IROP – Standard konektivity škol

V rámci projektu je řešena vnitřní konektivita školy a připojení k internetu. Parametry vnitřní konektivity a připojení k internetu musí být v souladu s přílohou std. Konektivity. Do následující tabulky je nutné uvést informace, zda je konkrétní kritérium naplněno (a popsat jak), a pokud ne, tak jaká opatření budou podniknuta za účelem jeho naplnění.

|  |  |
| --- | --- |
| **1.** | **Konektivita školy k veřejnému internetu (WAN)** |
| **1.2.** | **Povinné parametry projektu** | **Splněno?**  **(ANO X NE)** | **Současné technické řešení** | **Technické řešení zajišťující naplnění kritéria** |
| 1.2.1. | 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** | Aktuálně je v SVČ technicky vyřešeno |  |
| 1.2.2. | Vlastní nebo poskytovatelem přidělené veřejné IPv4 adresy | **Nyní NE, řešeno výzvou** | Aktuálně není v SVČ dostatečně technicky řešeno | Bude řešeno s poskytovatelem internetové konektivity, dle požadavku std. konektivity škol. |
| 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 | **Nyní NE, řešeno výzvou** | Aktuálně není v SVČ technicky řešeno | **FIREWALL**  Nový firewall loguje a monitoruje vnitřní i veřejné IP. |
| 1.2.5. | Schopnost snadné/automatické rekonfigurace pravidel firewallu (access listů) na základě identifikovaných útoků | **Nyní NE, řešeno výzvou** | Aktuálně není v SVČ technicky řešeno | **FIREWALL**  Snadná konfigurace na základě logů – ano funkcionalita firewallu |
| 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.). | **Nyní NE, řešeno výzvou** | Aktuálně není v SVČ technicky řešeno | Podepsání DNSSEC bude řešeno s registrátorem domény a šifrovaný přístup bude řešen nákupem potřebného certifikátu |
| 1.2.7. | Validující DNSSEC resolver na straně školy, nebo poskytovatele konektivity, nebo otevřeným DNSSEC validujícím resolverem | **Nyní NE, řešeno výzvou** | Aktuálně není v SVČ technicky řešeno | DNSSEC bude řešeno otevřeným DNSSEC validujícím resolverem |
| 1.2.8. | Software a firmware je aktualizován po dobu udržitelnosti projektu, jsou-li aktualizace k dispozici | **Nyní NE, řešeno výzvou** | Aktuálně není v SVČ technicky řešeno | **FIREWALL**  update všech definicí je automatický a velmi častý (několikrát za den). |
| 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 | **Nyní NE, řešeno výzvou** | Aktuálně není v SVČ technicky řešeno | Bude řešeno s poskytovatelem internetové konektivity, dle požadavku std. konektivity škol. |
| **1.3.** | **Doporučené parametry projektu** |  |  |  |
| 1.3.1. | Symetrické připojení (zajištění konektivity) bez agregace a omezení, doporučujeme postupně směřovat ke kapacitě konektivity 1Gbps | **Nyní NE** | Nebude řešeno v rámci této výzvy |  |
| 1.3.2. | Plná podpora připojení do veřejného internetu přes protokol IPv4 i IPv6, včetně zajištění dostupnosti online služeb školy na IPv6 adresách | **Nyní NE** | Nebude řešeno v rámci této výzvy |  |
| 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 | **Nyní NE** | Nebude řešeno v rámci této výzvy |  |
| 1.3.4. | Antivirová kontrola internetového provozu | **Nyní NE** | Nebude řešeno v rámci této výzvy |  |
| **2.** | **Vnitřní konektivita školy (LAN a WLAN)** |  |  |  |
| **2.2.** | **Povinné parametry projektu (bez ohledu typ síťového připojení)** | **Splněno?**  **(ANO X NE)** | **Současné technické řešení** | **Technické řešení zajišťující naplnění kritéria** |
| 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) | **Nyní NE, řešeno výzvou** | Aktuálně není v SVČ technicky řešeno | **FIREWALL**  řešeno active directory (AD)/ LDAP serverem na domain controleru.  IMPORT do nového firewallu s podporou. FSSO přes collector import o loginech přímo do nového firewallu. |
| 2.2.2. | Logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas-počítačový systém | **Nyní NE, řešeno výzvou** | Aktuálně není v SVČ technicky řešeno | **SERVER**  řešeno active directory (AD)/ LDAP serverem na domain controleru a LOGMNGMNT SW. |
| 2.2.3. | Systémy zálohování a obnovy dat serverové infrastruktury | **Nyní NE, řešeno výzvou** | Aktuálně není v SVČ technicky řešeno | **SERVER SW –** Zálohování serverové infrastruktury nativními prostředky WIN SERVER/případně BACKUP SW |
| 2.2.4. | Systémy pro antivirovou ochranu počítačových systémů, antispamovou ochranu poštovních serverů | **ANO** | Aktuálně je v SVČ technicky řešeno |  |
| **2.3.** | **Povinné parametry projektu v oblasti pevné LAN** |  |  |  |
| 2.3.1. | Minimální konektivita koncových uživatelských zařízení 1000 Mbps fullduplex | **Nyní NE, řešeno výzvou** | Aktuálně není v SVČ technicky řešeno | Kompletní podpora 1000Mbit/s fullduplex u všech koncových zařízení bude řešeno vybudováním strukturované kabeláže LAN včetně LAN pro WIFI |
| 2.3.2. | Minimální konektivita serverů, aktivních síťových prvků, bezpečnostních zařízení (např. IPS, IDS, Next Generation Firewall aj.), datových úložišť (NAS) 1000 Mbps fullduplex | **Nyní NE, řešeno výzvou** | Aktuálně není v SVČ technicky řešeno | Kompletní podpora 1000Mbit/s fullduplex u všech koncových zařízení bude řešeno vybudováním strukturované kabeláže LAN |
| 2.3.3. | 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.] | **Nyní NE, řešeno výzvou** | Aktuálně není v SVČ technicky řešeno | Bude řešeno nákupem nových centrálních aktivních prvků switchů |
| 2.3.4. | Strukturovaná kabeláž pro připojení počítačových systémů a dalších zařízení (tiskárny, servery, AP aj.) | **Nyní NE, řešeno výzvou** | Aktuálně není v SVČ technicky řešeno | Bude řešeno vybudováním strukturované kabeláže LAN pro WIFI |
| 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 | **-** | Pouze jedna budova |  |
| **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 | **Nyní NE, řešeno výzvou** | Aktuálně není v SVČ technicky řešeno | Analýza stávajícího stavu ICT. Dle stávajícího stavu potřeb pokrytí navržena infrastruktura LAN / WIFI |
| 2.4.2. | Zabezpečení minimálně AES šifrováním a standardem WPA2-Enterprise nebo WPA3-Enterprise, multi SSID, ACL pro filtrování provozu | **Nyní NE, řešeno výzvou** | Aktuálně není v SVČ technicky řešeno | Bude řešeno nákupem nových bezdrátových přístupových bodů, které budou splňovat požadované vlastnosti. |
| 2.4.3. | Zajištění vzájemně oddělených sítí pro zaměstnance školy, žáky/studenty školy a externí zařízení (hosty) | **Nyní NE, řešeno výzvou** | Aktuálně není v SVČ technicky řešeno | Bude řešeno nákupem nových bezdrátových přístupových bodů, které budou splňovat požadované vlastnosti. |
| 2.4.4. | Podpora mechanismu izolace uživatelů | **Nyní NE, řešeno výzvou** | Aktuálně není v SVČ technicky řešeno | Bude řešeno nákupem nových bezdrátových přístupových bodů, které budou splňovat požadované vlastnosti. |
| 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 | **Nyní NE, řešeno výzvou** | Aktuálně není v SVČ technicky řešeno | Bude řešeno nákupem nových bezdrátových přístupových bodů, které budou splňovat požadované vlastnosti. |
| **2.5.** | **Doporučené parametry projektu (bez ohledu typ síťového připojení)** |  |  |  |
| 2.5.1. | Logování provozu za účelem dohledatelnosti na úroveň koncového uživatele | **Nyní NE, řešeno výzvou** | Aktuálně není v SVČ technicky řešeno | Bude řešeno na nákupem LOGMNGMNT SW |
| 2.5.2. | Řešení dočasných přístupů (hosté, brigádníci, praktikanti, zákonní zástupci, externí subjekty) a systému blokace Wi-Fi v určitém čase | **Nyní NE, řešeno výzvou** | Aktuálně není v SVČ technicky řešeno | Bude řešeno nákupem nových bezdrátových přístupových bodů, které budou splňovat požadované vlastnosti. |
| 2.5.3. | Federované služby autentizace a autorizace (včetně aktivního zapojení do národních vzdělávacích federací (např. aktvní zapojení do federovaného systému www.eduroam.cz) | **Nyní NE** | Nebude řešeno v rámci této výzvy |  |
| 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) | **Nyní NE, řešeno výzvou** | Aktuálně není v SVČ technicky řešeno | Bude řešeno nákupem nových bezdrátových přístupových bodů, které budou splňovat požadované vlastnosti. |
| 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] | **Nyní NE, řešeno výzvou** | Aktuálně není v SVČ technicky řešeno | Bude řešeno nákupem nových bezdrátových přístupových bodů, které budou splňovat požadované vlastnosti. |
| 2.5.6. | Propojení aktivních prvků a důležitých systémů (např. Servery, NAS, propojení budov) rychlostí 10 Gbps, včetně uplinku | **Nyní NE, řešeno výzvou** | Aktuálně není v SVČ technicky řešeno | Bude řešeno nákupem nových aktivních prvků switchů s uplinkem SFP+ a INFRASTRUKTURY s SFP+ (SVR a NAS) |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **3.** | **Další doporučené bezpečnostní prvky projektu** | **Splněno?**  **(ANO X NE)** | **Současné technické řešení** | **Technické řešení zajišťující naplnění kritéria** |
| 3.1.1. | Systémy nebo zařízení pro sledování infrastruktury sítě a sledování IP provozu sítě (umožňující funkce RFC 3917 – IPFIX nebo ekvivalent) | **Nyní NE** | Nebude řešeno v rámci této výzvy |  |
| 3.1.2. | Systémy schopné detekovat nelegitimní provoz nebo síťové anomálie | **Nyní NE** | Nebude řešeno v rámci této výzvy |  |
| 3.1.3. | Systémy vyhodnocování a správy událostí a bezpečnostních incidentů (log management, incident management) | **Nyní NE** | Nebude řešeno v rámci této výzvy |  |
| 3.1.4. | Systémy pro monitorování funkčnosti síťové a serverové infrastruktury | **Nyní NE** | Nebude řešeno v rámci této výzvy |  |
| 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 | **Nyní NE, řešeno výzvou** | Aktuálně není v SVČ technicky řešeno | Bude řešeno nákupem nového Next generation firewallu splňujícím tyto požadované funkcionality |
| 3.1.6. | Systémy uživatelské podpory naplňující principy ITIL (HelpDesk, ServiceDesk aj.) | **Nyní NE** | Nebude řešeno v rámci této výzvy |  |
| 3.1.7. | Nástroje pro centrální správu a audit ICT prostředků | **Nyní NE** | Nebude řešeno v rámci této výzvy |  |
| 3.1.8. | Podpora vzdáleného přístupu (VPN) | **Nyní NE, řešeno výzvou** | Aktuálně není v SVČ technicky řešeno | Bude řešeno nákupem nového Next generation firewallu splňujícím tyto požadované funkcionality |
| 3.1.9. | Zavedení více-faktorové autentizace | **Nyní NE** | Nebude řešeno v rámci této výzvy |  |