TECHNICKÁ SPECIFIKACE - část - Konektivita

Základní škola, Brno, Bosonožská 9, příspěvková organizace

TECHNICKÁ SPECIFIKACE

Základní požadavky na technické řešení

(1) Cílem projektu je zvýšení bezpečnosti a související modernizace IT infrastruktury, aby implementací projektu byly naplněny Standardy konektivity škol [1] - uvedené v příloze č.1 (dále jen Standard konektivity). Dílčí cíle dle jednotlivých komodit jsou specifikovány následovně:

Označení	Komodita	Počet
K1	Virtualizační platforma	1
K2	Zabezpečení LAN a Wifi	1

(2) Je požadováno řešení zachovávající a rozvíjející současné softwarové platformy Microsoft pro zachování kompatibility se stávajícími systémy a aplikacemi. Přechod na jinou platformu by způsobil 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, přičemž nesmí překročit předpokládanou hodnotu zakázky.

(5) Veškeré produkty, které dodavatel dodává v rámci plnění zadavateli, musí splňovat následující podmínky a dodavatel splnění těchto podmínek potvrdí samostatným čestným prohlášením:

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

Tyto skutečnosti dodavatel doloží čestným prohlášením distributora, popř. dodavatelovým samotným, nelze-li prohlášení distributora získat.

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.

(6) 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. Struktura i forma dokumentace musí být před předáním předána ke kontrole a výslovně schválena zadavatelem.

1. TECHNICKÁ SPECIFIKACE – Konektivita

1.1. Specifické požadavky na technické řešení

(1) **K1 - Virtualizační platforma**

(a) Pro provoz veškerých pořízených systémů a aplikací bude pořízen jeden server vybavený interním úložištěm s vysokou kapacitou. Hardware serveru bude virtualizován a na serveru bude možno provozovat **min 4** virtuálních serverů.

(b) 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.). Technické provedení bude založeno min. na 1 řadiči adresářové služby. Řadič bude provozován a bude pravidelně automaticky zálohovány. Součástí řadičů budou základní síťové služby – DNS, DHCP.

(2) **K2- Zabezpečení LAN a Wifi**

(a) Bude implementováno řízení přístupů k mediu (síti) na základě rolí a členství v uživatelské skupině adresářové služby.

(b) 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 (QualityofServices).

(c) Ověřování přístupu do WiFi sítě bude realizováno na stejném principu jako LAN. Wifi bude nabízet více SSID (učitelé, žáci, Guest), které budou obsluhovány samostatnými VLAN a budou napojeny na raduis servery. Učitelé a žáci budou prostřednictvím radius serveru ověřováni v adresářové služby. 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 (GuestWiFi).

1.2. Implementační služby

(1) V rámci implementace předmětu plnění dodavatel realizuje pro všechny nabízené komodity K1 až K2

(a) Dodávka a implementace předmětu plnění musí respektovat a využívat osvědčené praktiky (tzv. Best Practice) a doporučení výrobců nabízených technologií. Musí být v souladu s nabídkou uchazeče a se Standardem konektivity.

(b) Zajištění projektového vedení realizace předmětu plnění.

(c) 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) ActiveDirectory – správa uživatelů a skupin

(ii) Hypervizor – ovládání virtuálních serverů, změna jejich konfigurace

(iii) LAN a Wifi - připojení zařízení uživatelských postupů pro Wifi.

(d) Provedení akceptačních testů.

(e) Předání do plného provozu.

(2) Zadavatel 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 díla 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
a) Návrh a kompletní implementace serverové virtualizační platformy b) Implementace pořízených technologií c) Návrh vhodné struktury ActiveDirectory, její vybudování d) Implementace automatické odstávky a najetí serveru v případě výpadku a obnovení dodávky elektrické energie e) Návrh a provedení akceptačních testů
K2: Zabezpečení LAN a Wifi
a) Implementace pořízených technologií b) Návrh a implementace 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 c) Respektování min. 3 různých skupinu uživatelů (učitelé, studenti, hosté) v návrzích a implementaci bezpečnostních a ostatních politik d) Zajištění ostatních nezbytných činností pro naplnění Standardu konektivity

(3) Akceptační testy musí pro všechny komodity vždy zahrnovat minimálně prokázání kompletnosti dodávky a požadované funkčnosti. Povinným akceptačním kritériem bude prokázání naplnění požadavků Standardu konektivity dle manuálu k postupu při prokazování a kontrole 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.

1.3. Školení

(1) Školení bude pokrývat všechna zařízení a systémy všech komodit, dodávané v rámci této veřejné zakázky, a to minimálně v rozsahu:

(a) běžných administrátorských činností pro implementované systémy

(b) standardní údržby systémů pro administrátory zadavatele

(2) 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.

(3) Minimální rozsah školení pro každou komoditu je 1 hodina, není-li uvedeno jinak. Školení bude probíhat v sídle zadavatele.

1.4. Popis povinných parametrů dodávaného řešení

(1) V dále uvedených tabulkách jsou uvedeny povinné parametry prvků nabízeného 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.

(2) Dodavatel ve své nabídce uvede značkové specifikace nabízených dodávek formou přesného popisu produktů (přesné obchodní označení typu), nebo tzv PN (PART NUMBER). Z popis způsobu naplnění bude možno určit, že nabízené řešení jednoznačně splňuje všechny aspekty povinného parametru.

Povinné parametry pro Komoditu K1 - Virtualizační platforma:

Parametr	
Formát serveru	Rackové provedení, min.. 1U. Pro přístup ke všem komponentám serveru není nutné nářadí. Barevně značené hot-plug vnitřní i vnější komponenty
CPU	Server musí být osazen min. 1x CPU, minimálně s šestnácti procesorovými jádry. Hodnocení výkonu nabídnutého serveru musí být publikované na webu: https://www.cpubenchmark.net s minimálními parametry: • Passmark CPU Mark, hodnota min: 25 100
RAM	128GB v provedení min. DDR4, min. 3200 MHz rozšiřitelnou minimálně na 256GB
Diskový subsystém	Server musí disponovat alespoň 4x diskovou hotswap šachtou pro disky 3,5”, přístupnou zpředu. Požadujeme osazení min. dvěma SSD s kapacitou alespoň 480GB min. dvěma 8TB 7.2K RPM SATA 6Gbps
Optická mechanika	Není požadována.
Diskový řadič	• typu SAS12 • podpora hot-plug disků SAS, SSD i SATA • podpora min. RAID - 0, 1, 5, 6, 10, 50, 60 • Cache řadiče alespoň 8GB se zálohováním proti výpadku napájení na dobu min. 72 hodin • Řadič nezabírá volné PCI-e sloty
Síťové rozhraní	• 2x 1000Base-T, onboard (nezabírající volné PCI-e sloty) • 2 x 10/25GbE SFP28
Napájení	Redundantní napájecí zdroje 230V, max. 700W
Chlazení	Možnost provozu při okolní teplotě stabilně až do 40°C (provoz chlazení čerstvým vzduchem)
Interface	2 x přední, 2x zadní a 1x vnitřní USB port (alespoň jeden zadní a vnitřní s podporou USB3.0) Interaktivní LCD display indikující základní informace o systému (min. IP adresa, model, chybové stavy, atd.), možnost nastavení IP konfigurace a čtení chybových stavů z out-of-band managementu, bez potřeby připojení monitoru a klávesnice
Rozšiřující sloty	Minimálně 1x PCI-e x16 Gen 3 slot, LP – volný pro budoucí rozšiřování

	Dedikovaný RAID slot pro RAID kartu OCP 3.0 slot
Kolejnice	Zásuvné ližiny pro rack
Podpora OS a virtualizace	Microsoft Windows Server 2016 Microsoft Windows Server 2019 Microsoft Windows Server 2022 VMware ESX 6.7 až 8.0 RedHatEnterprise Linux 7 RedHatEnterprise Linux 8 RedHatEnterprise Linux 9 SUSE Linux ES 15 Ubuntu 20.04 LTS Ubuntu Server 22.04 LTS
Management a vzdálená správa	Management serveru nezávislý na operačním systému poskytující následující management funkce a vlastnosti: • web GUI a dedikovaná IP adresa, dedikovaný management LAN port s podporou VLAN • SW LAN adaptér pro management mapovaný prostřednictvím z předu přístupného USB portu, podpora přímého připojení USB kabelem z notebooku správce nebo servisního technika (není nutné zpřístupňovat management LAN) • Agent-less hardware FW update vč. možnosti rollback při neúspěchu • Podpora asistovaného OS Deploymentu • LifeCycle Log • sledování hardwarových sensorů (teplota, napětí, stav, chybové sensory) • erroralerty (server reset, kritické sensorové hodnoty, atd.) za použití email traps, paging, atd. • možnost failoveru management LAN portu na jinou síťovou kartu na desce serveru (LOM) • podpora IPv6 • podpora WS-MAN/SMASH-CLP • plná podpora a IPMI funkcionalita • vestavěný Unified Server Configurator GUI (není třeba asistenční/driverové nebo HW-test CD/DVD) • vzdálená konfigurace RAID, přímo v OOB managementu • server remote reset, reboot, power-on/off/cycle • power management a powercaping • integrace managementu do ActiveDirectory a dvoufaktorováauthentikace (TFA), encryption) • podpora RemotevirtualSerial support • BIOS recovery • Management serveru nepožaduje instalaci agenta jak pro monitoring, tak pro update SW/FW/BIOS v jednotlivých HW komponentech serveru • Podpora hromadné konfigurace více serverů pomocí XML souborů (z USB, nebo síťovým PXE bootem), hesla v takovém souboru musí být hashována proti zneužití (zerotouchdeployment) • Management serveru ukládá nastavení komponent do vyhrazené paměti, která je neoddělitelnou součástí chassis. Tato konfigurace je pak použitelná po výměně kterékoliv HW komponenty • Interaktivníčelníinformační panel, informující o stavu a názvu serveru s možností zobrazení názvu aktuálně spuštěných virtuálních strojů. Panel musí umožňovat kontrolu a nastavení parametrů out-of-band vestavěné správy systemu, včetně přiřazení IP adres a přístupu do HW logu • management nástroje musí umět poskytovat ovladače instalovaným operačním systémům bez speciální dedikované partition na interních discích serveru a nezávisle na těchto discích • Integrovatelnost s dohledovou konzolí OpenManage Essentials
Podpora a servis	Podpora na 5 let typu NBD, oprava v místě instalace serveru, servis je poskytován výrobcem serveru, možnost rozšíření záruky min. na 7 let. Podpora prostřednictvím internetu musí umožňovat stahování ovladačů a manuálů adresně pro konkrétní zadané sériové či produktové číslo každého serveru. Možnost provázání managementu serveru pro online spojení technickou podporou výrobce a automatickým otevíráním servisních požadavků včetně automatického odeslání HW a OS logů pro následný troubleshooting proces.

SW licence operačních systémů <u>NELZE použít v nabídce druhotných licencí</u>	Serverové operační systémy	2ks licencí 64-bitového serverového operačního systému v aktuální verzi. Licence musí umožnit provoz hypervizoru a 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 umožňující využívat těchto systémů uživatelům celkem na **160** zařízeních.

Síťové úložiště NAS 1 ks	Provedení	Tower nebo RACK pro 4x HDD 3,5“
	Výkon	1xCPU min 2500bodu v CPU MARK na https://www.cpubenchmark.net
	Rozšiřitelnost	2x USB 3.2 Gen 1
	Kapacita	Osazeno 4x 8TB/HDD/3.5"/SATA/7200 RPM, určených výrobcem pro NAS (nepřipouští se HDD určené jiným účelům (desktop, kamerové systémy apod.).
	Konektivita	2x RJ-45 1GbE LAN
	RAM	min. 2GB DDR4 non-ECC SODIMM s možností rozšíření až na 6GB
	Záruka	min. 36 měsíců

Povinné parametry pro Komoditu K2 – Zabezpečení LAN a Wifi:

1x SWITCH PoE + 2x 1G SFP SM Transceiver

24-port GbE Smart Managed Switch
24x Gigabit RJ45
4x Gigabit SFP
24x PoE ports
Total PoE budget (Watts) min: 375
Switching capacity (Gbps) min:56
Forwarding rate (Mpps) min: 42
2x Transceiver SM SFP

Záruka 5let

9x INTERNI WiFi přístupové body (AP) + montáž na strop

Technické parametry

Standard: IEEE802.11 ax / ac / n / g / b / a
MIMO: MU-MIMO
Rychlost bezdrátového připojení: 2,4 GHz: 575 Mb/s, 5 GHz: 2400 Mb/s
Frekvenční pásmo: 2.4 GHz a 5 GHz
Typ antény: Duální optimalizovaná anténa
Zisk antény: 2,4 GHz: Peak Gain 5dBi, 5GHz: Peak Gain 6dBi
Minimální citlivost příjmu: Rx až -101 dBm
Ethernetový port: 1 x LAN 10/100/1000/2500M, 1 x 10/100/1000M LAN
Napájení: PoE (802.3) při: příkon 19 W, DC vstup: 12 VDC 2A
Záruka 5let
Součástí musí být veškeré potřebné licence pro provoz (napr s kontrolerem)

1x EXTERNI OUTDOOR WiFi + 3x ANTENA + montáž na strop

Technické parametry WIFI

Wi-Fi standard: IEEE 802.11 ax/ac/n/g/b/a
Přenosová rychlost:
Link rates up to 575 Mbps for 2.4 GHz
Link rates up to 4.8 Gbps for 5 GHz
Porty:

1 x 1/2.5 Gbps LAN

Technické parametry ANTENY

Úroveň zisku antény (max): 7 dBi
Frekvenční pásmo: 2.4/5 GHz
Zisk antény (2,4 GHz): 4,5 dBi
Typ antény: Vícesměrová anténa
Typ anténního konektoru: Konektor N-type
Polarizace: Vertikální polarizace
Záruka 5let
Součástí musí být veškeré potřebné licence pro provoz (napr s kontrolerem)

Kabelové rozvody včetně příslušenství pro AP 10 přípojných míst Min. cat 5e - UTP LSOH	Popis	Kabelové rozvody včetně příslušenství a souvisejících služeb pro připojení 10KS WIFI AP -ukončení kabeláže WIFI do patch panelu (patch panel je součástí dodávky) -ukončení konektorem RJ45 – strana WIFI -délku trasy (povrchová montáž do lišty) a kabeláže cenit na 95m/AP - montáž AP – 10KS (strop/stena)
	Záruka	Kabelové rozvody min 5let

Kabelové rozvody včetně příslušenství pro 24 přípojných míst Min. cat 5e - UTP LSOH	Popis	Kabelové rozvody včetně příslušenství a souvisejících služeb pro připojení 24 přípojných míst -ukončení kabeláže do patch panelu (patch panel je součástí dodávky) -ukončení v zásuvce/liste (součástí dodávky) -délku trasy (povrchová montáž do lišty) a kabeláže cenit na 95m/PM - FO propoj SM do centrálního podružného DR – kalkulace na 500m SM
	Záruka	Kabelové rozvody min 5let

Kabelové rozvody včetně příslušenství pro PC učebnu Min. cat 5e - UTP LSOH	Popis	Kabelové rozvody včetně příslušenství a souvisejících služeb pro připojení PC učebny -ukončení kabeláže do patch panelu (patch panel je součástí dodávky) -ukončení v zásuvce/liste (součástí dodávky) - Datový rozvaděč min 12U - FO propoj SM do centrálního DR – kalkulace na 500m SM
	Záruka	Kabelové rozvody min 5let

Datový rozvaděče – INFRA technologie		
Specifikace	Datový rozvaděč min 19U pro INFRA technologie	**1 ks**
Provedení	kovové robustní provedení	
Záruka	min. 24 měsíců	

Příloha č.1

1. Konektivita školy k veřejnému internetu (WAN)

1.1. Obecný popis

Pro základní způsobilost projektu naplňujícího opatření „vnitřní konektivita škol“ musí příslušná škola zajistit kvalitní připojení ke službám veřejného internetu, a to i v případě, že vybavení pro připojení k internetu není předmětem projektové žádosti.

Za toto připojení je považováno zajištění konektivity splňující následující parametry v době ukončení realizace a v průběhu udržitelnosti projektu.

1.2. Povinné parametry projektu:

1.2.1. Šíře pásma (bandwidth) odpovídající 0,25 Mbps/žák či student[2] nebo 0,5 Mbps/koncové uživatelské zařízení[3][4] a zároveň taková šířka pásma, která neomezuje provoz zařízení a uživatelů[5]. Šíře pásma se vztahuje na počet žáků/studentů/koncových uživatelských zařízení v budově/areálu, kde se projekt realizuje.

1.2.2. Vlastní nebo poskytovatelem přidělené veřejné IPv4 adresy.

1.2.3. Zajištění monitoringu a logování NAT (RFC 2663) provozu za účelem dohledatelnosti veřejného provozu k vnitřnímu koncovému zařízení v minimální délce 3 měsíců.

1.2.4. Síťové zařízení podporující rate limiting, antispoofing, access listy - zařízení musí obsahovat všechny potřebné komponenty a licence pro zajištění řádné funkcionality.

1.2.5. Schopnost snadné/automatické rekonfigurace pravidel firewallu (access listů) na základě identifikovaných útoků.

1.2.6. Zajištění šifrovaného přístupu (SSL/TLS) a podepsání DNSSEC domén pro služby školy dostupné online (např. emailové služby, webové servery, studijní a ekonomické agendy atp.).

1.2.7. Validující DNSSEC resolver na straně školy, nebo poskytovatele konektivity, nebo otevřeným DNSSEC validujícím resolverem;

1.2.8. Software a firmware je aktualizován po dobu udržitelnosti projektu, jsou-li aktualizace k dispozici.

1.2.9. Poskytovatel konektivity je schopen zajistit kontaktní bod pro komunikaci, trvalý monitoring dostupnosti konektivity, realizovat blokování nežádoucí komunikace zahlcující nebo jinak omezující konektivitu a systémy školy na straně poskytovatele na základě požadavku školy.

1.3. Doporučené parametry projektu:

Nad rámec těchto povinných parametrů je dále doporučeno v projektu realizovat:

1.3.1. Symetrické připojení (zajištění konektivity) bez agregace a omezení, doporučujeme postupně směřovat ke kapacitě konektivity 1Gbps.

1.3.2. Plná podpora připojení do veřejného internetu přes protokol IPv4 i IPv6, včetně zajištění dostupnosti online služeb školy na IPv6 adresách.

---

[2] *Počet žáků/studentů je definovaný celkovým počtem žáků/studentů školy.*

[3] *Koncové uživatelské zařízení je počítačový systém, který je aktivně využíván uživatelem (např. žákem, studentem nebo zaměstnancem školy) ke vzdělávacím či pracovním účelům (typicky počítač, notebook, tablet apod.).*

[4] *Metrika vhodná typicky pro školy bez mobilních popř. BYOD zařízení*

[5] *Definováno jako saturace šířky pásma připojení k veřejnému internetu, která ani ve špičkách nedosáhne, a to ani krátkodobě 100 %.*

1.3.3. Poskytovatel konektivity je schopen zajistit funkci systému incident response, monitoring a aktivní notifikaci anomálií síťového provozu, zamezení podvržení zdrojových IP adres (anti-spoofing), funkci pro blokování nežádoucí komunikace zahlcující nebo jinak omezující konektivitu a systémy školy pro zamezení zahlcení linky (např. RTBH, FlowSpec, služby AntiDDoS řešení), detekci a zamezení amplifikačních útoků, zabezpečení směrování síťového provozu pomocí RPKI a konfigurace odmítnutí nevalidních prefixů.

1.3.4. Antivirová kontrola internetového provozu.

2. Vnitřní konektivita školy (LAN a WLAN)

2.1. Obecný popis

Vnitřní síťové prostředí školy pořizované v rámci projektu může být řešeno pevnou sítí, bezdrátovou sítí, nebo kombinací těchto síťových technologií. Připojení je nutné zajistit v prostorách dotčených hlavním projektem, rovněž je možné pokrýt ostatní prostory školy, včetně chodeb, jídelen, internátu a dalších školských zařízení. Potřebnost a účelnost takového pokrytí musí být odůvodněna ve studii proveditelnosti.

2.2. Povinné parametry projektu (bez ohledu typ síťového připojení):

2.2.1. Systém správy uživatelů (Identity Management), tj. centrální databáze identit (LDAP, AD apod.) a její využití pro autentizaci uživatelů (žáci i učitelé) za účelem bezpečného a auditovatelného přístupu k síti, resp. službám. Využívání jednoho účtu více uživateli není povoleno (využívání tzv. anonymních účtů).

2.2.2. Logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas-počítačový systém[6].

2.2.3. Systémy zálohování a obnovy dat serverové infrastruktury.

2.2.4. Systémy pro antivirovou ochranu počítačových systémů, antispamovou ochranu poštovních serverů.

2.3. Povinné parametry projektu v oblasti pevné LAN:

2.3.1. Minimální konektivita koncových uživatelských zařízení 1000 Mbps fullduplex.

2.3.2. Minimální konektivita serverů, aktivních síťových prvků, bezpečnostních zařízení (např. IPS, IDS, Next Generation Firewall aj.), datových úložišť (NAS) 1000 Mbps fullduplex.

2.3.3. Síťové prvky musí splňovat následující funkcionality: centrální směrovače a centrální přepínače (L2 i L3)[7] s neblokující architekturou přepínacího subsystému (wire speed), management, podpora 802.1Q VLAN (možnost tvorby virtuálních sítí - VLAN), základní bezpečnostní prvky proti zneužití přístupu k síti [např. MAC based omezení (port-sec), 802.1X autentizace aj.].

2.3.4. Strukturovaná kabeláž pro připojení počítačových systémů a dalších zařízení (tiskárny, servery, AP aj.).

2.3.5. Páteřní rozvody mezi budovami v areálu, kde probíhá výuka nebo příprava na ni, realizovány prostřednictvím optických vláken nebo metalických kabelů. Vztahuje se na budovu/areál, kde se projekt realizuje.

2.4. Minimální parametry projektu v případě řešení bezdrátových sítí (WLAN):

[6] *Počítačový systém je každý prvek informačních a komunikačních technologií využívající pro svoji činnost jak hardware, tak software. Pro účely standardů jsou rozlišována: 1. koncová uživatelská zařízení (např. osobní počítače, notebooky, tablety, mobily aj.) a 2. servery, síťové prvky, datová úložiště apod.*

[7] *Požadavek se týká prvků, přes které je veden veškerý provoz, resp. jde o centrální prvky. Podružné přepínače (chodbové, učebnové) musí splňovat pouze požadavek na neblokující architekturou přepínacího subsystému.*

2.4.1. Návrh topologie Wi-Fi sítě a analýza pokrytí signálem počítající s konzistentní Wi-Fi službou v příslušných prostorách školy a s kapacitami pro provoz mobilních zařízení pedagogického sboru i studentů.

2.4.2. Zabezpečení minimálně AES šifrováním a standardem WPA2-Enterprise nebo WPA3-Enterprise, multi SSID, ACL pro filtrování provozu.

2.4.3. Zajištění vzájemně oddělených sítí pro zaměstnance školy, žáky/studenty školy a externí zařízení (hosty).

2.4.4. Podpora mechanismu izolace uživatelů.

2.4.5. Podpora standardu IEEE 802.11ac (Wi-Fi 5) a případně novějších (Wi-Fi 6), současná funkce AP v pásmu 2,4 a 5 GHz a novějších protokolů a pásem.

2.5. Doporučené parametry projektu (bez ohledu typ síťového připojení):

Nad rámec těchto povinných parametrů je dále doporučeno v projektu realizovat:

2.5.1. Logování provozu za účelem dohledatelnosti na úroveň koncového uživatele.

2.5.2. Řešení dočasných přístupů (hosté, brigádníci, praktikanti, zákonní zástupci, externí subjekty) a systému blokace Wi-Fi v určitém čase.

2.5.3. Federované služby autentizace a autorizace (včetně aktivního zapojení do národních vzdělávacích federací (např. aktvní zapojení do federovaného systému www.eduroam.cz).

2.5.4. Centralizovaná architektura správy Wi-Fi sítě (centrální řadič, centrální management, tzv. thin access pointy, popř. alespoň centrální řešení distribuce konfigurací s podporou automatického rozložení zátěže klientů, roamingu mezi spravované access pointy a automatickým laděním kanálů a síly signálu včetně detekce a reakce na non-Wi-Fi rušení).

2.5.5. Doporučená podpora pro ověřování uživatelů oproti databázi účtů [např. pomocí protokolu IEEE 802.1X vůči centrální evidenci uživatelů (např. LDAP, MS AD) nebo pomocí Captive portalu].

2.5.6. Propojení aktivních prvků a důležitých systémů (např. Servery, NAS, propojení budov) rychlostí 10 Gbps, včetně uplinku.

3. Další doporučené bezpečnostní prvky projektu

Nad rámec povinných parametrů uvedených v bodech 1 a 2 je dále doporučeno v projektu realizovat:

3.1.1. Systémy nebo zařízení pro sledování infrastruktury sítě a sledování IP provozu sítě (umožňující funkce RFC 3917 - IPFIX nebo ekvivalent).

3.1.2. Systémy schopné detekovat nelegitimní provoz nebo síťové anomálie.

3.1.3. Systémy vyhodnocování a správy událostí a bezpečnostních incidentů (log management, incident management).

3.1.4. Systémy pro monitorování funkčnosti síťové a serverové infrastruktury.

3.1.5. Zařízení umožňující kontrolu http a https provozu, kategorizaci a selekci obsahu dostupného pro vybrané skupiny uživatel (učitel, žák), blokování nežádoucích kategorií obsahu.

3.1.6. Systémy uživatelské podpory naplňující principy ITIL (HelpDesk, ServiceDesk aj.).

3.1.7. Nástroje pro centrální správu a audit ICT prostředků.

3.1.8. Podpora vzdáleného přístupu (VPN).

3.1.9. Zavedení více-faktorové autentizace.