POPIS OPTIMÁLNÍ ÚROVNĚ IT VYBAVENOSTI PŘÍSPĚVKOVÝCH ORGANIZACÍ KRAJE VYSOČINA

Leden 2022

Odbor informatiky KrÚ

Obsah:

1. Obsah

2. Konektivita organizace k veřejnému internetu a dalším WAN sítím

- Vysokorychlostní, bezpečné a stabilní připojení organizace k veřejnému internetu a dalším WAN sítím (neveřejným) s důrazem na využití sítí a služeb poskytovaných krajem (ROWANet, Cesnet, síťové služby TCK, CMS, hSOC VRF, FENIX).
- Připojení organizace by mělo podporovat moderní technické standardy (IPv6 resp. dual-stack).
- Ochrana připojení do veřejného internetu před kybernetickými útoky (firewall, emailové brány, antivirové filtry, penetrační testy).
- Síťové zařízení WAN-LAN (router, firewall, NAT; s podporou přepínání/směrování protokolů IPv4/IPv6 a minimální propustností přepínacího/směrovacího subsystému 1 Gbps).
- Bezpečnostní zařízení (IDS, IPS, aplikační firewall).
- Nezbytné vybavení pro umístění, instalaci a provoz technologie (např. rack, napájení, UPS/přepěťová ochrana, kabeláž, chlazení).
- Systém pro záznam síťového provozu (NetFlow, sFlow)
- Systémy bezpečného přístupu uživatelů ke službám veřejného internetu (proxy s antivirovou kontrolou, kategorizací zdrojů, autorizací uživatelů)
- Minimalizace přístupu serverových technologií k veřejnému internetu

3. Vnitřní konektivita organizace (LAN)

- Zajištění vnitřního síťového prostředí organizace a to prostřednictvím pevné metalické sítě, bezdrátové sítě, optické sítě nebo kombinací těchto síťových technologií.
- Řešení LAN sítě musí respektovat standardní bezpečnostní parametry (bez ohledu na typ síťového připojení), a to včetně monitorování IP datových toků a přidělování IP adres (DHCP log).
- V případě pevné LAN musí rozvody splňovat požadavek minimální konektivity 100 Mbps fullduplex na klienta (PC, IP telefon) ideálně ve standardu kabeláže Cat 6, a dále by měly zahrnovat strukturovanou kabeláž pro připojení WiFi AP a aktivních prvků prostřednictvím páteřních rozvodů 1 až 25Gbps na bázi kabeláže Cat 6A

- Rozvody mezi budovami realizované optickým vláknem (ideálně SM, konektory SC/APC), včetně aktivních prvků s neblokující architekturou přepínacího subsystému (wirespeed) podpora 802.1Q VLAN, podpora 802.1X, RADIUS based MAC autentizace.
- Wi-Fi vysílače, systém centrálního řízení Wi-Fi (centrální řadiče).
- Podpora technicky autentizace uživatelů při přístupu k síti (802.1X, Eduroam ve školách).
- SW nezbytný pro provoz infrastruktury (licence OS, přístupové licence).

4. Bezpečnost

- Systémy pro zálohování (včetně offline záloh), obnovu a archivaci dat a ochranu záloh - SW i HW.
- Systémy nebo zařízení pro sledování IP provozu sítě (dle RFC 3954 (NetFlow) nebo ekvivalent (flow based).
- Systémy pro ukládání a správu událostí (log management).
- Identity management systémy (IDM) – systém správy identit, řízení životního cyklu uživatelů, integrace do provozních a bezpečnostních systémů a to včetně integrace na IDM kraje.
- Síťový firewall s pravidelnou údržbou.
- Centralizovaný autentizační systém napojený na systém správy identit (např. na bázi LDAP, AD, studijní a personální agendy apod.).
- Vícefaktorová autentizace do citlivých systémů.
- Bezpečné řešení dočasných přístupů k síti/systémům (hosté, brigádníci, praktikanti, zákonní zástupci, externí subjekty). Možnost využití krajského hot-spot systému.
- Monitoring- systémy pro monitorování funkčnosti síťové a serverové infrastruktury (např. Nagios, Icinga, Zabbix, ….).
- Systémy pro antivirovou ochranu zařízení, antispamovou ochranu poštovních serverů.
- Zabezpečení přístupových protokolů (TLS) služeb (např. emailové služby, webové služby, studijní a ekonomické agendy) pomocí certifikátů globálně uznávaných certifikačních autorit.
- Podpora vzdáleného přístupu (VPN) bez výjimek ve firewallových pravidlech (např. přímý přístup prostřednictvím RDP, VNC a to i na základě ověření zdrojové IP)
- Systémy pro řízení a dohled nad koncovými stanicemi a telefony.
- Přístup uživatelů k www službám přes proxy včetně možnosti kategorizace webových stránek.
- Zapojení do autentizační federace kraje VysocinaID - https://vysocinaid.kr-vysocina.cz/.
- Federované služby autentizace a autorizace (včetně aktivního zapojení do národních federací a zpřístupnění jejich služeb – NIA, EDUID, EDUROAM).
- Vynucování dostatečně silné politiky hesel
- Práce výhradně s pojmenovanými uživatelskými účty (eliminace sdílených účtů)
- Pravidelné aplikování oprav (záplat) OS a dalších SW

5. Software

- Zvážení využití sdílených služeb kraje - https://portalpo.kr-vysocina.cz/sds_public_view.php
- Vlastní systém elektronické pošty (napoužívat freemaily)
- Systém správy a bezpečného sdílení dokumentů – DMS
- Systém centrální správy stanic a SW – AD, Asset Management
- Využívaní výhradně výrobcem podporovaných klientských a serverových operačních systémů

6. Virtualizace

- Techniky serverové virtualizace s dostatečným počtem hypervisorů pro zajištění vysoké dostupnosti (2+N)
- SW řešení virtualizace se zajištěným servisem a právem na nové verze (záplaty)
- Virtualizace desktopů (VDI)

7. Ostatní vybavení organizace

- Koncové stanice a notebooky s pravidelným cyklem obnovy 5-7 let
- HW serverové technologie s pravidelným cyklem obnovy 6-8 let
- Technologie datových úložišť (NAS, SAN) na bázi SAS a SATA disků s pravidelným cyklem obnovy 6-8 let.
- Technologie datových úložišť (NAS, SAN) na bázi SSD disků s pravidelným cyklem obnovy 10 let.
- Zabezpečení klíčových technologií a dat proti nebezpečí požáru, záplavy, krádeže a přehřátí.

Případné připomínky a náměty k tomuto popisu optimální úrovně IT vybavenosti organizace adresujte vedoucím odboru informatiky KrÚ – it@kr-vysocina.cz