Příloha č. 3: Požadavky na implementaci díla obecně platné pro všechny PO

Požadavky na implementaci díla

Obecné požadavky

- Každé dodané zařízení bude označeno štítkem, který bude obsahovat identifikátor zařízení, případně IP adresu.

Firewall

- Upgrade firmware na poslední stable verzi.
- Defaultně musí být zakázána veškerá komunikace.
- Vzdálený přístup do organizace bude pouze přes VPN připojení.
- Definovat odchozí a příchozí komunikaci - externí a interní v rámci jednotlivých VLAN (subnetů).
- Definovat VLANy (minimálně v rozsahu):
    - Management prvků
    - Technologie
    - Servery
    - Tiskárny
    - Zaměstnanci, žáci (školy)
    - Stanice (učebny)
- Nastavení monitoringu a logování NAT (RFC 2663).
    - Monitoring základních funkcí jako dostupnost přes ICMP, vytížení CPU, RAM, provoz na jednotlivých interface.
    - Dostupnost internetové konektivity, dostupnost DNS serverů poskytovatele internetu.
    - Nastavení sběru logů na syslog + centrální server.
    - Nastavení SNMP pro monitoring.
- Přístup pouze z management sítě zabezpečeným protokolem - HTTPS, SSH.
- Nastavení funkcionalit NGF - IPS/IDS, web filtering, thread protection, AV control.
- Nastavení site-to-site IPSEC VPN včetně pravidel mezi sítěmi a povolení komunikace daných aplikací.
- Provedena záloha konfigurace.

Switch

- Upgrade firmware na poslední stabilní verzi.
- Minimálně 1 agregovaná trunk linka (2 fyzické spoje) směrem k firewallu a dalším switchům (síťovým prvkům).
- Nastavení stohu (stacku) mezi prvky v jednom racku (pokud to prvky umožňují).
- Přístup pouze z management sítě zabezpečeným protokolem - HTTPS, SSH.
- Nastavení VLAN dle segmentace sítě.
- 802.1X ověřování uživatelů oproti databázi účtů přes protokol radius (LDAP, MS AD, eduroam).
- Nastavení security minimálně v rozsahu - DHCP snooping, Switch port security, IP source guard, Allowed VLAN na trunkových linkách, Loopback protection.

- Nastavení sledování datových toků (Flow).
- Nastavení SNMP pro monitoring.
- Nastaven monitoring - ICMP, provoz na jednotlivých interface.
- Nastavení zasílání logů na Syslog server.
- Provedena záloha konfigurace.

Přístupový bod Wi-Fi

- Upgrade firmware na poslední stabilní verzi.
- Připojení prvků do Centrálního managementu WiFi AP.
- Zabezpečený management - HTTPS, SSH; management povolen pouze z interní sítě.
- IEEE 802.1X - ověřování uživatelů přes protokol radius (LDAP, MS AD, eduroam).
- Nastavení monitoringu jednotlivých AP, povoleno SNMP.
- Nastavení VLAN dle segmentace sítě.
- Nastavení zasílání logů na Syslog server.
- Nastavení izolace klientů.
- ACL filtrování provozu.
- Multi-SSID:
    - zaměstnanci
    - hosté
    - studenti (volitelné)
    - eduroam (volitelné)
- Podpora automatického rozložení zátěže klientů.
- Nastavení Roamingu mezi AP a automatické ladění kanálů a síly signálu včetně detekce a reakce na non-Wi-Fi rušení.
- Nastavení omezení pro Wi-Fi síť hostů, nutnost odsouhlasit podmínky přístupu k síti, omezení (rychlost in/out, povoleny protokoly HTTP, HTTPS, POP3S, IMAPS, SMTPS).
- Zpracovat mapu (model) pokrytí.

MS Active Directory

- Active Directory Domain Services (AD) role je nainstalována minimálně na Windows Server 2012 R2, instalováno do kontejneru s izolací Hyper-V.
- Nastavit Recycle Bin funkcionalitu pro rychlou obnovu smazaných objektů.
- Nastavit zálohování v pravidelných intervalech programem nativně podporující zálohu a obnovu AD databáze nebo jednotlivých AD objektů.
- Vytvořit účty pro každého Domain Administrátora pro správu AD.
- Vytvořit doménové účty pro uživatele (účty nebudou sdíleny mezi uživateli).
- Nastavit skupiny uživatelů.
- Nastavit službu Radius.
- Pro připojení k AD serveru vyžadováno LDAPS.
- V případě vytvoření Self-Signed Certifikátu může být použit OpenSSL.
- Stanice s operačním systémem Windows spravovány pomocí Group Policy s nastavením automatického zamknutí po 15 minutách neaktivity. *(GPO>Computer Settings>Windows Settings>Security Settings>Local Policy>Security Options>Interactive logon: Machine inactivity limit).*
- Politika hesel - minimální požadavky:
    - Vynucení komplexního hesla;
    - Délka hesla minimálně 8 znaků;

- Platnost hesla minimálně 1 den;
- Doporučená maximální doba platnosti hesla 12 měsíců;
- Uzamčení účtu po 10 neúspěšných pokusech o přihlášení.

Syslog Server:

- Instalací syslog serveru s napojením na centralizované řešení;
- Nastavení sběru logů ve formátu syslog;
- Nastavení šifrované komunikace mezi centrální instalací v TCK a instalací v organizaci.
- Nastavení archivace záznamů min. 2 měsíce;
- Nastavení vyhledávání informací v reálném čase i v historii - prohlížení logů z historie - filtrování událostí, alerty, reportovací funkce, sestavy bezpečnostních incidentů;
- Nastavení zasílání alertů a reportů na e-mail.
- Nastavení sběru dat ze všech prvků dodávaných v rámci řešení (firewally, switche, wifi, ...);
- Nastaven sběr logů ze všech interních serverů organizace.
- Parametry sběru dat:
  - Firewally, switche, Wi-Fi - logon, logoff, změna konfigurace, zablokování uživatelského účtu, 5x špatně zadaný login během 1 minuty,
  - Servery - logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa - čas - uživatel, logování chybových zpráv a bezpečnostních událostí.

Monitoring

- Implementace v jednotlivých organizacích instalací monitoring serveru s napojením na centralizované řešení v TCK Zlínského Kraje;
- Přístup uživatelů přes webové rozhraní zabezpečeným kanálem (HTTPS);
- Šifrovaná komunikace mezi organizací a centrálním řešením;
- Nastavení archivace záznamů min. 2 měsíce;
- Nastavení historie záznamů a jejich prohlížení;
- Nastavení zasílání alertů;
- Monitorována všechna dodaná zařízení minimálně v rozsahu:
  - Dostupnost přes ICMP (ping);
  - dostupnost managementu prvků- SSH, HTTPS, SNMP;
  - vytížení CPU, RAM;
  - využití disků;
  - u firewallu dostupnost internetové konektivity, DNS.

Centrální správa WiFi AP

- Instalace ve virtualizovaném prostředí VMware verze 6.5.
- Zabezpečený management - HTTPS, SSH.
- Připojení všech instalovaných organizací a všech instalovaných prvků.
- Nastavení rozdělení managementu po jednotlivých organizacích, přidělování práv na jednotlivé uživatele a organizace.
- Nastavení sběru logů, flow a monitoringu všech instalovaných zařízení.
- Nastavení alarmů a alertů.
- Provedena záloha konfigurace.

Datový rozvaděč (RACK)

- Instalace datového rozvaděče dle norem ČSN50173, ČSN50174.
- Zhotovení samostatně jištěného přívodu 230V, 16A, ukončeno dvěma zásuvkami (v souladu s předpisy ČSN).