje. Za nevyhovující je považováno zabezpečení, které v současnosti neumožňuje využívat všech moderních metod pro řízení provozu (např. filtrace URL adres, antivirová kontrola internetového provozu) ani jeho sledování.

Škola využívá vlastní firewall Microsoft ISA (Internet Security and Acceleration) Server ve verzi 2000.

Žadatel má v současnosti přidělenu veřejnou IPv4 adresu 46.23.56.69, nemá IPv6 adresu. Žadatel v současné době nemá validující DNSSEC resolver na straně školy, neprovádí žádný monitoring provozu. Zabezpečení internetového provozu je jen základní (NAT a statická pravidla), bez pokročilých bezpečnostních funkcí UTM (Unified threat management).

1. LAN

Existující rozvody LAN pokrývají pouze nejzákladnější potřeby – jde o jednotlivé kabely rozvedené do některých třída a učeben. Ve třídách je instalována maximálně jedna LAN zásuvka. Kabeláž není strukturovaná a použité kabely a jejich zapojení neumožňují plošně zajistit připojení koncových zařízení alespoň rychlostí 100 Mbit. Další jednotlivé rozvody slouží k napájení WiFi přístupových bodů. Kabeláž je rozvedena částečně ve vkládacích lištách a v omítkách. Propojení budov je zajištěno optickým kabelem zavěšeným nad parkovištěm školy.

Aktivní prvky – přepínače – disponují převážně základními možnostmi správy bez podpory standardu 802.1X a poskytují převážně porty o rychlosti 10/100 Mbit. Přepínače jsou od různých výrobců – Ubiquity, Zyxel, TP-Link. Přepínače jsou většinou umístěny v datových rozvaděčích. Rozvaděče nejsou uzamykatelné a prvky nejsou zabezpečeny proti neoprávněné manipulaci.

1. WiFi

Škola provozuje síť WiFi, která pokrývá pouze část prostor. Síť je logicky (různá SSID) rozčleněna na 2 sítě – jedna slouží pro potřeby učitelů, druhá žákům pro účely výuky. Síť je sestavena z přístupových bodů pracujících v pásmu 2,4 GHz. Pro ověřování přístupu do sítě je používáno sdílené heslo. Přístupové body jsou umístěny bezpečně mimo dosah osob.

Žadatel v současné době není zapojen do federovaného systému Eduroam.

1. Racková skříň, datový rozvaděč

Stávající hlavní datový rozvaděč nemá kapacitu pro umístění nových aktivních prvků a zakončení nových rozvodů. Žadatel nemá žádný datový rozvaděč pro umístění serverových technologií.

1. Diesel agregát

Zadavatel nemá k dispozici dieselagregát.

1. Záložní zdroj napájení (UPS)

UPS jsou používány jen u serverů – malokapacitní, určené pro PC. Stávající zařízení nemají dostatečný výkon na pokrytí energetických nároků nově pořizovaných technologií.

1. Zhášecí systém

Zadavatel nemá k dispozici zhášecí systém.

1. Napojení na EZS

Škola je napojena na EZS.

1. Zabezpečení přístup do budovy

Žadatel v současné době používá přístupový systém umožňující vstup do budovy osobám na základě identifikace elektronickým prvkem (např. čipovou kartou) nebo biometrickým údajem (např. otiskem prstů).

Přístupový systém je realizován čipy, které užívají učitelé i žáci systémem ZWare.

1. Monitorovací systém serverovny

Žadatel nepoužívá žádné monitorovací systém pro sledování prostředí serverovny (teplota, vlhkost apod. a systém pro sledování a řízení přístupů).

1. Klimatizace

Zadavatel nemá k dispozici klimatizační jednotku.

1. Systémová infrastruktura

Systémová infrastruktura poskytuje služby sdílení souborů a tiskáren a služby webového serveru. Pro sdílení souborů i další služby (webové aplikace) je využívána bezplatná (školní) verze GoogleApps. V LAN je implementována adresářová služba Active Directory. Pro přihlašování uživatelů jsou používány sdílené účty. Jako školský informační systém je využíván systém Bakaláři s webovým přístupem na adrese http://www.zskom17.cz:82.

1. Správa identit

Zadavatel nepoužívá žádný systém pro řízení životního cyklu identit typu Identity management.

1. Servery

Žadatel používá 1 fyzický server bez virtualizace s operačním systémem Windows Server verze 2012R2. Hlavním účelem serverů je sdílení souborů – uživatelských dat a výukových programů – a provoz adresářové služby.

1. Virtualizace serverová

Žadatel nemá k dispozici serverovou virtualizaci.

1. Zálohování a obnova dat

Zálohování a obnova dat serverů je řešeno pomocí interního zálohování Windows serverů s ukládáním záloh a druhý server. Zálohování dat na počítačích si provádějí učitelé na přidělených zařízení sami.

1. Vzdálený přístup (VPN), terminálový přístup, VDI

Vzdálený přístup (VPN) je realizována RDP vzdáleným přístupem pro jednoho zaměstnance, terminálový přístup ani VDI nejsou k dispozici

1. Pracovní stanice (učebny a učitelé)

Žadatel využívá 54 učitelských, žákovských a administrativních počítačů. Počítače jsou průměrně 5 let staré. Operační systémy na počítačích jsou převážně Windows 7 až 10 Professional. Počítačů, které nemají licenci Windows 10 Pro, je 25.

Na konci projektu bude žadatel používat 172 počítačů a 45 nově pořízených tabletů.

1. Technické a technologické aspekty projektu

Technické řešení konektivity školy bude založeno na synergickém využití již existujících technologií Technologického centra ORP (dále jen technologické centrum), vybudovaného a rozšířeného Zřizovatelem (městem Domažlice) v rámci Výzev IOP 06 a 22, metropolitní sítě města a nových technologií pořízených v rámci tohoto projektu. Dojde tak k optimálnímu využití již investovaných prostředků Zřizovatele a škola nebude zatížena provozem a správou náročných serverových technologií – tu zajistí Zřizovatel v rámci již nastavených a ověřených postupů a systémů Technologického centra. Server školy bude umístěn v tomto technologickém centru města.

Blokové schéma na následujícím obrázku představuje rozmístění a vazby jednotlivých systémů. Je patrné, že ve škole budou umístěny a provozovány jen technologie, které jsou nezbytné pro připojení koncových zařízení. Tím budou škole minimalizovány provozní nároky.



Součástí dodávky bude:

Server  
UPS  
NAS  
Licence SW OS  
Licence antiviru  
Licence zálohování  
Centrální přepínač  
Přístupové přepínače  
Přístupové body WiFi  
Kabelové rozvody včetně příslušenství  
Optické moduly  
Bezpečnostní Certifikát

Ostatní technologie nebude Žadatel pořizovat, pro naplnění cílů projektu budou použity stávající technologie poskytnuté Zřizovatelem. Jde především o Non-IT technologie a MAN

1. Zvolené technologie
   * 1. WAN + připojení k internetu

Současné připojení k Internetu o rychlosti 100 Mbit bude zachováno. Na konci projektu bude ve škole využíváno a připojeno k Internetu 172 počítačů.. Zajištěním **internetového připojení o rychlosti 100 Mbit tak bude s výraznou rezervou zajištěno plnění požadavků výzvy.** Připojení bude symetrické, nebude uplatňováno řízení provozu ani FUP. V rámci zřízení nové přípojky bude škole poskytnuta ke stávající veřejná **IP adresa v4 i v6 adresa** a tyto adresy budou nakonfigurovány na externím rozhraní firewallu**.**

Poskytovatel internetové konektivity společnost United Networks SE má vlastní autonomní systém číslo AS197296 a je členem ISP Alliance, přes kterou propojena (peeruje) s ostatními poskytovateli. ISP Alliance je zapojena v projektu FENIX.

* + 1. DNSSEC

DNSEC je bezpečnostním rozšířením překladu doménových názvů za pomoci digitálních podpisů DNS zóny a v ní vnořených záznamů. Díky tomuto rozšíření nelze podvrhnout nebo jinak upravit odpověď DNS serveru. DNSSEC dále vylučuje většinu známých praktik zneužití regulérních DNS serverů k útokům na třetí cíle. Významně tak zvyšuje bezpečnost a zajišťuje autenticitu odpovědí. Pro plné nasazení DNSSEC budou v rámci projektu realizována opatření ve dvou oblastech:

**Externí zóna** - škola používá doménu **zskom17.cz** registrovanou v TLD (Top Level Domain) .cz, pod jejímiž DNS záznamy jsou publikovány služby na jmenných (NS) serverech externího registrátora, nikoliv na svém vlastním NS serveru. V rámci projektu budou ve spolupráci s registrátorem domény doplněny podpisy DNSSEC k používaným zónám a zároveň budou doplněny záznamy pro služby publikované skrz IPv6 adresy, viz výše v kapitole - Chyba: zdroj odkazu nenalezen. Pokud současný registrátor neumožní doplnění podpisů DNSSEC, bude zóna převedena k jinému registrátorovi.

**Externě zajišťované služby** (hostování webu školy a Bakaweb) budou ve spolupráci s poskytovateli či provozovateli těchto služeb nastaveny i pro publikaci na **IPv6** adresách, pokud již nejsou. Pokud současný provozovatel neumožní provoz služby na IPv6, budou služby převedeny k jinému provozovateli.

**Publikované interní služby** (vzdálený přístup) bude publikováno na přidělených IPv4 a IPv6 adresách a bezpečnost přenášených informací bude zajištěna šifrováním pomocí SSL – webové rozhraní bude přístupné protokolem https.

**Vnitřní validující resolver** - řešení zajistí bezpečný překlad DNS jmen na IP pro veškerá uvnitř připojená zařízení a to, vzhledem k vyžadovanému dual-stacku, shodně pro obě verze IP protokolu. Bezpečným překladem se rozumí DNS server (resp. 2 servery pro redundanci) uvnitř organizace, který bude schopen za pomoci rozšíření DNSSEC ověřovat podpisy dotazovaných zón resp. hash podpisy jednotlivých záznamů jako odpovědí na DNS dotazy vnitřních zařízení. Tento DNS server musí současně zajišťovat i překlady pro dosud nepodepsané externí domény a zóny.

DNSSEC kontroly (tzv. validace) budou probíhat výhradně na DNS resolveru tak, aby nebyla nutná jakákoliv úprava konfigurace vnitřních klientů. Validující DNSSEC resolver bude konfigurován tak, aby se sám dotazoval výhradně tzv. ROOT serverů nebo jiných důvěryhodných DNSSEC serverů, které bude zároveň používat jako tzv. Trust Anchors. V rámci projektu bude validující DNSSEC resolver vytvořen jako funkční rozšíření nově instalovaných DNS serverů rolí v rámci nově pořízených operačních systémů.

* + 1. FireWall

V rámci projektu bude využit stávající vysoce dostupný cluster dvou UTM firewallů Fortinet FG-200D Technologického centra. Žadateli bude v rámci clusteru vytvořen vlastní virtuální kontext (virtuální firewall) a tento bude nasazen jako bezpečná brána připojující organizaci k Internetu resp. ke konektivitě poskytovatele s využitím technologie **NAT dle RFC 2663**. Firewall zajistí oddělení vnitřního a vnějšího provozu na základě tzv. zón a mezi nimi postavených komunikačních pravidel (**ACL/xACL**), tzv. politik. Bude plně podporovat dual-stack (IPv4 a IPv6 provoz), musí umožnit budoucí rozšíření do vysoké dostupnosti (tzv. HA) min. v režimu Active/Pasive) a bude plně vybaven (vč. potřebné sady licencí) tzv. next-gen funkcemi vč. komplexní sady pro unified-threat-management (UTM). Firewall bude schopen blokovat nejčastější útoky typu odepření služby (DoS) a bude účinně blokovat podvržení adresy (**spoofing**).

Firewall zajistí zosobnění žáků a zaměstnanců s jejich Internetovými aktivitami napojením na účty v doméně adresářové služby tak, aby byla na firewallu neustále k dispozici aktuální vazba uživatel-IP adresa, případně i zdrojový rozsah portů. Konfigurace politik firewallu a jeho jednotlivých rolí umožní pohodlnou práci s účty i skupinami adresářové služby namísto IP adres a to ve všech úrovních, tedy vč. kategorizace a filtrace provozu. Role politiky budou schopny pracovat minimálně s těmito objekty – IP/subnet, uživatel/skupina, typ zařízení/operační systém.

Pro splnění požadavku Standardu konektivity škol na logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas – uživatel, a to včetně ošetření v případě sdílených učeben (pracovních stanic apod. bude realizováno napojení firewallu na adresářovou službu pomocí softwarového agenta instalovaného na doménové kontroléry. Agent bude vyčítat statické informace o skupinách a účtech v LDAP adresáři a bude periodicky čerpat informace o aktuálně přihlášených uživatelských účtech ze security logu řadičů adresářové služby a také bude zajišťovat trvalost vazby IP-uživatel.

Firewall bude schopen omezovat šířku pásma (tzv. **rate limiting)** ve vybraných komunikačních pravidlech libovolné politiky firewallu. Omezení bude možno aplikovat jen pro vybrané skupiny vnitřních uživatelů. Firewall tedy musí umožnit rychlostní omezení určených komunikací, ale zároveň musí být schopen jiné druhy komunikace naopak upřednostnit (prioritizovat).

**Kontrola webového provozu** nešifrovaného i šifrovaného (protokoly **http a https**) je mandatorním požadavkem Standardu konektivity škol a firewall ji bude umožňovat spolu s další UTM funkcionalitou. Pořízený firewall umožní provádět shodně inspekci šifrovaných (SSL) spojení vybraných protokolů i jejich nešifrovaných verzí – minimálně protokoly HTTPS, SMTPS, POP3S, IMAPS, FTPS a inspekce na jejich výchozích portech. Pokud bude předkládán certifikát firewallem, musí být platný a důvěryhodný min. ve vnitřní síti.

**Kategorizace a selekce obsahu** bude odlišná v závislosti na uživatelské skupině – požadovány budou minimálně dva profily – **žák (student) a učitel**. V obou případech bude kategorizace a selekce prováděna na základě kategorií automaticky aktualizovaných v rámci aktualizací UTM. Veškerá varování uživatele v souvislosti s kontrolou obsahu musí být v českém jazyce a formou zobrazené náhradní webové stránky (např. s upozorněním na pravidla využívání ICT a vysvětlením důvodu blokování). K dispozici musí být možnost přesměrování uživatele na původní požadovanou stránku po stanovené době. V případě chybné blokace bude mít uživatel možnost požádat pohodlnou formou o uvolnění, resp. změnu kategorie stránky. Kategorizace a selekce obsahu bude prováděna i pro šifrovanou (**https, SSL**) verzi http protokolu.

**Identifikace útoků a IPS** bude dalším bezpečnostním prvkem pořízeného next-gen firewallu. Ochrana proti průniku (IPS) pracuje podobně jako antivirus na základě definic připravených výrobcem. Definice mají výrobcem nastavenu zároveň i výchozí akci, jak s identifikovanou komunikací naložit (min. blokace, monitorování, reset). Ve většině případů jsou výchozí akce plně vyhovující a důvěřovat výrobci firewallu, že v definicích použité výchozí akce jsou pravidelně revidovány stejně jako jejich další rozšiřování o nově identifikované hrozby vč. jejich případně blokace. Zařazením profilů IPS do vybraných v komunikačních pravidlech firewallu bude zajištěna **automatická blokace identifikovaného útoku** bez nutnosti zásahu správce. Firewallem zaznamenané útoky nebo jim podobné nežádoucí komunikace se mohou dále odrazit v rekonfiguraci pravidel firewallu popřípadě ve filtračních (ACL) pravidlech na páteřním L3 přepínači, to však již bude vyžadovat zásah správce. Rekonfigurace pravidel bude možné snadno provádět v intuitivním grafickém rozhraní zařízení.

**Antivirová kontrola** prováděná firewallem bude umožňovat konfiguraci minimálně dvou úrovní hloubky kontroly/rychlosti a vytvoření tzv. profilů, které bude možno dle potřeby uplatnit v jednotlivých komunikačních pravidlech (politikách) firewallu dle druhu a povahy konkrétního pravidla. Antivirová kontrola bude aplikována i na šifrovaná spojení (https, SSL). Infikované soubory musí být možno odstranit či zablokovat.

**Vzdálený přístup** formou zabezpečeného tunelu skrze Internet bude sloužit především zaměstnancům k jejich práci z míst mimo školu a dodavatelům IT služeb. Zaměstnanci by neměli být omezováni technologicky, firewall musí umožnit vytvoření tunelu zabezpečeného protokolem SSL nejlépe na výchozím portu tcp/443 a musí být k dispozici multiplatformní klientská aplikace nebo nativní (reverse proxy) přístup skrze webový portál firewallu a jeho aplikace (SMB, RDP, SSH, HTTPS apod.). Konfigurace VPN musí být provedena tak, aby bylo možné bezpečně ověřovat uživatelské účty v adresářové službě a autorizovat je pro přístup na základě členství ve skupině adresářové služby. K tomuto účelu může být využit standardní RADIUS protokol nebo zabezpečený LDAP. Obojí může být konfigurováno jako role interního serveru, ovšem s důrazem na redundanci. Ověřování musí být konfigurováno proti dvěma nezávislým serverům, nehledě na použitý protokol. K zabezpečení SSL komunikace (VPN) musí být pořízen a na firewallu instalován a konfigurován certifikát (nejlépe typu wildcard) vystavený některou veřejnou a důvěryhodnou certifikační autoritou (root CA) tak, aby byl na straně uživatele považován za validní a platný. Certifikát výrobce hardware či software nebo vystavený pomocí interní CA organizace nemůže být považován za dostatečný pro tento účel. Certifikát bude též použit pro zabezpečení publikovaných služeb školy (např. webového portálu školského informačního systému).

**Publikace (zpřístupnění z Internetu) online služeb školy** na adresách **IPv4 i IPv6** bude zajištěna funkcionalitou tzv. reverzního proxy firewallu společně s inspekcí provozu – přístupu k těmto službám. Pro **zabezpečení přístupových protokolů (SSL/TLS) publikovaných služeb** bude pořízen a instalován tzv. hvězdičkový (wildcard) certifikát vydaný veřejnou certifikační autoritou.

* + 1. Pokrytí LAN

Současné pokrytí LAN je nedostatečné jak v prostorech dotčených hlavním projektem, tak v celém prostoru základní školy. Některé prostory, kde probíhá výuka nebo příprava na ni, nejsou LAN pokryty vůbec. Proto bude v rámci projektu vybudována nová strukturovaná kabeláž, která pokryje prostory, ve kterých probíhá výuka a/nebo příprava na ni.

Celkový rozvod LAN bude veden z hlavního datového rozvaděče umístěného v budově 1. stupně 2. NP. V hlavním rozvaděči bude umístěn centrální přepínač, NAS a UPS. Z hlavního rozvaděče budou optickými trasami připojeny všechny podružné rozvaděče a bude svedeno i připojení MAN, které ústí na půdě budovy 1. stupně. Horizontální (patrové) rozvody budou provedeny metalickými kabely min. CAT 6 uloženými v omítce obvodového zdiva - v době realizace projektu bude již hotová příprava (stavební práce pro kabeláž jako jsou průrazy, připravené drážky v omítce pro pokládku kabelů a optiky; součástí přípravy nejsou flex trubky a příslušenství pro kabeláž jako takovou..) a tyto kabely budou ukončeny v datových rozvaděčích viz. kapitola 4.2.4.

* + 1. Rozvody, kabeláž

Vnitřní kabelové rozvody budou provedeny metalickými kabely min CAT 6. Páteřní spoje mezi datovými rozvaděči budou provedeny optickými kabely se singlemodovými vlákny a mezi datovými rozvaděči budou k dispozici vždy min. 2 vlákna.

* + 1. Rychlosti, zapojení

Veškeré metalické rozvody budou dostatečné pro komunikaci o **rychlosti 1Gb až na úroveň koncových zařízení**, **serverů a ostatních zařízení**. Optické rozvody vyhoví rychlostem **min 10 Gb.**

V rámci projektu bude navýšena rychlost připojení do metropolitní sítě a Technologického centra na 10 Gb pro zajištění nízké latence komunikace se serverem a logovacím systémem umístěnými v Technologickém centru. Na straně Technologického centra jsou k dispozici příslušné 10 Gb porty.

Současné aktivní prvky LAN technicky nevyhovují nárokům na požadovanou úroveň zabezpečení. V rámci projektu budou proto pořízeny a implementovány následující aktivní prvky, které umožní připojit všechna síťová i koncová zařízení rychlostí min. 1 Gb, servery 10 Gb:

**centrální přepínač** L2, L3 s neblokující architekturou a podporou 802.1Q VLAN, 802.1X, RADIUS based, MAC autentizace, s minimálně 24 metalickými 1GbE porty, 16 porty SFP a 4 porty 10 Gb SFP+. Přepínač bude umožňovat export provozních informací o přenesených datech v členění minimálně zdrojová/cílová IP adresa, zdrojový/cílový TCP/UDP port (či ICMP typ) - RFC3954 nebo ekvivalent (např. NetFlow) bez negativního dopadu na výkon přepínače. Přepínač bude pořízen včetně potřebných optických modulů (SFP, SFP+) a propojovacích kabelů.

**přístupový přepínač** s neblokující architekturou a podporou stohování pro snadnou správu a s plnou podporou 802.1Q VLAN a 802.1X, včetně potřebných optických modulů (SFP, SFP+) a propojovacích kabelů. Bližší specifikace přepínačů jsou uvedeny v kapitole **Chyba: zdroj odkazu nenalezen**.

Všechny přepínače budou podporovat **současný provoz IPv4 a IPv6** protokolu – tzv. **dualstack**.

Součástí dodávky projektu budou i potřebné propojovací kabely.

* + 1. WiFi a její pokrytí

Aktuální pokrytí WiFi nedostačuje potřebám Žadatele a použité prvky neumožňují provoz v pásmu 5 GHz. Bude vybudována nová WiFi síť pokrývající nejen prostory dotčené hlavním projektem, ale prostory i dalších tříd, učeben a prostory pro přípravu výuky – kabinety, sborovny, družinu apod.

Širší pokrytí umožní více zapojit výpočetní techniku do výuky i mimo specializované učebny a podpořit spolupráci žáků formou např. virtuálních týmů, mezitřídní spolupráce apod.

Učitelům umožní širší pokrytí trvale využívat osobní pracovní notebook jak pro přípravu výuky, tak pro vlastní výuku i nezbytnou administrativu (zápisy do elektronické třídnice apod.), což přispěje k většímu pohodlí a vyšší efektivitě práce učitelů a také k lepšímu zabezpečení dat, než jakého lze dosáhnout na sdílených počítačích.

Pokrytí WiFi je navrženo s ohledem na trendy v oblasti notebooků i stolních počítačů – všechny notebooky na trhu umožňují WiFi připojení a počet dostupných notebooků s integrovaným RJ-45 LAN konektorem klesá. I u stolních počítačů se stává integrovaný WiFi adaptér standardem a výkon (rychlost) současných WiFi řešení je dostatečný i pro multimediální a obdobně náročné aplikace.

Architektura WiFi bude založena na **centralizovaném řešení** s **centrální správou** prováděnou **centrálním kontrolérem** (řadičem) zajišťujícím **automatické rozložení zátěže klientů**, **roaming mezi spravovanými access pointy** a **automatické ladění kanálů a síly signálu včetně detekce a reakce na non-Wi-Fi rušení**. Centrální kontrolér bude realizován jako virtuální – tj. jako softwarová součást přístupových bodů.

Pro pokrytí požadovaných prostor hlavního projektu a dalších prostor bude pořízeno **45 tenkých přístupových bodů** (thin access pointů) standardu **802.11ac** se současnou funkcí v pásmu **2,4** a **5 GHz** s podporou spektrální analýzy zajišťující **detekci a reakci na non-WiFi rušení** a band stearingu zajišťujícím automatické přepínání klientů na rychlejší komunikaci v 5 GHz pásmu. Pořízené AP budou podporovat **WPA2, PoE, multi SSID a ACL pro filtrování provozu.**

Přesné umístění a směrování pořízených AP bude provedeno na základě provedené analýzy pokrytí signálem pro zajištění konzistentní WiFi služby v pokrytých prostorách v době realizace projektu. Provedení analýzy bude součástí implementace, protože musí respektovat konkrétní technologii (vzejde z výběrového řízení) a doporučení jejího výrobce.

Řízení přístupu do sítě WiFi bude zajištěno implementací technologie **802.1X**. Ověřování a autorizace uživatelů a zařízení bude probíhat protokolem **radius** vůči vybudované adresářové službě a v budoucnu případným dalším (federovaným) systémům, např. eduroam. V rámci projektu **nebude realizováno zapojení do systému eduroam**, neboť s ohledem na umístění školy nejsou v blízké budoucnosti očekáváni a v průběhu zpracování studie nebyli identifikováni žádní zájemci o využití **eduroam**.

1. Identity, ověřování
   * 1. Architektura

Pro zajištění bezpečnosti a možnosti řízení provozu v síti a zajištění prokazatelného monitoringu, logování a auditu interního i externího síťového provozu bude vybudována centrální databáze identit na bázi adresářové služby. Identity adresářové služby budou přeneseny ze stávající Active Directory a tato bude následně zrušena, neboť vykazuje provozní chyby způsobené několikanásobným upgradem a není vhodné na ni navazovat další systémy.

Adresářová služby umožní ukládání a přehlednou správu identit (účtů včetně metadat) učitelů, žáků i externích subjektů, ale i technických prostředků – serverů, tiskáren, pracovních stanic apod. Adresářová služba bude poskytovat službu LDAP a umožní snadné napojení autentizačních mechanismů a protokolů – RADIUS, agent firewallu a dalších. Adresářová služba zajistí ověřování uživatelů pro účely jejich autorizace k přístupu k síťovým prostředkům (LAN, Internet atd.) i výpočetním zdrojům (pracovní stanice, tiskárny, sdílené složky atd.).

Technické provedení bude založeno min. na 2 řadičích adresářové služby kvůli vysoké dostupnosti. Řadiče budou provozovány ve virtuálním prostředí a budou pravidelně automaticky zálohovány. Součástí řadičů budou základní síťové služby – DNS, DHCP, obě v konfiguraci pro vysokou dostupnost.

Všechny provozované počítače, resp. jejich operační systémy musí umožnit ověřování uživatelů vůči adresářové službě.

* + 1. Zprostředkování identity, protokoly

Ověřování identit musí být dostupné i systémům, které přímo nepodporují LDAP nebo jiný protokol adresářové služby. Součástí projektu bude proto i vybudování tzv. zprostředkovatelů identit, které umožní ověřování i jinými protokoly. Technicky půjde o softwarové komponenty transformující požadavky na ověření identity do formátu akceptovaného adresářovou službou.

Pro napojení systémů implementovaných v rámci projektu budou vybudovány zprostředkovatelé pro následující systémy a protokoly:

* Operační systémy Windows – ADSI, RPC, Kerberos, SAM
* Aktivní prvky LAN, WiFi vč. kontroleru – RADIUS, EAP
* Firewall – LDAP, protokol pro komunikaci s agentem
* Monitoring, logování – LDAP
  + 1. Ověřování LAN

Ověřování přístupu do LAN bude realizováno protokolem 802.1X vůči adresářové službě prostřednictvím protokolů RADIUS a P/EAP. Zařízení musí vybavena tzv. suplikantem - softwarovou komponentou, která dokáže předávat ověřovací požadavky síťovým prvkům, které tyto požadavky ověří vůči adresářové služby. Pro ověření zařízení bez suplikantů (např. starší tiskárny, zařízení na bázi jednoduchých operačních systémů či firmware apod.) bude použita tzv. MAC based autentication – ověření na bázi MAC adresy zařízení. Neověřená zařízení nezískají přístup do sítě vůbec nebo jim bude zpřístupněna pouze VLAN s omezeným přístupem (např. Intranet).

Spolu s ověřováním (autentizací) bude implementována i autorizace, tedy dynamické zařazení klientského zařízení nebo uživatele do určené VLAN.

* + 1. Ověřování WiFi

Ověřování přístupu do WiFi sítě bude realizováno na stejném principu jako LAN (tj. protokol 802.1X + RADIUS). WiFi bude nabízet min. 4 SSID (učitelé, žáci, Guest, tabletová učebna), které budou obsluhovány samostatnými VLAN a budou napojeny RADIUS server. Učitelé a žáci budou prostřednictvím RADIUS serveru ověřováni v adresářové službě. Zabezpečení vnitřních sítí (BSSID) školy bude provedeno dle 802.1i, tedy - WPA2 s AES šifrováním a konfigurováno shodně pro obě frekvenční pásma.

Výjimkou bude síť určená výhradně pro hosty (Guest WiFi), kde bude realizován tzv. captive portál zajišťující webovou autentizaci hostů pomocí přidělených účtů nebo za pomoci před-generovaných číselných kupónů. Preferován bude captive portál firewallu s tzv. lobby přístupem pro správu a generování účtů/kupónů ne-technickou osobou.

* + 1. Vazba na monitoring

Bezchybné poskytování identit je nezbytné pro správnou funkci monitoringu, resp. logovacího systému. Pro účely sledování a řízení provozu, popřípadě jeho auditu je klíčové zajistit dohledatelnost vazeb čas-uživatel-IP-port (protokol). Monitorovací a logovací systém bude proto napojen na adresářovou službu.

* + 1. Správa identit

Pro automatizaci správy identit a řízení jejich životního cyklu bude implementován Identity management (IDM). IDM bude napojen na referenční databázi identit, kterou bude školský systém Bakaláři. IDM na základě přednastavených pravidel (včetně schvalovacích) zajistí automatické vytvoření, aktualizaci a zrušení přístupových účtů a oprávnění v adresářové službě, vůči které se ověřuje většina ICT systémů.

Nasazením systému IDM získá škola nástroj, který zajistí bezpečné a automatizované nakládání s identitami. To výrazně přispěje ke zvýšení bezpečnosti ICT a současně dojde ke snížení zátěže ICT správce.

* + 1. Monitoring a logování

Řešení systému pro monitoring a logování provozu je významným bezpečnostním prvkem, který umožňuje sledovat a vyhodnocovat chování systémů a uživatelů v reálném čase (či s minimálním zpožděním) a ukládat (logovat) historii komunikace pro pozdější řešení incidentů, audit apod. V rámci projektu bude využit stávající SIEM (Security Information and Event Management) od výrobce Extreme networks. Systém je umístěný v Technologickém centru a provozovaný Zřizovatelem. Toto řešení umožní:

• monitoring a logován NAT (RFC 2663) provozu za účelem dohledatelnosti veřejného provozu k vnitřnímu zařízení (ve spolupráci s firewallem)

• logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas – uživatel a to včetně ošetření v případě sdílených učeben (pracovních stanic apod.)

• monitorování IP (IPv4 a IPv6) datových toků formou exportu provozních informací o přenesených datech v členění minimálně zdrojová/cílová IP adresa, zdrojový/cílový TCP/UDP port (či ICMP typ) - RFC3954 nebo ekvivalent (např. NetFlow) – systém pro monitorování a sběr provozně-lokačních údajů minimálně na úrovni rozhraní WAN, ideálně i LAN, a to bez negativních vlivů na zátěž a propustnost zařízeni s kapacitou pro uchování dat po dobu minimálně 2 měsíců

* + 1. Architektura

Bude implementováno řešení, které umožní příjem a vyhodnocení všech požadovaných informací – jde o jediné komplexní zařízení, které zajistí veškeré požadované služby. Data Žadatele a přístupy k nim budou na logické úrovni bezpečně odděleny od dat ostatních subjektů. Řešení umožní správu z jedné grafické konzole a bude přístupné nativně skrze https bez nutnosti instalace klienta. Řešení umožňuje realizovat multikriteriální vyhledávání napříč informacemi z různých zdrojů (např. NETFLOW a syslog).

Veškeré dále požadované informace si bude systém automatiky získávat, vyčítat z monitorovaných systémů a současně bude umožňovat příjem protokolů určených pro přenos logovacích, provozních informací, alertů a událostí. Systém bude přijímat informace standardními, minimálně níže jmenovanými, protokoly, ze síťových zařízení a Windows server systémů. Bude umožňovat uchování každého záznamu v jeho nezměněné podobě, ale zároveň bude schopný dávat jednotlivé události ihned do souvislostí a vyhodnocovat riziko a případné bezpečnostní události aktivně notifikovat resp. reportovat.

* + 1. Zdroje logů, identit a provozních informací

Mandatorní informace, která bude v systému vždy obsažena a uchována, je vazba IP-uživatel-čas. Tuto informaci bude systém čerpat ze security event-logu adresářové služby, dále z informací o probíhajících komunikacích na straně firewallu za pomoci jeho SSO agentů či logů a dalších přístupových a autentifikačních systémů (např. RADIUS logy). Dále budou získávány informace o překladu zdrojových, vnitřních IPv4 adres na externím výstupním rozhraní firewallu, kde bude prováděn NAT. Bude se tedy jednat o informace obsažené v NAT tabulce. Spolu s tím bude po stanovenou dobu možné zpětně dohledat i vnější provoz k vnitřnímu zařízení.

Další funkcionalitou bude plnohodnotná práce se síťovými toky, jejich zpracování a archivace. Nástroje systému budou umožňovat i analytickou práci s přijímanými toky a to i zpětně.

Řešení bude umožňovat příjem provozních informací a metadat minimálně těmito protokoly:

• NetFLow nebo ekvivalent

• Syslog

• SNMP trap

• LOG Soubory

• SQL Databáze

Zároveň bude schopno vyčítat informace z Windows Event logu nativně či za pomoci vlastní sondy.

Protokol Netflow nebo ekvivalent - síťové toky budou exportovány z páteřního přepínače a z firewallu. Konfigurace flow exportu bude sladěna s konfigurací na straně příjemce – monitorovacího a logovacího nástroje (verze, porty apod.). Je požadovaný takový rozsah dat, který zahrne maximum možných toků jdoucích přes páteřní přepínač s důrazem na komunikace z/do externích sítí (WAN). Bude zpracováván minimálně tento rozsah informací - monitorování IP (IPv4 a IPv6) s obsaženou informací o přenesených datech v členění minimálně zdrojová/cílová IP adresa, zdrojový/cílový TCP/UDP port (či ICMP typ).

Protokolem SYSLOG budou exportovány veškeré provozní informace, logy, síťových zařízení včetně firewallu na všech úrovních sítě. Obsaženy musí být veškeré informace, které zařízení loguje vč. informačních s důrazem na změny konfigurace, přihlášení odhlášení, stavy jednotlivých portů a výstupy z procesu ověřování 802.1X.

LOG soubory - monitorovací a logovací nástroj bude načítat textové log soubory a v nich obsažené informace. Především se bude jednat o RADIUS log soubory. Tyto soubory budou obsahovat identitu uživatele a časy a stavy jeho žádosti o přístup. Bude se tedy jednat o kritické soubory.

SQL databáze - pro případy, kdy budou logy uchovány v SQL databázích, bude monitorovací systém podporovat i načítání těchto logů.

Eventlog – důležitou schopností monitorovacího a logovacího systému je práce s Windows Event logem. Z hlediska bezpečnosti, záznamu přístupů a statistických a provozních informací se jedná o zásadní zdroj informací. Napojení na Windows Event log bude řešeno jako nativní nebo formou samostatného agenta či sondy nebo sensoru monitorovacího a logovacího systému. Možným zdrojem musí být min. Security a System Eventlog všech serverů i pracovních stanic

* + 1. Retence

Kombinací požadavků zákona o uchování informací v elektronické komunikaci spolu s požadavky Standardu konektivity škol a praktického pohledu na možné časové prodlení mezi vznikem incidentu a jeho vyšetřováním bylo definováno, že monitorovací a logovací systém bude umožňovat retenci dat min. 180 dnů. Na tento rozsah retence musí být dostatečně dimenzován, především z hlediska diskové kapacity, RAM i CPU tak, aby nedocházelo k výkonovým ani kapacitním problémům a systém měl dostatečnou rezervu pro očekávatelný budoucí nárůst informací a jejich zdrojů.

1. Technická infrastruktura

Technická infrastruktura poskytuje prostředky pro provoz operačních systémů a softwarových aplikací, ukládání dat a jejich zálohování.

* + 1. Servery a úložiště

Pro provoz veškerých pořízených systémů a aplikací bude pořízen jeden server vybaveným rychlým interním úložištěm s vysokou kapacitou. Hardware serveru bude virtualizován a na serveru bude možno provozovat několik virtuálních serverů. Server bude připojen do sítě technologického centra úřadu duální linkou 2x 10 Gb. Server bude umístěn v Technologickém centru a bude spravován administrátory Zřizovatele.

* + 1. Zálohování

Pro zálohování bude v rámci projektu pořízeno síťové uložiště NAS s dostatečnou kapacitou pro ukládání provozních záloh a archivů logů monitorovacího a logovacího systému. Zálohování bude řízeno pokročilým zálohovacím software, který bude prostřednictvím virtualizačního hypervizoru zálohovat všechny virtuální servery – software je součástí Technologického centra. Síťové úložiště NAS bude kvůli bezpečnému oddělení záloh od produkčních dat na serveru umístěno v budově školy v centrálním datovém rozvaděči.

* + 1. Provozní zabezpečení

Provozní zabezpečení serveru bude zajištěno jeho umístěním v Technologickém centru, které je vybaveno duální klimatizací, nepřetržitým napájením včetně diesel-generátoru, zabezpečeným přístupem a environmentálním monitorovacím systémem.

Provozní zabezpečení technologií umístěných v objektu Žadatele bude tvořeno souborem non-IT technologií, které zajistí optimální podmínky pro spolehlivý chod technologií – především centrálního přepínače a NAS:

• Záložní zdroj napájení UPS zajistí min. 30 min chodu technologií při výpadku napájení

• Uzamykatelný rozvaděč zajistí bezpečné uložení technologií, správné větrání a zamezí neoprávněné manipulaci.

Vzhledem k předpokládanému nízkému tepelnému vyzařování technologií nebude pořizována klimatizační jednotka a postačí umístění technologií v běžné, dobře větrané místnosti. Tím dojde k úspoře investičních i provozních nákladů spojených s pořízením a provozem chladícího či klimatizačního zařízení.

1. Vybavení učeben

Pro nově vybudované učebny budou sloužit pro výuku a přípravu na ni tyto prostředky:

• 93x pracovních stanic včetně myši a klávesnice, 98x monitor

• 1x notebook pro přípravu výuky

• 45x tablet pro výuku, 3x uzavíratelný box pro tablety

• 10x interaktivní tabule 3křídla s projektorem

• 3x interaktivní tabule bez křídel s projektorem

• 1x projekce

• 3x barevná tiskárna A3

• 2x software pro řízení učebny

• 1x 3D tiskárna

• 1x digitální fotoaparát (zrcadlovka)

• 1x digitální kamera

• 17x software pro úpravu videa

• 85x rozhlasový IP reproduktor

1. Antivirový systém

V rámci projektu bude pro všechny stávající i nově pořízené pracovní stanice a virtuální servery (6 ks) pořízen integrovaný antivirový systém zajištující komplexní ochranu nejen před viry, ale i před ostatními typy škodlivého software (malware). Systém bude centrálně spravován a aktualizován.

Celkově bude pořízeno 172 licencí.

1. Použití konkrétních názvů a označení v této technické specifikaci

Pokud tyto zadávací podmínky obsahují požadavky nebo přímé či nepřímé odkazy na určité dodavatele nebo výrobky, nebo patenty na vynálezy, užitné vzory, průmyslové vzory, ochranné známky nebo označení původu, pak je to z důvodů, že se jedná o stávající zařízení v majetku zadavatele a systémy, se kterými musí být nabízené vybavení kompatibilní. V ostatních případech, pokud by se v některé části ZP takové požadavky nebo přímé či nepřímé odkazy na určité dodavatele nebo výrobky, nebo patenty na vynálezy, užitné vzory, průmyslové vzory, ochranné známky nebo označení původu vyskytly, pak je to z důvodů, že stanovení technických podmínek jiným způsobem nemůže být dostatečně přesné a srozumitelné. V každém takovém případě je v souladu s § 89 odst. 6 zákona č. 134/2016 Sb. o zadávání veřejných zakázek v platném znění možné nabídnout i jiné, rovnocenné řešení.

1. Popis cílového stavu a specifikace předmětu plnění

## Základní požadavky na technické řešení

* + - 1. Cílem předmětu plnění je zvýšení bezpečnosti a související modernizace IT infrastruktury, aby implementací předmětu plnění byly naplněny Standardy konektivity škol [[1]](#footnote-2) (dále jen Standard konektivity) a rozšířena funkčnosti ICT prostředí školy. Dílčí cíle dle jednotlivých komodit jsou specifikovány následovně:

| Označení | Komodita | Počet |
| --- | --- | --- |
|  | Část A |  |
| K1 | Virtualizační platforma | 1 |
| K2 | Zabezpečení LAN a Wifi | 1 |
| K3 | Monitorovací a logovací systém | 1 |
|  | Část B |  |
| K4 | Koncová zařízení | 1 |
| K5 | Systém pro podporu výuky | 1 |

Viz. aktuální verze <http://www.irop.mmr.cz/cs/Vyzvy/Seznam/Vyzva-c-47-Infrastruktura-zakladnich-skol-SVL>, Přílohy\_Specifická pravidla pro žadatele a příjemce\_výzva č.47\_7.2.2017 (zip soubor)-příloha P9\_Standard konektivity škol \_ZŠ\_- 47. výzva\_ v.1.5.docx

* + - 1. Je požadováno řešení zachovávající a rozvíjející současné softwarové platformy Microsoft pro zachování kompatibility se stávajícími systémy a aplikacemi. Přechod na jinou platformu by způsobil nepřiměřené uživatelské a provozní potíže.
      2. Pokud dodavatel vyžaduje využití konkrétních softwarových produktů a jím zvolený přístup k realizaci zadání je na takových konkrétních řešeních závislý, musí jejich pořízení zahrnout ve své nabídce v potřebném rozsahu a v rámci nabídnuté ceny.
      3. Pokud dodavatelem nabízené řešení vyžaduje komponenty či služby neobsažené v požadavcích zadání, zahrne dodavatel do své ceny všechny náklady na jejich pořízení, instalaci, konfiguraci a další služby potřebné pro uvedení do provozu.
      4. Zadavatel z důvodů co nejjednodušší a jednotné správy a minimalizace provozních nákladů vyžaduje využití stávajících prostředků a používaných technologií. V případě, že dodavatel vyžaduje ve svém řešení stejné nebo podobné funkce, jaké poskytují stávající prostředky a technologie, je povinen využít nebo vhodným způsobem rozšířit stávající prostředky.
      5. Veškeré produkty, které dodavatel dodává v rámci plnění zadavateli, musí splňovat následující podmínky:
         * jsou nové, byly oprávněně uvedeny na trh v EU nebo pochází z autorizovaného prodejního kanálu výrobce,
         * mají plnou záruku od výrobce,
         * mohou být podporovány výrobcem a mohou být součástí servisního a podpůrného programu výrobce,
         * obsahují všechny nezbytné licence na používání příslušného softwaru,
         * jsou v databázi výrobce uvedeny jako prodaná kupujícímu – zadavateli,
         * jsou určeny pro provoz v České republice.

Zadavatel si vyhrazuje právo na zjištění původu výrobků při jejich předávání, a to dle příslušných sériových čísel a právo podpisu akceptačního protokolu, osvědčujícího převzetí dodávky, až po ověření původu výrobku.

* + - 1. Veškerá dokumentace vytvořená v rámci realizace veřejné zakázky, musí být zhotovena výhradně v českém jazyce, bude dodána v elektronické formě ve standardních formátech (např. MS Office, Open Office, PDF) používaných zadavatelem na datovém nosiči a 1x v papírové formě. Struktura i forma dokumentace musí být před předáním předána ke kontrole a výslovně schválena zadavatelem.

1. Specifické požadavky na technické řešení
2. K1 - Virtualizační platforma (server, virtualizace, UPS A, NAS, SW OS, SW antivirus, zálohovací SW)

Pro provoz veškerých pořízených systémů a aplikací bude pořízen jeden server vybavený rychlým interním úložištěm s vysokou kapacitou. Hardware serveru bude virtualizován a na serveru bude možno provozovat 6 virtuálních serverů. Server bude připojen do sítě duální optickou linkou 2x 10 Gb. Pořízený server musí být výrobcem určen pro provoz v běžném, neklimatizovaném prostředí do teploty 40 stupňů Celsia (krátkodobě až 45 stupňů Celsia) – např. dle ASHRAE Class A4. Server musí obsahovat serverovou licenci v aktuální verzi a zároveň 4 licence pro provoz virtuálních serverů.

Pro zálohování bude v rámci projektu pořízeno síťové uložiště NAS s dostatečnou kapacitou pro ukládání provozních záloh a archivů logů monitorovacího a logovacího systému. Zálohování bude řízeno pokročilým zálohovacím software, který bude prostřednictvím virtualizačního hypervizoru zálohovat všechny virtuální servery. Zálohovací systém umožní zálohovat i fyzické servery a osobní počítače. Sítové úložiště NAS bude kvůli bezpečnému oddělení záloh od produkčních dat umístěno mimo místnost serveru – zadavatel určí uzamykatelnou místnost v době zpracování předimplementační analýzy, do které bude zařízení umístěno.

Provozní zabezpečení bude tvořeno souborem non-IT technologií, které zajistí optimální podmínky pro spolehlivý chod technologií – především serveru:

Záložní zdroj napájení UPS zajistí chod serveru při výpadku napájení, Další UPS zajistí chod centrálního přepínače, chod přístupových přepínačů a WiFi.

Pro zajištění bezpečnosti a možnosti řízení provozu v síti a zajištění prokazatelného monitoringu, logování a auditu interního i externího síťového provozu bude vybudována centrální databáze identit na bázi adresářové služby. Adresářová služby umožní ukládání a přehlednou správu identit (účtů včetně metadat) učitelů, žáků i externích subjektů, ale i technických prostředků – serverů, tiskáren, pracovních stanic apod. Adresářová služba bude poskytovat službu LDAP a umožní snadné napojení autentizačních mechanismů a protokolů – radius, agenta firewallu a dalších. Adresářová služba zajistí ověřování uživatelů pro účely jejich autorizace k přístupu k síťovým prostředkům (LAN, Internet atd.) i výpočetním zdrojům (pracovní stanice, tiskárny, sdílené složky atd.). Řadiče budou provozovány ve virtuálním prostředí a budou pravidelně automaticky zálohovány. Součástí řadičů budou základní síťové služby – DNS, DHCP, obě v konfiguraci pro vysokou dostupnost. Ověřování identit musí být dostupné i systémům, které přímo nepodporují LDAP nebo jiný protokol adresářové služby. Součástí projektu bude proto i vybudování tzv. zprostředkovatelů identit, které umožní ověřování i jinými protokoly. Technicky půjde o softwarové komponenty transformující požadavky na ověření identity do formátu akceptovaného adresářovou službou.

Součástí bude dodání a zprovoznění centrálního systému pro výměnu a sdílení dokumentů. Tento systém musí být plně integrován se systémy MS Office a adresářovou službou školy. Systém musí licenčně pokrývat všechna zařízení školy.

Součástí bude dodání a zprovoznění centrálního poštovního groupware systému. Tento systém musí být plně integrován se systémy MS Office a adresářovou službou školy. Systém musí licenčně pokrývat všechna zařízení školy.

Součástí bude dodání upgradu licencí pro starší počítače, které nevyužívají aktuální verzi Windows 10 Pro.  
Z hlediska bezpečnosti musí mít všechny počítače tuto licenci. Celkově bude takto upgradováno 25 zařízení.

Součástí dodávky bude antivirový SW pro 172 koncových zařízení školy. Tento počet zahrnuje jak stávající, tak nová zařízení a fyzický a virtuální server.

1. K2- Zabezpečení LAN a Wifi (centrální přepínač, přepínače, 802.1x, Přístupové body WiFi, LAN a kabelové rozvody a příslušenství, UPS B, optické moduly, bezp. certifikát)
   * 1. Centrální přepínač, přepínače

Současné aktivní prvky LAN školy technicky nevyhovují nárokům na požadovanou úroveň zabezpečení. V rámci projektu budou proto pořízeny a implementovány následující aktivní prvky, které umožní připojit všechna síťová i koncová zařízení rychlostí min. 1 Gb, s:

1x centrální přepínač L2, L3 s neblokující architekturou a podporou 802.1Q VLAN, 802.1X, RADIUS based, MAC autentizace, s minimálně 24 metalickými 1GbE porty, a 16ti porty 1 Gb SFP. Pro připojení serverů bude využit stávající přepínač technologického centra města. Tento přepínač umožňuje export provozních informací o přenesených datech v členění minimálně zdrojová/cílová IP adresa, zdrojový/cílový TCP/UDP port (či ICMP typ) - RFC3954 nebo ekvivalent (např. NetFlow) bez negativního dopadu na výkon přepínače. Pro přepínač budou pořízeny potřebné optické moduly (SFP, SFP+) a propojovací kabely.

16x přístupový přepínač s neblokující architekturou a podporou stohování pro snadnou správu a s plnou podporou 802.1Q VLAN a 802.1X, včetně potřebných optických modulů (SFP, SFP+) a propojovacích kabelů. Bližší specifikace přepínačů jsou uvedeny v kapitole Technické parametry jednotlivých zařízení včetně jejich životnosti.

Všechny přepínače budou podporovat současný provoz IPv4 a IPv6 protokolu – tzv. dualstack.

Součástí dodávky projektu budou i potřebné propojovací kabely.

* + 1. 802.1x

Na všech koncových zařízeních školy a všech relevantních aktivních prvcích bude implementováno řízení přístupů k mediu (síti) na základě rolí a členství v uživatelské skupině adresářové služby s využitím technologie 802.1X.

Pro hosty a externí uživatele bude zřízena samostatná VLAN (Guest VLAN), které bude komunikačně (min. L3 pravidla, ACL) oddělena od vnitřních sítí organizace. Tato VLAN bude mít své L3 rozhraní až na úrovní firewallu, tak aby bylo možné komunikaci podrobit kontrole za pomoci UTM nástrojů (min. AV, IPS, kategorizace obsahu) a mohl jí být přiřazen samostatný profil odlišný od profilů pro učitele a žáky. Ověřování přístupu do této VLAN bude zajištěno pomocí tzv. captive portálu – webové autorizace. Captive portál bude zajištěn firewallem případně jiným samostatným řešením nebo prvkem, ale vždy s důrazem na bezpečné oddělení uživatelského provozu od zbytku vnitřních sítí.

Řízení provozu v LAN bude realizováno vytvořením VLAN (802.1Q), segmentací sítě s routováním (přepínáním) provozu mezi VLAN na úrovni centrálního přepínače s nastavitelnými ACL. Pro řízení provozu na úrovni kvality služeb bude k dispozici technologie QoS (Quality of Services). Pro zajištění vysoké dostupnosti služeb budou klíčové aktivní prvky propojeny duálními trasami s automatickým rozkládáním zátěže a převzetím služeb v případě výpadku jedné trasy.

* + 1. Přístupové body WiFi

Ověřování přístupu do WiFi sítě bude realizováno na stejném principu jako LAN (tj. protokol 802.1X + radius). Wifi bude nabízet více SSID (učitelé, žáci, Guest, tabletová učebna), které budou obsluhovány samostatnými VLAN a budou napojeny na raduis servery. Učitelé a žáci budou prostřednictvím radius serveru ověřováni v adresářové službě. Zabezpečení vnitřních sítí (BSSID) školy bude provedeno dle 802.1i, tedy – WPA2 s AES šifrováním a konfigurováno shodně pro obě frekvenční pásma (2,4 a 5 GHz). Výjimkou bude síť určená výhradně pro hosty (Guest WiFi), kde bude realizován tzv. captive portál zajišťující webovou autentizaci hostů pomocí přidělených účtů nebo za pomoci před-generovaných číselných kupónů. Preferován bude captive portál firewallu s tzv. lobby přístupem pro správu a generování účtů/kupónů ne-technickou osobou.

Architektura WiFi bude založena na centralizovaném řešení s centrální správou prováděnou centrálním kontrolérem (řadičem) zajišťujícím automatické rozložení zátěže klientů, roaming mezi spravovanými access pointy a automatické ladění kanálů a síly signálu včetně detekce a reakce na non-Wi-Fi rušení. Centrální kontrolér bude realizován jako virtuální – tj. softwarový provozovaný v prostředí hypervizoru serveru nebo jako součást firmware přístupových bodů.

Pro pokrytí požadovaných prostor hlavního projektu a dalších prostor bude pořízeno 20 tenkých přístupových bodů (thin access pointů) standardu 802.11ac se současnou funkcí v pásmu 2,4 a 5 GHz s podporou spektrální analýzy zajišťující detekci a reakci na non-WiFi rušení a band stearingu, zajišťujícím automatické přepínání klientů na rychlejší komunikaci v 5 GHz pásmu. Pořízené AP budou podporovat WPA2, PoE, multi SSID a ACL pro filtrování provozu.

Pořízené přístupové body budou rozmístěny následovně:

• Budova 1. stupně 1. NP – 7x AP WiFi

• Budova 1. stupně 2. NP – 7x AP WiFi

• Budova 1. stupně 3. NP – 7x AP WiFi

• Budova 2. stupně 1. NP – 6x AP WiFi

• Budova 2. stupně 2. NP – 7x AP WiFi

• Budova 2. stupně 3. NP – 7x AP WiFi

• Budova 2. stupně Podkroví – 5x AP WiFi

• Přístavba - 1. NP – 1x AP WiFi

• Přístavba - 2. NP – 7x AP WiFi

• Sportovní hala - 1. NP – 2x AP WiFi

• Sportovní hala - 2. NP – 1x AP WiFi

* + 1. LAN

Současné pokrytí a kvalita LAN je nedostatečné jak v prostorech dotčených hlavním projektem, tak v celém prostoru základní školy. Některé prostory, kde probíhá výuka nebo příprava na ni, nejsou LAN pokryty vůbec. Proto bude v rámci projektu stávající kabeláž rekonstruována tak, aby pokryla požadované prostory, zajistila rozvody pro WiFi pokrytí a odpovídala běžným standardů strukturované kabeláže.

V serverovně v 2. NP hlavní budovy bude umístěn nový hlavní datový rozvaděč, do kterého bude připojený optickými trasami 1 podružný rozvaděč. V hlavním datovém rozvaděči budou umístěny klíčové technologii – centrální přepínač, NAS a UPS.

Rozmístění datových rozvaděčů bude následující:

Budova 1. stupně:

* 1. NP – 1 ks
* 2. NP – 1 ks – hlavní rozvaděč
* 3. NP – 1 ks

Budova 2. stupně:

* 1. NP – 1 ks
* 2. NP – 1 ks
* 3. NP – 1 ks
* Podkroví – 2 ks

Přístavba (družina, jídelna, třídy)

* 1. PP – 0 ks
* 1. NP – 1 ks
* 2. NP – 1 ks

Sportovní hala

1.NP – 1 ks (do tohoto rozvaděče budou svedeny horizontální rozvody celého objektu)

Veškeré metalické rozvody budou dostatečné pro komunikaci o rychlosti 1Gb až na úroveň koncových zařízení, serverů a ostatních zařízení. Ověřování přístupu do LAN bude realizováno protokolem 802.1X vůči adresářové službě prostřednictvím protokolů radius a P/EAP. Nabízená zařízení (min. stolní i přenosné počítače) musí být vybavena tzv. suplikantem – softwarovou komponentou, která dokáže předávat ověřovací požadavky síťovým prvkům, které tyto požadavky ověří vůči adresářové služby. Pro ověření zařízení bez suplikantů (např. starší tiskárny, zařízení na bázi jednoduchých operačních systémů či firmware apod.) bude použit jiný – dodavatelem navržený - vhodný způsob ověření. Neověřená zařízení nezískají přístup do sítě vůbec nebo jim bude zpřístupněna pouze VLAN s omezeným přístupem (např. Intranet). Spolu s ověřováním (autentizací) bude implementována i autorizace, tedy dynamické zařazení klientského zařízení nebo uživatele do určené VLAN. Součástí dodávky je konfigurace 802.1x na všech koncových zařízení školy.

Rozmístění LAN portů bude následující:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Budova 1. stupně 1. NP | 1xRJ45PoE pro IP rozhlas na místě stávajícího rozhlasu | 1xdvojzásuvka RJ45PoE  u katedry vyučujícího | 1xRJ45PoE pro Wifi | 1xRJ45PoE pro přístupový systém  u rámu dveří | 1xdvojzásuvka RJ45PoE  k pracovnímu stolu |
| Učebna | 1 | 1 | 1 | 1 |  |
| Učebna | 1 | 1 | 1 | 1 |  |
| Učebna | 1 | 1 | 1 | 1 |  |
| Učebna | 1 | 1 | 1 | 1 |  |
| Učebna | 1 | 1 | 1 | 1 |  |
| Učebna | 1 | 1 | 1 | 1 |  |
| učebna dílny | 1 | 1 | 1 | 1 | 2 |
| kancelář školníka |  |  |  |  | 2 |
| Chodba | 1 |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Budova 1. stupně 2. NP | 1xRJ45PoE pro IP rozhlas na místě stávajícího rozhlasu | 1xdvojzásuvka RJ45PoE  u katedry vyučujícího | 1xRJ45PoE pro Wifi | 1xRJ45PoE pro přístupový systém  u rámu dveří | 1xdvojzásuvka RJ45PoE  k pracovnímu stolu |
| Učebna | 1 | 1 | 1 | 1 |  |
| Učebna | 1 | 1 | 1 | 1 |  |
| Učebna | 1 | 1 | 1 | 1 |  |
| Učebna | 1 | 1 | 1 | 1 |  |
| Učebna | 1 | 1 | 1 | 1 |  |
| Učebna | 1 | 1 | 1 | 1 |  |
| Kabinet | 1 |  |  | 1 | 1 |
| Kabinet | 1 |  |  | 1 | 1 |
| Kabinet | 1 |  |  | 1 | 1 |
| sborovna č. dveří 15 | 1 |  | 1 | 1 | 2 |
| učebna přírodovědy č. dveří 14 | 1 | 1 | 1 | 1 | 2 |
| Chodba | 1 |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Budova 1. stupně 3. NP | 1xRJ45PoE pro IP rozhlas na místě stávajícího rozhlasu | 1xdvojzásuvka RJ45PoE  u katedry vyučujícího | 1xRJ45PoE pro Wifi | 1xRJ45PoE pro přístupový systém  u rámu dveří | 1xdvojzásuvka RJ45PoE k pracovnímu stolu |
| Učebna | 1 | 1 | 1 | 1 |  |
| Učebna | 1 | 1 | 1 | 1 |  |
| Učebna | 1 | 1 | 1 | 1 |  |
| Učebna | 1 | 1 | 1 | 1 |  |
| Učebna | 1 | 1 | 1 | 1 |  |
| Učebna | 1 | 1 | 1 | 1 |  |
| učebna hudební výchovy č. dveří 27 | 1 | 1 | 1 | 2 |  |
| Kabinet | 1 |  |  | 1 | 1 |
| Kabinet | 1 |  |  | 1 | 1 |
| Chodba | 1 |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Budova 2. stupně 1. NP | 1xRJ45PoE pro IP rozhlas  na místě stávajícího rozhlasu | 1xdvojzásuvka RJ45PoE  u katedry vyučujícího | 1xRJ45PoE pro Wifi | 1xRJ45PoE pro přístupový systém  u rámu dveří | 1xdvojzásuvka RJ45PoE  k pracovnímu stolu |
| Učebna | 1 | 1 | 1 | 1 |  |
| Učebna | 1 | 1 | 1 | 1 |  |
| Učebna | 1 | 1 | 1 | 1 |  |
| Učebna | 1 | 1 | 1 | 1 |  |
| Učebna | 1 | 1 | 1 | 1 |  |
| Kabinet | 1 |  |  | 1 | 1 |
| kabinet chemie č. dveří 10 | 1 |  |  | 1 | 4 |
| kancelář č. dveří 2 |  |  |  | 1 | 3 |
| ředitelna č. dveří 1 |  |  | 1 | 1 | 3 |
| Chodba | 1 |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Budova 2. stupně 2. NP | 1xRJ45PoE  pro IP rozhlas na místě stávajícího rozhlasu | 1xdvojzásuvka RJ45PoE  u katedry vyučujícího | 1xRJ45PoE pro Wifi | 1xRJ45PoE pro přístupový systém  u rámu dveří | 1xdvojzásuvka RJ45PoE  k pracovnímu stolu |
| Učebna | 1 | 1 | 1 | 1 |  |
| Učebna | 1 | 1 | 1 | 1 |  |
| Učebna | 1 | 1 | 1 | 1 |  |
| Učebna | 1 | 1 | 1 | 1 |  |
| Učebna | 1 | 1 | 1 | 1 |  |
| Učebna | 1 | 1 | 1 | 1 |  |
| Učebna | 1 | 1 | 1 | 1 |  |
| Kabinet | 1 |  |  | 1 | 1 |
| kabinet přírodopisu č. dveří 14 | 1 |  |  | 1 | 2 |
| kabinet českého jazyka č. dveří 13 | 1 |  |  | 1 | 2 |
| kabinet zeměpisu č. dveří 19 | 1 |  |  | 1 | 2 |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Budova 2. stupně 3. NP | 1xRJ45PoE pro IP rozhlas  na místě stávajícího rozhlasu | | 1xdvojzásuvka RJ45PoE  u katedry vyučujícího | 1xRJ45PoE pro Wifi | 1xRJ45PoE pro přístupový systém  u rámu dveří | 1xdvojzásuvka RJ45PoE  k pracovnímu stolu | 1xRJ45 PoE  K  žákovským PC |
| Učebna | 1 | 1 | | 1 | 1 |  |  |
| Učebna | 1 | 1 | | 1 | 1 |  |  |
| Učebna | 1 | 1 | | 1 | 1 |  |  |
| Učebna | 1 | 1 | | 1 | 1 |  |  |
| Učebna | 1 | 1 | | 1 | 1 |  |  |
| učebna informatiky č. dveří 27 | 1 | 1 | | 1 | 1 |  | 16 |
| učebna informatiky č. dveří 29 | 1 | 1 | | 1 | 1 |  | 16 |
| kabinet fyziky č. dveří 25 | 1 |  | |  | 1 | 4 |  |
| kabinet jazyků č. dveří 30 | 1 |  | |  | 1 | 4 |  |
| kabinet informatiky č. dveří 28 | 1 |  | |  | 1 | 4 |  |
| Chodba | 1 |  | |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Budova 2. stupně podkroví | 1xRJ45PoE pro IP rozhlas  na místě stávajícího rozhlasu | 1xdvojzásuvka RJ45PoE  u katedry vyučujícího | 1xRJ45PoE pro Wifi | 1xRJ45PoE pro přístupový systém  u rámu dveří | 1xdvojzásuvka RJ45PoE  k pracovnímu stolu | 1xRJ45 PoE k žákovským PC |
| Učebna | 1 | 1 | 1 | 1 |  |  |
| Učebna informatiky I | 1 | 1 | 1 | 1 |  | 16 |
| Učebna informatiky II | 1 | 1 | 1 | 1 |  | 16 |
| Jazyková učebna I | 1 | 1 | 1 | 1 |  | 16 |
| Jazyková učebna II | 1 | 1 | 1 | 1 |  | 16 |
| kabinet jazykové učebny I | 1 |  |  | 1 | 3 |  |
| kabinet jazykové učebny II | 1 |  |  | 1 | 3 |  |
| kabinet informatiky | 1 |  |  | 1 | 3 |  |
| kabinet speciálního pedagoga | 1 |  |  | 1 | 3 |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Přístavba 1. PP - prostor šaten | 1xRJ45PoE pro IP rozhlas  na místě stávajícího rozhlasu | 1xdvojzásuvka RJ45PoE  u katedry vyučujícího | 1xRJ45PoE pro Wifi | 1xRJ45PoE pro přístupový systém  u rámu dveří | 1xdvojzásuvka RJ45PoE  k pracovnímu stolu |
| prostor šaten | 2 |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Přístavba 1. NP | 1xRJ45PoE pro IP rozhlas  na místě stávajícího rozhlasu | 1xdvojzásuvka RJ45PoE  u katedry vyučujícího | 1xRJ45PoE pro Wifi | 1xRJ45PoE pro přístupový systém  u rámu dveří | 1xdvojzásuvka RJ45PoE  k pracovnímu stolu |
| prostor vrátnice | 1 |  |  |  | 2 |
| Jídelna | 1 |  | 1 |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Přístavba 2. NP | 1xRJ45PoE pro IP rozhlas  na místě stávajícího rozhlasu | 1xdvojzásuvka RJ45PoE  u katedry vyučujícího | 1xRJ45PoE pro Wifi | 1xRJ45PoE pro přístupový systém  u rámu dveří | 1xdvojzásuvka RJ45PoE  k pracovnímu stolu |
| Učebna | 1 | 1 | 1 | 1 |  |
| Učebna | 1 | 1 | 1 | 1 |  |
| Učebna | 1 | 1 | 1 | 1 |  |
| Učebna | 1 | 1 | 1 | 1 |  |
| Učebna | 1 | 1 | 1 | 1 |  |
| Učebna | 1 | 1 | 1 | 1 |  |
| Učebna | 1 | 1 | 1 | 1 |  |
| sborovna č. dveří 14 | 1 |  |  | 1 | 1 |
| kabinet speciálního pedagoga č. dveří 6 | 1 |  |  | 1 | 3 |
| Chodba | 1 |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Sportovní hala 0. NP | 1xRJ45PoE pro IP rozhlas  na místě stávajícího rozhlasu | 1xdvojzásuvka RJ45PoE  u katedry vyučujícího | 1xRJ45PoE pro Wifi | 1xRJ45PoE pro přístupový systém u rámu dveří | 1xdvojzásuvka RJ45PoE  k pracovnímu stolu |
| Kotelna |  |  |  |  | 1 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Sportovní hala 1. NP | 1xRJ45PoE pro IP rozhlas na místě stávajícího rozhlasu | 1xdvojzásuvka RJ45PoE  u katedry vyučujícího | 1xRJ45PoE pro Wifi | 1xRJ45PoE pro přístupový systém u rámu dveří | 1xdvojzásuvka RJ45PoE  k pracovnímu stolu |
| Tělocvična | 1 |  | 1 |  | 1 |
| kabinet TV | 1 |  | 1 | 1 | 1 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Sportovní hala 2. NP | 1xRJ45PoE pro IP rozhlas na místě stávajícího rozhlasu | 1xdvojzásuvka RJ45PoE  u katedry vyučujícího | 1xRJ45PoE pro Wifi | 1xRJ45PoE pro přístupový systém  u rámu dveří | 1xdvojzásuvka RJ45PoE  k pracovnímu stolu |
| judo tělocvična | 1 |  | 1 |  | 1 |

|  |  |
| --- | --- |
| Výtahy (jeho přesný popis je uveden v příloze č. 2, č. 3, č. 4 | 1xRJ45PoE pro přístupový systém a ovládání výtahu |
| U každých výtahových dveří vedle tlačítka pro přivolání výtahu | 1 |

* + 1. Bezpečnostní certifikát

Certifikát veřejné certifikační autority pro zabezpečení služeb publikovaných do internetu.

1. K3 - Monitorovací a logovací systém, Identity management IDM
   * 1. Monitorovací a logovací systém

Řešení systému pro monitoring a logování provozu je významným bezpečnostním prvkem, který umožňuje sledovat a vyhodnocovat chování systémů a uživatelů v reálném čase (či s minimálním zpožděním) a ukládat (logovat) historii komunikace pro pozdější řešení incidentů, audit apod. Řešení umožní:

* + - * + monitoring a logován NAT (RFC 2663) provozu za účelem dohledatelnosti veřejného provozu k vnitřnímu zařízení (ve spolupráci s firewallem)
        + logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas – uživatel a to včetně ošetření v případě sdílených učeben (pracovních stanic apod.)
        + monitorování IP (IPv4 a IPv6) datových toků formou exportu provozních informací o přenesených datech v členění minimálně zdrojová/cílová IP adresa, zdrojový/cílový TCP/UDP port (či ICMP typ) - RFC3954 nebo ekvivalent (např. NetFlow) – systém pro monitorování a sběr provozně-lokačních údajů minimálně na úrovni rozhraní WAN, ideálně i LAN) a to bez negativních vlivů na zátěž a propustnost zařízeni s kapacitou pro uchování dat po dobu minimálně 2 měsíců

Vazba na monitoring: Bezchybné poskytování identit je nezbytné pro správnou funkci monitoringu, resp. logovacího systému. Pro účely sledování a řízení provozu, popřípadě jeho auditu je klíčové zajistit dohledatelnost vazeb čas-uživatel-IP-port (protokol). Monitorovací a logovací systém bude proto napojen na adresářovou službu.

Bude implementováno řešení, které umožní příjem a vyhodnocení všech požadovaných informací – může se jednat o jediné zařízení, softwarový nástroj či appliance nebo o řešení složené z více samostatných a vzájemně kompatibilních komponent. Preferované bude takové řešení, které umožní správu z jedné grafické konzole integrovaných komponent, ideálně přístupné nativně skrze https bez nutnosti instalace klienta. Další preferencí bude ukládání všech informací do jedné databáze (nebo více integrovaných databází) tak, aby bylo možno realizovat multikriteriální vyhledávání napříč informacemi z různých zdrojů (např. NETFLOW a syslog).

Veškeré dále požadované informace si bude systém automatiky získávat, vyčítat z monitorovaných systémů a současně bude umožňovat příjem protokolů určených pro přenos logovacích, provozních informací, alertů a událostí. Systém bude přijímat informace standardními, minimálně níže jmenovanými protokoly ze síťových zařízení a Windows server systémů. Bude umožňovat uchování každého záznamu v jeho nezměněné podobě, ale zároveň bude schopný dávat jednotlivé události ihned do souvislostí a vyhodnocovat riziko a případné bezpečnostní události aktivně notifikovat, resp. reportovat.

Mandatorní informace, která bude v systému vždy obsažena a uchována, je vazba IP-uživatel-čas. Tuto informaci bude systém čerpat ze security event-logu adresářové služby, dále z informací o probíhajících komunikacích na straně firewallu za pomoci jeho SSO agentů či logů a dalších přístupových a autentifikačních systémů (např. RADIUS logy). Dále budou získávány informace o překladu zdrojových, vnitřních IPv4 adres na externím výstupním rozhraní firewallu, kde bude prováděn NAT. Bude se tedy jednat o informace obsažené v NAT tabulce. Spolu s tím bude po stanovenou dobu možné zpětně dohledat i vnější provoz k vnitřnímu zařízení.

Další funkcionalitou bude plnohodnotná práce se síťovými toky, jejich zpracování a archivace. Nástroje systému budou umožňovat i analytickou práci s přijímanými toky, a to i zpětně.

Řešení bude umožňovat příjem provozních informací a metadat minimálně těmito protokoly:

* + - * + NetFLow nebo ekvivalent
        + Syslog
        + SNMP trap
        + LOG Soubory
        + SQL Databáze

Zároveň bude schopno vyčítat informace z Windows Event logu nativně či za pomoci vlastní sondy.

Protokol Netflow nebo ekvivalent – síťové toky budou exportovány z páteřního přepínače a z firewallu. Konfigurace flow exportu bude sladěna s konfigurací na straně příjemce – monitorovacího a logovacího nástroje (verze, porty apod.). Je požadovaný takový rozsah dat, který zahrne maximum možných toků jdoucích přes páteřní přepínač s důrazem na komunikace z/do externích sítí (WAN). Bude zpracováván minimálně tento rozsah informací - monitorování IP (IPv4 a IPv6) s obsaženou informací o přenesených datech v členění minimálně zdrojová/cílová IP adresa, zdrojový/cílový TCP/UDP port (či ICMP typ).

Protokolem SYSLOG budou exportovány veškeré provozní informace, logy, síťových zařízení včetně firewallu na všech úrovních sítě. Obsaženy musí být veškeré informace, které zařízení loguje vč. informačních s důrazem na změny konfigurace, přihlášení odhlášení, stavy jednotlivých portů a výstupy z procesu ověřování 802.1X.

LOG soubory - monitorovací a logovací nástroj bude načítat textové log soubory a v nich obsažené informace. Především se bude jednat o RADIUS log soubory. Tyto soubory budou obsahovat identitu uživatele a časy a stavy jeho žádosti o přístup. Bude se tedy jednat o kritické soubory.

SQL databáze - pro případy, kdy budou logy uchovány v SQL databázích, bude monitorovací systém podporovat i načítání těchto logů.

Eventlog – důležitou schopností monitorovacího a logovacího systému je práce s Windows Event logem. Z hlediska bezpečnosti, záznamu přístupů a statistických a provozních informací se jedná o zásadní zdroj informací. Napojení na Windows Event log bude řešeno jako nativní nebo formou samostatného agenta či sondy nebo sensoru monitorovacího a logovacího systému. Možným zdrojem musí být min. Security a System Eventlog všech serverů i pracovních stanic

Kombinací požadavků zákona o uchování informací v elektronické komunikaci spolu s požadavky Standardu konektivity škol a praktického pohledu na možné časové prodlení mezi vznikem incidentu a jeho vyšetřováním bylo definováno, že monitorovací a logovací systém bude umožňovat retenci dat min. 180 dnů. Na tento rozsah retence musí být dostatečně dimenzován, především z hlediska diskové kapacity, RAM i CPU tak, aby nedocházelo k výkonovým ani kapacitním problémům a systém měl dostatečnou rezervu pro očekávatelný budoucí nárůst informací a jejich zdrojů.

* + 1. Identity management – IDM

V rámci předmětu plnění bude implementován systém pro správu identit (IDM – Identity management). Systém bude čerpat údaje o uživatelích (identitách) ze školského informačního systému Bakaláři (popis integrace přílohou č. 1 a 2 této Technické dokumentace) a bude umožňovat doplňovat uživatele ručně, pokud nejsou v systému Bakaláři.

IDM bude na základě atributů uživatele (např. třída, doba studia apod.) a zadaných pravidel automaticky vytvářet/měnit/mazat uživatelské účty a nastavovat jejich oprávnění v řízených systémech. Automaticky tak bude vytvářeno a průběžně upravováno pracovní prostředí žáků a učitelů v počítačové síti (přihlášení do sítě, přístup k programům a datům, přístup k internetu, mapování sdílených složek a tiskáren atd.) tak, aby vždy odpovídalo nastaveným pravidlům a aktuálním atributům uživatele.

1. K4 - Koncová zařízení (Pracovní stanice + monitor, notebook, tablet, úložný box pro tablet)

Pro každé dodané zařízení určené k připojení do počítačové sítě bude provedena jeho konfigurace, předvedena plné funkcionalita zařízení v síti, provedeno seznámení s vazbami zabezpečení sítě včetně vysvětlení konfigurace zařízení a demonstrováno logování provozu zařízení a činnosti jeho uživatele.

1. K5 - Systém pro podporu výuky (SW pro správu učebny, interaktivní tabule, tiskárna A3, 3D tiskárna, digitální zrcadlovka, digitální kamera, sw pro střih videa, školní rozhlas)

Předmětem plnění zahrnuje SW a HW vybavení sloužící pro výuku odborných předmětů.

Součástí dodávky bude vždy plnohodnotná instalace a konfigurace dodaných komponent. Dodavatel garantuje plnou funkcionalitu (kompatibilitu výstupů řešení) na zařízeních dodaných v rámci ostatních komodit dle této technické specifikace (serverové komponenty, koncová zařízení apod.)

1. Implementační služby

V rámci implementace předmětu plnění dodavatel realizuje pro všechny dodávané komodity K1 až K5 – následující služby, **které jsou zahrnuté v ceně dodávky**:

* Provedení předimplementační analýzy (včetně plánovaných změn v konfiguraci současné infrastruktury) a zpracování detailního finálního popisu cílového stavu a postupu implementace. Výstupem bude prováděcí dokumentace, podle které bude dodavatel řešení implementovat. Prováděcí dokumentace musí být před zahájením implementace výslovně schválena objednatelem. Prováděcí dokumentace musí respektovat a využívat osvědčené praktiky (tzv. Best Practice) a doporučení výrobců nabízených technologií.
* Dodávka a implementace předmětu plnění dle schválené prováděcí dokumentace včetně technické podpory.
* Zprovoznění a zavedení MS ActiveDirectory, integrace všech stávajících i nově dodávaných zařízení do adresářové služby.
* Vytvoření centrálních politik pro správu a ověřování uživatelů.
* Migrace uživatelských informací a uživatelských dat do nové infrastruktury.
* Provedení předimplementační analýzy (včetně plánovaných změn v konfiguraci současné infrastruktury) a zpracování detailního finálního popisu cílového stavu a postupu implementace. Výstupem bude prováděcí dokumentace, podle které bude dodavatel řešení implementovat. Prováděcí dokumentace musí být před zahájením implementace výslovně schválena objednatelem. Prováděcí dokumentace musí respektovat a využívat osvědčené praktiky (tzv. Best Practice) a doporučení výrobců nabízených technologií.
* Dodávka a implementace předmětu plnění dle schválené prováděcí dokumentace včetně technické podpory.
* Zprovoznění a zavedení MS ActiveDirectory, integrace všech stávajících i nově dodávaných zařízení do adresářové služby.
* Vytvoření centrálních politik pro správu a ověřování uživatelů.
* Migrace uživatelských informací a uživatelských dat do nové infrastruktury.

Jde o migraci dat ze stávajících serverů (sdílené adresáře učitelů, sdílené adresáře žáků) – max 50GB dat

Migrace uživatelských dat na nahrazovaných PC – max 50GB dat

Migrace služeb, které poskytuje stávající server na novou infrastrukturu (DHCP, DNS)

Příprava prostředí pro migraci systému Bakaláři (příprava virtuálního serveru MS Windows, zbylé činnosti zajistí Zadavatel ve spolupráci s dodavatelem systému Bakaláři)

* Migrace centrálních systémů do nové infrastruktury (migrace uživatelských dat a adresářových služeb ze stávající MS Active directory, do 400 uživatelů; migraci dalších dat si provede objednatel po realizaci plnění svépomocí). Migrace bude provedeno do stavu, který je specifikován: Viz. aktuální verze <http://www.irop.mmr.cz/cs/Vyzvy/Seznam/Vyzva-c-47-Infrastruktura-zakladnich-skol-SVL>, Přílohy\_Specifická pravidla pro žadatele a příjemce\_výzva č.47\_7.2.2017 (zip soubor)-příloha P9\_Standard konektivity škol \_ZŠ\_- 47. výzva\_ v.1.5.docx. Ostatní nastavení bude zmigrováno ve stávající podobě.
* Zajištění projektového vedení realizace předmětu plnění certifikovaným projektovým managerem.
* Zpracování provozní dokumentace v rozsahu detailního popisu skutečného provedení popisu činností běžné údržby a činností pro spolehlivé zajištění provozu. Popis činností běžné údržby bude pokrývat minimálně následující oblasti:

1. Active Directory – správa uživatelů a skupin, zařazení počítače do domény
2. Zálohování – kontrola činnosti, obnova souborů
3. Hypervizor – ovládání virtuálních serverů, změna jejich konfigurace
4. Monitorovací a logovacího systém – vyhledávání činnosti uživatelů a systémů, běžná správa a kontrola funkce
5. LAN a Wifi – připojení zařízení vč. podrobných uživatelských postupů pro Wifi připojení mobilních zařízení (tablety, chytré telefony, notebooky) s operačními systémy Windows 7 a 10, Android, iOS a masOS.
6. Firewall – blokování stránek, dohledání činnosti uživatele, práce s kategoriemi stránek, zablokování přístupu pro uživatele skupiny
7. Systém pro řízení učeben – podrobná příručka pro správce i uživatele

* Zpracování dokumentu Zásady využívání ICT a přístupu k síti dle Standardu konektivity pro začlenění do vnitřních předpisů školy.
* Zpracování materiálů pro školení a provedení školení v rozsahu dle kapitoly 341. této technické specifikace
* Zajištění zkušebního provozu infrastruktury v délce minimálně 2 týdnů včetně technické podpory specialistů na dané zařízení/službu s dostupností maximálně do 2 hodin na místě realizace od nahlášení požadavku v pracovní den v době od 8h do 17h.
* Provedení akceptačních testů.
* Předání do plného provozu.

Realizace dodávky bude probíhat za úplného provozu školy, dle konkrétních podmínek uvedených v kupní smlouvě na předmět plnění této technické specifikace.

Objednatel dále požaduje provést minimálně následující implementační práce na dodaných komponentech a případně dalších zařízeních. Dodavatel je dále povinen zahrnout do nabídky veškeré další činnosti a prostředky, které jsou nezbytné pro provedení předmětu plnění v rozsahu doporučeném výrobci a dle tzv. nejlepších praktik i v případě, pokud nejsou explicitně uvedeny, ale jsou pro realizaci předmětu plnění podstatné.

|  |
| --- |
| K1: Virtualizační platforma |
| * 1. Návrh a kompletní implementace serverové virtualizační platformy   2. Implementace pořízených technologií   3. Analýza dat a systémů na stávajících serverech a jejich migrace na novou platformu   4. Návrh vhodné struktury Active Directory s redundantními řadiči, její vybudování a migrace stávající   5. Návrh a realizace zálohovacího řešení   6. Implementace automatické odstávky a najetí serveru v případě výpadku a obnovení dodávky elektrické energie   7. Návrh a provedení akceptačních testů, musí zahrnovat výkonové testy   8. Upgrade stávajících zařízení zadavatele na systém Windows 10 Pro v počtu dle dodaných licenčních upgradů |
| K2: Zabezpečení LAN a Wifi |
| * 1. Analýza stávajícího síťového prostředí a návrh nového architektury LAN i WiFi   2. Implementace pořízených technologií   3. Provedení segmentace LAN – VLAN, adresování, routování   4. Zavedení IPv6 pro přístup k internetovým zdrojům publikovaným na IPv6 adresách. Dodavatel předá veškeré parametry, které je nutné nastavit na straně externích poskytovatelů zadavatele (poskytovatelé hostingových služeb, poskytovatelé připojení do internetu, poskytovatelé DNS služeb). Zadavatel následně na základě konkrétního smluvního vztahu zajistí provedení těchto změn.   5. Zabezpečení komunikace publikovaných služeb školy pomocí nabízeného certifikátu.   6. Zavedení DNSSEC pro interní DNS služby i zabezpečení domény školy   7. Návrh a implementace 802.1X pro kabelovou LAN i WiFi včetně uživatelské dokumentace pro konfigurace obvyklých zařízení a jejich systémů - PC, notebooky, chytré telefony, tablety, tiskárny - Windows, Linux, MacOS, Android, IOS, embedded systémy periferií   8. Návrh a implementace firewallu včetně vhodné konfigurace UTM (antivir, IPS, aplikační kontrola, URL filtrace dle kategorií) pro školu   9. Vybudování VPN pro vzdálený přístup uživatelů LAN na bázi webového portálu   10. Respektování min. 3 různých skupinu uživatelů (učitelé, studenti, hosté) v návrzích a implementaci bezpečnostních a ostatních politik   11. Implementace portálu pro registraci a řízení přístupů hostů – tzv. captive portál   12. Zajištění ostatních nezbytných činností pro naplnění Standardu konektivity, ovšem pouze ve vztahu k dodávaným komponentám. Pokud se jedná o činnosti, které musí realizovat Zadavatel nebo externí poskytovatel služeb, předá Dodavatel pouze podklady k požadovaným činnostem. |
| K3: Centrální logování, identity management IDM |
| * 1. Návrh a implementace systému pro centrální logování pro naplnění požadavků Standardu konektivity, především, ale nejen:      + monitoring a logování NAT (RFC 2663) provozu za účelem dohledatelnosti veřejného provozu k vnitřnímu zařízení (ve spolupráci s firewallem)      + logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas – uživatel, a to včetně ošetření v případě sdílených učeben (pracovních stanic apod.)      + monitorování IP (IPv4 a IPv6) datových toků formou exportu provozních informací o přenesených datech v členění minimálně zdrojová/cílová IP adresa, zdrojový/cílový TCP/UDP port (či ICMP typ) - RFC3954 nebo ekvivalent (např. netflow) – systém pro monitorování a sběr provozně - lokačních údajů minimálně na úrovni rozhraní WAN, ideálně i LAN) a to bez negativních vlivů na zátěž a propustnost zařízeni   2. Provedení souvisejících konfigurací monitorovaných systémů   Předimplementační analýza bude obsahovat následující oblasti specifické pro komoditu Identity management - IDM:   * 1. provedení analýzy ICT prostředí ŠKOLY se zaměřením na oblast správy uživatelských účtů, přidělování oprávnění a rolí,   2. technologický popis stávajících technologií s vazbou na systém správy identit   3. návrh životního cyklu identity uživatelů,   4. model organizační struktury,   5. přiřazení zaměstnanců a studentů k pracovním pozicím a rolím   6. atributy poskytované systémem Bakaláři ve vazbě na řízené systémů a návrh jejich využití,   7. analýzu možností správy výstupních struktur,   8. analýzu evidenčních údajů a logů,   9. návrh a provedení akceptačních testů, musí zahrnovat výkonové testy a prokázat plnou funkčnost integrací v obvyklých scénářích použití   Následně budou veškeré kroky definované v předimplementační analýze realizovány dodavatelem. |
| K4: Koncová zařízení |
| * 1. Dodávka a kompletní zprovoznění nabízených zařízení včetně potřebných montážních prací   2. Konfigurace a zprovoznění systému pro správu učebny, integrace se systémem pro ověřování zařízení přistupujících do sítě |
| K5: Systém podpory výuky |
| V předimplementační analýze budou detailně popsány veškeré integrační vazby dílčích systémů, které jsou předmětem dodávky komodity K5, dodávaných v rámci K6, primárně ve vazbě na dodávky zbylých komodit dle této technické specifikace (např. systém pro ověřování zařízení přistupujících do sítě, MS ActieDirectory) |

Akceptační testy musí pro všechny komodity vždy zahrnovat minimálně prokázání kompletnosti dodávky a požadované funkčnosti. Návrh vhodných akceptačních kritérií bude součástí návrhu předimplementační analýzy ze strany dodavatele ve vazbě na konkrétně dodávané technologie. Povinným akceptačním kritériem bude prokázání naplnění požadavků Standardu konektivity dle manuálu uveřejněného na <http://www.irop.mmr.cz/getmedia/36c80ac4-db39-48f4-a730-4a4bea8f65aa/Standard-konektivity_overeni-a-kontrola_cerven-2017_final.pdf> včetně úspěšného provedení a doložení testu na <https://www.standardkonektivity.cz/>. Prokázání naplnění požadavků poskytne dodavatel v písemné formě vhodné jako příloha k Závěrečné zprávě o realizaci projektu dle požadavků výše uvedeného dokumentu Standardu konektivity.

Náklady na provedení implementačních služeb musí být zahrnuty v nabídkové ceně k položce (komoditě), ke které se vztahují a nesmějí být vyčísleny zvlášť.

1. Školení
   * + 1. Dodavatel provede pro každou komoditu dle této technické specifikace odborné školení na obsluhu a práci s dodanými zařízeními, a to minimálně v rozsahu provozní dokumentace.
       2. Školení bude pokrývat všechna zařízení a systémy všech komodit dle této technické specifikace, dodávané v rámci předmětu plnění této technické specifikace, a to minimálně v rozsahu:
          - běžných administrátorských činností pro implementované systémy
          - standardní údržby systémů pro administrátory zadavatele
       3. Nad rámec výše uvedeného budou součástí dodávky následující školení pro 2 osoby objednatele:
          - Školení administrace konkrétně dodaných licencí serverového operačního systému – správa a konfigurace prostředí, správa virtualizace. Školení v rozsahu minimálně 2 dny (1 den teoretická část, druhý den praktická část), realizováno v místě a na prostředcích dodavatele. Je vyžadováno, aby školitel disponoval odpovídající akreditací společnosti Microsoft
          - Školení administrace systému správy a řízení adresářových služeb – správa a konfigurace adresářových služeb, správa služeb 802.1x. Školení v rozsahu minimálně 2 dny (1 den teoretická část, druhý den praktická část), realizováno v místě a na prostředcích dodavatele. Je vyžadováno, aby školitel disponoval odpovídající akreditací společnosti Microsoft
          - Školení administrace zálohovacího SW – správa systému, best practice pro zálohování a obnovu, včetně praktických ukázek. Školení v rozsahu minimálně 2 dny (1 den teoretická část, druhý den praktická část), realizováno v místě a na prostředcích dodavatele. Je vyžadováno, aby školitel disponoval odpovídající akreditací výrobce zálohovacího SW
          - Školení administrace síťového prostředí – správa systému, diagnostika chybových stavů, konfigurace nadstavbových služeb přepínačů, WiFi a firewallu, včetně praktických ukázek. Školení v rozsahu minimálně 2 dny, realizováno v místě a na prostředcích dodavatele. Je vyžadováno, aby školitel disponoval odpovídající akreditací výrobce síťových komponent
       4. Školení dále zajistí seznámení pracovníků zadavatele se všemi podstatnými částmi díla v rozsahu potřebném pro provoz, údržbu a identifikaci nestandardních stavů systému a jejich příčin.
       5. Minimální rozsah školení pro jednotlivé položky komodit K1-K5 jsou uvedeny v tabulce (celkem min. 24 hod). Školení bude probíhat v sídle zadavatele. Předpokládá se účast max. 2 osob.

|  |  |
| --- | --- |
| Položka dodávky | Počet hodin školení |
| Centrální přepínač | Viz výše |
| Přístupové přepínače | Viz výše |
| Optické moduly a příslušenství | 0 |
| Server | 2 |
| Software lic. server. OS | Viz výše |
| Upgrade na Win 10 | 0 |
| Klientské OS | 0 |
| Antivirus | 2 |
| Zálohovací software | Viz výše |
| Monitorovací a logovací systém, identity management | 8 |
| UPS | 1 |
| Síťové úložiště NAS | 2 |
| Kabelové rozvody | 0 |
| Pracovní stanice | 1 |
| Interaktivní tabule | 4 |
| Tablety, 3D tiskárna, zrcadlovka, digitální kamera | 4 |
| Celkem | 24 |

1. Harmonogram projektu

Zadavatel vyžaduje dodržení následujícího harmonogramu plnění – zde jsou uvedeny maximální možné lhůty pro jednotlivé kritické milníky. D1 značí datum nabytí účinnosti smlouvy na dodávku předmětu plnění této technické specifikace. Čísla značí počet kalendářních dnů.

Především je nutné respektovat předpokládané termíny realizace dle přiloženého souboru.

| Aktivita | Začátek | Termín |
| --- | --- | --- |
| Datum podpisu smlouvy | D | D |
| Zahájení projektu – úvodní projektová schůzka | D | D+5 |
| Předimplementační analýza – zpracování | D+5 | D+18 |
| Předimplementační analýza – připomínkové řízení, schválení | D+18 | D+25 |
| Prováděcí dokumentace – zpracování | D+25 | D+32 |
| Prováděcí dokumentace – připomínkové řízení, schválení | D+32 | D+40 |
| Realizace předmětu plnění | D+40 | D+85 |
| Školení administrátorů | D+70 | D+90 |
| Zkušební provoz | D+85 | D+90 |
| Akceptační testy | D+85 | D+90 |
| Zahájení ostrého provozu | D+90 | - |

Dodavatel může dle svého uvážení výše uvedené maximální lhůty trvání zkrátit při dodržení všech částí předmětu plnění a bez snížení kvality dodávaných služeb.

Dodavatel předloží objednateli konkrétní a závazný harmonogram plnění (tj. konkrétní termíny plnění jednotlivých aktivit) bezodkladně po úvodní schůzce k projektu. Maximální lhůty trvání uvedené výše nesmí dodavatel při tvorbě detailního harmonogramu prodloužit.

1. Popis povinných parametrů dodávaného řešení

V dále uvedených tabulkách jsou uvedeny povinné parametry prvků řešení. Dodavatel musí všechny parametry splnit, v případě nesplnění požadavku zadavatele bude nabídka dodavatele vyřazena a dodavatel bude následně vyloučen z účasti v zadávacím řízení.

Dodavatel ve své nabídce detailně popíše způsob naplnění každého povinného parametru včetně značkové specifikace nabízených dodávek. Dodavatel tedy uvede konkrétní technické parametry nabízeného zboží, vč. uvedení výrobce a obchodního / typového označení jednotlivých komponentů. Údaje o výrobci a obchodním (či typovém) označení budou uvedeny a doloženy v tabulkách povinných parametrů; konkrétní parametry mohou být buď rovněž doplněny do tabulky, nebo mohou být doloženy jinde v nabídce např. formou katalogových listů apod., v takovém případě ale musí být v tabulce odkázáno na část nabídky, ve které je možné naplnění parametru ověřit.

Popis způsobu naplnění každého povinného parametru musí být konkrétní, úplný a musí výslovně prokazovat, že nabízené řešení jednoznačně splňuje všechny aspekty povinného parametru.

**Vyplněné tabulky č. 1 až 5 z tohoto oddílu technické specifikace učiní dodavatel součástí své nabídky, k nim pak přiloží případné další dokumenty obsahující technickou specifikaci nabízeného plnění (katalogové listy apod.).**

**Tabulka č. 1** - Povinné parametry pro Komoditu **K1 - Virtualizační platforma:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **K1 - Virtualizační platforma (server, virtualizace, UPS A, NAS, SW OS, SW antivirus, zálohovací SW)** | | | | |
| **Část** | **Parametr** | **Popis parametru** | **Způsob naplnění tohoto povinného parametru – tzn. uvedení výrobce, obchodního označení, případně uvedení konkrétních parametrů** | **Odkaz na přiloženou část nabídky, kde je případně možné ověřit naplnění parametru** |
| **Server 1x** | Provedení | rackové provedení max. 2U včetně montážního materiálu do racku |  |  |
| CPU | Minimálně 2x procesor osmi-jádrový (dohromady tedy min 16 jader) a každý procesor 16 vláken. Výkon serveru dle http://www.spec.org/ CINT2006 Rates Result min. 690 bodů, CFP2006 Rates Result min. 650 bodů. |  |  |
| RAM | 128 GB, min. 2666 MT/s |  |  |
| Rozšiřitelnost RAM | min. 512 GB bez výměny modulů |  |  |
| HDD | server musí podporovat min. 10x2,5" diskové sloty typu hotplug. Server musí akceptovat disky s rozhraním SATA|NLSAS|SAS typu HDD (rotační)|SSD nebo jejich libovolné kombinace. Požadujeme osadit: 8x 1,2TB SAS 10k |  |  |
| RAID | • typu SAS, PCI Express 3.0 kompatibilní, dvoukanálový (2 konektory) |  |  |
| • podpora RAID 0, 1, 5, 6, 10, 50, 60 |
| • podpora 6/12Gbps technologie rozhraní disků, 12Gbps na port |
| • podpora Non-RAID (Pass-through) |
| • podpora Online Capacity Expansion (OCE) |
| • podpora Online RAID Level Migration (RLM) |
| • podpora Auto resume po ztrátě napájení |
| • podpora disků s formátem bloku 512n/512e/4Kn |
| • podpora TRIM/UNMAP příkazů pro SAS/SATA SSDs |
| • podpora NVRAM “Wipe” |
| • podpora End Device Frame Buffering (EDFB) |
| • podpora šifrování dat na discích (SED) |
| • přímý přístup na SSD |
| • podpora až 64 logických disků a 64TB LUN |
| • podpora DDF, uložení konfigurace na discích (COD) |
| • podpora S.M.A.R.T. |
| • podpora globálního i dedikovaného hot-spare |
| • minimálně 2GB cache, zálohované akumulátorem |
| • volba režimu RAID nebo HBA |
| • možnost interního USB rozhraní s podporou zavádění hypervisoru. |
| • možnost osadit duální SD drive s podporou RAID1 na úrovni hardware pro zavádění hypervisoru na úrovni hardware (navíc oproti internímu USB). |
| • možnost osazení PCIe karty s M.2 SSD, podpora RAID1 na úrovni hardware. Požadujeme osadit 2x 240GB M.2 SSD |
| LAN | LAN 2x Dual Port 10Bbe SFP+ Dual Port 1Gbe RJ45 BASE-T rNDC s podporou virtualizace - VMware NetQueue, Microsoft VMQ. Podpora NIC partitioning (NPAR) |  |  |
| management | Servisní modul s možnosti samostatného přístupu po management síti, možnost vzdálené klávesnice, myši a obrazovky bez nutnosti běhu OS, možnost zapínat a vypínat server, možnost bootování se vzdáleného média. Vyhrazený LAN port, podpora http/s, ssh, SNMP, syslog. Okamžité a historické hodnoty teplot a napájení. Podpora vícefaktorového ověřování (autentizace) |  |  |
| certifikace | pro nabízenou virtualizaci a provoz v běžném neklimatizovaném prostředí do 35 stupňu celsia |  |  |
| Napájení | 2x napájecí zdroj, redundance, musí splňovat požadavky na certifikaci energetické účinnosti, např. dle 80 PLUS (min. Platinum https://cs.wikipedia.org/wiki/80\_Plus ), popř. je nutno doložit, že mají při napětí 230V a zatížení zdroje 50% účinnost min. 94% |  |  |
| Záruční podmínky | Záruční servis na min. 60 měsíců zajištěný výrobcem, oprava následující pracovní den od nahlášení v místě instalace |  |  |
| Management | Stavový a diagnostický grafický displej, Stavové informace na čelním panelu s výraznou indikací nestandardních a chybových provozní stavů či parametrů (min. napájení, teplota, vada HDD. Aktivní indikace standardního provozního stavu. |  |  |
| **SW Virtualizace 1x** | Virtualizace | SW pro virtualizaci nabízeného serveru, podpora PV, BT, HW (paravirtualization, binary translation, harware-assist) virtualizace |  |  |
| Úložiště | Možnost instalace hypervizoru na SD kartu nebo USB flash |  |  |
| Zálohování | Rozhraní pro zálohovací SW třetí strany pro zálohování pouze datových bloků virtuálních disků změněných od poslední zálohy pro snížení zátěže a zrychlení zálohování |  |  |
| Management | Kompletní správa prostřednictvím webové konzole |  |  |
| Řízení zdrojů | Virtualizace a agregace fyzických serverů a připojených síťových prvků a datových úložišť do unifikovaných souborů zdrojů |  |  |
| Kompatibilita | Podpora operačních systémů Windows Vista a novější, Linux, FreeBSD jako OS ve virtuálních strojích |  |  |
| Kompatibilita | s nabízeným zálohovacím software a se stávající serverovou virtualizací |  |  |
| Bezpečnost | Možnost detailního nastavení oprávnění administrátorů k jednotlivým virtuálním serverům pro bezpečný přístup externích správců, pro poštovní server typu Exchange součástí řešení antivirová a antispamová ochrana. |  |  |
| Správa | Bezvýpadková migrace virtuálních strojů za provozu zajišťující plynulou správu a údržbu IT |  |  |
| USB podpora | Mapování fyzických USB portů do virtuálních strojů (např. licenčních klíčů) |  |  |
| Podpora | min. 60 měsíců včetně opravných a funkčních aktualizací |  |  |
| **UPS A 1x** | Provedení | Provedení do racku, max. 2U, včetně montážního materiálu |  |  |
| Elektrické provedení | Jmenovité́ napětí́ 230 V, jednofázová na vstupu i výstupu |  |  |
| Výkon (VA/W) | 2200 VA / 1980 W |  |  |
| Technologie | Line- interaktivní |  |  |
| Účinnost | Min. 95%, účiník 0,9 |  |  |
| Stabilizace | Výstupní napětí – odchylka max. ±10 % od jmenovité́ hodnoty |  |  |
| Kapacita | Doba běhu na baterie min. 7 min při 50% zátěži |  |  |
| Vstup | Zásuvka IEC C14 (16 A) |  |  |
| Výstupy | Min. 8 zásuvek IEC C13 s měřením spotřeby |  |  |
| Napájecí segmenty | Min. 2 nezávisle ovládané napájecí segmenty pro postupný náběh napájených technologií |  |  |
| Diagnostika | Vestavěný úplný́ systémový́ autotest, možnost automatického plánovaného provádění |  |  |
| Servis | Baterie musí být vyměnitelné za chodu, aniž by bylo nutné odstavovat připojená zařízení. |  |  |
| Bypass | Automatický interní bypass |  |  |
| Komunikační porty | USB, vzdálené zapnutí/vypnutí |  |  |
| Stavové informace | Stavový grafický displej pro konfiguraci a základní informace o stavu UPS |  |  |
| Řízení | Schopnost ovládání a restartování nabízeného serveru, korektní shutdown operačních systémů |  |  |
| SW kompatibilita | UPS musí být plně podporovaná výrobcem pro použití ve virtualizačních prostředích VMware a Microsoft Hyper-V, příslušný SW bude součástí dodávky |  |  |
| Záruka | min. 36 měsíců (min. 24 na baterie) |  |  |
| **NAS 1x** | Provedení | umístění do RACKu, max. 2U |  |  |
| HDD | Min. 8 pozice pro HDD hotPlug |  |  |
| Rozšiřitelnost | Podpora připojení externích disků přes USB 3.0 (min. 2 porty) |  |  |
| Hot-swap | Disky vyměnitelné za chodu. |  |  |
| Kapacita | Osazeno min. 8x 4TB  HDD SATAIII/64MB cache určených výrobcem pro NAS (nepřipouští se HDD určené jiným účelům (desktop, kamerové systémy apod.). |  |  |
| Konektivita | Min. 4 x 1GBit Ethernet porty s podporou agregace linek a redundance. |  |  |
| Výkon | Rychlost zápisu min. 110 MB/sec při RAID5 a CIFS |  |  |
| Kompatibilita | Plná podpora Microsoft Hyper-V a Windows ADS a ACL. |  |  |
| Komunikace LAN | Síťové protokoly CIFS, WebDAV, iSCSI, SSH, SNMP, http/s |  |  |
| RAM | 2 GB DDR3 SO-DIMM, rozšiřitelná až na 16 GB |  |  |
| Ochrana dat | Integrované typy ochrany dat RAID 1, RAID 5, RAID 6, RAID 10 |  |  |
| Záruka | min. 36 měsíců včetně HDD |  |  |
| **licence SW OS** | Serverové operační systémy | 3 ks licencí 64-bitového serverového operačního systému v aktuální verzi. Každá licence musí umožnit provoz min. 2 virtuálních serverů stejné verze v prostředí nabízené serverové virtualizace, dále provoz všech nabízených aplikací a management nástrojů. |  |  |
| Klientské licence | klientské licence pro nabízené operační systémy umožńující využívat těchto systémů uživatelům celkem na 172 zařízeních. |  |  |
| Klientské operační systémy pro stávající počítače | 25x Upgrade operačního systému Windows na aktuální verzi operačního systému Windows 10 Pro s možností práce v doméně |  |  |
| **Antivirus 172x** | Bezpečnost | ochrana před malware včetně ransomware, integrovaný firewall, ochrana před průnikem HIPS (Host based intrusion prevention), řízení a ochrana webového přístupu |  |  |
| Správa | Centrální správa součástí dodávky ,  jedna konzole na ochranu klientů, mailů a serveru |  |  |
| Správa navíc umožňuje | správa nedoménových klientů, nastavování politik dle vlastních dynamických skupin, přehled zastaralých aplikací, možnost nastavení vynucení obnovy OS na stanici, možnost využití příkazového řádku |  |  |
| Správa aplikací | Řízení aplikací - centrální vzdálená instalace, povolení/zákaz spouštění |  |  |
| Výměnná zařízení | Řízení přístupu (zákaz/povolen) k výměnným zařízením – USB flash/disky CD/DVD |  |  |
| Mobilní zařízení | Správa mobilních zařízení iOS a Android – omezení spouštění aplikací, řízení internetového přístupu |  |  |
| Podporované operační systémy | všechny desktopové a serverové operační systémy Microsoft aktuálně podporované výrobcem, macOS, iOS a Android |  |  |
| Lokální podpora a záruka | Lokální podpora v českém jazyce, záruka 60 měsíců včetně opravných a funkčních aktualizací |  |  |
| **Zálohovací SW 1x** | Licence | Licence zálohovacího software pro nabízený server bez omezení počtu zálohovaných virtuálních serverů a objemu dat. |  |  |
| Efektivita ukládání dat | Integrované technologie komprimace a deduplikace. |  |  |
| Nároky na správu | „bezagentové“ řešení – bez instalace agentů do zálohovaných virtuálních serverů či aplikací |  |  |
| Ochrana dat | provádění datově konzistentních záloh hlavních serverových aplikací – Microsoft SQL server, Active Directory, souborové systémy – bez nutnosti odstávky aplikace |  |  |
| Fyzické servery | Vestavěná podpora zálohování stávajících fyzických serverů – pro fyzické servery je přípustné využívat agenty |  |  |
| Podpora WAN | možnost plnohodnotné replikace přes WAN pro replikaci virtuálních serverů do vzdálených lokalit (např. Technologického centra Plzeňského kraje) |  |  |
| Snapshoty | využívání snapshotů, zálohování pouze dat změněných od poslední úspěšné zálohy |  |  |
| Kompatibilita | podpora operačních systémů Windows a Linux v zálohovaných virtuálních serverech |  |  |
| Uložiště záloh | Možnost ukládání záloh na diskový prostor a páskovou jednotku/knihovnu |  |  |
| Fyzické servery | Podpora ukládání záloh nevirtualizovaných serverů a PC do společného úložiště a monitorování zálohovacích úl |  |  |
| Správa | vytváření a správa úloh (zálohování, obnova apod.) pomocí vestavěných průvodců včetně konfigurace automatického spouštění úloh |  |  |
| Správa | automatický reporting úspěšných i neúspěšných úloh |  |  |
| Správa | Běžné úlohy obnovy (obnovení souboru, databáze SQL, objekty Active Directory) provádět pomocí průvodců. |  |  |
| Záruka | min. 12 měsíců včetně opravných a funkčních aktualizací |  |  |

**Tabulka č. 2** - Povinné parametry pro Komoditu **K2 – Zabezpečení LAN a WiFi:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **K2- Zabezpečení LAN a Wifi (centrální přepínač, přepínače, 802.1x, Přístupové body WiFi, LAN a kabelové rozvody a příslušenství, UPS B, optické moduly, bezp. certifikát)** | | | | |
| **Část** | **Parametr** | **Popis parametru** | **Způsob naplnění tohoto povinného parametru – tzn. uvedení výrobce, obchodního označení, případně uvedení konkrétních parametrů** | **Odkaz na přiloženou část nabídky, kde je případně možné ověřit naplnění parametru** |
| **Centrální přepínač 1x** | Základní parametry | L2/L3 přepínač v rackovém provedení max. 1U, osazeno duálními interními napájecími zdroji. Uživatelsky vyměnitelné redundantní ventilátory |  |  |
| Porty | minimálně 16x 1 GbE SFP, 8x 1000-BASE-T, 4x 10Gb SFP+ |  |  |
| Propustnost | neblokovaná architektura, propustnost min. 250 Gb |  |  |
| Agregace portů | podpora LACP |  |  |
| Směrování | statické a dynamické routování, policy based routing, jak pro IPv4 tak i pro IPv6 |  |  |
| Řízení provozu | víceúrovňový QoS |  |  |
| VLAN | VLAN 802.1Q, MAC i protocol based, podpora zařazování do VLAN a přidělení QoS a přístupových filtrů na základě 802.1X ověření |  |  |
| Ověřování uživatelů a zařízení | podpora 802.1X |  |  |
| Dualstack | plný IPv4 a IPv6 dualstack včetně směrování a QoS |  |  |
| Pokročilé funkce | podpora MPLS a VPLS včetně L2 a L3 MPLS VPN |  |  |
| Stohování | pokročilé stohování - až 8ks přepínačů ve stohu se chovají jako jeden z pohledu správy i připojených zařízení |  |  |
| Sledování toků | export síťových toků, minimálně sFlow nebo ekvivalent |  |  |
| Monitoring a správa | plná podpora CLI, SSH, SNMP 1-3, syslog, sFlow, RMON, web rozhraní |  |  |
| Záruční servis | Záruční servis na min. 60 měsíců, odeslání náhradního zařízení max. následující pracovní den po nahlášení závady, včetně nároku na opravné verze firmware |  |  |
| **Přepínače** | Společné parametry |  |  |  |
| Základní parametry | L2 přepínač v rackovém provedení max. 1U |  |  |
| Stohování | podpora stohování pro jednotný management (přepínače musí stohovatelné vzájemně bez ohledu na provedení - viz. Porty a propustnost) |  |  |
| Propustnost | neblokovaná architektura |  |  |
| Agregace portů | podpora LACP |  |  |
| Dualstack | IPv4 a IPv6 dualstack včetně podpory ACL a QoS |  |  |
| VLAN | VLAN 802.1Q, MAC i protocol based, podpora zařazování do VLAN a přidělení QoS a přístupových filtrů na základě 802.1X ověření |  |  |
| Ověřování uživatelů a zařízení | podpora 802.1X |  |  |
| Monitoring a správa | plná podpora CLI, SSH, SNMP 1-3, syslog, sFlow, RMON, web rozhraní |  |  |
| Záruka | Záruční servis na min. 60 měsíců, odeslání náhradního zařízení max. následující pracovní den po nahlášení závady, včetně nároku na opravné verze firmware |  |  |
| Specifické parametry |  |  |  |
| Porty | 6ks -24x 1GB RJ-45 PoE+ + 4x1Gb SFP (nesdílené) min 55Gb/s |  |  |
|  | 10ks - 48x 1GB RJ-45 PoE+ + 4x1Gb SFP (nesdílené) min. 100Gb/s |  |  |
| **Přístupové body Wifi 57x** | Základní funkce | Přístupový bod (AP) WiFi včetně montážního materiálu na stěnu nebo strop |  |  |
| Frekvence | činnost v radiovém pásmu 2,4 a 5 GHz současně, 2 radiové moduly |  |  |
| Anténní systém | interní systém min. MIMO 3x3 (5 GHz) a MIMO 2x2 (2,4 GHz), optimalizovaný pro montáž na strop |  |  |
| Přenosové rychlosti | SU-MIMO (5GHz) až 1300Mbps, MU-MIMO až 867Mbps. 2,4GHz MIMO až 300Mbps. |  |  |
| Standardy | podpora 802.3at, 802.11n, 802.11ac, 802.1x včetně přiřazování do VLAN |  |  |
| Řízení klientů | automatické směrování komunikace klientů z 2.4 GHz na 5 GHz (pokud klienti podporují obě pásma) |  |  |
| Rušení | průběžná detekce non-WiFi rušení a spektrální analýza |  |  |
| Multi SSID | podpora vysílání min. 8 SSID (WiFi sítí) současně, podpora přiřazení každého SSID samostatné VLAN |  |  |
| Zatížení | min. 250 přiřazených (asociovaných) klientů na radiový modul |  |  |
| Porty | min. 1x 1Gb, PoE s podporou standardů 802.3at |  |  |
| Řízení provozu | klasifikace a kontrola provozu, detekce obvyklých aplikací s možností určení priority nebo šířky pásma zvoleného provozu |  |  |
| Řízení kvality služeb | automatické řízení kvality služeb (QoS) pro hlas a video |  |  |
| Současná obsluha více klientů | Podpora MU-MIMO (Multi-User MIMO) - multi-user multiple input/multiple output |  |  |
| Přenosové rychlosti | SU-MIMO (Single-User MIMO) min. 1300Mb, MU-MIMO min. 850 Mb |  |  |
| Bezpečnost | Detekce cizích přístupových bodů zjištěných v LAN i v radiofrekvenčním pásmu |  |  |
| Virtuální kontroler | Virtuální, vysoce dostupný kontroler obsažený ve firmware každého přístupového bodu. Umožňuje kompletní centrální správu WiFi infrastruktury a řízení jejího provozu včetně roamingu klientů. |  |  |
| Monitoring a správa | plná podpora CLI, SSH, SNMP 1-3, syslog, web rozhraní |  |  |
| Správa frekvenčního pásma | automatické dynamické přidělování kanálů a řízení výkonu přístupových bodů pro vyrovnané pokrytí a minimalizaci interference |  |  |
| Záruka | min. 24 měsíců |  |  |
| **Kabelové rozvody a příslušenství 1x** | Popis | Kabelové rozvody včetně příslušenství a souvisejících služeb dle podrobného výkazu výměr - Kapitola 8 - Výkaz výměr dle této technické specifikace |  |  |
| Záruka | Kabelové rozvody min. 10 let, rozvaděče (racky) min. 24 měsíců |  |  |
| **UPS B 11x** | Provedení | Provedení do racku nebo mimo rack, max. 2U, včetně montážního materiálu |  |  |
| Elektrické provedení | Jmenovité́ napětí́ 230 V, jednofázová na vstupu i výstupu |  |  |
| Výkon (VA/W) | 1500 VA / 1350 W |  |  |
| Technologie | Line- interaktivní |  |  |
| Účinnost | Min. 95%, účiník 0,9 |  |  |
| Stabilizace | Výstupní napětí – odchylka max. ±10 % od jmenovité́ hodnoty |  |  |
| Kapacita | Doba běhu na baterie min. 10 min při 50% zátěži |  |  |
| Vstup | Zásuvka IEC C14 (16 A) |  |  |
| Výstupy | Min. 8 zásuvek IEC C13 s měřením spotřeby |  |  |
| Napájecí segmenty | Min. 2 nezávisle ovládané napájecí segmenty pro postupný náběh napájených technologií |  |  |
| Diagnostika | Vestavěný úplný́ systémový́ autotest, možnost automatického plánovaného provádění |  |  |
| Servis | Baterie musí být vyměnitelné za chodu, aniž by bylo nutné odstavovat připojená zařízení. |  |  |
| Bypass | Automatický interní bypass |  |  |
| Komunikační porty | USB, vzdálené zapnutí/vypnutí |  |  |
| Stavové informace | Stavový grafický displej pro konfiguraci a základní informace o stavu UPS |  |  |
| Řízení | Schopnost ovládání a restartování nabízeného serveru, korektní shutdown operačních systémů |  |  |
| SW kompatibilita | UPS musí být plně podporovaná výrobcem pro použití ve virtualizačních prostředích VMware a Microsoft Hyper-V, příslušný SW bude součástí dodávky |  |  |
| Záruka | Prodloužená záruka na min. 36 měsíců (min. 24 na baterie) |  |  |
| **Optické moduly a příslušenství** | SFP+ moduly | 2 ks modulů SFP+ 10 Gb, SM, 10km, včetně DMI diagnostiky pro nabízený centrální přepínač |  |  |
| SFP+ moduly | 2 ks moduly SFP+ 10 Gb, MM, 300m, včetně DMI diagnostiky pro nabízený server |  |  |
| SFP moduly | 11 ks moduly SFP 1 Gb, SM, 1 km, včetně DMI diagnostiky pro nabízený centrální přepínač |  |  |
| SFP+ moduly | 2 ks modulů SFP+ 10 Gb, SM, 10km, včetně DMI diagnostiky pro přepínač technologického centra HP 5800 |  |  |
| SFP+ moduly | 2 ks moduly SFP+ 10 Gb, MM, 300m, včetně DMI diagnostiky pro přepínač technologického centra HP 5800 |  |  |
| SFP moduly | 11 ks moduly SFP 1 Gb, SM, 1 km, včetně DMI diagnostiky pro nabízené přístupové přepínače |  |  |
| Optické patch kabely | ke každému SFP/SFP+ modulu kabel SM s konektory SC - dle modulu, délka 3m |  |  |
| **Certifikát** | Popis | Hvězdičkový (tzv. wildcard) certifikát veřejné certifikační autority pro zabezpečení služeb publikovaných do internetu. Kořenový certifikát certifikační autority musí být standardně obsažen v běžných desktopových a mobilních operačních systémech a být automaticky aktualizován v rámci aktualizace operačního systému. Certifikát s platností min. 60 měsíců. |  |  |

**Tabulka č. 3** - Povinné parametry pro Komoditu **K3 - Monitorovací a logovací systém, Identity management IDM:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **K3 - Monitorovací a logovací systém, Identity management IDM** | | | | |
| **Část** | **Parametr** | **Popis parametru** | **Způsob naplnění tohoto povinného parametru – tzn. uvedení výrobce, obchodního označení, případně uvedení konkrétních parametrů** | **Odkaz na přiloženou část nabídky, kde je případně možné ověřit naplnění parametru** |
| **Monitorovací a logovací systém 1ks** | Základní funkce | Systém pro sběr, ukládání a správu provozních a bezpečnostních informací a událostí ze sledovaných systémů |  |  |
| Protokoly sběru logů | syslog, TCP, UDP, HTTP, AMQP, JSON |  |  |
| Sběr síťových toků | netflow či kompatibilní dle nabízeného firewallu a centrálního přepínače |  |  |
| Zdroje logů | Min. REST API, textové soubory, Radius, Active Directory, MS SQL databáze, Windows Event Log - včetně rozšířených "Applications and Services Logs", síťové prvky - syslog a netflow, ostatní aktivní prvky - syslog, SNMP trap |  |  |
| Parsování logů | Integrovaný nástroj pro parsování logů. Možnost nahrání části logu, online vytváření parseru a snadné testování výsledku. Podpora vytváření opakovaně použitelných vzorků - např. definice IP adresy regulárním dotazem apod. |  |  |
| Retence | Uchovávání logů min. 6 měsíců, automatická retence logů a indexů |  |  |
| Geolokace | Podpora automatické doplňování logů o informaci o lokalitě podle IP adresy |  |  |
| Normalizace logů | Sjednocení názvů shodných dat z různých zdrojů logů např. pro snadné vyhledávání napříč zdroji |  |  |
| Rozšíření logů | Podpora rozšíření logů o vlastní statické a dynamické (kalkulované) položky integrovaným nástrojem. |  |  |
| Rozšiřitelnost | Podpora snadného rozšíření funkčnosti pomocí plug-inů nebo modulů |  |  |
| Bezpečnost | Podpora šifrované komunikace se zdroji (SSL apod.), ověřování zdrojů (TLS apod.) |  |  |
| Výkon | Min. 500 EPS (event per second), 5000 FPM (flows per minute) |  |  |
| Dashboardy | Uživatelské vytváření dashboardů (pracovních desek) včetně možnosti využití grafických prvků (grafy, mapy, histogramy apod.) i strukturovaných dat (tabulek) |  |  |
| Export dat | Export dat do csv a/nebo xls - min. výsledky hledání |  |  |
| Kanály | Možnost vytváření kanálů - datových sad či toků - na základě pravidel (logických podmínek) a to i napříč různými zdroji. Podpora dalšího zpracování - tvorba alarmů, zobrazení na dashboardu, online odesílání do nadřazeného systému apod. |  |  |
| Alerty, notifikace | Podpora vytváření alertů - překročení okamžitých či kumulovaných hodnot, zasílaní upozornění |  |  |
| Active Directory | integrace s Active Directory pro ověřování uživatelů, nastavení oprávnění min. administrátor a operátor |  |  |
| Vyhledávání | Rychlé a intuitivní vyhledávání v záznamech napříč všemi zdroji i při velkých objemech dat (řády TB). Jednoduchý dotazovací jazyk. Rychlá vyhledávání či filtrování bez tvorby dotazů - např. výběrem v kontextovém menu vybraného pole uloženého záznamu. |  |  |
| Ovládání | Intuitivní grafické rozhraní |  |  |
| Kompatibilita | Podpora provozu v prostředí nabízené serverové virtualizace |  |  |
| Ukládání dat | do databáze, případná databázová licence musí být součástí dodávky |  |  |
| Výstupy | Možnost výstupů do nadřazeného systému pro účely vzdáleného expertního dohledu. Zabezpečený přenos vhodným protokolem |  |  |
| Záruka | min. 12 měsíců včetně poskytnutí opravných verzí |  |  |
| **Identity management 1x** | Důvěryhodnost logování | Veškeré požadavky na změny v IDM bude možné zadávat výhradně prostřednictvím Portálu. Není přípustné realizovat požadavky ručními změnami textových soubory jako XML, CSV, atd. z důvodu zajištění úplného logování všech změn jednotlivých konfigurovaných parametrů IDM. |  |  |
| Auditní report | IDM umožní export auditního reportu z údajů o identitách uložených v IDM a to i historických. Auditní reporty budou minimálně ve formátu XML nebo CSV a budou obsahovat souhrnné zobrazení daných uživatelů (identit) a jejich rolí v IS napojených na IDM, přiřazených skupin ve vybraném časovém okamžiku od aktuálního času do minulosti. |  |  |
| Auditní report - výběr | Identity pro generování auditního reporty musí být možné vybrat (filtrovat) dle libovolných atributů identity včetně přidružených referenčních objektů. |  |  |
| Reporty uživatelů | Vestavěné reporty obsahující uživatele s přímo přiřazenými aplikačními rolemi a s aplikačními rolemi delegovanými od jiných uživatelů. Reporty budou exportovatelný do CSV souboru. |  |  |
| Reporty - historie | Automatické ukládání vygenerovaných reportů s možností pozdějšího zobrazení či stažení. |  |  |
| Webové služby (WS) | IDM bude poskytovat rozhraní webových služeb pro napojení dalších systémů s možností konfigurace v Portálu. |  |  |
| Standardy WS | Webové služby IDM budou definované v rozšířeném standardu WSDL a podporovat protokol SOAP. |  |  |
| Bezpečnost WS | Konfigurace webových služeb umožní konfigurovat přístup pro volání jednotlivých vybraných služeb pro každý odpovídající systémový účet samostatně. |  |  |
| Logování WS | Volání webových služeb bude logováno a bude možné je zobrazit v prostředí Portálu |  |  |
| Služby rozhraní WS | Rozhraní bude poskytovat minimálně následující služby: |  |  |
| - Získání organizační struktury |  |  |
| - Získání hierarchie pracovních pozic |  |  |
| - Získání seznamu identit |  |  |
| - Získání nadřízené osoby pro daného zaměstnance |  |  |
| - Získání seznamu aplikační rolí |  |  |
| - Získání seznamu uživatelů dané aplikace |  |  |
| - Zápis seznamu aplikačních rolí do IDM |  |  |
| - Zápis a změna identit |  |  |
| Synchronizace | Ruční i automatické spuštění synchronizací s propojenými systémy. |  |  |
| Synchronizace - simulace | Spuštění synchronizací i v simulačním režimu pro ověření dopadu reálného spuštění bez ovlivnění produkčních dat a napojených systémů. Simulační logy budou zobrazitelné v Portálu. |  |  |
| Simulace - průběh | Zobrazení jednotlivých stavů průběhu synchronizace bude k dispozici v přehledné grafické podobě. |  |  |
| Synchronizace - režimy | Pro napojení na jednotlivé systémy a implementaci jejich synchronizací s IDM umožní IDM u každého systému využít více režimů synchronizací (za předpokladu podpory napojovaného systému): |  |  |
| - Plná synchronizace – prochází všechny objekty v IDM a synchronizuje je s objekty daného systému |  |  |
| - Změnová synchronizace – synchronizuje vždy jen změny od poslední spuštěné synchronizace. |  |  |
| - Simulační synchronizace – synchronizace vytvoří report očekávaných změn v napojeném systému pro provedení ostré synchronizace. Report změn bude evidován jako pohled nebo přehledná souhrnná tabulka. |  |  |
| - Historie běhu synchronizací – jednotlivé běhy synchronizací budou zaznamenány v historii dostupné v Portálu. Historie plné synchronizace bude obsahovat odkazy na objekty, které byly synchronizovány a log, co bylo u těchto objektů změněno v synchronizovaném systému. V případě změnové synchronizace pak bude v historii dále informace o události, která změnovou synchronizaci vyvolala. |  |  |
| Synchronizace - správa | Vestavěná správa jednotlivých synchronizací včetně nastavení připojení na synchronizované systémy, nastavení plné a změnové synchronizace, počet změn, které je možné zpracovat, nastavení časového intervalu spouštění, nastavení intervalu odstávky. Správa bude součástí Portálu. |  |  |
| Obecný konektor | Pro správu identit nenapojených aplikací a testování. Konektor simuluje aplikaci, požadavky na změny nastavení v aplikaci zasílá e-mailem správci aplikace. Podpora zpětné vazby - správce v IDM potvrzuje provedení požadavků pro účely logování |  |  |
| Aplikační konektory | IDM bude spravovat identity a řídit oprávnění v dále vyjmenovaných systémech. V těchto systémech bude IDM vytvářet, aktualizovat, vytvářet uživatele a nastavovat jim oprávnění k rolím. |  |  |
| - Microsoft Active Directory |  |  |
| - Microsoft Office 365 |  |  |
| Zdrojový systém | IDM bude napojeno na školský informační systém Škola online. Ze systému Škola online budou načítány údaje o organizační struktuře, osobách a tyto údaje budou pro IDM sloužit jako zdrojové (popis integrace přílohou č. 1 a 2 této Technické dokumentace) |  |  |
| Podpora | Podpora software na 60 měsíců včetně nároku na opravné a nové verze |  |  |

1. Záruky a servisní podmínky
2. Požadavky na záruky a servisní podmínky
   * + 1. Zadavatel uvádí u jednotlivých komodit požadovanou min. záruku, záruční servis a podporu. V případě, že není hodnota výslovně uvedena, požaduje zadavatel standardní záruku v délce 24 měsíců s odstraněním vady nebo náhradou zařízením novým do 30 dnů od nahlášení vady v místě plnění.
       2. Z důvodu zajištění udržitelnosti projektu a zajištění bezpečnosti provozu po dobu 60-ti měsíců požaduje zadavatel poskytnutí prodloužených záruk pro některé komponenty, v jejichž popisu je informace o prodloužené záruce uvedena, při zachování ostatních parametrů původní záruky (rychlost opravy, rozsah aktualizací firmware apod.). Cenu tohoto prodloužení zahrne dodavatel pro tyto položky v Cenové tabulce (viz. Příloha č. 5 Zadávací dokumentace) do samostatných řádků označených vždy názvem položky a upřesněním prodloužené záruky. Tyto náklady nebudou hrazeny z dotace, proto je nutné vyčíslit je zvlášť.
       3. Zadavatel v rámci této technické specifikace požaduje specifické služby, které se odvíjejí od konkrétního typu plnění a to zejména následující:

* záruka – záruku v intencích zákona č. 89/2012 Sb., občanského zákoníku, ve znění pozdějších předpisů, tedy, že si předmětné plnění po dobu záruky zachová své vlastnosti a parametry z doby jeho dodávky a dále, že po celou dobu záruky bude mít parametry a vlastnosti požadované objednatelem;
* prodloužená záruka – jedná se o záruku v intencích výše uvedené odrážky „záruka“ na dobu delší než standardní nebo obvyklou za dodržení parametrů a požadavků na záruku zařízení;
* záruční servis – záruční servis v parametrech konkrétního SLA (service level agreement) uvedeného u každého jednotlivého zařízení, u kterého je záruční servis požadován; předmětem záručního servisu je zajištění podpory provozu a odstraňování závad dodaných zařízení dodavatelem nebo výrobcem zařízení s garancí po požadovanou dobu; je-li požadován u zařízení záruční servis a není-li jeho specifikace blíže upřesněna je požadován záruční servis Next business day on-site;
* podpora – u části plnění spočívající v dodávce software a jejich licencí, kde není relevantní požadovat záruku ani záruční servis, požaduje objednatel technickou podporu daného software po dobu stanovenou vždy u konkrétního softwarového produktu; primární součástí takové podpory musí být nárok na opravné verze software a přístup k řešení problémů s takovým software, další specifické požadavky podpory jako nárok na veškeré nové verze nebo další požadavky jsou vždy konkrétně uvedeny u předmětné podpory a konkrétního software v této technické specifikaci.
  + - 1. Zadavatel požaduje bezplatný (zahrnutý v ceně zakázky) přístup k aktualizacím software a firmware dodaných komodit minimálně po dobu záruky.
      2. Veškeré opravy po dobu záruky budou provedeny bez dalších nákladů pro zadavatele.
      3. Veškeré komponenty, náhradní díly a práce, poskytnuté v rámci záruky budou poskytnuty bezplatně.
      4. Není-li uvedeno u konkrétní komodity jinak, požaduje objednatel záruční servis - provedení opravy nejpozději do 30 kalendářních dnů ode dne nahlášení závady v místě dodávky.
      5. Pro hlášení servisních požadavků zajistí dodavatel zhotoviteli přístup ke svému helpdeskovému systém s on-line přístupem pro kompletní správu požadavků včetně uchování historie požadavků a jejich řešení. Detailní popis helpdeskového systému a jeho obsluhy musí být součástí nabídky. Provozní doba helpdeskového systému musí být minimálně 7-17 hod. v pracovních dnech.

1. Výkaz výměr síťových kabelových rozvodů včetně příslušenství

V ceně položky označené v Cenové tabulce (viz. Příloha č. 5 Zadávací dokumentace) u komodity K2 jako „**Kabelové rozvody včetně příslušenství“**, jsou zahrnuty následující dílčí položky. Dodavatel v cenové tabulce oceňuje kabelové rozvody včetně příslušenství jako celek, následující výkaz výměr slouží dodavateli pro kalkulaci celkové ceny této položky.

Následující tabulka obsahuje výkaz výměr pro vybudování kabelových rozvodů LAN:

|  |  |
| --- | --- |
| Položka | ks/m |
| Rozvaděč RACK samostatně stojící kompletní výška 42U 800x1000 (ŠxH) prosklené dveře | 1 |
| Montážní sada M6 (šroub, matice, podložka - sada 50 ks) | 2 |
| Rozvaděč Rack nástěnný, dvoudílný 9U hloubka 515mm, prosklené dveře | 7 |
| Rozvaděč Rack nástěnný, dvoudílný 12U hloubka 515mm, prosklené dveře | 1 |
| Rozvaděč Rack nástěnný, s odnímatelnými bočnicemi 18U hloubka 515mm, prosklené dveře | 2 |
| Demontáž rozvaděče jídelna, úprava kabeláže | 1 |
| Napájecí panel PDU 19",8xČSN,1xC14,10A,1U,kabel 2m | 13 |
| Vyvazovací panel 1U, plastová oka | 29 |
| Patchpanel nekompletní pro osazení 24x keystone, 1U | 32 |
| Police 1U, hloubka 450mm perforovaná | 2 |
| Svislá vyvazovací oka kovová | 24 |
| Ventilační jednotka 4x ventilátor s termostatem | 1 |
| Zemnící materiál pro datové rozvaděče | 11 |
| Zámek pro datový rozvaděč | 12 |
| Zásuvka panelová do rack rozvaděče | 12 |
| Optický box 12x SC duplex plně vybavený | 13 |
| Zatažení a příprava FO kabelu do opt.vany | 13 |
| Kabelová forma optických vláken | 13 |
| Navaření optických vláken (včetně pigtailů a ochran) | 86 |
| Patchkabel optický SM 2m SC/LC | 20 |
| Zásuvka datová pro instalaci 2xkeystone | 186 |
| Zásuvka datová pro instalaci 1xkeystone | 82 |
| Značení kabelů, popis dat.zásuvek a PATCH panelů | 1 |
| Ověřovací měření kabeláže | 1 |
| Sestavení technické dokumentace - manuály apod., dotační dokumentace, dokumentace skutečného provedení | 1 |
| Patchkabel 1m cat5e | 250 |
| Wifi přístupový bod 802.11ac | 57 |
| Demontáž stávajícího školního rozhlasu - soubor | 1 |
| Instalace IP rozhlasu | 85 |
| Keystone samozářezový | 1036 |
| Krabička instalační KU68 | 360 |
| Kabel FO 12vl 9/125um SM | 1420 |
| Kabel UTP cat.6 300MHz, LSOH | 23340 |
| Kabel UTP cat.6 300MHz, LSOH- přístupový systém a IP rozhlas | 7200 |
| Trubka flex, kabelová trasa smíšená | 17400 |
| Průraz zdivem (0,2-1,2m) - soubor | 1 |
| Pomocný instalační materiál - drobné úpravy zdiva (drážka, začištění) | 1 |

1. Zajištění podpory provozu
2. Služba poskytování technické podpory dodavatele k dodaným technologiím v rámci části A

Služby podpory zajištění provozu bude dodavatel zajišťovat na dobu neurčitou od předání technologií do provozu. Jako součást nabídky na veřejnou zakázku, na jejímž základě dochází k tomuto plnění, dodavatel nacení služby za 60 měsíců.

Dodavatel zajistí systémem HelpDesk následující služby:

* Dostupnost jednotného kontaktního místa helpdesku uchazeče pro hlášení závad je 7x24x365 s garantovanou dobou odezvy do následujícího pracovního dne od nahlášení závady. Veškeré požadavky zadavatele budou evidovány v helpdesk systému uchazeče minimálně takto:
  + na telefonním čísle dodavatele v režimu 5×10×365 v době od 8 do 17 hodin,
  + systémem servisní podpory dodavatele (HelpDesk) v režimu 7×24×365.
* Telefonické zadání požadavku bude zajištěno česky mluvící lidskou obsluhou, helpdesk systém dále zajišťuje zadavateli nepřetržitý přístup do webové aplikace helpdesk systému, kde lze upřesnit nebo doplnit požadavek přímo zadavatelem. Současně je také zajištěn přístup k uzavřeným požadavkům zadavatele a k databázi řešených požadavků. Helpdesk systém umožňuje export dat, včetně obsahu požadavku a způsobu vyřešení ve formátu \*.XLS a\* .CSV.
* Součástí poskytování této služby ze strany dodavatele budou následující činnosti v následujícím rozsahu:
  + Proaktivní činnosti
  + monitoring dodané infrastruktury,
  + analýza log záznamů.
  + Reaktivní činnosti:
  + řešení chybových stavů,
  + aktualizace firmware a software,
  + nasazení bezpečnostních update,
  + nasazení bezpečnostních update,
  + konzultace,
  + rozsah do 3 hodin měsíčně.

1. Viz. aktuální verze <https://www.strukturalni-fondy.cz/cs/Microsites/IROP/Vyzvy/Vyzva-c-66-Infrastruktura-pro-vzdelavani-integrovane-projekty-ITI>, příloha č. 8B Standard konektivity středních škol a vyšších odborných škol [↑](#footnote-ref-2)