PŘÍLOHA č. 4

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

Č.j.: MSMT-16039/2022-2

STANDARD KONEKTIVITY ŠKOL

Ministerstvo školství, mládeže a tělovýchovy

červenec 2022

Úvod

Tento dokument definuje základní technická kritéria cílového stavu školní síťové infrastruktury a přijatelnosti aktivit projektů naplňující požadavky na školy v 21. století mj. i strategický cíl IROP 4.1 v oblasti zajištění vnitřní konektivity škol a připojení k internetu - rozvoj vnitřní konektivity v prostorách škol a školských zařízení a připojení k internetu[1].

Další podmínky a pravidla výzev IROP jsou uvedeny ve Specifických pravidel výzev IROP.

Níže uvedené parametry konektivity jsou relevantní pro základní školy, střední školy, vyšší odborné školy a konzervatoře, u kterých Integrovaný regionální operační program 2021–2027 stanovuje ve specifickém cíle 4.1. intervenci v oblasti budování vnitřní konektivity škol.

Metodická podpora ke Standardu konektivity škol je k dispozici na https://edu.cz/digitalizujeme.

[1] *Viz Programový dokument IROP 2021-2027 (*https://irop.mmr.cz/cs/irop-2021-2027/dokumenty*)*

1. Konektivita školy k veřejnému internetu (WAN)

1.1. 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 parametry v době ukončení realizace a v průběhu udržitelnosti projektu.

1.2. Povinné parametry projektu:

1.2.1. Šíře pásma (bandwidth) odpovídající 0,25 Mbps/žák či student[2] nebo 0,5 Mbps/koncové uživatelské zařízení[3][4] a zároveň taková šířka pásma, která neomezuje provoz zařízení a uživatelů[5]. Šíře pásma se vztahuje na počet žáků/studentů/koncových uživatelských zařízení v budově/areálu, kde se projekt realizuje.

1.2.2. Vlastní nebo poskytovatelem přidělené veřejné IPv4 adresy.

1.2.3. Zajištění monitoringu a logování NAT (RFC 2663) provozu za účelem dohledatelnosti veřejného provozu k vnitřnímu koncovému zařízení v minimální délce 3 měsíců.

1.2.4. Síťové zařízení podporující rate limiting, antispoofing, access listy - zařízení musí obsahovat všechny potřebné komponenty a licence pro zajištění řádné funkcionality.

1.2.5. Schopnost snadné/automatické rekonfigurace pravidel firewallu (access listů) na základě identifikovaných útoků.

1.2.6. Zajištění šifrovaného přístupu (SSL/TLS) a podepsání DNSSEC domén pro služby školy dostupné online (např. emailové služby, webové servery, studijní a ekonomické agendy atp.).

1.2.7. Validující DNSSEC resolver na straně školy, nebo poskytovatele konektivity, nebo otevřeným DNSSEC validujícím resolverem;

1.2.8. Software a firmware je aktualizován po dobu udržitelnosti projektu, jsou-li aktualizace k dispozici.

1.2.9. Poskytovatel konektivity je schopen zajistit kontaktní bod pro komunikaci, trvalý monitoring dostupnosti konektivity, realizovat blokování nežádoucí komunikace zahlcující nebo jinak omezující konektivitu a systémy školy na straně poskytovatele na základě požadavku školy.

1.3. Doporučené parametry projektu:

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

1.3.1. Symetrické připojení (zajištění konektivity) bez agregace a omezení, doporučujeme postupně směřovat ke kapacitě konektivity 1Gbps.

---

[2] Počet žáků/studentů je definovaný celkovým počtem žáků/studentů školy.

[3] Koncové uživatelské zařízení je počítačový systém, který je aktivně využíván uživatelem (např. žákem, studentem nebo zaměstnancem školy) ke vzdělávacím či pracovním účelům (typicky počítač, notebook, tablet apod.).

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

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

1.3.2. Plná podpora připojení do veřejného internetu přes protokol IPv4 i IPv6, včetně zajištění dostupnosti online služeb školy na IPv6 adresách.

1.3.3. Poskytovatel konektivity je schopen zajistit funkci systému incident response, monitoring a aktivní notifikaci anomálií síťového provozu, zamezení podvržení zdrojových IP adres (anti-spoofing), funkci pro blokování nežádoucí komunikace zahlcující nebo jinak omezující konektivitu a systémy školy pro zamezení zahlcení linky (např. RTBH, FlowSpec, služby AntiDDoS řešení), detekci a zamezení amplifikačních útoků, zabezpečení směrování síťového provozu pomocí RPKI a konfigurace odmítnutí nevalidních prefixů.

1.3.4. Antivirová kontrola internetového provozu.

2. Vnitřní konektivita školy (LAN a WLAN)

2.1. Obecný popis

Vnitřní síťové prostředí školy pořizované v rámci projektu může být řešeno pevnou sítí, bezdrátovou sítí, nebo kombinací těchto síťových technologií. Připojení je nutné zajistit v prostorách dotčených hlavním projektem, rovněž je možné pokrýt ostatní prostory školy, včetně chodeb, jídelen, internátu a dalších školských zařízení. Potřebnost a účelnost takového pokrytí musí být odůvodněna ve studii proveditelnosti.

2.2. Povinné parametry projektu (bez ohledu typ síťového připojení):

2.2.1. Systém 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. službám. Využívání jednoho účtu více uživateli není povoleno (využívání tzv. anonymních účtů).

2.2.2. Logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas-počítačový systém[6].

2.2.3. Systémy zálohování a obnovy dat serverové infrastruktury.

2.2.4. Systémy pro antivirovou ochranu počítačových systémů, antispamovou ochranu poštovních serverů.

2.3. Povinné parametry projektu v oblasti pevné LAN:

2.3.1. Minimální konektivita koncových uživatelských zařízení 1000 Mbps fullduplex.

2.3.2. Minimální konektivita serverů, aktivních síťových prvků, bezpečnostních zařízení (např. IPS, IDS, Next Generation Firewall aj.), datových úložišť (NAS) 1000 Mbps fullduplex.

2.3.3. Síťové prvky musí splňovat následující funkcionality: centrální směrovače a centrální přepínače (L2 i L3)[7] s neblokující architekturou přepínacího subsystému (wire speed), management, podpora 802.1Q VLAN (možnost

---

[6] *Počítačový systém je každý prvek informačních a komunikačních technologií využívající pro svoji činnost jak hardware, tak software. Pro účely standardů jsou rozlišována: 1. koncová uživatelská zařízení (např. osobní počítače, notebooky, tablety, mobily aj.) a 2. servery, síťové prvky, datová úložiště apod.*

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

tvorby virtuálních sítí - VLAN), základní bezpečnostní prvky proti zneužití přístupu k síti [např. MAC based omezení (port-sec), 802.1X autentizace aj.].

2.3.4. Strukturovaná kabeláž pro připojení počítačových systémů a dalších zařízení (tiskárny, servery, AP aj.).

2.3.5. Páteřní rozvody mezi budovami v areálu, kde probíhá výuka nebo příprava na ni, realizovány prostřednictvím optických vláken nebo metalických kabelů. Vztahuje se na budovu/areál, kde se projekt realizuje.

2.4. **Minimální parametry projektu v případě řešení bezdrátových sítí (WLAN):**

2.4.1. Návrh topologie Wi-Fi sítě a analýza pokrytí signálem počítající s konzistentní Wi-Fi službou v příslušných prostorách školy a s kapacitami pro provoz mobilních zařízení pedagogického sboru i studentů.

2.4.2. Zabezpečení minimálně AES šifrováním a standardem WPA2-Enterprise nebo WPA3-Enterprise, multi SSID, ACL pro filtrování provozu.

2.4.3. Zajištění vzájemně oddělených sítí pro zaměstnance školy, žáky/studenty školy a externí zařízení (hosty).

2.4.4. Podpora mechanismu izolace uživatelů.

2.4.5. Podpora standardu IEEE 802.11ac (Wi-Fi 5) a případně novějších (Wi-Fi 6), současná funkce AP v pásmu 2,4 a 5 GHz a novějších protokolů a pásem.

2.5. **Doporučené parametry projektu (bez ohledu typ síťového připojení):**

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

2.5.1. Logování provozu za účelem dohledatelnosti na úroveň koncového uživatele.

2.5.2. Řešení dočasných přístupů (hosté, brigádníci, praktikanti, zákonní zástupci, externí subjekty) a systému blokace Wi-Fi v určitém čase.

2.5.3. Federované služby autentizace a autorizace (včetně aktivního zapojení do národních vzdělávacích federací (např. aktvní zapojení do federovaného systému www.eduroam.cz).

2.5.4. Centralizovaná architektura správy Wi-Fi 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).

2.5.5. Doporučená podpora pro ověřování uživatelů oproti databázi účtů [např. pomocí protokolu IEEE 802.1X vůči centrální evidenci uživatelů (např. LDAP, MS AD) nebo pomocí Captive portalu].

2.5.6. Propojení aktivních prvků a důležitých systémů (např. Servery, NAS, propojení budov) rychlostí 10 Gbps, včetně uplinku.

3. Další doporučené bezpečnostní prvky projektu

Nad rámec povinných parametrů uvedených v bodech 1 a 2 je dále doporučeno v projektu realizovat:

3.1.1. Systémy nebo zařízení pro sledování infrastruktury sítě a sledování IP provozu sítě (umožňující funkce RFC 3917 - IPFIX nebo ekvivalent).

3.1.2. Systémy schopné detekovat nelegitimní provoz nebo síťové anomálie.
3.1.3. Systémy vyhodnocování a správy událostí a bezpečnostních incidentů (log management, incident management).
3.1.4. Systémy pro monitorování funkčnosti síťové a serverové infrastruktury.
3.1.5. Zařízení umožňující kontrolu http a https provozu, kategorizaci a selekci obsahu dostupného pro vybrané skupiny uživatel (učitel, žák), blokování nežádoucích kategorií obsahu.
3.1.6. Systémy uživatelské podpory naplňující principy ITIL (HelpDesk, ServiceDesk aj.).
3.1.7. Nástroje pro centrální správu a audit ICT prostředků.
3.1.8. Podpora vzdáleného přístupu (VPN).
3.1.9. Zavedení více-faktorové autentizace.