Příloha č. 1 výzvy – „Sítě a bezpečnost“

Tento dokument definuje základní technická kritéria cílového stavu infrastruktury organizace a přijatelnosti aktivit projektů v rámci Zásad pro poskytování finančních příspěvků na zvyšování IT vybavení organizací zřizovaných Krajem Vysočina.

Téma č. 1 – Konektivita organizace k veřejnému internetu (WAN)

Obecný popis: pro základní způsobilost projektu řešící toto téma musí organizace 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 minimální parametry v době ukončení realizace projektu:

- šíře pásma (bandwidth) odpovídající 128 kbps na studenta nebo zaměstnance nebo 512 kbps/počítač nebo taková šířka pásma, která neomezuje provoz zařízení a uživatelů[1]
- symetrické připojení bez agregace a omezení (FUP)
- vlastní nebo poskytovatelem přidělené veřejné IPv4 i IPv6 adresy
- plná podpora připojení do veřejného internetu přes protokol IPv4 i IPv6 (dual-stack)
- podpora monitoringu a logování NAT (RFC 2663) provozu za účelem dohledatelnosti veřejného provozu k vnitřnímu zařízení
- logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas – uživatel, a to včetně ošetření v případě sdílených pracovišť (učeben, sdílených pracovních stanic apod.)
- v případě dostupnosti konektivity sítě ROWANet přímé směrování na adresní rozsahy kraje prostřednictvím sítě ROWANet
- u softwaru a firmwaru je vyžadována dostupnost aktualizací, zejména bezpečnostního charakteru, po celou dobu udržitelnosti projektu.

Způsobilé výdaje:

- síťové zařízení WAN-LAN (router, firewall, NAT; s podporou přepínaní/směrování protokolů IPv4/IPv6 a minimální propustností přepínacího/směrovacího subsystému 1 Gbps);
- bezpečnostní zařízení (IDS, IPS, aplikační firewall)
- nezbytné vybavení a vedení poslední míle k přípojnému bodu poskytovatele internetu nebo sítě ROWANet popř. propojení budov organizace (rádiový přijímač, anténní zařízení, metalické nebo optické vedení na pozemku a v budovách organizace)
- nezbytné licence SW a nákup HW související s funkcionalitou síťového nebo bezpečnostního zařízení (např. síťové rozhraní atp.) rozhraním WAN-LAN včetně funkcionality možnosti vzdálené správy a monitoringu funkčnosti zařízení (ICMP echo, SNMP v3, HTTPS, SSH apod.)
- nezbytné vybavení pro umístění, instalaci a provoz technologie (např. rack, napájení, UPS/přepěťová ochrana, kabeláž, chlazení atp.) a zajištění DMZ zóny pro síťové a serverové technologie, včetně rezervy/možnosti rozšíření navrhovaného řešení

Nezpůsobilé výdaje: zřizovací a provozní náklady na zajištění připojení (konektivity) organizace, náklady na licenční poplatky ČTÚ, služby údržby aktivních prvků a bezpečnostních zařízení s výjimkou standardní záruky, povinné servisní poplatky.

Téma č. 2 – Vnitřní konektivita organizace (LAN)

Obecný popis: vnitřní síťové prostředí organizace pořizované v rámci projektu může být řešeno pevnou sítí, bezdrátovou sítí, nebo kombinací těchto síťových technologií.

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

Povinné minimální bezpečnostní parametry projektu (bez ohledu na typ síťového připojení):

- Monitorování IP (IPv4 a IPv6) datových toků formou exportu provozních informací o přenesených datech v členění minimálně: zdrojová/cílová IP adresa, zdrojový/cílový TCP/UDP port (či ICMP typ) – RFC3954 nebo ekvivalent (např. NetFlow); systém pro monitorování a sběr provozně-lokačních údajů minimálně na úrovni rozhraní WAN, ideálně i LAN) a to bez negativních vlivů na zátěž a propustnost zařízeni s kapacitou pro uchování dat po dobu minimálně 2 měsíců – s možností využití krajského kolektoru FTAS.
- Povinné řešení systému 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. síťovým službám alespoň pro bezdrátovou síť.
- logování přístupu uživatelů do sítě umožňující dohledání vazeb *IP adresa – čas – uživatel*.

V oblasti pevné LAN musí projekt, pokud ji řeší, splňovat následující minimální parametry:

- Minimální konektivita stanic a dalších koncových zařízení zařízení 100 Mbps, fullduplex.
- Strukturovaná kabeláž pro připojení pracovních stanic a dalších zařízení (tiskárny, servery, AP, …)
- Minimální konektivita serverů, aktivních síťových prvků, bezpečnostních zařízení, NAS 1 Gbps, fullduplex.
- Páteřní rozvody mezi budovami v areálu realizovány prostřednictvím optických vláken.
- Aktivní prvky (centrální směrovače a centrální přepínače; L2 i L3)[2] s neblokující architekturou přepínacího subsystému (wire speed), podpora 802.1Q VLAN, podpora 802.1X, RADIUS based MAC autentizace.

V případě řešení bezdrátových sítí (Wi-Fi), pokud je projekt řeší, pak musí projekt naplňovat následující minimální parametry:

- Podpora mechanismu izolace klientů.
- Návrh topologie Wi-Fi sítě a analýza pokrytí signálem počítající s konzistentní Wi-Fi službou v příslušných prostorách organizace a s kapacitami pro provoz mobilních zařízení.
- 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).
- Podpora protokolu IEEE 802.1X, resp. ověřování uživatelů oproti databázi účtů přes protokol RADIUS (např. LDAP, MS AD, …).
- Podpora standardu IEEE 802.11n a případně novějších (AC, AD), současná funkce AP v pásmu 2,4 a 5 GHz.
- V případě školských zařízení minimálně pasivní zapojení[3] do federovaného systému eduroam (www.eduroam.cz). Optimálně aktivní zapojení do systému eduroam, pro zajištění národní i mezinárodní mobility žáků a učitelů.
- Podpora WPA2, PoE, multi SSID, ACL pro filtrování provozu.

Způsobilé výdaje: aktivní prvky, servery, síťové sondy a analyzátory, Wi-Fi vysílače, systém centrálního řízení Wi-Fi (centrální řadiče), úložiště pro kolektory, SW nezbytný pro provoz infrastruktury (licence OS, přístupové licence), standardní záruka.

---

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

[3] *Pasivním zapojením se rozumí poskytování služeb sítě eduroam na úrovni poskytovatele zdrojů – viz http://www.eduroam.cz/_media/cs/cz_roam_policy_v2.0.pdf*

Nezpůsobilé výdaje: počítačové stanice, realizace poskytnutí formou služby (X as a service) kromě služeb přímo souvisejících s dodávkou a implementací HW a SW; cloudové služby (např. cloud management) způsobilé jen v investiční fázi projektu, služby údržby aktivních prvků a bezpečnostních zařízení s výjimkou standardní záruky, pozáruční servis, rozšířená záruka.

Téma č. 3 – Další bezpečnostní prvky

Obecný popis: v rámci projektů je možné realizovat aktivity naplňující principy bezpečného využívání IT prostředků. Zejména pak jde o:

- Identity management systémy (IDM) – systém správy identit, řízení životního cyklu uživatelů, integrace do provozních a bezpečnostních systémů, a to včetně integrace na IDM kraje.
- Centralizovaný autentizační systém napojení na systém správy identit (např. na bázi LDAP, AD, studijní a personální agendy apod.) včetně zapojení a autentizační federace kraje.
- Řešení dočasných přístupů (hosté, brigádníci, praktikanti, zákonní zástupci, externí subjekty, blokace Wi-Fi v určitém čase). Možnost využití krajského hot-spot systému.
- Federované služby autentizace a autorizace (včetně aktivního zapojení do národních federací a zpřístupnění jejich služeb).
- Systémy nebo zařízení pro sledování infrastruktury sítě a sledování IP provozu sítě (umožňující funkce RFC 3954 nebo ekvivalent – NetFlow)
- Systémy schopné detekovat nelegitimní provoz nebo síťové anomálie.
- Systémy vyhodnocování a správy událostí a bezpečnostních incidentů (log management, incident management).
- Systémy pro monitorování funkčnosti síťové a serverové infrastruktury (např. Nagios / Icinga).
- Systémy zálohování a obnovy dat – SW i HW.
- Systémy pro antivirovou ochranu zařízení, antispamovou ochranu poštovních serverů.
- Zabezpečení přístupových protokolů (SSL/TLS) služeb (např. emailové služby, webové servery, studijní a ekonomické agendy) atp.
- Podpora vzdáleného přístupu (VPN).

Způsobilé výdaje: SW, HW, licence, náklady na implementaci a integraci přímo související s pořizovaným SW a HW.

Nezpůsobilé výdaje: Vypracování postupů, standardů a politik pro ochranu a řešení bezpečnosti uživatelů, zařízení, infrastruktury a služeb organizace.