PROKÁZÁNÍ A KONTROLA NAPLNĚNÍ STANDARDU KONEKTIVITY ŠKOL

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

Praha, březen 2024

Č.j. MSMT-27467/2023-1

Úvod

Ministerstvo školství, mládeže a tělovýchovy (dále jen „MŠMT“) publikovalo Standard konektivity škol (dále také „Standard“), který je dostupný na webových stránkách https://edu.cz/digitalizujeme. Standard definoval 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].

Dokument *Prokázání a kontrola naplnění Standardu konektivity škol* je jednou ze tří metodických pomůcek pro školy, které mají za cíl pomoci jim se orientovat v problematice digitální infrastruktury školy. Jedná se o dokument pro všechny školy/příjemce, které mají prokázat naplnění parametrů uvedených ve Standardu. Je spíše technického rázu a slouží pro administrativní účely, proto je určen pro manažery projektů nebo správce/administrátory IT. U každého z parametrů Standardu je uvedeno, jakým způsobem by měl příjemce prokázat jeho naplnění. U parametrů, u kterých je to smysluplné, je uveden i způsob případného ověření na místě.

Nezapomeňte se na své cestě k digitalizaci školy podívat i na dva další metodické materiály a další zdroje z edu.cz/digitalizujeme:

- **Průvodce ke Standardu konektivity škol** blíže vysvětluje problematiku digitální infrastruktury školy, proč je potřeba ji kvalitně a funkčně zajistit a jak to udělat. Dokument je určen pro ředitele, ICT koordinátory, správce IT i zřizovatele. Dostupné na: https://www.edu.cz/digitalizujeme/standard-konektivity-skol#pruvodce
- **Bezpečná digitální infrastruktura školy** představuje základní principy, postupy a doporučení v oblasti kybernetické bezpečnosti pro školy. Dokument je určen především IT správcům či administrátorům. Dostupné na: https://www.edu.cz/digitalizujeme/bezpecna-skolni-ict-infrastruktura/
- **Bezpečná školní ICT infrastruktura** – edukační videa – dostupná na https://www.edu.cz/digitalizujeme/bezpecna-skolni-ict-infrastruktura/
- **IT správa** – Příručka ke správě ICT ve škole a příklady dobré praxe (rozhovory i videa) – dostupné na https://www.edu.cz/digitalizujeme/it-sprava/.

Nevíte, jak si Vaše škola stojí na poli digitální infrastruktury? Zda je dostatečná, funkční a bezpečná? Obraťte se na specializované IT guru, kteří Vám rádi pomohou a zdarma prověří stav digitální infrastruktury vaší školy. Více informací naleznete na https://www.edu.cz/digitalizujeme/it-guru/.

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

Další informace o metodické podpoře naleznete na https://www.edu.cz/digitalizujeme/metodicka-podpora/.

V případě dotazů nás kontaktujte na digitalizujeme@msmt.cz.

Věříme, že Vám tento dokument a další metodická podpora poskytnutá MŠMT a Národním pedagogickým institutem ČR na cestě digitalizace Vaší školy pomůže a bude pro Vás inspirativní.

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.

Příklad: Určuje podle počtu žáků nebo podle počtu koncových zařízení. Např. pokud má škola 100 žáků a 40 koncových uživatelských zařízení, šířka pásma musí být buď 25 Mb/s (dle počtu žáků) nebo 20 Mb/s dle počtu koncových zařízení. V obou případech však platí, že šířka pásma neomezuje provoz zařízení a uživatelů.

Prokázání:

- Příjemce si ověří šíři pásma například nástrojem na webu www.standardkonektivity.cz[6] a doloží export výsledku **nebo**
- příjemce doloží smlouvu s poskytovatelem konektivity, která musí být nastavena tak, aby poskytovaná šíře pásma neomezovala běžný školní provoz, příjemce doloží smlouvu **nebo**
- příjemce slovně popíše a vypočítá, že v rámci jeho parametrů (počet studentů/žáků, počet počítačů, počet zařízení přistupujících k internetu) dané připojení nijak neomezuje provoz zařízení a uživatelů.

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 %.
6 Další weby, na kterých lze šíři pásma ověřit, jsou: https://speedtest.cesnet.cz/ či https://netmetr.cz.

1.2.2. Vlastní nebo poskytovatelem přidělené veřejné IPv4 adresy.

Prokázání:

- Příjemce ověří nástrojem na webu www.standardkonektivity.cz[7] a doloží export výsledku **a zároveň**
- příjemce doloží smlouvu s poskytovatelem konektivity.

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.

Prokázání:

- Příjemce doloží nastavení logování požadovaných záznamů ze zařízení **a zároveň** popíše, jaký mechanismus logování používá (jak loguje a jak dlouho ukládá záznamy).

Ověření na místě:

- V případě prověření na místě bude přivolán technik a kontrolor ověří, že příjemce ukládá logy po deklarovanou dobu (namátkový záznam logu).

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

Prokázání:

- Příjemce slovně popíše potřebné komponenty a licence pro zajištění řádné funkcionality **a zároveň**
- příjemce doloží smlouvu, ze které bude patrná podpora rate limitingu, antispoofingu, access listy, **nebo**
- datasheet (produktový list) zařízení, ze kterého bude splnění parametru patrné.

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

Prokázání

- Příjemce slovně popíše potřebné komponenty a licence pro zajištění řádné funkcionality **a zároveň**
- příjemce doloží smlouvu s dodavatelem, ze které bude patrná podpora požadované funkce **nebo**
- datasheet (produktový list) zařízení, ze kterého bude splnění parametru patrné.

7 Případně na https://www.dnssec.cz/

Příklad slovního popisu:

- V případě útoku, který detekuje firewall, router reaguje. Zdrojová IP adresa útočníka je vložena do Access listu útočníků. Ve firewallu je připraveno pravidlo, které všechny pokusy o přístup z adres útočníků blokuje.

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.).

Prokázání:

- Příjemce doloží nastavení domén ze svých systémů, ze které bude patrná podpora šifrovaného přístupu (SSL/TLS) a podepsání DNSSEC domén **nebo**
- příjemce doloží smlouvu s poskytovatelem domén, ze které bude patrná podpora šifrovaného přístupu (SSL/TLS) a podepsání DNSSEC domén **nebo**
- příjemce doloží export z online validátorů https://dnssec-analyzer.verisignlabs.com nebo https://www.dnssec.cz/ (v případě české domény).

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

Prokázání:

- Příjemce ověří nástrojem na webu www.standardkonektivity.cz[8] a doloží export výsledku **nebo**
- příjemce doloží smlouvu s poskytovatelem konektivity, ze které splnění parametru vyplývá.

Ověření na místě:

- Kontrolor se připojí zařízením do sítě a připojí se na stránky www.standardkonektivity.cz.

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

Prokázání:

- Příjemce popíše systém aktualizace koncových počítačových systémů a softwaru. Uvede, zda jsou aktualizace k dispozici. Pokud aktualizace nejsou k dispozici, uvede, kterého softwaru a firmwaru se to týká.

Ověření na místě:

- Kontrolor na místě ověří verzi softwaru vůči vydaným aktualizacím u výrobce.

8 Případně na stránce https://www.dnssec.cz/

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.

Prokázání

- Příjemce doloží smlouvu s poskytovatelem konektivity dokládající naplnění parametru **nebo**
- příjemce doloží prohlášení poskytovatele konektivity dokládající naplnění parametru.

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.

Prokázání:

- Příjemce splnění parametru ověří například nástrojem na webu www.standardkonektivity.cz[9] a doloží export výsledku.

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

Prokázání:

- Příjemce ověří nástrojem na webu www.standardkonektivity.cz[10] a doloží export výsledku **a zároveň**
- příjemce doloží smlouvu s poskytovatelem konektivity dokládající naplnění parametru společně s doprovodným XML otiskem databáze RIPE.

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.

9 Další weby, na kterých lze šíři pásma ověřit, jsou: https://speedtest.cesnet.cz/ či https://netmetr.cz.
10 Případně i https://www.dnssec.cz/

Prokázání:

- Příjemce doloží smlouvu s poskytovatelem konektivity dokládající naplnění parametru **nebo**
- příjemce doloží prohlášení poskytovatele konektivity dokládající naplnění parametru.

1.3.4. Antivirová kontrola internetového provozu.

Prokázání:

- Příjemce doloží fakturu, licenci nebo datasheet (produktový list) zařízení zabezpečující antivirovou kontrolu internetového provozu a důkaz (např. printscreen) o aktivaci této funkcionality **nebo**
- příjemce doloží prohlášení poskytovatele konektivity dokládající naplnění parametru.

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 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 TYPU 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).

Prokázání:

- Příjemce popíše, jak je tento parametr naplněn (zejména to, že je dosaženo bezpečného a auditovatelného přístupu k síti, resp. službám, a to, jakým způsobem je ošetřeno zamezení využívání tzv. anonymních účtů) **nebo**
- příjemce doloží vnitřní předpis (např. směrnici) zajišťující naplnění parametru.

2.2.2. Logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas- počítačový systém[11].

Prokázání:

- Příjemce doloží nastavení logování požadovaných záznamů ze zařízení a popíše, jaký mechanismus logování používá (jak loguje a jak dlouho ukládá záznamy) **a zároveň**
- příjemce doloží vnitřní předpis (např. směrnici) zajišťující naplnění parametru.

Ověření na místě:

- Kontrolor na místě ověří způsob logování do počítačového systému.
- Kontrolor na místě ověří, že příjemce ukládá logy po deklarovanou dobu (namátkový záznam logu).

11 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.

2.2.3. Systémy zálohování a obnovy dat serverové infrastruktury.

Prokázání:

- Příjemce popíše, jak je tento parametr naplněn (zejména popíše technologie a procesy pro zálohování a obnovu dat) **nebo**
- příjemce doloží vnitřní předpis (např. směrnici) zajišťující naplnění parametru.

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

Prokázání:

- Příjemce doloží fakturu nebo čestné prohlášení dodavatele prokazující nákup služby pro antivirovou ochranu počítačových systémů a antispamovou ochranu poštovních serverů **a zároveň**
- příjemce popíše, jak je tento parametr naplněn (zejména popíše, zda je v organizaci nasazena centrální správa antivirového programu, pokud ano, jaká data ukazuje, dále, jak často je antivirová ochrana aktualizována, jaké hrozby byly detekovány, jaká je platnost licence apod.) **nebo**
- příjemce doloží vnitřní předpis (např. směrnici) zajišťující naplnění parametru**.**

2.3. POVINNÉ PARAMETRY PROJEKTU V OBLASTI PEVNÉ LAN:

2.3.1. Minimální konektivita koncových uživatelských zařízení 1000 Mbps fullduplex.

Prokázání

- Příjemce doloží datasheety (produktové listy) prokazující naplnění parametru **a zároveň** příjemce doloží smlouvy s poskytovatelem/i prokazující naplnění parametru**.**

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

Prokázání

- Příjemce doloží datasheety (produktové listy) prokazující naplnění parametru **a zároveň**
- příjemce doloží smlouvy s poskytovatelem/i prokazující naplnění parametru**.**

2.3.3. Síťové prvky musí splňovat následující funkcionality: centrální směrovače a centrální přepínače (L2 i L3)[12] s neblokující architekturou přepínacího subsystému (wire speed), management, podpora 802.1Q VLAN (možnost tvorby virtuálních sítí – VLAN), základní bezpečnostní prvky proti zneužití přístupu k síti [např. MAC based omezení (port-sec), 802.1X autentizace aj.].

Prokázání

- Příjemce doloží datasheety (produktové listy) prokazující naplnění parametru **a zároveň**
- příjemce popíše, jak je tento parametr naplněn (zejména technické parametry používaného hardwaru, zejm. zda podporuje všechny požadované funkcionality, jaká je konfigurace jednotlivých síťových prvků, jak jsou síťové prvky v praxi využívány, příp. ukázka konfigurace na vybraném síťovém zařízení) **nebo**
- příjemce doloží smlouvy s poskytovatelem/i prokazující naplnění parametru**.**

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

Prokázání

- Příjemce doloží datasheety (produktové listy) prokazující naplnění parametru **a zároveň**
- příjemce popíše, jak je tento parametr naplněn (zejména popíše, jakým způsobem je kabeláž strukturována, jaká kategorie strukturované kabeláže byla použita, případně přiloží projekt) **nebo**
- příjemce doloží smlouvy/faktury od dovatele/ů, ze kterých bude zřejmé, jaká kategorie strukturované kabeláže byla použita, případně přiloží projekt**.**

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.

Prokázání

- Příjemce popíše, jak je tento parametr naplněn (zejména popíše, jakým způsobem je kabeláž strukturována, jaká kategorie strukturované kabeláže byla použita, včetně typu optického vlákna/metalického kabelu, případně přiloží projekt) **nebo**
- příjemce doloží smlouvy/faktury od dodavatele/ů, ze kterých bude zřejmé, jaká kategorie strukturované kabeláže byla použita a jaký typ optického vlákna/metalického kabelu byl použit, případně přiloží projekt.

12 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.

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.

Prokázání

- Příjemce doloží smlouvy či jinou dokumentaci prokazující naplnění parametru (návrh topologie, projekt, dokumentace o měření apod. od dodavatele).

Ověření na místě:

- Příjemce ukáže fyzické rozmístění jednotlivých access pointů.

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

Prokázání

- Příjemce doloží datasheety (produktové listy) prokazující naplnění parametru **a zároveň**
- příjemce popíše, jak je tento parametr naplněn (zejména popíše konfiguraci centrálního managementu Wi-Fi sítí (security profile) a zda jsou aplikovány požadované parametry) **nebo**
- příjemce doloží smlouvy s poskytovatelem/i prokazující naplnění parametru**.**

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

Prokázání

- Příjemce doloží vnitřní předpis (např. směrnici) zajišťující naplnění parametru **a zároveň**
- příjemce popíše, jak je tento parametr naplněn (zejména počet oddělených sítí pro konkrétní skupiny, jakým způsobem je zajištěno jejich oddělení, zda podporují VLAN, jaká je konfigurace síťových prvků apod.) **nebo**
- příjemce doloží smlouvy s poskytovatelem/i prokazující naplnění tohoto parametru **nebo**
- příjemce doloží datasheety (produktové listy) prokazující naplnění parametru.

Ověření na místě

- Kontrolor se na místě pokusí připojit k síti Wi-Fi příjemce jako host.

2.4.4. Podpora mechanismu izolace uživatelů.

Prokázání

- Příjemce popíše, jak je tento parametr naplněn (zejména popíše postup v případě zjištění incidentu v síti způsobeného konkrétním uživatelem a blokaci daného uživatele, zanesení na black list) **nebo**
- příjemce doloží smlouvy s poskytovatelem/i prokazující naplnění parametru **nebo**
- příjemce doloží datasheety (produktové listy) prokazující naplnění parametru.

Ověření na místě

- Příjemce namátkou provede izolaci uživatele, jeho zanesení na black list a následné odebrání uživatele z black listu.

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.

Prokázání

- Příjemce doloží smlouvy s poskytovatelem/i prokazující naplnění parametru **nebo**
- příjemce doloží datasheety (produktové listy) prokazující naplnění parametru.

2.5. DOPORUČENÉ PARAMETRY PROJEKTU (BEZ OHLEDU TYPU 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.

Prokázání:

- Příjemce doloží nastavení logování požadovaných záznamů ze zařízení a popíše, jaký mechanismus logování používá (jak loguje a jak dlouho ukládá záznamy).

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

Prokázání

- Příjemce doloží vnitřní předpis (např. směrnici) zajišťující naplnění parametru **a zároveň**
- příjemce popíše, jak je tento parametr naplněn (zejména popíše, jak jsou dočasné přístupy poskytovány, jak dochází k jejich odebrání, jak je nastaven systém blokace Wi-Fi apod.) **nebo**
- příjemce doloží smlouvy s poskytovatelem/i prokazující naplnění parametru **nebo**
- příjemce doloží datasheety (produktový list) prokazující naplnění parametru.

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

Prokázání:

- Příjemce doloží potvrzení od CESNET pomocí exportu výsledků z webu https://pripojovani.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).

Prokázání

- Příjemce doloží smlouvy či jinou dokumentaci prokazující naplnění parametru (projektová dokumentace, konfigurace centrálního managementu).

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].

Prokázání

- Příjemce popíše, jak je tento parametr naplněn (zejména popíše způsob ověřování uživatelů, jaké protokoly a centrální evidenci uživatelů využívá, jak jsou nastaveny parametry v centrálním managementu Wi-Fi apod) **nebo**
- příjemce doloží smlouvy s poskytovatelem/i prokazující naplnění parametru **nebo**
- příjemce doloží datasheety (produktový list) prokazující naplnění parametru.

Ověření na místě:

- Kontrolor se pokusí připojit k Wi-Fi síti příjemce (dojde k ověření certifikátu nebo jména a hesla)

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

Prokázání

- Příjemce doloží datasheety (produktový list) prokazující naplnění parametru.

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).

Prokázání

- Příjemce popíše, jak je tento parametr naplněn (zejména popíše, jaké systémy nebo zařízení jsou využívány), **nebo**
- příjemce doloží smlouvy s poskytovatelem/i prokazující naplnění parametru **nebo**
- příjemce doloží datasheety (produktové listy) prokazující naplnění parametru.

3.1.2. Systémy schopné detekovat nelegitimní provoz nebo síťové anomálie.

Prokázání

- Příjemce popíše, jak je tento parametr naplněn (zejména popíše, jaké systémy jsou využívány), **nebo**
- příjemce doloží smlouvy s poskytovatelem/i prokazující naplnění parametru **nebo**
- příjemce doloží datasheety (produktové listy) prokazující naplnění parametru.

3.1.3. Systémy vyhodnocování a správy událostí a bezpečnostních incidentů (log management, incident management).

Prokázání

- Příjemce popíše, jak je tento parametr naplněn (zejména popíše, jaké systémy jsou využívány), **nebo**
- příjemce doloží smlouvy s poskytovatelem/i prokazující naplnění parametru **nebo**
- příjemce doloží datasheety (produktové listy) prokazující naplnění parametru.

3.1.4. Systémy pro monitorování funkčnosti síťové a serverové infrastruktury.

Prokázání

- Příjemce popíše, jak je tento parametr naplněn (zejména popíše, jaké systémy jsou využívány) **nebo**
- příjemce doloží smlouvy s poskytovatelem/i prokazující naplnění parametru **nebo**
- příjemce doloží datasheety (produktové listy) prokazující naplnění parametru.

3.1.5. Zařízení umožňující kontrolu http a https provozu, kategorizaci a selekci obsahu dostupného pro vybrané skupiny uživatelů (učitel, žák), blokování nežádoucích kategorií obsahu.

Prokázání

- Příjemce popíše, jak je tento parametr naplněn (zejména popíše, jaká zařízení jsou využívána) **nebo**
- příjemce doloží smlouvy s poskytovatelem/i prokazující naplnění parametru **nebo**
- příjemce doloží datasheety (produktové listy) prokazující naplnění parametru.

3.1.6. Systémy uživatelské podpory naplňující principy ITIL (HelpDesk, ServiceDesk aj.).

Prokázání

- Příjemce doloží smlouvy s poskytovatelem/i prokazující naplnění parametru **nebo**
- příjemce doloží prohlášení poskytovatele prokazující naplnění parametru.

3.1.7. Nástroje pro centrální správu a audit ICT prostředků.

Prokázání

- Příjemce popíše, jak je tento parametr naplněn (zejména jaké nástroje pro centrální správu a audit ICT prostředků jsou využívány) **nebo**
- příjemce doloží smlouvy s poskytovatelem/i prokazující naplnění parametru **nebo**
- příjemce doloží datasheety (produktové listy) prokazující naplnění parametru.

3.1.8. Podpora vzdáleného přístupu (VPN).

Prokázání

- Příjemce popíše, jak je tento parametr naplněn a **zároveň**
- příjemce doloží smlouvy **nebo**
- příjemce doloží datasheety (produktové listy) prokazující naplnění parametru.

3.1.9. Zavedení více-faktorové autentizace.

Prokázání

- Příjemce popíše, jak je tento parametr naplněn **nebo**
- příjemce doloží smlouvy, faktury nebo licence prokazující splnění parametru **nebo**
- příjemce doloží datasheety prokazující naplnění parametru (záznam nastavení zařízení, výpis z operačního logu řešení).

Ověření na místě:

- Kontrolor se pokusí připojit k systémům vyžadující více-faktorovou autentizaci