

1.7 Počítačové vybavení

1.7.1 Všeobecné údaje

Název stavby:

Objekt: Základní škola Zachar, Kroměříž **Název**

PS: Slaboproud – SLP

Místo stavby:

Zpracovatel projektu: Zdeněk Indra, Ing. Jan Bartoň

1.7.2 Výchozí podklady

Pro zpracování této zprávy bylo použito následujících podkladů:

- Ing. Zona Jan - projekce
- Standard konektivity škol
- Současný stav počítačového vybavení

Základní normy:

Všeobecné

Vyhláška č. 268/2011 Sb., kterou se mění vyhláška č. 23/2008 Sb., o technických podmínkách požární ochrany staveb

Vyhláška č. 221/2014 Sb., kterou se mění vyhláška č. 246/2001 Sb., o stanovení podmínek požární bezpečnosti a výkonu státního požárního dozoru (vyhláška o požární prevenci)

ČSN 34 2300, změna Z1, 09/2014 - Předpisy pro vnitřní rozvody sdělovacích vedení

ČSN 73 0804, změna Z2 02/2015 - Požární bezpečnost staveb – Výrobní objekty

ČSN 73 0848, 04/2009 - Požární bezpečnost staveb – Kabelové rozvody

ČSN 33 4000, změna 09/1990 - Požadavky na odolnost sdělovacích zařízení proti přepětí a nadproudu

STRUKTUROVANÁ KABELÁŽ

ČSN EN 50173-1 ed.3, 04/2012 - Informační technologie - Univerzální kabelážní systémy – Část 1:

Všeobecné požadavky

ČSN EN 50173-2, 05/2008 - Informační technologie - Univerzální kabelážní systémy – Část 2: Kancelářské prostory

ČSN EN 50174-1 ed.2, 05/2010 - Informační technologie - Instalace kabelových rozvodů – Část 1:

Specifikace a zabezpečení kvality

ČSN EN 50174-2 ed.2, 05/2010 - Informační technologie - Instalace kabelových rozvodů – Část 2:

Projektová příprava a výstavba v budovách

1.7.3 ZÁKLADNÍ TECHNICKÉ ÚDAJE

Napěťové soustavy:

- Silová soustava – síťové napájení 230V/50Hz: 1 NPE AC 230 V / TN-S

Ochrana před úrazem elektrickým proudem dle ČSN EN 61140:

- základní ochrana, ochrana při poruše

Ochranná opatření dle ČSN 332000-4-41 ed. 2

- Ochrana před dotykem neživých částí elektrického zařízení dle čl. 413:
- Silové rozvody 230V/50Hz: samočinným odpojením od zdroje, dvojítá, nebo zesílená izolace
- Sdělovací rozvody: malým napětím SELV
- Ochrana před dotykem živých částí elektrického zařízení dle čl. 412:
- je dána jejich konstrukčním uspořádáním a je řešena některou z těchto ochran: polohou, zábranou, krytem nebo přepážkami, izolací živých částí, doplňkovou izolací a doplňkovou ochranou proudovým chráničem.

Vnější vlivy dle ČSN 33 2000-3, 332000-5-51

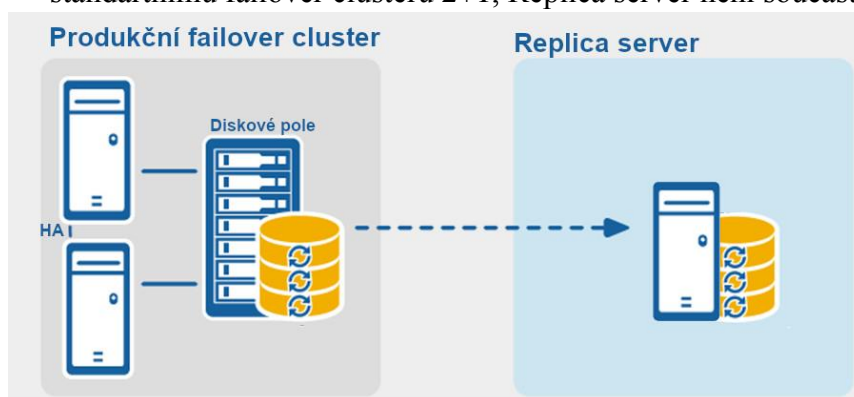
- Prostředí: protokol o vnějších vlivech nebyl v době zpracování této projektové dokumentace k dispozici. Dle získaných podkladů a dle charakteru objektu, by mělo být zařízení, včetně rozvodů, umístěno v prostorech s prostředím normálním.

1.7.4 TECHNICKÁ ZPRÁVA

1. Popis řešení

▪ Serverový cluster

V objektu bude provedena instalace nového serverového řešení včetně konfigurace a migrace stávajících fyzických serverů a dat školy na virtuální stroje běžící na serverovém clusteru. Model fyzických hostitelů bude odpovídat standardnímu failover clusteru 2+1, Replica server není součástí dodávky:



- **Instalace nové rackové skříně a přesunutí staré**

V místnosti Serverovny bude zabudována, osazena a zapojena 1 skříň (rack) nového hlavního datového rozvaděče.

Hlavní datový rozvaděč bude propojen s podružným rozvaděčem (který vznikne přesunem staré rackové skříně z místnosti serverovny do místnosti kabinetu TV) páteřním propojem optickým vláknem.

V místnosti Serverovny budou v nové rackové skříně instalovány a zapojeny aktivní síťové prvky – 2x switch, HW firewall, serverový cluster a diskové pole.

Ve staré rackové skříně přesunuté do Kabinetu TV budou instalovány a zapojeny 1x switch, dále budou do této skříně napojeny současné trasy vedoucí z kabinetu ke kamerovému systému a do školní jídelny.

Síťové zásuvky určené pro připojení aktivních prvků budou opatřeny přepětovou ochranou.

- **Rozvody strukturované kabeláže**

V objektu budou instalovány rozvody strukturované kabeláže (SK) UTP cat. 5e. a optický kabel min. 24 vláken, SM, 9/125μm. Zásuvky RJ 45 budou řešeny jako jednoportové a dvouportové do zdi, nebo na omítku. Rozmístění zásuvek je patrné z výkresové dokumentace. Nová kabeláž bude tvořit páteřní propoj Serverovny a Kabinetu TV. Práce s kabeláží zahrnují připojení nové i staré rackové skříně na stávající síťovou infrastrukturu školy a vytvoření tras pro osazení WiFi. Kabeláž a zásuvky budou rekonstruovány také v učebně informatiky.

- **Příprava WAN připojení**

Z místnosti serverovny bude vyvedena k patě budovy chránička HDPE umožňující budoucí zafouknutí optického kabelu pro připojení poskytovatele WAN. Samotné venkovní přípojky operátorů (poskytovatelé internetových a TV služeb) nejsou v rámci projektu řešeny.

- **Přebudování učebny informatiky**

V učebně Informatiky bude zasíťováno 15 pracovišť žáků se stolními PC a 12 pracovišť žáků vybavenými nově notebooky připojovanými přes LAN (celkově tedy 27 žákovských pracovišť). V současné době je zasíťováno 15 zásuvek, které budou přesunuty a zbývající budou nově vytvořeny (ostrůvek v podlaze s elektrickými a LAN zásuvkami). Dále bude vytvořeno jedno pracoviště učitele se stolním PC.

- **Připojení učebny chemie**

V učebně Chemie bude 10 pracovišť žáků vybavených notebooky připojovanými přes WiFi a 1 pracoviště učitele se stolním PC připojovaným přes LAN (zásuvka již existuje). Učebna chemie bude vybavena pylonovou a interaktivní tabulí s dataprojektorem.

- **Osazení WiFi AP**

V rámci projektu je navrženo osazení přístupových bodů (access point) bezdrátové WiFi sítě. Přístupové body budou rozmístěny tak, aby co nejlépe pokryly všechny prostory daného objektu školy. Všechna AP budou napojena na strukturovanou kabeláž (nejsou přípustné repeatery nebo bezdrátové extendery) Přesné rozmístění a připojení přístupových bodů bude optimalizováno v rámci realizace projektu a signál v objektu proměřen pomocí SW. Přístupové body budou řízeny a spravovány hromadně a centrálně.

▪ **Tvorba AD, konverze fyzických serverů a migrace dat**

Správa uživatelů bude řešena prostřednictvím virtualizovaného serveru s AD (active directory). Zařízení bude dimenzováno pro správu všech uživatelů v přistupujících do LAN – tj 600 členů. Stávající struktura školní sítě využívá hostitele VMWARE, virtuální servery jsou umístěny na diskovém poli s připojením typu iSCSI, kapacita stávajícího diskového pole je vyčerpána. Stávající VM budou v rámci zakázky přemigrovány do nového diskového pole a na nové hostitele, kteří budou pracovat jako cluster v režimu vysoké dostupnosti (HA). V rámci projektu bude přemigrován obsah stávajícího AD (uživatelské profily i data uživatelů) na nový Windows 2019 DC server. W2019 server DC bude sloužit jako primární doménový řadič. Nastavení domény je upřesněno v dokumentu „Požadavky na nastavení prostředí školní domény“

2. Provedení

- Veškeré metalické rozvody (horizontální i páteřní) budou provedeny kabely UTP 4x2x0,5, cat. 5e. Optické rozvody budou provedeny univerzálním optickým kabelem 24 vl., SM, 9/125 µm, OS1.
- Kabely budou vedeny jednak v páteřních kovových drátěných žlabech osazených pod podlahou a v podlaze, a jednak v trubkách zasekaných do zdi, nebo v plastových lištách či ohebných trubkách, popřípadě žlabech v nábytku. V technických prostorech může být kabeláž vedena v tuhých trubkách po povrchu. Veškeré kabelové prostupy požárně dělicími konstrukcemi mezi jednotlivými požárními úseky budou dle ČSN 73 0848, 04/2009 – Požární bezpečnost staveb – Kabelové rozvody, kap. 5.2.8. utěsněny požárními ucpávkami.
- Veškerý dodávaný HW musí být určen k prodeji na českém trhu a musí být nový.
- Servery a Diskové pole požadujeme od stejného výrobce.
- "Cílem naší organizace je zajistit soulad se standardem konektivity, který definuje základní technická kritéria pro projekty předložené ve výzvách č. 32 a 33 (SŠ, VOŠ) a č. 46 a 47 (ZŠ) a č. 66 a 67 (ZŠ, SŠ a VOŠ) v rámci specifického cíle 2.4 IROP a dále ve výzvě č. 68 (ZŠ, SŠ a VOŠ) v rámci specifického cíle 4.1 IROP. "
- Není žádoucí dodávat produkty určené do domácností, jejich konstrukce postrádá odolnost potřebnou pro použití ve školství, požadované síťové a serverové produkty navrhujte tak, aby mohly fungovat bezproblémově po celou dobu své životnosti, jejich ovládání minimalizovalo nutnost servisu a případné úpravy konfigurace byly rychlé a snadné. Požadujeme co nejstandardnější řešení renomovaných výrobců.

- Software pro implementaci virtualizace:
 - Licence musí pokrývat
 - provoz min. 3 fyzických serverů
 - využití min. 6 fyzických procesorů
 - využití min. 64GB vRAM na každý fyzický procesor
 - podpora min. 8 vCPU pro každý virtuální server
 - podpora min. 64GB vRAM na každý virtuální server
 - funkcionality vysoké dostupnosti (HA)
 - funkcionality, která automaticky nainstaluje virtuální stroje při výpadku fyzického hostitele na jiném produkčním hostiteli ze společného diskového pole
 - rozhraní, které umožní zálohovacímu SW třetí strany provádět konzistentní plné, rozdílové a přírůstkové zálohy virtuálních strojů bez nežádoucího zvyšování režie a zátěže hostitelského serveru a virtuálních strojů
 - komplexní správu virtuální infrastruktury z jedné konzole, která umožňuje integraci s produkty třetích stran
 - podpora OS Win server2000 - 2019, Win XP - Win 10, Linux, FreeBSD...
 - funkcionality, která umožní virtuálním strojům přidávat více diskového prostoru, než je reálná disková kapacita
 - bezvýpadkovou migraci virtuálních strojů za provozu
 - podporu aktualizací min. 3 roky
- Software pro replikaci VM a zálohování dat:
 - zálohování podporuje server Windows 2019
 - podpora Linuxu (alespoň RedHat a SLES)
 - umožnění tvorby inkrementálních snapshotů, které respektují běžící databáze (Exchange, MSSQL) a umožní jejich zprovoznění z tohoto snapshotu
 - podpora aktualizací min. 3 roky
- OS virtuálních serverů
 - Musí splňovat podmínku, že touto dodávkou bude korektně licencován libovolný počet virtuálních serverů na každém jednom fyzickém serveru
- Instalační práce + zaškolení obsluhy
 - Součástí dodávky je instalace a oživení HW ve škole
 - instalace virtuální vrstvy
 - Konverze fyzických strojů na virtuální, případné vytvoření nových virtuálních strojů s plnou funkcionalitou předchozích fyzických
 - Migrace dat, doménových účtů
 - Nastavení Firewallu dle potřeb školy, propojení s AD, zaškolení
 - Nastavení služeb logování
 - Nastavení zálohování a replikací na replikačním serveru, zálohovací politiky a kalendáře
 - Nastavení GPO dle potřeb školy
 - Zaškolení obsluhy doménových účtů
- Poimplementační podpora
 - po dobu 45ti dnů od předání nové infrastruktury do užívání musí dodavatel zajistit součinnost při nastavování infrastruktury a případném řešení problémů takto:

- zajistí nepřetržitý monitoring HW komponent tak, aby mohl včas zajistit výměnu případných vadných dílů přímo se servisní podporou výrobce
 - zajistí nepřetržitý monitoring stavu vytižení HW komponent včetně teploty, vytižení CPU, RAM, kapacity HDD, odezvu při zápisu a čtení z diskových jednotek
 - na základě těchto dat zajistí proaktivní a prediktivní podporu pro prevenci a řešení problémů.
- Dodavatel bude řešit požadavky školy na řešení problémů souvisejících se změnou HW s reakční dobou 1 hod. od vzniku požadavku nebo vzniku incidentu na sledovaných zařízeních

3. Aktivní prvky –AP

Z důvodu zabezpečení standardu konektivity škol je navrženo osazení prvky s možností plného managementu. Na rozhraní WAN/ LAN bude v rámci projektu osazen řídicí prvek zajišťující následující funkce:

- podpora monitoringu a logování NAT (RFC 2663) provozu za účelem dohledatelnosti veřejného provozu k vnitřnímu zařízení
- logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas – uživatel a to včetně ošetření v případě sdílených učebeň (pracovních stanic apod.)
- síťové zařízení podporující rate limiting, antispoofing, ACL/xACL, rozhraní musí obsahovat všechny potřebné komponenty a licence pro zajištění řádné funkcionality
- zařízení umožňující kontrolu http a https provozu, kategorizaci a selekci obsahu dostupného pro vybrané skupiny uživatel (učitel, žák, správni zaměstnanec, host – podle skupin v AD), blokování nežádoucích kategorií obsahu, antivirovou kontrolou stahovaného obsahu
- možnost snadné/automatické rekonfigurace ACL/FW na základě identifikovaných útoků
- podpora DNSSEC a IPv6 protokolů pro služby školy dostupné online
- Aktivní prvky (centrální směrovače a centrální přepínače; L2 i L3 s neblokující architekturou přepínacího subsystému (wire speed), podpora 802.1Q VLAN, podpora 802.1X, radius based MAC autentizace,...
- 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 s kapacitou pro uchování dat po dobu minimálně 2 měsíců
- Povinné řešení systému 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. síťovým službám.
- logování přístupu uživatelů do sítě umožňující dohledání vazeb *IP adresa – čas – uživatel*

Aktivní prvky (switche) zajišťující vnitřní konektivitu umožňují následující funkce:

- Minimální konektivita stanic a dalších dodávaných koncových zařízení uvnitř sítě - 1000Mbit/s (po metalických spojích)
- Minimální konektivita serverů, aktivních síťových prvků, bezpečnostních zařízení 1Gbit/s full duplex po metalických spojích – aktivní prvky napojené na optické vlákno pak 10Gbit/s.
- Páteční rozvody mezi budovami v areálu budou realizovány prostřednictvím optických vláken
- Aktivní prvky (centrální směrovače a centrální přepínače; L2 i L3 s neblokující architekturou přepínacího subsystému (wire speed), podpora 802.1Q VLAN, podpora 802.1X, radius based MAC autentizace,...

Bezdrátové komponenty splňují následující parametry:

- Podpora mechanismu izolace klientů
- Návrh topologie wifi sítě a analýza pokrytí signálem počítající s konzistentní Wi-Fi službou v příslušných prostorách školy a s kapacitami pro provoz mobilních zařízení pedagogického sboru, studentů i návštěv, každé AP musí splňovat požadavek na současnou obsluhu minimálně 30 klientů
- Centralizovaná architektura správy wifi 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)
- Podpora protokolu IEEE 802.1X resp. ověřování uživatelů oproti databázi účtů přes protokol radius (např. LDAP, MS AD ...)
- Podpora standardu IEEE 802.11n a případně novějších (ac, ad), současná funkce AP v pásmu 2,4 a 5 GHz
- Minimálně pasivní zapojení do federovaného systému eduroam.
- Podpora WPA2, PoE, multi SSID, ACL pro filtrování provozu

V LAN jsou navržena další zařízení vyhovující následujícím bezpečnostním požadavkům:

- Identity management systémy (IDM) – systém správy identit, řízení životního cyklu uživatelů, integrace do provozních a bezpečnostních systémů
- Centralizovaný autentizační systém napojení na systém správy identit (např. na bázi LDAP, AD, studijní a personální agendy apod.)
- Řešení dočasných přístupů (hosté, brigádníci, praktikanti, zákonní zástupci, externí subjekty, blokáce wifi v určitém čase, oddělené VLAN)
- Federované služby autentizace a autorizace (včetně zapojení do národních vzdělávacích federací a zpřístupnění jejich služeb)
- Systémy nebo zařízení pro sledování infrastruktury sítě a sledování IP provozu sítě (umožňující funkce RFC 3954 nebo ekvivalent (NetFlow))
- Systémy schopné detekovat nelegitimní provoz nebo síťové anomálie
- Systémy vyhodnocování a správy událostí a bezpečnostních incidentů (log management, incident management)
- Systémy pro monitorování funkčnosti síťové a serverové infrastruktury (např. Nagios / Icinga)
- Systémy uživatelské podpory naplňující principy ITIL (HelpDesk, ServiceDesk)
- Nástroje pro centrální správu a audit ICT prostředků
- Systémy zálohování a obnovy dat serverové infrastruktury

- Systémy pro antivirovou ochranu zařízení, antispamovou ochranu poštovních serverů
- Zabezpečení přístupových protokolů (SSL/TLS) služeb (např. emailové služby, webové servery, studijní a ekonomické agendy) atp.
- Podpora vzdáleného přístupu (VPN)

Způsob ověření splnění standardu konektivity bude otestován a validován v součinnosti s odběratelem za pomoci dokumentu „Ověření standardu konektivity“. Dodavatel prokáže, že tento standard škola naplnila.

4. Dokumentace

Součástí díla je dokumentace a to zejména:

- technická dokumentace (produktové listy atd.)
- návody k použití (manuály), v tištěné nebo elektronické podobě v českém jazyce
- Implementační dokumentace
 - Obsahem dokumentace bude minimálně:
 - textový popis řešení jako celku,
 - schema zapojení HW
 - výrobce a typ zařízení,
 - kompletní přehled dodaných a použitých licencí,
 - Přístupové údaje nastavené při implementaci – přehledová tabulka o tabulka musí obsahovat veškeré přístupové údaje k jednotlivým komponentám a jejich managementu tak, aby zadavatel měl po převzetí řešení neomezený přístup ke všem jeho částem.
 - kontaktní informaci na technickou poimplementační podporu
 - kontaktní informace na servisní pracoviště zajišťující podporu jednotlivých HW komponent.
 - všechny funkcionality, které jsou využity, musí být podrobně zdokumentovány, tak aby uživatel neznalý těchto funkcionalit byl s nimi podle dokumentace schopný pracovat
- Měřicí protokoly na síťovou infrastrukturu
- Popis datových zásuvek v místnostech a Racku

Zásady bezpečnosti a ochrany zdraví při práci na staveništi a ochrany zdraví podle jiných právních předpisů

Při montáži budou dodržovány v době realizace platné zákony, vyhlášky, prováděcí předpisy, ČSN a technologické předpisy, především: Zákon č. 262/2006 Sb. zákoník práce, NVč.591/2006 Sb.

O bližších minimálních požadavcích na bezpečnost práce a ochranu zdraví při práci na staveništích, NV č. 494/2001Sb. o evidenci a hlášení pracovních úrazů, z.č.309/2006 Sb. o BOZP, NV č. 362/2005 Sb. o bližších požadavcích na bezpečnost práce a ochranu zdraví při práci na pracovištích s nebezpečím pádu z výšky nebo do hloubky.

Přesný postup prací stanoví zhotovitel.

Technologické postupy a opatření se musí vždy přizpůsobit aktuální situaci na místě montáže.

Montáž bude prováděna za provozu, je potřeba vyžádat součinnost bezpečnostního technika investora stavby.

Na realizaci se bude podílet více než jeden zhotovitel, je tedy dle z. č. 309/2006 Sb. potřeba koordinátor BOZP.