Modernizace a ZŠ Přerov, Trávník 27

1. Konektivita školy k veřejnému internetu (WAN) - povinné	Současný stav splněno / nesplněno	Popis opatření ke splnění standardu IROP
šíře pásma (bandwidth) odpovídající 128kbps/student[1] nebo 512kbps/počítač[2] nebo taková šířka pásma, která neomezuje provoz zařízení a uživatelů[3]	Podle smlouvy o konektivitě do internetu vybrat výpočet, který požadavek splňuje, případně navýšit rychlost připojení	
vlastní nebo poskytovatelem přidělené veřejné IPv4 i IPv6 adresy	Přidělené poskytovatelem	
plná podpora připojení do veřejného internetu přes protokol IPv4 i IPv6 (dual-stack)	NE (částečně ANO – pouze na rozhraní FW)	konfigurace LAN
validující DNSSEC resolver na straně školy	NE	Konfigurace DNS na Windows serveru
podpora monitoringu a logování NAT (RFC 2663) provozu za účelem dohledatelnosti veřejného provozu k vnitřnímu zařízení	ANO	
logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas – uživatel a to včetně ošetření v případě sdílených učeben (pracovních stanic apod.)	NE (částečně ANO - chybí vazba IP adresa uživatel)	Instalace a konfigurace technologie správy
síťové zařízení podporující rate limiting, antispoofing, ACL/xACL, rozhraní musí obsahovat všechny potřebné komponenty a licence pro zajištění řádné funkcionality	ANO	

[1] *Počet studentů je definovaný celkový počet studentů školy*

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

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

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	Částečně ANO	HW požadavky splňuje, nutná konfigurace technologie správy
možnost snadné/automatické rekonfigurace ACL/FW na základě identifikovaných útoků	ANO	
podpora DNSSEC a IPv6 protokolů pro služby školy dostupné online	NE	Doména zstravnik.cz nemá zapnuto DNSSEC – musí se nastavit u registrátora domény, Bakaláři – pouze na IPv4 – konfigurace LAN pro IPv6 a registrace IPv6 u DNS bakalari.cz
u software a firmware je vyžadována dostupnost aktualizací, zejména bezpečnostního charakteru po celou dobu udržitelnosti projektu.	ANO (STÁVAJÍCÍ PRVKY)	
Nad rámec těchto povinných parametrů je dále doporučeno v rámci projektu realizovat:		projekt nezahrnuje tyto parametry
symetrické připojení bez agregace a omezení (FUP)	-	Neřeší se
zapojení poskytovatele připojení v bezpečnostním projektu FENIX resp. veřejné adresy využívané školou jsou zapojeny do infrastruktury FENIX[4] nebo ISP splňuje alespoň technické standardy definované projektem FENIX – viz http://nix.cz/cs/file/NIX_PRAVIDLA_FENIX	NE	Neřeší se

[4] *V případě, kdy má ISP přidělené IP adresy od člena FENIX, musí být součástí projektu prohlášení ISP, ze kterého bude patrné, že příslušné adresy jsou v rámci FENIX propagovány. V případě, kdy má ISP vlastní ASn a není přímý člen FENIX, musí být součástí projektu prohlášení ISP, ze kterého bude patrné, že příslušné ASn propaguje do FENIX na základě smluvního vztahu některý ze členů FENIX.*

2. Vnitřní konektivita školy (LAN) - povinné	Současný stav Splněno/nesplněno	Popis opatření ke splnění standardu IROP
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	ANO/NE	Instalace a konfigurace technologie správy
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.	NE (Částečně ANO - uživatelé AD, ale bez přihlášení je přístup do internetu také funkční)	Instalace a konfigurace technologie správy
logování přístupu uživatelů do sítě umožňující dohledání vazeb *IP adresa – čas – uživatel*	NE (částečně ANO bez vazby na uživatele)	Instalace a konfigurace technologie správy
Minimální konektivita stanic a dalších koncových zařízení zařízení 100Mbit/s fullduplex	ANO	
Strukturovaná kabeláž pro připojení pracovních stanic a dalších zařízení (tiskárny, servery, AP,…)	ANO	
Minimální konektivita serverů, aktivních síťových prvků, bezpečnostních zařízení, NAS 1Gbit/s fullduplex	ANO / NE pro NAS	Dodávka HW, konfigurace zálohování
Páteřní rozvody mezi budovami v areálu realizovány prostřednictvím optických, metalických vláken popř. bezdrátovými spoji v licencovaném pásmu (povolení ČTÚ)	ANO	

Aktivní prvky (centrální směrovače a centrální přepínače; L2 i L3)[5] s neblokující architekturou přepínacího subsystému (wire speed), podpora 802.1Q VLAN, podpora 802.1X, radius based MAC autentizace,…	ANO (STÁVAJÍCÍ PRVKY ARUBA)	
V případě řešení bezdrátových sítí (wifi) pak musí projekt naplňovat následující minimální parametry:		
Podpora mechanismu izolace klientů	ANO	
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	ANO	
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)	ANO	
Podpora protokolu IEEE 802.1X resp. ověřování uživatelů oproti databázi účtů přes protokol radius (např. LDAP, MS AD …)	ANO (nenakonfigurováno)	Konfigurace technologie správy
Podpora standardu IEEE 802.11n a případně novějších (ac, ad), současná funkce AP v pásmu 2,4 a 5 GHz	ANO	
Podpora WPA2, PoE, multi SSID, ACL pro filtrování provozu	ANO (nenakonfigurováno)	Konfigurace technologie správy

[5] *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*

3. -Další bezpečnostní prvky – doporučené, nepovinné	Současný stav Splněno/nesplněno	Popis opatření ke splnění standardu IROP
Identity management systémy (IDM) – systém správy identit, řízení životního cyklu uživatelů, integrace do provozních a bezpečnostních systémů	NE	Neřeší se
Centralizovaný autentizační systém napojení na systém správy identit (např. na bázi LDAP, AD, studijní a personální agendy apod.)	Jen AD	Neřeší se
Řešení dočasných přístupů (hosté, brigádníci, praktikanti, zákonní zástupci, externí subjekty, blokace wifi v určitém čase)	NE	Neřeší se
Federované služby autentizace a autorizace (včetně aktivního zapojení do národních vzdělávacích federací a zpřístupnění jejich služeb)	NE	Neřeší se
Systémy nebo zařízení pro sledování infrastruktury sítě a sledování IP provozu sítě (umožňující funkce RFC 3954 nebo ekvivalent (NetFlow))	NE	Neřeší se
Systémy schopné detekovat nelegitimní provoz nebo síťové anomálie	NE	Neřeší se
Systémy vyhodnocování a správy událostí a bezpečnostních incidentů (log management, incident management)	NE	Neřeší se
Systémy pro monitorování funkčnosti síťové a serverové infrastruktury (např. Nagios/Icinga)	NE	Neřeší se
Systémy uživatelské podpory naplňující principy ITIL (HelpDesk, ServiceDesk)	Nezjištěno	Neřeší se
Nástroje pro centrální správu a audit ICT prostředků	Nezjištěno	Neřeší se
Systémy zálohování a obnovy dat serverové infrastruktury	Nezjištěno	Neřeší se
Systémy pro antivirovou ochranu zařízení, antispamovou ochranu poštovních serverů	Nezjištěno	Neřeší se
Zabezpečení přístupových protokolů (SSL/TLS) služeb (např. emailové služby, webové servery, studijní a ekonomické agendy) atp.	ANO	Neřeší se
Podpora vzdáleného přístupu (VPN)	ANO	Neřeší se