Popis současného a nového stavu ICT

1 Současný stav technické infrastruktury

Školní budova se skládá z jednoho areálu.

Gymnázium Václava Hlavatého, Louny, Poděbradova 661, příspěvková organizace

Poděbradova 661, 440 01 Louny

Současná kabeláž školy vznikala nárazově bez dlouhodobého konceptu dle momentálních potřeb a neodpovídá dnešním standardům a potřebám školy, projektu, ČSN.

Zadavatel (škola) v současnosti nedisponuje serverovnou či technologickým centrem, které by odpovídalo požadovaným standardům pro implementaci a provoz plánovaných řešení obsažených ve standardu konektivity.

Stav jednotlivých technických zařízení je uveden níže.

WAN/Internet

Rychlost a kvalita současného internetového připojení je nevyhovující. Konektivitu zajišťuje společnost Česká data s.r.o., která je přivedena k hlavním datovým rozvaděčům. Přípojka disponuje přenosovou rychlostí 200/200Mbps, není uplatňováno žádné omezení FUP.

Zadavatel má v současnosti přidělenou veřejnou adresu IPv4 (1 ks), IPv6 (0ks). Zadavatel nemá v současné době validující DNSSEC resolver na straně školy, neprovádí žádný monitoring provozu. V současné době není nijak řešeno zabezpečení síťového provozu. Zadavatel provozuje stavový firewall/router Mikrotik (RouterBoard). LAN je od internetu oddělena pouze NATem realizovaným na vlastních routerech.

LAN

V objektu školy se nachází větší množství datových rozvaděčů. Rozvody LAN (převážně kabely CAT5/5E/6) jsou vedeny převážně v plastových lištách. Kabelové trasy jsou v datových rozvaděčích zakončeny porty v patchpanelech. Jednotlivé rozvaděče jsou spojeny metalickým a optickým kabelem. Nedostatečné délky kabelů nebo nedostatečný počet přípojných míst je řešen malými vloženými přepínači (8 portů, bez managementu). Současné trasy pokrývají jen základní potřeby a neodpovídají požadavkům projektu. Aktivní prvky disponují převážně porty 100/1000 Mb/s neumožňující řízení přístupu pomocí 802.1X.

Síť nedisponuje samostatnými řadiči. Žáci a učitelé se ke svým stanicím přihlašují pomocí vlastních jmenných účtů a dále generickými/hromadnými účty.

WiFi

Zadavatel provozuje WiFi síť, která nepokrývá celou školu. Síť je tvořena AP (WiFi access point – přístupový bod) SOHO kategorie.

Zadavatel v současné době není zapojen do federovaného systému Eduroam.

Dieselagregát a elektrické napájení

Zadavatel nemá k dispozici dieselagregát.

Záložní zdroj napájení (UPS)

UPS není používána.

Monitorovací systém serverovny

Zadavatel nepoužívá žádné monitorovací systémy pro sledování prostředí serverovny (teplota, vlhkost apod.) ani systém pro sledování a fyzických přístupů do serverovny.

Klimatizace

Zadavatel nemá k dispozici klimatizační jednotky. Teploty serverů/kritických aktivních prvků přes léto jsou vysoké.

Systémová infrastruktura

Zadavatel nepoužívá adresářovou službu Active Directory. Zadavatel používá školský informační systém Bakaláři. Pro podporu administrativní činnosti i podporu výuky jsou využívány Office365 – groupwarové služby, sdílení dokumentů apod.

Správa identit

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

Servery

Systémová infrastruktura je tvořena 1ks fyzickým serverem, HP ML 360. Operační systém serveru je Windows Server 2008 (Aplikační a Systémové). Server je umístěn ve vyhrazené místnosti – „serverovně“.

Virtualizace serverová

Zadavatel nemá k dispozici serverovou virtualizaci.

Zálohování a obnova dat

Zálohování dat není prováděno.

Vzdálený přístup (VPN), terminálový přístup

Vzdálený přístup (VPN) neexistuje, terminálový/RDP přístup není k dispozici.

Pracovní stanice

Škola pro výuku a administrativní činnost využívá počítače převážně s Windows 10 a novější v edici EDUCATION.

Žákovské počítače jsou průměrně 4-8 let staré.

Pro ochranu před škodlivým kódem je používán antivirus (MS Defender) na koncových stanicích a ESET na serveru.

Použití konkrétních názvů a označení v této technické specifikaci

Pokud by se v některé části PD vyskytly 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 důvodu, 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.

Popis cílového stavu a specifikace předmětu plnění

Základní požadavky na technické řešení nového – cílového stavu

(1) Cílem projektu je zvýšení bezpečnosti a související modernizace IT infrastruktury, aby implementací projektu byly naplněny Standardy konektivity škol (dále jen Standard konektivity) a rozšířena funkčnosti ICT prostředí školy. Dílčí cíle dle jednotlivých sektorů jsou specifikovány následovně:

Označení	Sektor	Počet
S1	Servery	1
S2	LAN, WiFi, kabeláž	1
S3	Monitorovací a logovací systém	1
S4	Ostatní služby	1

(2) Je požadováno řešení zachovávající a rozvíjející současné softwarové platformy Microsoft. Přechod na jinou platformu by způsobil nepřiměřené uživatelské a provozní potíže.

(3) 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.

(4) 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 a jejich následný provoz.

(5) 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.

(6) Veškeré produkty, které dodavatel dodává v rámci plnění zadavateli, musí splňovat následující podmínky:

(a) jsou nové, byly oprávněně uvedeny na trh v EU nebo pochází z autorizovaného prodejního kanálu výrobce,
(b) mají plnou záruku od výrobce, jsou první jakosti, bez vad,
(c) mohou být podporovány výrobcem a jsou součástí servisního a podpůrného programu výrobce,
(d) obsahují všechny nezbytné licence na používání příslušného softwaru,
(e) jsou v databázi výrobce uvedeny jako prodaná kupujícímu – zadavateli,
(f) jsou určeny pro provoz v České republice a vyhovují aplikovatelným ČSN a ES.

(7) 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.

(8) Veškerá dokumentace vytvořená v rámci realizace veřejné zakázky musí být zhotovena výhradně v českém jazyce a 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.

Technické požadavky na řešení

S1 – Servery

(1) Pro provoz veškerých pořízených systémů a aplikací bude pořízen výkonný (aplikační) server spolu s diskovým polem. Hardware serveru bude virtualizován a na serveru bude možno provozovat neomezený počet virtuálních serverů dle výpočetních možností dodávaného serveru. Servery budou připojeny do LAN sítě optickou linkou 4x 10 Gb/s.

(2) 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 softwarem, který bude prostřednictvím virtualizačního hypervizoru zálohovat všechny virtuální servery. Zálohovací systém umožní zálohovat i fyzický server a kritické osobní počítače v počtu maximálně šesti zařízení. Sítové úložiště NAS bude kvůli bezpečnému oddělení záloh od produkčních dat umístěno mimo místnost hlavní serverovny v podružném rozvaděči.

(3) Provozní zabezpečení bude tvořeno souborem zařízení, která zajistí optimální podmínky pro spolehlivý chod technologií – především serveru:

Záložní zdroj napájení UPS zajistí chod serveru, diskového pole, agregačního přepínače a firewallu při krátkodobém výpadku napájení.

(4) 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 služba 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, 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.). Řadič bude provozován ve virtuálním prostředí a bude pravidelně automaticky zálohován do NAS. Součástí řadiče bude základní síťové služba – DNS (DHCP variantně na firewallu). 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.

(5) Součástí bude dodání a zprovoznění centrálního systému pro výměnu a sdílení dokumentů. Tento systém musí být plně integrován se systémy MS Office 365 a adresářovou službou školy. Systém musí licenčně pokrývat všechna zařízení školy. Součástí dodávky jsou všechny licence dle rozpočtu.

(6) Součástí dodávky bude antivirový SW pro 170 koncových zařízení školy. Tento počet zahrnuje jak stávající, tak nová zařízení i fyzické a virtuální servery.

S2 - LAN, WiFi a kabelové rozvody

Firewall

(1) V rámci projektu bude pořízen a nasazen firewall jakožto bezpečná brána připojující organizaci k internetu, resp. ke konektivitě poskytovatele s využitím technologie NAT dle RFC 2663 (NAT bude využit pouze pro IPv4). 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 (včetně potřebné sady licencí) tzv. next-gen funkcemi, včetně komplexní sady pro unified-threat-management (UTM). Firewall bude schopen blokovat nejčastější útoky typu odepření služby (DoS) a bude účinně blokovat podvržení adresy (spoofing).

(2) Firewall zajistí identifikaci žáků, zaměstnanců a externistů s jejich internetovými aktivitami napojením na účty v doméně adresářové služby tak, aby bylo možné pomocí monitorovacího nástroje síťového provozu k dispozici aktuální dohledatelná vazba uživatel-IP adresa v4-v6, 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 včetně kategorizace a filtrace provozu. Role politiky budou schopny pracovat minimálně s těmito objekty – IP/subnet, uživatel/skupina, typ zařízení/operační systém.

(3) 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 přihlášením a logováním oprávněného uživatele.

(4) Firewall bude schopen omezovat šířku pásma (tzv. rate limiting) ve vybraných komunikačních pravidlech libovolné politiky firewallu. Omezení bude možno aplikovat též 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 – QoS).

(5) Kontrola webového provozu, nešifrovaného i šifrovaného (protokoly http a https), je povinným požadavkem Standardu konektivity škol a firewall ji bude umožňovat spolu s další UTM funkcionalitou. Pořízený firewall umožní provádět shodně inspekci šifrovaných (TLS) spojení vybraných protokolů i jejich nešifrovaných verzí – minimálně protokoly HTTPS, SMTP over TLS, POP3 over TLS, IMAP over TLS, FTP a inspekce na jejich výchozích portech. Pokud bude předkládán certifikát firewallem, musí být platný a důvěryhodný min. ve vnitřní síti.

(6) Kategorizace a selekce obsahu bude odlišná v závislosti na uživatelské skupině – požadováno bude minimálně pět profilů – žák (student), učitel, guest, THP a administrátor. Ve všech 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 nebo anglickém jazyce a formou zobrazené náhradní webové stránky (např. s upozorněním na pravidla využívání ICT a vysvětlení důvodu blokování). Kategorizace a selekce obsahu bude prováděna i pro šifrovanou (HTTPS, SSL) verzi http protokolu.

(7) 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 firewallu. Definice mají výrobcem nastavenou zároveň i výchozí akci, jak s identifikovanou komunikací naložit (min. blokace, monitorování, reset, pass). Ve většině případů jsou výchozí akce plně vyhovující a doporučujeme důvěřovat výrobci firewallu, že v definicích použité výchozí akce jsou pravidelně revidovány, stejně jako jejich další rozšiřování o nově identifikované hrozby, včetně jejich případné blokace. Zařazením profilů IPS do vybraných pravidel 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. Rekonfigurace pravidel bude možné provádět v intuitivním grafickém rozhraní zařízení.

(8) Antivirová kontrola bude aplikována i na šifrovaná spojení (https, SSL). Infikované soubory musí být možno odstranit či blokovat.

(9) Vzdálený přístup formou zabezpečeného tunelového spojení skrze internet bude sloužit především zaměstnancům k jejich práci z míst mimo školu a dodavatelům IT a jiných služeb.

Zaměstnanci by neměli být omezováni technologicky, firewall musí umožnit vytvoření tunelového spojení pomocí zabezpečeného protokolu (včetně 2FA), např. SSL. 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. K zabezpečení SSL komunikace (VPN) musí být pořízen a na firewallu instalován a konfigurován certifikát. Certifikát výrobce nebo vystavený pomocí interní CA organizace nemůže být považován za dostatečný pro tento účel. Stejný nebo jiný certifikát bude také použit pro zabezpečení publikovaných služeb školy (např. webového portálu školského informačního systému).

(10) Publikace (zpřístupnění z internetu) online služeb školy na adresách IPv4 i IPv6 bude zajištěno 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 certifikát vydaný veřejnou certifikační autoritou.

(11) Bližší specifikace firewallu: minimální výkon/parametry silného FW: formát rack 19“, porty min. 6x 1Gb FE a 2x 10 Gb SFP+, 2x zdroje, port pro management, interní HDD/SDD 480 Gb min. pro data, licence nutné pro provoz na 5 let, technická podpora v českém jazyce, minimální výkon Firewall Throughput - 10 Gbps, NGFW Throughput - 4 Gbps, Threat Protection Throughput - 2.5 Gbps, IPS Throughput- 6 Gbps, IPsec VPN Throughput- 5 Gbps, SSL VPN min. 45 uživatelů, podpora XDR nativně od výrobce FW, SW a HW od jednoho výrobce.

Přepínače (síťové switche)

(1) 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/s servery + páteřní propoje 10 Gb/s:

(a) 1 agregační přepínač L3 s neblokující architekturou a podporou 802.1Q VLAN, 802.1X, RADIUS based, MAC autentizace, s minimálně 24 porty po 10GbE fiber optics nebo lepší . 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 (např. pro připojení serverů duálními optickými linkami).

(b) 8x přístupový přepínač L3 (6 ks 48portový a 2 ks 24portový 1Gb/s, min. 2 SFP+, min. 24x/48x POE+) s neblokující architekturou a podporou stohování pro

snadnou správu a s plnou podporou 802.1Q VLAN a 802.1X, včetně potřebných optických modulů (SFP+) a propojovacích kabelů.

(2) Všechny přepínače budou podporovat současný provoz IPv4 a IPv6 protokolu – tzv. dualstack. Podpora RFC 1757, 1981, 2080, 2374, 2460, 2463, 3315, 3513, 4193. Minimální výkon – aggregated switching bandwidth – 200 Gbps (přístupový přepínač), 1050 Gbps (agregační přepínač).

802.1x

(1) Na zařízeních školy bude implementováno řízení přístupů k síti (drátová i bezdrátová síť) na základě rolí a členství v uživatelské skupině adresářové služby s využitím technologie 802.1X včetně AD.

(2) Pro hosty a externí uživatele bude zřízena samostatná VLAN nebo Private VLAN (např. Guest VLAN), která 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, IDS, IPS, kategorizace obsahu) a mohl jí být přiřazen samostatný profil odlišný od ostatních profilů. Ověřování přístupu do této VLAN bude zajištěno pomocí tzv. captive portálu – webové autentizace. Captive portál bude zajištěn firewallem, případně jiným samostatným řešením nebo prvkem, ale vždy s důrazem na bezpečné izolované oddělení uživatelského provozu od zbytku vnitřních sítí.

(3) Řízení provozu WiFi bude realizováno vytvořením VLAN (802.1Q), segmentací sítě s routováním provozu mezi VLAN na úrovni centrálního L3 přepínače s nastavitelnými ACL. Pro řízení provozu na úrovni kvality služeb bude k dispozici technologie QoS (Quality of Services).

Přístupové body WiFi

(1) Ověřování přístupu do WiFi sítě bude realizováno na principu protokolu 802.1X + radius. WiFi bude nabízet více SSID (učitelé, žáci, guest, atd.), které budou obsluhovány samostatnými VLAN a budou napojeny na radius server. Učitelé a žáci budou prostřednictvím radius serveru ověřováni v adresářové službě. Zabezpečení vnitřních sítí (SSID) školy bude provedeno dle 802.11i, tedy – WPA3 s AES šifrováním a konfigurováno shodně pro frekvenční pásma (2, 4 a 5 a 6 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.

(2) 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-wifi rušení.

(3) Centrální kontrolér bude realizován jako SW komponent (1 ks).

(4) Pro pokrytí požadovaných prostor hlavního projektu a dalších prostor bude pořízeno 72 přístupových bodů (WiFi access pointů) standardu 802.11ax (WiFi 6E), se současnou funkcí v pásmu 2, 4, 5 a 6 Ghz, s podporou spektrální analýzy zajišťující detekci a reakci na non-WiFi rušení. Pořízené AP budou podporovat WiFi 6E - AX, WPA2, WPA3, PoE+, multi SSID a ACL pro filtrování provozu.

(5) Současné pokrytí a kvalita LAN je nedostatečná, a to jak v prostorech dotčených hlavním projektem, tak v celém prostoru 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 standardům strukturované kabeláže Cat 6A.

(6) V serverovně, bude umístěn nový hlavní datový rozvaděč, do kterého budou připojeny optickými trasami podružné rozvaděče. V hlavním datovém rozvaděči budou umístěny klíčové technologie – agregační přepínač, firewall, server, diskové pole a UPS.

(7) V hlavních serverovnách bude instalována nová klimatizace pro zajištění provozní teploty vhodné pro všechna technologická zařízení (nově pořízená v rámci této zakázky).

LAN – pasivní část

(1) Vnitřní rozvody metalických a optických rozvodů budou provedeny dle požadavků školy a dle rozpočtu včetně vystrojení všech rozvaděčů dle rozpočtu.

(2) Vnitřní kabelové rozvody budou provedeny metalickými kabely min. CAT 6A. Optické trasy budou provedeny optickými kabely se SM (single mode) vlákny a zakončeny optickou vanou. Bližší technické parametry jsou uvedeny v samostatné příloze.

(3) Kabely budou vedeny ve vkládacích lištách, kabelových žlabech nebo parapetních kanálech. Zásuvky budou umístěny povrchově na omítce nebo budou zapuštěny v parapetních kanálech.

(4) Veškeré metalické rozvody budou dostatečné pro komunikaci o rychlosti 1Gb/s až na úroveň koncových zařízení, serverů a ostatních zařízení.

Požadavky na záruky a prokazování způsobilosti k instalaci kabelážního systému:

(5) V rámci celé instalace rozvodů metalické horizontální kabeláže je striktně požadována dodávka všech metalických kabelážních komponent datových přenosových linek pouze od jednoho výrobce a to tak, aby:

  (a) Byla dodržena vzájemná interoperabilita použitých komponent.

  (b) Byly dodrženy požadované technické požadavky na kabelážní systém jednotně a v celém rozsahu instalace.

  (c) Bylo možné na celý výše uvedený systém poskytnout pouze jedinou a komplexní záruku výrobce přes všechny části metalického systému a v rozsahu a plnění uvedeném v této kapitole.

(6) Požadavky na záruku výrobce:

  (a) Je požadována záruka výrobce kabelážního systému v rozsahu systémové záruky, tedy mimo záruky na každý individuální komponent bude poskytnuta i záruka na fungování celého systému v rozsahu a přenosových parametrech daných přenosovými standardy definovanými dále v tomto dokumentu.

  (b) Záruka výrobce bude zahrnovat plnění i pro případy, kdy za ztrátou deklarovaných garantovaných parametrů kabeláže jsou vady instalace provedené instalačním partnerem výrobce před vlastní certifikací kabeláže. Tato garance je podmíněna realizací instalace výrobcem certifikovaným instalačním partnerem, který musí svou způsobilost k poskytnutí této záruky prokázat platným certifikátem výrobce a osvědčením o jeho platnosti ze strany zástupce výrobce ne starším 6 měsíců.

  (c) Požadovaná délka trvání systémové záruky výrobce na strukturovanou kabeláž je minimálně 25-30 let.

  (d) Poskytovatelem záruky musí být skutečný výrobce kabelážního systému, tedy ten, kdo prokazatelně vlastní výrobní kapacity pro výrobu systémů, na něž je záruka poskytnuta.

(7) Součástí dodávky budou i záložní zdroje napájení, viz rozpočet a technické specifikace.

(8) Součásti dodávky je i montáž nového vedení 230 V pro všechny rozvaděče (jak podružné tak hlavní) včetně revize a vystrojení rozvaděčů.

S3 – Monitorovací a logovací systém

(1) Řešení systému pro monitoring a logování provozu je důležitým bezpečnostním prvkem, který umožňuje sběr dat síťové komunikace z jednotlivých prvků sítě. Následně je možno nad nimi provádět dotazy a vyhodnocovat chování uživatelů v síti (datum, čas, zdrojová IP adresa, koncová IP adresa, komunikační port), ukládat historii komunikace pro pozdější řešení incidentů, audit apod.

Hlavní body řešení:

(a) monitoring a logování NAT (RFC 2663) provozu za účelem dohledatelnosti veřejného provozu k vnitřnímu zařízení (ve spolupráci s firewallem). Síťová sonda z důvodu vysoké ekonomické náročnosti nebude uplatněna.

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

(c) 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 verze 5 nebo 9) – systém pro monitorování a sběr provozně-lokačních údajů minimálně na úrovni rozhraní WAN, ideálně i LAN) a to po dobu minimálně 2 měsíců.

(2) Vazba na monitoring: monitorovací a logovací systém bude proto napojen na adresářovou službu.

(3) 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 vícekriteriální vyhledávání napříč zdroji (např. NETFLOW a syslog).

(4) Povinná informace, která bude v systému vždy obsažena a uchována, je vazba IP-uživatel-čas. 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.

(5) 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.

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

(a) NetFLow nebo ekvivalent

(b) Syslog

(c) SNMP trap

(d) LOG soubory

(7) Protokol Netflow nebo ekvivalent – síťové toky budou exportovány z firewallu. Konfigurace flow exportu bude sladěna s konfigurací na straně příjemce – monitorovacího a logovacího nástroje (verze, porty apod.). Je požadován 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).

(8) Protokolem SYSLOG budou exportovány veškeré provozní informace, logy síťových zařízení včetně firewallu na signifikantních úrovních sítě. Obsaženy musí být veškeré důležité informace, které zařízení loguje, včetně informačních s důrazem na změny konfigurace, přihlášení – odhlášení, stavy jednotlivých portů a výstupy z procesu ověřování 802.1X. Tato data mohou mít povahu osobních dat a musí k nim být kontrolovaný přístup (ideálně token USB s certifikátem) a logování přístupu.

(9) Logy z monitoru událostí systému – monitorovací a logovací nástroj bude načítat logy událostí systému a informace v nich obsažené. Především se bude jednat o RADIUS logy událostí. Tyto logy budou obsahovat identitu uživatele a časy a stavy jeho žádostí o přístup.

(10) 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 dimenzovány, 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.

(11) Jako doplněk k výše uvedeným logovacím nástrojům bude dodán také systém centralizovaného monitorování dostupnosti kritických služeb a komponent, mezi které budou povinně patřit:

(a) agregační přepínač, přístupové přepínače,

(b) WiFi kontroler, WIFI AP,

(c) webové a jiné aplikační servery dostupné z internetu,

(d) aplikační intranetové servery,

(e) VPN a jiné přístupové servery,

(f) řadiče domén adresářových služeb,

(g) infrastrukturní servery (např. DHCP, DNS).

Monitorování bude realizováno přednostně pomocí open-source řešení (např. Nagios, Zabbix), a to pomocí obou síťových protokolů (IPv4, IPv6). Součástí počáteční konfigurace monitorovacího nástroje bude pokročilá notifikace minimálně do sdílené e-mailové schránky administrátorů (tuto schránku zřídí dodavatel v rámci konfigurace monitorovacího systému, přičemž postačí alias, případně též přes SMS gateway zadavatele.

(12) Centrální správa aktivních síťových prvků bude realizována specializovaným softwarem. Tento software bude nejen monitorovat stav aktivních prvků v síti (tedy např. přepínačů na L2 i L3, směrovačů, WiFi přístupových bodů, WiFi kontroleru), ale zejména bude umožňovat oprávněným administrátorům na základě silné autentizace provádět změny konfigurace síťových prvků, a to v plném rozsahu jejich konfiguračních možností. Software může být instalován na vhodném serveru nebo administrátorské stanici v síti, nemůže být realizován jako webová cloudová aplikace. Switche a WiFi access pointy budou z důvodu správy od jednoho výrobce.

S4 – Ostatní služby

(1) V rámci implementace předmětu plnění dodavatel realizuje pro všechny dodávané sektory S1 až S4 – následující služby, které jsou zahrnuty v ceně dodávky:

(a) Provedení předimplementační analýzy (včetně všech změn v konfiguraci budoucí infrastruktury) a zpracování detailního finálního popisu cílového stavu a postupu implementace. Výstupem bude prováděcí dokumentace (včetně vedení a prostupů kabeláže), 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.

(b) Dodávka a implementace předmětu plnění dle schválené prováděcí dokumentace včetně technické podpory, následná technická podpora není zahrnuta.

(c) Zprovoznění a zavedení MS Active Directory.

(d) Vytvoření centrálních politik pro správu a ověřování uživatelů.

(e) Migrace uživatelských informací a uživatelských dat do nové infrastruktury.

(i) Jde o migraci dat ze stávajícího serveru (sdílené adresáře učitelů, sdílené adresáře žáků) – max. 10.000 GB dat.

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

(iii) Příprava prostředí pro migraci systému Bakaláři a migrace samotná dle dohody v předimplementační analýze.

(f) Migrace centrálních systémů do nové infrastruktury (migrace uživatelských dat a adresářových služeb ze stávající MS Active Directory do 440 uživatelů).

(g) Zajištění projektového vedení projektovým managerem.

(h) 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:

(i) Active Directory – správa uživatelů a skupin, zařazení počítače do domény.

(ii) Zálohování – kontrola činnosti, obnova souborů, plán obnovy.

(iii) Hypervizor – ovládání virtuálních serverů, změna jejich konfigurace.

(iv) Monitorovací a logovací systém – vyhledávání činnosti uživatelů a systémů, běžná správa a kontrola funkce.

(v) LAN a WiFi – připojení zařízení, včetně podrobných uživatelských postupů pro WiFi připojení mobilních zařízení (tablety, chytré telefony, notebooky) s operačními systémy Windows 7, 10 a 11, Android, iOS a macOS.

(vi) Firewall – blokování stránek, dohledání činnosti uživatele, práce s kategoriemi stránek, zablokování přístupu pro uživatele skupiny.

(i) Zpracování dokumentu Zásady využívání ICT a přístupu k síti dle Standardu konektivity pro začlenění do vnitřních předpisů školy.

(j) Zpracování materiálů pro školení.

(k) Zajištění zkušebního provozu infrastruktury v délce minimálně 3 týdny včetně technické podpory specialistů na dané zařízení/službu, s dostupností maximálně do 24 hodin na místě realizace od nahlášení požadavku v pracovní den v době od 7h do 16h.

(l) Provedení akceptačních testů.

(m) Předání do plného provozu.

(2) Realizace dodávky bude probíhat v daném období dle konkrétních podmínek uvedených v kupní smlouvě na předmět plnění této technické specifikace.

(3) Objednatel dále požaduje provést následující práce na dodaných zařízeních, pokud nejsou uvedeny výše. 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.

S1
a) návrh a kompletní implementace serverové virtualizační platformy b) implementace pořízených technologií c) analýza dat a systémů na stávajících serverech a jejich migrace na novou platformu d) návrh vhodné struktury Active Directory, její vybudování a migrace e) návrh a realizace zálohovacího řešení včetně plánu obnovy f) implementace automatické odstávky a najetí serveru v případě výpadku a obnovení dodávky elektrické energie g) návrh a provedení akceptačních testů
S2
a) analýza síťového prostředí a návrh nové architektury LAN i WiFi b) implementace pořízených technologií c) provedení segmentace LAN – VLAN, adresování, routování… d) zavedení IPv4+6 pro přístup k internetovým zdrojům publikovaným na IPv4+6 adresách h) zabezpečení komunikace publikovaných služeb školy pomocí certifikátu i) zavedení DNSSEC pro interní DNS služby i zabezpečení domény školy j) 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 k) návrh a implementace firewallu včetně vhodné konfigurace UTM (antivir, IPS, aplikační kontrola, URL filtrace dle kategorií) pro školu l) vybudování VPN pro vzdálený přístup uživatelů LAN m) respektování min. 5 různých skupinu uživatelů (učitelé, studenti, hosté, THP, admin) v návrzích a implementaci bezpečnostních a ostatních politik n) implementace portálu pro registraci a řízení přístupů hostů – tzv. captive portál o) zajištění ostatních nezbytných činností pro naplnění Standardu konektivity
S3
a) 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 zařízení b) Provedení souvisejících konfigurací monitorovaných systémů
S4
V předimplementační analýze budou detailně popsány veškeré integrační vazby dílčích systémů, které jsou předmětem dodávky S1-S4, primárně ve vazbě na dodávky sektorů dle

této technické specifikace (např. systém pro ověřování zařízení přistupujících do sítě, MS Active Directory).

(4) Akceptační testy musí pro všechny sektory vždy zahrnovat minimálně prokázání kompletnosti dodávky a požadované funkčnosti, dále prokázání aktivací software i hardware aktivačními klíči či licencemi, je-li aktivace potřebná. Dále pro každý sektor navrhne uchazeč vhodné doplňující testy a kritéria, kterými bude prokázána funkčnost a stabilita dodaného řešení. Návrh vhodných akceptačních kritérií bude součástí předimplementační analýzy, zadavatel může v průběhu zpracování Prováděcí dokumentace provést jejich upřesnění či rozšíření.

(5) Povinným akceptačním kritériem bude prokázání naplnění požadavků Standardu konektivity 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.

(6) Náklady na provedení implementačních služeb musí být zahrnuty v nabídkové ceně k položce, ke které se vztahují a nelze je vyčíslit zvlášť.

Závazný detailní harmonogram plnění projektu

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