Plnění Standardu konektivity a návrh opatření – SŠSS Karlovy Vary

SPRAVEDLIVÁ TRANSFORMACE – projekt Konektivita školy

Parametr	Plnění (ano/ne/ nerelevantní)	Komentář
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	Ano	Tento parametr škola v současné době splňuje.
Vlastní nebo poskytovatelem přidělené veřejné IPv4 adresy.	Ano	Tento parametr škola v současné době nesplňuje, v rámci projektu bude veřejná IPv4 adresa pořízena a nakonfigurována na nově pořízeném firewallu. Tím bude parametr naplněn.
Zajištění monitoringu a logování NAT (RFC 2663) provozu za účelem dohledatelnosti veřejného provozu k vnitřnímu koncovému zařízení v minimální délce 3 měsíců.	Ano	Tento parametr škola v současné době nesplňuje, proto bude v rámci projektu implementován systém centrálního logování. Tím bude parametr naplněn.
Síťové zařízení podporující rate limiting, antispoofing, access listy – zařízení musí obsahovat všechny potřebné komponenty a licence pro zajištění řádné funkcionality.	Ano	Tento parametr škola v současné době nesplňuje, proto budou v rámci projektu pořízeny aktivní síťové prvky (firewall, přepínače, WiFi AP) s požadovanými funkcemi. Tím bude parametr naplněn.
Schopnost snadné/automatické rekonfigurace pravidel firewallu (access listů) na základě identifikovaných útoků.	Ano	Tento parametr škola v současné době nesplňuje, v rámci projektu bude pořízen firewall s požadovanými funkcemi. Tím bude parametr naplněn.
Zajištění šifrovaného přístupu (SSL/TLS) a podepsání DNSSEC domén pro služby školy dostupné online (např. emailové služby, webové servery, studijní a ekonomické agendy atp.).	Ano	Tento parametr škola v současné době splňuje částečně, proto bude v rámci projektu provedeno nastavení interních i externích systémů a služeb pro zajištění naplnění požadavků. Tím bude parametr naplněn.
Validující DNSSEC resolver na straně školy, nebo poskytovatele konektivity, nebo otevřeným DNSSEC validujícím resolverem	Ano	Tento parametr škola v současné době nesplňuje, proto bude v rámci projektu implementován validující DNSSEC resolver na systémech školy. Tím bude parametr naplněn.

Software a firmware je aktualizován po dobu udržitelnosti projektu, jsou-li aktualizace k dispozici	Ano	Tento parametr škola v současné době nesplňuje, proto budou v rámci projektu pořízeny či smluvně zajištěny potřebné aktualizace. Tím bude parametr naplněn.
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.	Ano	Tento parametr škola v současné době nesplňuje, proto dojde v rámci projektu k zajištění plnění požadavků smluvně i technicky se současným poskytovatelem, popřípadě bude řešeno změnou či doplněním dalšího poskytovatele. Tím bude parametr naplněn.
Konektivita školy k veřejnému internetu (WAN) - doporučené parametry		
Symetrické připojení (zajištění konektivity) bez agregace a omezení.	Ano	Tento parametr škola v současné době splňuje.
Plná podpora připojení do veřejného internetu přes protokol IPv4 i IPv6, včetně zajištění dostupnosti online služeb školy na IPv6 adresách.	Ano	Tento parametr škola v současné době nesplňuje, v rámci projektu bude provedeno připojení do veřejného internetu i přes protokol IPv6 a provedeny odpovídají konfigurace služeb pro jejich dostupnost na IPv6 adresách. Tím bude parametr naplněn.
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.	Nerelevantní pro tento projekt	Tento doporučený/nepovinný 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	Ano	Tento parametr škola v současné době nesplňuje, v rámci projektu bude pořízen firewall s požadovanými funkcemi. Tím bude parametr naplněn.
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).	Ano	Tento parametr škola v současné době nesplňuje, proto bude v rámci projektu bude pořízen systém IdM (identity management) a konsolidovány 2 stávající databáze AD pro plné řízení identit, jejich oprávnění a přístupů k síti i službám. Tím bude parametr naplněn.
Logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas-počítačový systém	Ano	Tento parametr škola v současné době nesplňuje, proto bude v rámci projektu pořízen

		a implementován systém centrálního logování. Tím bude parametr naplněn.
Systémy zálohování a obnovy dat serverové infrastruktury	Ano	Tento parametr škola v současné době zcela nesplňuje proto bude v rámci projektu pořízen systém pro zálohování a obnovu dat serverové infrastruktury včetně nově pořízených systémů. Tím bude parametr naplněn.
Systémy pro antivirovou ochranu počítačových systémů, antispamovou ochranu poštovních serverů	Ano	Tento parametr škola v současné době splňuje, v rámci projektu budou využity stávající systémy antivirové ochrany počítačových systémů a antispamové ochrany poštovních serverů. Tím bude parametr naplněn.
Vnitřní konektivita školy (LAN a WLAN) - povinné parametry pevné LAN		
Minimální konektivita koncových uživatelských zařízení 1000 Mbps fullduplex	Ano	Tento parametr škola v současné době nesplňuje, proto budou v rámci projektu pořízeny aktivní prvky s minimální rychlostí portů min. 1 000 Mbps. Tím bude parametr naplněn.
Minimální konektivita serverů, aktivních síťových prvků, bezpečnostních zařízení (např. IPS, IDS, Next Generation Firewall aj.), datových úložišť (NAS) 1000 Mbps fullduplex	Ano	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. Tím bude parametr naplněn.
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.].	Ano	Tento parametr škola v současné době nesplňuje, proto budou v rámci projektu pořízeny aktivní prvky splňující všechny požadované parametry. Tím bude parametr naplněn.
Strukturovaná kabeláž pro připojení počítačových systémů a dalších zařízení (tiskárny, servery, AP aj.).	Ano	Tento parametr škola v současné době nesplňuje, proto bude v rámci projektu stávající kabeláž rozšířena ve standardu min Cat6 pro připojení pořizovaných Wi-Fi AP. Tím bude parametr naplněn.
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.	Nerelevantní pro tento projekt	Tento parametr pro školu není relevantní, neboť škola působí pouze v jedné budově. Datové rozvaděče uvnitř budovy jsou propojeny optickými vlákny.
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.	Ano	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). Tím bude parametr naplněn.
Zabezpečení minimálně AES šifrováním a standardem WPA2-Enterprise nebo WPA3-Enterprise, multi SSID, ACL pro filtrování provozu.	Ano	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. Tím bude parametr naplněn.
Zajištění vzájemně oddělených sítí pro zaměstnance školy, žáky/studenty školy a externí zařízení (hosty).	Ano	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. Tím bude parametr naplněn.
Podpora mechanismu izolace uživatelů.	Ano	Tento parametr škola v současné době nesplňuje, proto budou v rámci projektu pořízeny aktivní prvky (WiFi AP) s podporou izolace uživatel/klientů. Tím bude parametr naplněn.
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.	Ano	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. Tím bude parametr naplněn.
Vnitřní konektivita školy (LAN a WLAN) - společné doporučené parametry		
Logování provozu za účelem dohledatelnosti na úroveň koncového uživatele.	Ano	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 koncového uživatele. Tím bude parametr naplněn.
Řešení dočasných přístupů (hosté, brigádníci, praktikanti, zákonní zástupci, externí subjekty) a systému blokace Wi-Fi v určitém čase.	Ano	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 konkrétních časech. Tím bude parametr naplněn.

Federované služby autentizace a autorizace (včetně aktivního zapojení do národních vzdělávacích federací (např. aktivní zapojení do federovaného systému www.eduroam.cz).	Ano	Tento parametr škola v současné době nesplňuje, proto bude v rámci projektu autentizační a autorizační systém (radius, 802.1X) vybudován jako federativní a WiFi síť školy bude aktivně zapojena do federovaného systému www.eduroam.cz. Tím bude parametr naplněn.
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).	Ano	Tento parametr škola v současné době nesplňuje, proto budou v rámci projektu pořízeny aktivní prvky (WiFi AP) s plných centrálním 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. Tím bude parametr naplněn.
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].	Ano	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. Tím bude parametr naplněn.
Propojení aktivních prvků a důležitých systémů (např. Servery, NAS, propojení budov) rychlostí 10 Gbps, včetně uplinku.	Ano	Tento parametr škola v současné době nesplňuje, proto budou v rámci projektu pořízeny aktivní prvky (přepínače) a ostatní zařízení, které umožní propojení důležitých systémů (server, NAS, LAN prvky, firewall) rychlostí 10 Gbps. Tím bude parametr naplněn.
Doporučené bezpečnostní prvky projektu		
Systémy nebo zařízení pro sledování infrastruktury sítě a sledování IP provozu sítě (umožňující funkce RFC 3917 - IPFIX nebo ekvivalent)	Ano	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. Tím bude parametr naplněn.
Systémy schopné detekovat nelegitimní provoz nebo síťové anomálie.	Ano	Tento parametr škola v současné době nesplňuje, proto budou v rámci projektu pořízeny aktivní prvky (firewally) s podporou detekce nelegitimního provozu včetně aplikačních protokolů. Tím bude parametr naplněn.

Systémy vyhodnocování a správy událostí a bezpečnostních incidentů (log management, incident management).	Ano	Tento parametr škola v současné době nesplňuje, proto bude v rámci projektu pořízen systém centrálního logování (log management). Tím bude parametr naplněn.
Systémy pro monitorování funkčnosti síťové a serverové infrastruktury.	Ano	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. Tím bude parametr naplněn.
Zařízení umožňující kontrolu http a https provozu, kategorizaci a selekci obsahu dostupného pro vybrané skupiny uživatel (učitel, žák), blokování nežádoucích kategorií obsahu.	Ano	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, student), blokování nežádoucích kategorií obsahu. Tím bude parametr naplněn.
Systémy uživatelské podpory naplňující principy ITIL (HelpDesk, ServiceDesk aj.).	Nerelevantní pro tento projekt	Tento doporučený/nepovinný parametr škola v současné době nesplňuje. Stávající systém uživatelské podpory využívající helpdeskové systémy partnerů a poskytovatelů služeb a interní groupwarový systém je postačující potřebám školy a nebude v rámci projektu měněn.
Nástroje pro centrální správu a audit ICT prostředků.	Nerelevantní pro tento projekt	Tento doporučený/nepovinný parametr škola v současné době nesplňuje. Stávající systém centrální správy a auditu PC využívají technologie Group Policy, Intune a nástroje zahrnuté v operačních systémech je postačující potřebám školy a nebude v rámci projektu měněn.
Podpora vzdáleného přístupu (VPN).	Ano	Tento parametr škola v současné době nesplňuje pro všechny uživatele, proto pro bude v rámci projektu systém VPN rozšířen v rámci nově pořízeného firewallu. Tím bude parametr naplněn.
Zavedení více-faktorové autentizace.	Nerelevantní pro tento projekt	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 – zejména firewallu.