Odborné a bezbariérové vzdělávání v nových učebnách ZŠ Vančurova Hodonín V Brně dne : 18.12.2019

Protokol o stavu konektivity

Konektivita školy k veřejnému internetu WAN	současný stav	**Po realizaci projektu**
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 minimální parametry v době ukončení realizace projektu:		
Šíře pásma (bandwidth) odpovídající 128kbps/student nebo 512kbps/počítač nebo taková šířka pásma, která neomezuje provoz zařízení a uživatelů	vyhovuje 512kbps/počítač	vyhovuje 512kbps/počítač
Vlastní nebo poskytovatelem přidělené veřejné IPv4 i IPv6 adresy	1x veřejná adresa	2x Veřejná adresa
Plná podpora připojení do veřejného internetu přes protokol IPv4 i IPv6 (dual-stack)	pouze IPv4	IPv4 a IPv6
validující DNSSEC resolver na straně školy	vyhovuje	nutno ověřit jestli to zajišťuje poskytovatel domeny
Podpora monitoringu a logování NAT (RFC 2663) provozu za účelem dohledatelnosti veřejného provozu k vnitřnímu zařízení	částečně	FlowMon řešení s exportem Flow z FW
Logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas – uživatel a to včetně ošetření v případě sdílených učeben (pracovních stanic apod.)	Není řešeno	FlowMon s 802.1x s autentifikací proti AD ?
Síťové zařízení podporující rate limiting, antispoofing, ACL/xACL, rozhraní musí obsahovat všechny potřebné komponenty a licence pro zajištění řádné funkcionality	vyhovuje	NGFW Fortigate společně s Aruba/HPE
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	vyhovuje	NGFW Fortigate a FlowMon řešení
Možnost snadné/automatické rekonfigurace ACL/FW na základě identifikovaných útoků	Nevyhovuje	NGFW Fortigate společně s Aruba/HPE
Podpora DNSSEC a IPv6 protokolů pro služby školy dostupné online	vyhovuje	NGFW FortiGate společně s AD s doménou pod serverem
U software a firmware je vyžadována dostupnost aktualizací, zejména bezpečnostního charakteru po celou dobu udržitelnosti projektu.	vyhovuje	ANO NGFW Fortigate a FlowMon řešení jsou garantovány
Nad rámec těchto povinných parametrů je dále doporučeno v rámci projektu realizovat:		
Zapojení poskytovatele připojení v bezpečnostním projektu FENIX resp. veřejné adresy využívané školou jsou zapojeny do infrastruktury FENIX[1] nebo ISP splňuje alespoň technické standardy definované projektem FENIX – viz http://nix.cz/cs/file/NIX_PRAVIDLA_FENIX	Není řešeno	není řešeno v projektu
Symetrické připojení bez agregace a omezení (FUP)	ano splnuje	ano splnuje
Vnitřní konektivita školy (LAN)		
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 uchovávání dat po dobu minimálně 2 měsíců	Není řešeno	NGFW a FlowMon řešení
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.	vyhovuje AD	FREE radius server
Logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas – uživatel	logovaní pouze v rámci záznamů v AD	radius server pod DC+ FlowMon
V oblasti pevné LAN musí projekt splňovat následující minimální parametry:		
Minimální konektivita stanic a dalších koncových zařízení zařízení 100Mbit/s fullduplex	splňuje	ano, zajištěno konektivitou aktvních prvků 1 Gbps
Strukturovaná kabeláž pro připojení pracovních stanic a dalších zařízení (tiskárny, servery, AP,…)	splňuje	ANO, nová SK ve vychovujícím stavu min v cat 6
Minimální konektivita serverů, aktivních síťových prvků, bezpečnostních zařízení, NAS 1Gbit/s fullduplex	splňuje	ano, zajištěno konektivitou aktvních prvků 1 Gbps /10Gbps
Páteřní rozvody mezi budovami v areálu realizovány prostřednictvím optických, metalických vláken popř. bezdrátovými spoji v licencovaném pásmu (povolení ČTÚ)	nevyhovující -páteř realizovaná metalickým propojem	ano nové páteřní propoje v optické trase
Aktivní prvky (centrální směrovače a centrální přepínače; L2 i L3)[1] s neblokující architekturou přepínacího subsystému (wire speed), podpora 802.1Q VLAN, podpora 802.1X, radius based MAC autentizace,…	částečně - 5 přepínačů ano, další 4 ne	ano, zajištěno konektivitou aktvních prvků s plným managementem
V případě řešení bezdrátových sítí (wifi) pak musí projekt naplňovat následující minimální parametry:	řešení na zařízení Unify pokryto pouze kanceláře vedení	pokrytí 100% Aruba
Podpora mechanismu izolace klientů	Není řešeno	podporováno
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	Není řešeno	bude splňovat nejpozději do ukončení realizace projektu
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)	Není řešeno	bude splňovat nejpozději do ukončení realizace projektu
Podpora protokolu IEEE 802.1X resp. ověřování uživatelů oproti databázi účtů přes protokol radius (např. LDAP, MS AD …)	Není řešeno	bude splňovat nejpozději do ukončení realizace projektu
Podpora standardu IEEE 802.11n a případně novějších (ac, ad), současná funkce AP v pásmu 2,4 a 5 GHz	Splňuje	bude splňovat nejpozději do ukončení realizace projektu
Podpora WPA2, PoE, multi SSID, ACL pro filtrování provozu	Splňuje	bude splňovat nejpozději do ukončení realizace projektu
Nad rámec těchto povinných parametrů je dále doporučeno v rámci projektu realizovat:		
Minimálně pasivní zapojení do federovaného systému eduroam (www.eduroam.cz). Optimálně aktivní zapojení do systému eduroam, pro zajištění národní i mezinárodní mobility žáků a učitelů.	nelze připravit na stávajícím řešení	bude možnost se připojit po realizaci projektu
Další bezpečnostní prvky		
Obecný popis: v rámci projektů **je možné** realizovat další aktivity naplňující principy bezpečného využívání IT prostředků. Zejména pak jde o:		
Identity management systémy (IDM) – systém správy identit, řízení životního cyklu uživatelů, integrace do provozních a bezpečnostních systémů	Není řešeno	Splňuje AD (Doména)
Centralizovaný autentizační systém napojení na systém správy identit (např. na bázi LDAP, AD, studijní a personální agendy apod.)	Není řešeno	bude možnost se připojit po realizaci projektu, Cisco
Řešení dočasných přístupů (hosté, brigádníci, praktikanti, zákonní zástupci, externí subjekty, blokace wifi v určitém čase)	Není řešeno	bude možnost se připojit po realizaci projektu
Federované služby autentizace a autorizace (včetně aktivního zapojení do národních vzdělávacích federací a zpřístupnění jejich služeb)	není řešeno	bude možnost se připojit po realizaci projektu
Systémy nebo zařízení pro sledování infrastruktury sítě a sledování IP provozu sítě (umožňující funkce RFC 3954 nebo ekvivalent (NetFlow))	není řešeno	bude možnost se připojit po realizaci projektu ŘEŠENÍ FlowMon
Systémy schopné detekovat nelegitimní provoz nebo síťové anomálie	není řešeno	bude možnost se připojit po realizaci projektu řešení SYSLOG, Radius
Systémy vyhodnocování a správy událostí a bezpečnostních incidentů (log management, incident management)	není řešeno	bude možnost se připojit po realizaci projektu NAGIOS
Systémy pro monitorování funkčnosti síťové a serverové infrastruktury (např. Nagios / Icinga)	není řešeno	povinné pouze pro střední školy
Systémy uživatelské podpory naplňující principy ITIL (HelpDesk, ServiceDesk)	není řešeno	bude možnost se připojit po realizaci projektu
Nástroje pro centrální správu a audit ICT prostředků	není řešeno	bude možnost se připojit po realizaci projektu
Systémy zálohování a obnovy dat serverové infrastruktury	není řešeno	NAS v oddělené lokalitě včetně zálohovacího SW
Systémy pro antivirovou ochranu zařízení, antispamovou ochranu poštovních serverů	Eset pouze antivir, poštovní server O365	řešeno přes FW FortiGate s funkcí NGFW
Zabezpečení přístupových protokolů (SSL/TLS) služeb (např. emailové služby, webové servery, studijní a ekonomické agendy) atp.	řešeno přes Fortigate	řešeno přes FW FortiGate s funkcí NGFW
Podpora vzdáleného přístupu (VPN)	řešeno přes Fortigate	řešeno přes FW FortiGate s funkcí NGFW