# Plnění Standardu konektivity a návrh opatření – ISŠTE Sokolov

| Požadavek | Způsob naplnění |
|---|---|
| **Konektivita školy k veřejnému internetu (WAN) - povinné parametry** | |
| Šíře pásma (bandwidth) odpovídající 0,25 Mbps/žák či student nebo 0,5 Mbps/koncové uživatelské zařízení a zároveň taková šířka pásma, která neomezuje provoz zařízení a uživatelů. Šíře pásma se vztahuje na počet žáků/studentů/koncových uživatelských zařízení v budově/areálu, kde se projekt realizuje | Tento parametr škola v současné době **splňuje**, v rámci projektu bude zachováno stávající připojení dvěma internetovými přípojkami. |
| Vlastní nebo poskytovatelem přidělené veřejné IPv4 adresy. | Tento parametr škola v současné době **splňuje**, v rámci projektu budou stávající veřejné IPv4 adresy převedeny na nový firewall |
| Zajištění monitoringu a logování NAT (RFC 2663) provozu za účelem dohledatelnosti veřejného provozu k vnitřnímu koncovému zařízení v minimální délce 3 měsíců. | Tento parametr škola v současné době **nesplňuje**, proto bude v rámci projektu implementován systém centrálního logování. |
| Síťové zařízení podporující rate limiting, antispoofing, access listy - zařízení musí obsahovat všechny potřebné komponenty a licence pro zajištění řádné funkcionality. | Tento parametr škola v současné době **nesplňuje**, proto budou v rámci projektu pořízeny aktivní síťové prvky (firewall, přepínače, WiFi AP) s požadovanými funkcemi |
| Schopnost snadné/automatické rekonfigurace pravidel firewallu (access listů) na základě identifikovaných útoků. | Tento parametr škola v současné době **nesplňuje**, v rámci projektu bude pořízen centrální firewall s požadovanými funkcemi. |
| Zajištění šifrovaného přístupu (SSL/TLS) a podepsání DNSSEC domén pro služby školy dostupné online (např. emailové služby, webové servery, studijní a ekonomické agendy atp.). | Tento parametr škola v současné době **nesplňuje**, proto bude v rámci projektu pořízen veřejný certifikát a provedena nastavení interních I externích systémů a služeb pro zajištění naplnění požadavků. |
| Validující DNSSEC resolver na straně školy, nebo poskytovatele konektivity, nebo otevřeným DNSSEC validujícím resolverem | Tento parametr škola v současné době **nesplňuje**, proto bude v rámci projektu implementován validující DNSSEC resolver na systémech školy. |
| Software a firmware je aktualizován po dobu udržitelnosti projektu, jsou-li aktualizace k dispozici | Tento parametr škola v současné době **nesplňuje**, proto budou v rámci projektu pořízeny či smluvně zajištěny potřebné aktualizace. |
| 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. | Tento parametr škola v současné době **nesplňuje**, proto dojde v rámci projektu k zajištění plnění požadavků smluvně i technicky se současný poskytovatelem, popřípadě bude řešeno změnou poskytovatele. |
| **Konektivita školy k veřejnému internetu (WAN) - doporučené parametry** | |
| Symetrické připojení (zajištění konektivity) bez agregace a omezení | Tento parametr škola v současné době **nesplňuje**, v rámci projektu dojde k úpravě parametrů jedné ze dvou linek - nastavení symetrického připojení |
| Plná podpora připojení do veřejného internetu přes protokol IPv4 i IPv6, včetně zajištění dostupnosti online služeb školy na IPv6 adresách. | Tento parametr škola v současné době zcela **nesplňuje**, v rámci projektu budou pořízeny veřejné IPv6 adresy a provedeny odpovídají konfigurace prvků a systémů pro naplnění požadavků. |
| 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. | Tento parametr škola v současné době **nesplňuje** a v rámci projektu nebude řešen z důvodu nedostupnosti požadovaných služeb u dostupných poskytovatelů připojení k internetu. |
| Antivirová kontrola internetového provozu | Tento parametr škola v současné době **nesplňuje**, proto bude v rámci projektu pořízen centrální firewall s funkcí antivirové kontroly internetového provozu. |
| **Vnitřní konektivita školy (LAN a WLAN) - společné povinné parametry** | |
| 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). | Tento parametr škola v současné době **nesplňuje**, proto bude v rámci projektu bude pořízen systém IdM (identity management) a rozšířena stávající databáze AD pro plné řízení identit, jejich oprávnění a přístupů k síti I službám. . |
| Logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas-počítačový systém | Tento parametr škola v současné době **nesplňuje**, proto bude v rámci projektu pořízen a implementován systém centrálního logování |
| Systémy zálohování a obnovy dat serverové infrastruktury | Tento parametr škola v současné době **nesplňuje**, proto bude v rámci projektu pořízen systém pro zálohování a obnovu dat serverové infrastruktury |
| Systémy pro antivirovou ochranu počítačových systémů, antispamovou ochranu poštovních serverů | Tento parametr škola v současné době **splňuje**, v rámci projektu budou využity stávající systémy antivirové ochrany počítačových systémů a antispamové ochrany poštovních serverů. |
| **Vnitřní konektivita školy (LAN a WLAN) - povinné parametry pevné LAN** | |

| Požadavek | Způsob naplnění |
|---|---|
| Minimální konektivita koncových uživatelských zařízení 1000 Mbps fullduplex | Tento parametr škola v současné době **nesplňuje**, proto budou v rámci projektu pořízeny aktivní prvky s minimální rychlostí portů min. 1 000 Mbps |
| Minimální konektivita serverů, aktivních síťových prvků, bezpečnostních zařízení (např. IPS, IDS, Next Generation Firewall aj.), datových úložišť (NAS) 1000 Mbps fullduplex | Tento parametr škola v současné době **nesplňuje**, proto budou v rámci projektu pořízeny aktivní prvky s minimální rychlostí portů min. 1 000 Mbps (u páteřních a serverových spojů 10 000 Mbps) |
| Síťové prvky musí splňovat následující funkcionality: centrální směrovače a centrální přepínače (L2 i L3) 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.]. | Tento parametr škola v současné době **nesplňuje**, proto budou v rámci projektu pořízeny aktivní prvky splňující všechny požadované parametry |
| Strukturovaná kabeláž pro připojení počítačových systémů a dalších zařízení (tiskárny, servery, AP aj.). | Tento parametr škola v současné době **nesplňuje**, proto bude v rámci projektu stávající kabeláž rozšířena. |
| 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. | Tento parametr škola v současné době **nesplňuje**, proto bude v rámci projektu stávající kabeláž rozšířena nebo nahrazena pro zajištění bezpotenciálového (optického) propojení mezi budovami a ve vnějších prostorech v areálu školy. |
| **Vnitřní konektivita školy (LAN a WLAN) - povinné parametry bezdrátové sítě WLAN** | |
| 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. | Tento parametr škola v současné době **nesplňuje**, proto bude v rámci projektu navržena nová topologie pokrytí WiFi signálem a pořízeny WiFi AP (přístupové body), které zajistí dostatečnou kapacitu pro provoz mobilních zařízení pedagogického sboru i studentů (tj. v prostředí s "vysokou hustotou" WiFi klientů) |
| Zabezpečení minimálně AES šifrováním a standardem WPA2-Enterprise nebo WPA3-Enterprise, multi SSID, ACL pro filtrování provozu. | Tento parametr škola v současné době **nesplňuje**, proto budou v rámci projektu pořízeny WiFi AP a související systémy (radius, autentizační databáze, systém pro řízení přístupu na bázi 802.1X) a podporou standardu WPA3-Enteprise na všech (min 4) SSID společně s filtrováním provozu založeným na ACL |
| Zajištění vzájemně oddělených sítí pro zaměstnance školy, žáky/studenty školy a externí zařízení (hosty). | Tento parametr škola v současné době **nesplňuje**, proto bude v rámci projektu provedeny segmentace sítě na bázi VLAN s automatickým zařazováním klientům do segmentů podle parametrů koncového zařízení a jeho uživatele založeným na standardu IEEE 802.1X |
| Podpora mechanismu izolace uživatelů. | Tento parametr škola v současné době **nesplňuje**, proto budou v rámci projektu pořízeny aktivní prvky (WiFi AP) s podporou izolace klientů |
| 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. | Tento parametr škola v současné době částečně **nesplňuje**, proto budou v rámci projektu pořízeny aktivní prvky (WiFi AP) s podporou standardu IEEE 802.11ax (Wi-Fi 6) nebo novějších podle aktuálních standardů |
| **Vnitřní konektivita školy (LAN a WLAN) - společné doporučené parametry** | |
| Logování provozu za účelem dohledatelnosti na úroveň koncového uživatele. | Tento parametr škola v současné době **nesplňuje**, proto bude v rámci projektu pořízen systém centrálního logování (log management), který zajistí logování provozu a jeho dohledatelnost na úroveň konceového uživatele |
| Řešení dočasných přístupů (hosté, brigádníci, praktikanti, zákonní zástupci, externí subjekty) a systému blokace Wi-Fi v určitém čase. | Tento parametr škola v současné době **nesplňuje**, proto bude v rámci projektu pořízen systém, který zajistí řešení dočasných přístupů (např. Na bázi captive portálu) a umožní blokovat WiFi komunikaci v kontkrétních časech. |
| Federované služby autentizace a autorizace (včetně aktivního zapojení do národních vzdělávacích federací (např. aktvní zapojení do federovaného systému www.eduroam.cz). | Tento parametr škola v současné době **nesplňuje**, proto bude v rámci projektu bude autentizační a autorizační systém (radius, 802.1X) vybudován jako federativní a WiFi síť školy bude aktivně zapojena do federovaného systému www.eduroam.cz |
| 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). | Tento parametr škola v současné době **nesplňuje**, proto budou v rámci projektu pořízeny aktivní prvky (WiFi AP) s plných centráním managementem včetně distribuce konfigurací, automatickým rozkládáním zátěže klientů, roamingu mezi spravovanými access pointy, automatickým směrováním podporovaných klientů do pásma 5 GHz, automatickým laděním kanálů a síly signálu včetně detekce a reakce na non-Wi-Fi rušení a podporou IoT zařízení. |
| 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]. | Tento parametr škola v současné době **nesplňuje**, proto bude v rámci projektu vybudován systém pro ověřování uživatelů vůči centrální databázi účtů MS Active Directory prostřednictvím protokolu IEEE 802.1X a prostřednictvím Captive portálu pro externí a dočasné uživatele. |
| Propojení aktivních prvků a důležitých systémů (např. Servery, NAS, propojení budov) rychlostí 10 Gbps, včetně uplinku. | Tento parametr škola v současné době **nesplňuje**, proto budou v rámci projektu pořízeny aktivní prvky (přepínače, firewally) a |

| Požadavek | Způsob naplnění |
|---|---|
| | ostatní zařízení, které umožní propojení důležitých systémů (serverů, NAS) rychlostí 10 Gb |
| **Doporučené bezpečnostní prvky projektu** | |
| Systémy nebo zařízení pro sledování infrastruktury sítě a sledování IP provozu sítě (umožňující funkce RFC 3917 - IPFIX nebo ekvivalent) | Tento parametr škola v současné době **nesplňuje**, proto budou v rámci projektu pořízeny aktivní prvky (přepínače, firewally) s podporou exportu síťových toků IPFIX či ekvivalentních, které budou zpracovávány centrálním logovacím systémem. |
| Systémy schopné detekovat nelegitimní provoz nebo síťové anomálie. | Tento parametr škola v současné době **nesplňuje**, proto budou v rámci projektu pořízeny aktivní prvky (firewally) s podporou detekce nelegitimního provozu včetně aplikačních protokolů. |
| Systémy vyhodnocování a správy událostí a bezpečnostních incidentů (log management, incident management). | Tento parametr škola v současné době **nesplňuje**, proto bude v rámci projektu pořízen systém centrálního logování. |
| Systémy pro monitorování funkčnosti síťové a serverové infrastruktury. | Tento parametr škola v současné době **nesplňuje**, proto budou v rámci projektu důsledně implementovány a využity monitorovací nástroje síťové a serverové infrastruktury poskytované výrobci prvků a zařízení jako součást jejich dodávky a podpory |
| Zařízení umožňující kontrolu http a https provozu, kategorizaci a selekci obsahu dostupného pro vybrané skupiny uživatel (učitel, žák), blokování nežádoucích kategorií obsahu. | Tento parametr škola v současné době **nesplňuje**, proto budou v rámci projektu pořízeny aktivní prvky (firewally), které zajistí provádění kontrolu http a https provozu, kategorizaci a selekci obsahu dostupného pro vybrané skupiny uživatel (učitel, žák), blokování nežádoucích kategorií obsahu. |
| Systémy uživatelské podpory naplňující principy ITIL (HelpDesk, ServiceDesk aj.). | Tento parametr škola v současné době **nesplňuje**, proto bude pro řízení uživatelské podpory v rámci projektu pořízen systém Service Desk naplňující principy ITIL. |
| Nástroje pro centrální správu a audit ICT prostředků. | Tento parametr škola v současné době **nesplňuje**, proto bude pro řízení uživatelské podpory v rámci projektu pořízen systém Asset Management naplňující principy ITIL, který umožní automatickou detekci, inventarizaci a audit ICT prostředků včetně SW auditu a řízení licencí. |
| Podpora vzdáleného přístupu (VPN). | Tento parametr škola v současné době **nesplňuje**, proto pro bude v rámci projektu pořízen systém pro vzdálený přístup k aplikacím typu "terminálové služby" a vybudován systém VPN v rámci nově pořízeného firewallu |
| Zavedení více-faktorové autentizace. | Tento parametr škola v současné době **nesplňuje** a tento nepovinný požadavek bude v rámci projektu realizován částečně pro autentizaci externistů a správců s využitím stávajících prostředků a prostředků pořízených pro plnění ostatních požadavků |