Příloha k technické zprávě - konektivita

Název akce	: **Zřízení specializovaných odborných učeben na základních školách ve městě Studénka - Multimediální výuka odborných předmětů – ZŠ Butovická**
Investor	: Město Studénka, nám. Republiky 762, Butovice, 74213 Studénka
Místo stavby	: Butovická 346, 742 13 Studénka
Zakázka číslo	: 024/16
Datum	: leden 2017
Projektant	: Adrian Banyacski

Zodpovědné osoby

Projekt vypracoval Adrian Banyacski – projektování IT technologií pro generálního projektanta DaF-PROJEKT s.r.o. .

Za obsah projektu a návrh technického řešení zodpovídá :

Adrian Banyacski

Předmět projektu

Projektová dokumentace konektivita v rámci akce : „Zřízení specializovaných odborných učeben na základních školách ve městě Studénka. Multimediální výuka odborných předmětů.

OBSAH PŘÍLOHY TECHNICKÉ ZPRÁVY:

1. Konektivita školy k veřejnému internetu

V rámci potřeb školy a v rámci požadavků dle kolové výzvy č.46 specifického cílu 2.4. bude konektivita do veřejného internetu řešena instalací nového hardware (router) i software . Hardware bude umístěn v nově instalovaném racku v učebně PC 3.NP(317) Dále, bude instalován firewall tak, aby splňoval minimální parametry. Dle požadavků konektivity do veřejného internetu musí mít řešení tyto minimální parametry:

- *šíře pásma (bandwidth) odpovídající 128kbps/student1 nebo 512kbps/počítač2 nebo taková šířka pásma, která neomezuje provoz zařízení a uživatelů3*
- *vlastní nebo poskytovatelem přidělené veřejné IPv4 i IPv6 adresy*
- *plná podpora připojení do veřejného internetu přes protokol IPv4 i IPv6 (dual-stack)*
- *validující DNSSEC resolver na straně školy*
- *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 učeben (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), 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 u software a firmware je vyžadována dostupnost aktualizací, zejména bezpečnostního charakteru po celou dobu udržitelnosti projektu.*

2. Vnitřní konektivita školy

V rámci potřeb školy a v rámci požadavků dle kolové výzvy č.46 specifického cílu 2.4. bude vnitřní konektivita řešena doplněním vybavení stávajícího racku. V rámci doplnění budou instalován nové patch panely a switch. Dále bude instalován controler pro wifi provoz školy. Bude instalováno řešení pro monitorování IP. Bude instalováno 10ks access pointů.

Řešení vnitřní konektivity školy musí splňovat tyto minimální parametry:

Povinné minimální bezpečnostní parametry projektu (bez ohledu typ síťového připojení):

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

V oblasti pevné LAN musí projekt splňovat následující minimální parametry:

- *Minimální konektivita stanic a dalších koncových zařízení zařízení 100Mbit/s fullduplex*
- *Strukturovaná kabeláž pro připojení pracovních stanic a dalších zařízení (tiskárny, servery, AP,…)*
- *Minimální konektivita serverů, aktivních síťových prvků, bezpečnostních zařízení, NAS 1Gbit/s fullduplex*
- *Páteřní rozvody mezi budovami v areálu realizovány prostřednictvím optických, metalických vláken popř. bezdrátovými spoji v licencovaném pásmu (povolení ČTÚ)*
- *Aktivní prvky (centrální směrovače a centrální přepínače; L2 i L3)[4] s neblokující architekturou přepínacího subsystému (wire speed), podpora 802.1Q VLAN, podpora 802.1X, radius based MAC autentizace,…*

V případě řešení bezdrátových sítí (wifi) pak musí projekt naplňovat následující minimální parametry:

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

- *Podpora mechanismu izolace klientů*
- *Návrh topologie wifi sítě a analýza pokrytí signálem počítající s konzistentní Wi-Fi službou ve v příslušných prostorách školy a s kapacitami pro provoz mobilních zařízení pedagogického sboru i studentů*
- *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*
- *Podpora WPA2, PoE, multi SSID, ACL pro filtrování provozu*

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

- *Minimálně pasivní zapojení*[5] *do federovaného systému eduroam (www.eduroam.cz). Optimálně aktivní zapojení do systému eduroam, pro zajištění národní i mezinárodní mobility žáků a učitelů.*

3. Další bezpečnostní prvky

V rámci potřeb školy a v rámci požadavků dle kolové výzvy č.46 specifického cílu 2.4. budou bezpečnostní prvky řešeny vhodným softwarovým zabezpečením. Jedná se zejména o:

- *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, blokace wifi v určitém čase)*
- *Federované služby autentizace a autorizace (včetně aktivního 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*

[5] *Pasivním zapojením se rozumí poskytování služeb sítě eduroam na úrovni poskytovatele zdrojů – viz.* http://www.eduroam.cz/_media/cs/cz_roam_policy_v2.0.pdf