Technická zpráva – aktivní prvky – ZŠ U Studny

Projekt:

Rekonstrukce odborných učeben ZŠ a MŠ Prameny, ZŠ a MŠ U Lesa a ZŠ a MŠ U Studny v Karviné

Organizace: **Základní škola a Mateřská škola U Studny, Karviná, příspěvková organizace**

- **Centrum 2290/14, 734 01 Karviná-Mizerov**
- **Čajkovského 2215, 734 01 Karviná-Mizerov**
- **Centrum 2314, 734 01 Karviná-Mizerov**

Žadatel: **Statutární město Karviná - Magistrát města Karviné**
Fryštátská 72/1, 733 24 Karviná-Fryštát
IČ: 00297534

Zpracovatel: **COMFOR STORES a.s.**
Sídlo: 624 00 Brno, Běly Pažoutové 742/1
Provozovna: 735 06 Karviná 6, Závodní 540/51
IČ: 26290944
Zpracoval: Dalibor Havel
Tel. +420 603 874 424
Mail: Dalibor_Havel@comfor.cz

Přílohy:

1. **Popis minimálních technických požadavků na IT vybavení**
2. **Schéma datové sítě v jednotlivých NP a budovách**
3. **Rozpočet**

Karviná 01/2017

Projektová dokumentace řeší komplexní dovybavení aktivní síťové infrastruktury na ZŠ a MŠ U Studny ve všech jejich objektech. Navrhované řešení se skládá z:

1. Doplnění, nebo výměna aktivních síťových prvků
2. Pokrytí všech objektů školy WiFi signálem
3. Vybudování monitorovaných přístupových systému u všech provozních vstupů ve všech objektech školy
4. Vybavení pro bezpečnost a monitorování datové sítě

Text níže popisuje jednotlivé části projektu, použité zkratky jsou blíže specifikovány v příloze č.1 tohoto dokumentu.

Centrálním síťovým prvkem datové sítě bude **FW** umístěný v datovém rozvaděči R1 plnící funkci firewallu tj. ochrany vnitřní datové sítě ve vztahu k veřejnému datovému prostoru (internetu). Hlavním páteřním prvkem datové sítě bude **SW1** s umístěním rovněž v datovém rozvaděči R1. Ponechán bude pouze stávající aktivní prvek vyhovující aktuálním standardům (Zyxel GS 1910-48 v 3.NP). Ostatní aktivní prvky budou nahrazeny za **SW2** nebo doplněny o **SW2**. Propojení jednotlivých aktivních prvků s hlavním aktivním prvkem bude pomocí **SFP** a optických patchcordů. Každý aktivní prvek v datové síti bude mít přímé spojení s hlavním aktivním prvkem (všechny budou na 1. úrovni). Součástí projektu je instalace a konfigurace FW, konfigurace site-to-site VPN k síti Magistrátu města Karviné, přepojení stávající LAN sítě do hvězdicové topologie.

Všechny datové rozvaděče (mimo hlavní), budou vybaveny elektrickými propojovacími poli **EPP** a **UPS1** pro krytí výpadku napájení přístupových bodů a aktivních prvků. Se stejným využitím bude hlavní rozvaděč R1 vybaven výkonnějším záložním zdrojem **UPS2**. Součástí projektu je instalace záložních zdrojů UPS1, UPS2 a propojovacích polí EPP do jednotlivých datových rozvaděčů a připojení rozvaděčů přes záložní zdroje.

Z přílohy (schéma) je rovněž patrno umístění navržených WiFi přístupových bodů **AP**. Napájení jednotlivých přístupových bodů bude centralizováno v datovém rozvaděči do **POE injektor** panelu s potřebným počtem portů. Součástí projektu je instalace, konfigurace a oživení centrální WIFI sítě.

Z přílohy je rovněž patrno umístění navržených monitorovaných přístupových systému. Jako jednotlivé přístupové body jsou použity **PSx** s potřebným počtem tlačítek (x = počet tlačítek) kompatibilní s instalovanými elektricky ovladatelnými dveřními zámky a softwarovým rozšířením funkčnosti **PSS**. Konkrétní umístění a typ přístupových bodů je patrno z přílohy (schéma).

Součástí navrhovaného řešení je i vybavení pro bezpečnost a monitorování datové sítě. Správa bezpečnostních informací a událostí (**EventManagement**) bude řešen zasíláním událostí do centrálního systému pro správu logů. Součástí projektu je konfigurace všech aktivních prvků sítě a min. 2 ks Windows serverů pro zasílání logů do centrálního systému.

Součástí projektu je vybavení učeben a kabinetů výpočetní technikou. Nová IT technika bude zapojena a nainstalována v místě určeném při realizaci. Popis minimálních technických parametrů je uveden v příloze č. 1 tohoto dokumentu.

Příloha č. 1: Popis minimálních technických požadavků na IT vybavení

FW: Firewall splňující tyto minimální technické parametry:

- 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,
- podpora rate limiting, antispoofing, ACL/xACL,
- rozhraní musí obsahovat všechny potřebné komponenty a licence pro zajištění řádné funkcionality,
- zařízení musí umožňovat kontrolu http a https provozu, kategorizaci a selekci obsahu dostupného pro vybrané skupiny uživatel (učitel, žák), blokování nežádoucích kategorií obsahu, antivirovou kontrolou stahovaného obsahu.
- zařízení musí umožnit snadnou/automatickou rekonfiguraci ACL/FW na základě identifikovaných útoků,
- je vyžadována neblokující architektura, podpora 802.1Q, 802.1X a MAC autentizace,
- zařízení musí podporovat DNSSEC a IPv6 protokoly pro služby školy dostupné online,
- pro software a firmware je vyžadována dostupnost aktualizací, zejména bezpečnostního charakteru po dobu minimálně 5 let, tato musí být garantována výrobcem zařízení,
- zařízení umožňuje 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) do systému pro správu logů (**EventManagement**),
- minimální propustnost FW (stavové filtrování, UDP paket) min 1.2 Gbps,
- propustnost FW paketů za sekundu - min. 255kpps,
- latence firewallu (64B UDP paket) – max. 90 mikro sec,
- počet současně otevřených spojení - min 1 500 000,
- minimální počet nových spojení za sekundu - min. 20 000,
- propustnost IPSEC VPN (512 B paket) - min. 200 Mbps,
- propustnost SSL VPN min 120 Mbps,
- propustnost IPS - min 700 Mbps,
- propustnost Aplikační kontroly - min. 250 Mbps,
- podpora virtualizace: min 10 virtuálních kontextů,
- režim fungování L2 – transparentní režim, L3 – NAT/Router,
- podpora multicast, vytváření politiky pro multicast routování,
- podpora VPN: SSL (portálový režim, tunelový režim), IPSEC (IKE, manual key, certifikát, gateway to gateway, hub and spoke, dial up konfigurace, internet browsing konfigurace, podpora vice tunelů – redundantní VPN,
- podpora dynamických routovacích protokolů – OSPF, BGP, ISIS,
- podpora Policy routingu,
- traffic Shaping, QoS,
- možnost nastavovat firewall politiku na základě geografických údajů,
- podpora funkce Load Balancing – možnost rozdělování zátěže směrující na virtuální IP na reálně servery, podpora health check funkcí,
- podpora centrální NATovácí tabulky,
- podpora UTM/NGFW funkcí (antispamová inspekce, antivirová kontrola, ochrana před bot-net komunikací, Intrusion Protection System (IPS/IDS), funkce kategorizace webových stránek, funkce rozpoznávání aplikací dle chování na L7, data leak prevention),
- funkce antiviru pro vybrané protokoly, možnost volby různých databází, podpora archivace škodlivého obsahu, podpora protokolu ICAP pro offload AV engine, možnost detekce rootkit, malware, spywave, keylogger, atd.,
- email filter – antispamová a antivirová inspekce elektronické pošty,

- Intrusion Protection System – detekce útoků a škodlivého kódu založena na signaturové části a na anomálním filtru, možnost vytvářet vlastní signatury,
- Web Filter – založená na kategorizaci webového obsahu, možnost monitorování navštívených kategorii na uživatele či skupinu, možnost kvóty – uživatel může strávit nad určitou kategorii webu jen stanovenou dobu během dne,
- Data Leak Prevention s funkcí document fingerprinting,
- Application Control – detekce, monitoring, povolení či zakázání na základě signatury dané aplikace, nikoliv dle portu,
- Deep scanning – možnost kontroly komunikace v SSL šifrovaných protokolech (HTTPS, IMAPS, POP3S atd.),
- podpora ochrany před DoS útoky, syn proxy,
- ověřování uživatelů LDAP, Active Directory, Radius, TACACS+, ověřování na základě certifikátu, dynamické profily – možnost přiřadit konkrétní profil uživateli na základě jeho ověření,
- podpora VoIP, SIP včetně zabezpečení, rate limitingu, analýzy protokolu,
- explicitní Proxy, WCCP,
- z důvodu nezávislosti na ostatních systémech musí být zařízení dodáno jako samostatný hardware s těmito minimálními hardwarovými parametry:
    - 4x LAN port
    - 1x console port
    - min. 16GB interní storage pro ukládání logu
    - výrobcem garantována podpora 5 let v režimu 8/5 s výměnou dílu NBD (následující pracovní den)

EventManagement - sběr bezpečnostních informací a událostí splňující tyto minimální technické parametry:

- Plná kompatibilita s centrálním systémem pro správu logů (centrální systém pro správu logů je zařízení LogManager firmy Sirwisa a.s. a je umístěn v technologickém centru magistrátu města Karviné). Plnou kompatibilitou se rozumí možnost zasílání událostí do centrálního systému při splnění níže uvedených požadavků,
- zařízení musí umožňovat sběr událostí s těchto systémů
    - OS Windows 7 a vyšší, OS Windows server 2008 a vyšší
    - OS Linux
    - Antivir Eset, včetně Eset remote administrator
    - switch HPE, Cisco
    - Mikrotik
    - UBNT UniFI
    - VMware
- z důvodu nezávislosti na ostatních systémech musí být zařízení dodáno jako samostatná hardwarová appliance připojena do vnitřní sítě školy,
- výkon zařízení min. 5000 událostí za sekundu
- zasílání logů do centrálního systému musí být realizováno pomocí zabezpečené komunikace (např. IPsec tunel),
- zasílané logy musí obsahovat informaci/značku o tom, z které školy jsou odesílané,
- v případě výpadku spojení s centrálním systémem, musí zařízení uchovávat logy pro následné odeslání s kapacitou 50GB,
- výrobcem garantována servisní podpora 5 let v režimu 8/5 s výměnou dílu NBD (následující pracovní den)

SW1: aktivní prvek – switch splňující tyto minimální technické parametry:

- montáž do 19“ datového rozvaděče
- 24x gigabitový SFP port
- 2x nesdílený metalický gigabitový port full duplex
- konfigurace přes WEB rozhraní
- řiditelný
- přepínající na vrstvě L3
- doživotní, výrobcem garantovaná záruka s opravou v místě instalace.

SW2: aktivní prvek – switch splňující tyto minimální technické parametry:

- montáž do 19“ datového rozvaděče
- 24x metalický gigabitový port full duplex
- 2x nesdílený gigabitový SFP port
- konfigurace přes WEB rozhraní
- řiditelný
- přepínající na vrstvě L2
- bez aktivního chlazení
- doživotní, výrobcem garantovaná záruka s opravou v místě instalace.

SFP: SFP modul splňující tyto minimální technické parametry:
- 1G SM 1310nm 20km LC 100% kompatibilní s navrženými aktivními prvky,
- záruka 2 roky.

AP: přístupový bod WiFi splňující tyto minimální technické parametry:
- podpora mechanismu izolace 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 přístupové body a automatickým laděním kanálů a síly signálu včetně detekce a reakce na nejen non-Wi-Fi rušení),
- podpora protokolu IEEE 802.1X resp. ověřování uživatelů oproti databázi účtů přes protokol radius (např. LDAP, MS AD atd.),
- podpora standardu IEEE 802.11n a případně novějších (ac, ad),
- současná funkce AP v pásmu 2,4 a 5 GHz,
- podpora WPA2,
- PoE napájení vč. adaptéru,
- multi SSID,
- ACL pro filtrování provozu,
- doživotní, výrobcem garantovaná záruka s opravou v místě instalace.

UPS1: Zařízení UPS splňující tyto minimální technické parametry:
- montáž do 19“ datového rozvaděče,
- výstupní výkon 1000W / 1500 VA, 230V,
- 4x IEC 320 C13,
- slot pro management kartu, včetně UPS Network Management karty podporující vzdálenou správu IP protokolem,
- záruka 3 roky s opravou v místě instalace.

UPS2: Zařízení UPS splňující tyto minimální technické parametry:
- výstupní výkon 325W / 650 VA, 230V, 4x IEC 320 C13,
- záruka 2 roky s opravou v místě instalace.

PS1: Monitorovaný přístupový systém splňující tyto minimální technické parametry:
- 1-tlačítkový variabilní komunikační systém podporující jak přenos hlasu (full duplex audio), tak videa (kodeky: H.263, H.263+, H.264). To vše v IP prostředí za pomoci protokolu SIP (kodeky: G.711, G.729) s možnosti vzdálené správy,
- POE napájení,
- Ethernet konektor,
- výstup k ovládání elektrického zámku,
- kompatibilní s instalovaným zámkem (stanovený minimální technologický standard např. 2N BEFO)
- záruka 2 roky s opravou v místě instalace.

PS3: Monitorovaný přístupový systém splňující tyto minimální technické parametry:
- 3-tlačítkový variabilní komunikační systém podporující jak přenos hlasu (full duplex audio), tak videa (kodeky: H.263, H.263+, H.264). To vše v IP prostředí za pomoci protokolu SIP (kodeky: G.711, G.729) s možnosti vzdálené správy,

- POE napájení,
- Ethernet konektor,
- výstup k ovládání elektrického zámku,
- kompatibilní s instalovaným zámkem (stanovený minimální technologický standard např. 2N BEFO)
- záruka 2 roky s opravou v místě instalace.

PS6: Monitorovaný přístupový systém splňující tyto minimální technické parametry:

- 6-tlačítkový variabilní komunikační systém podporující jak přenos hlasu (full duplex audio), tak videa (kodeky: H.263, H.263+, H.264). To vše v IP prostředí za pomoci protokolu SIP (kodeky: G.711, G.729) s možnosti vzdálené správy,
- POE napájení,
- Ethernet konektor,
- výstup k ovládání elektrického zámku,
- kompatibilní s instalovaným zámkem (stanovený minimální technologický standard např. 2N BEFO)
- záruka 2 roky s opravou v místě instalace.

PSS: Rozšiřující licence k PSx splňující tyto minimální technické parametry:

- Licence Enhanced Video umožňující audio/video streaming (RTSP Server) a podporující ONVIF.

EPP: Elektrické propojovací pole

- montáž do 19“ RACKu,
- min. 5 x eurozásuvka,
- 2 m přívodní kabel.
- záruka 2 roky s opravou v místě instalace.

POE injektor:

- montáž do 19“ RACKu,
- PoE napájení min. 12 zařízení
- včetně napájecího zdroje zajišťujícího výkon min. 10W na port
- záruka 2 roky s opravou v místě instalace.

NB SET:

- CPU s hodnotou 4 600 bodů dle http://www.cpubenchmark.net/,
- RAM 8GB DDR4,
- DVD+/-RW,
- HD SSD 250GB,
- integrovaná VGA s výstupy: VGA (D-SUB) + HDMI,
- GB LAN,
- LCD 15,6" s rozlišení 1920x1080,
- 4x USB z toho 2x USB 3.x,
- Bluetooth, WiFi 802.11ac, čtečka SD karet,
- Operační systém - platná podkladová licence (OEM verze operačního systému v aktuální verzi) pro multilicenční program Microsoft EA,
- USB klávesnice CZ + USB optická myš,
- Záruka 3 roky s opravou v místě instalace na celý SET,
- Součástí dodávky je instalace software (MS Windows 10 Pro CZ 64-bit + Office 2016 CZ 64-bit + antivirového programu - licence dodá zadavatel),
- Součástí dodávky je doprava, vybalení a zapojení v místě určeném zadavatelem.

PC SET:

- CPU s hodnotou 6 500 bodů dle http://www.cpubenchmark.net/,
- RAM 8GB DDR4,
- DVD+/-RW,
- HD SSD 250GB,
- integrovaná VGA s výstupy: VGA (D-SUB, DVI, HDMI),
- integrovaná LAN 1000Base-TX,

- 6x USB z toho 2x USB 3.x,
- provedení Mini nebo MicroTover s USB 3.x + audio na předním panelu,
- tichý zdroj s účinnosti větší než 85%,
- USB klávesnice CZ + USB optická myš,
- operační systém - platná podkladová licence (OEM verze operačního systému v aktuální verzi) pro multilicenční program Microsoft EA.
- LCD monitor 23.6", rozlišení 1920x1080, panel IPS, odezva 5ms, výstupy: VGA(D-SUB) + DVI nebo HDMI, MHL,
- záruka 3 roky s opravou v místě instalace na celý SET,
- součástí dodávky je instalace software (MS Windows 10 Pro CZ 64-bit + Office 2016 CZ 64-bit + antivirového programu - licence dodá zadavatel),
- součástí dodávky je doprava, vybalení a zapojení v místě určeném zadavatelem.

Tiskárna:

- multifunkční (kopírování/skenování/tisk),
- barevná, A4,
- tisk 20 str/min černě i barevně dle normy ISO/IEC 24734,
- automatický oboustranný tisk,
- automatický podavač pro kopírování a skenování,
- zásobník na 250 listů,
- skenování do USB/ e-mailu, FTP, složky po síti,
- podpora LDAP,
- bezpečný tisk - uvolňování úloh z tiskárny zadáním kódu PIN,
- USB, Ethernet, WiFi,
- záruka 3 roky s opravou v místě instalace.