Specifikace implementace - Komplexní řešení řízení přístupu k síti OU

Cílem požadovaného řešení je pokročilé řízení přístupu k síti OU pro zaměstnance, studenty, externí spolupracovníky, hosty, pro hosty organizací, kterým jsou pronajímány prostory OU včetně části síťové infrastruktury napojené na komerční konektivitu, a také pro speciální bezdrátová IoT zařízení.

Základním prvkem je využití standardního protokolu 802.1X v prostředí drátové sítě i bezdrátové Wi-Fi sítě pro ověřování zaměstnanců, studentů a externích spolupracovníků při přístupu do zaměstnanecké a studentské sítě. Naopak při přístupu do hostovských sítí je požadováno ověřování pomocí tzv. Captive Portal funkcionality. Další skupinou jsou zařízení typu IoT v prostředí Wi-Fi sítí, kde bohužel nelze využít obvyklé WPA Enterprise zabezpečení, zde je nutné implementovat ověřování individuálními klíči.
Je vyžadováno zvýšení zabezpečení datové sítě proti připojení neautorizovaných zařízení, řešení musí umožňovat přehledně identifikovat připojená zařízení a zamezit další komunikaci v případě jejich nestandardního chování.
Vzhledem k rozsahu sítě OU musí být řešení vysoce dostupné a škálovatelné, minimálně jako 2-uzlový klastr plně odolný proti výpadku jednoho uzlu, umožňující bezvýpadkovou údržbu.
Správa řešení musí být centralizovaná, přehledná, snadná, efektivní a flexibilní, aby bylo možné pružně reagovat na měnící se potřeby sítě, zároveň uživatelům nabídnout patřičný komfort a také usnadnit práci správcům sítě a technikům IT bez kompromisů v zabezpečení.
Dalším neméně důležitým parametrem je podpora vícefaktorového ověřování a podpora tzv. endpoint klientů, která umožní další zvyšování zabezpečení sítě OU.

Součástí dodávky musí být následující služby

- Analýza – účastník provede v rámci realizace díla vstupní analýzu a vytvoří „Implementační plán projektu“. Součástí tohoto plánu projektu bude technický popis řešení, vč. finální podoby implementace (nastavení) dodávaného řešení, testovacího scénáře, harmonogramu realizace projektu, potřebných instalačních postupů a požadavků na zajištění součinnosti.
- Konzultace a schválení plánu – v rámci konzultací mezi účastníkem a zadavatelem bude upřesněn či upraven implementační plán dle potřeb zadavatele. Další kroky bude účastník provádět po schválení implementačního plánu zadavatelem.
- Instalace – účastník zrealizuje dodávané řešení do prostředí Zadavatele ve shodě s Implementačním plánem projektu a s ohledem na infrastrukturu Zadavatele.
- Implementace – účastník provede potřebnou konfiguraci a nastavení celého systému pro přístup do sítě
- Testování – účastník zajistí řádné otestování řešení dle navržených testovacích scénářů v Implementačním plánu projektu
- Dokumentace – je vyžadována v následujícím rozsahu (pokud není uvedeno jinak, tak v českém jazyce):
    - Implementační plán projektu, vč. popisu architektury řešení a finální konfigurace
    - Produktová dokumentace výrobce ke všem dodávaným modulům v českém nebo anglickém jazyce
    - Instalační dokumentace a dokumentace k integrovaným systémům
    - Administrátorské a uživatelské příručky (manuály), uživatelské příručky budou v českém i anglickém jazyce
    - Metodiky / postupy pro běžné administrátorské úkony potřebné pro správu dodávaného řešení, včetně odhadu potřebného FTE pro jejich plnění
- Zaškolení administrátorů – v prostorách Zadavatele v českém jazyce

Minimální rozsah implementačních prací je (dále specifikováno podrobněji):

- Definice bezpečnostních politik a přístupových pravidel (včetně pravidel pro zařízení, které se ověřují jen pomocí MAC adresy)
- Identifikace zařízení a uživatelů, kteří se budou ověřovat v rámci NAC
- Součinnost při segmentací sítě (VLAN) v rámci nasazení NAC
- Instalace virtuálních serverů do prostředí Zadavatele a součinnost při nastavení síťového prostředí včetně prostupů ve firewallu
- Konfigurace politik pro přístup do sítě
- Součinnost v rámci nastavení suplikantů na koncových stanicích
- Součinnost v rámci integrace s adresářovými službami zadavatele (Microsoft Active Directory (AD), OpenLDAP)
- Testování a validace:
    - Testování kontrol přístupu a compliance s různými typy zařízení.
    - Validace správné funkčnosti a bezpečnosti.
- Vytvoření konfiguračních profilů koncových zařízení s OS MS Windows, Android, MacOS/iOS, Linux (provisioning)

Minimální požadavky na implementaci:

- Předimplementační analýza, zhodnocení výsledků a zapracování do implementačního plánu projektu
    - vytvoření autentizačních scénářů
    - vytvoření postupů pro připojování uživatelů a stanic
    - vytvoření postupů pro zotavení z chybových stavů uživatelů a stanic
    - návrh integrace se stávající síti OU
    - korekce implementačního postupu
- Dodání všech potřebných komponent, hardware, software, licencí, supportu, tak aby dodávané řešení splňovalo veškeré požadavky.
- Instalace ve virtualizovaném prostředí hostovaném na různých platformách
    - specifikace požadavků na zdroje
    - 1. uzel VMWare
    - 2. uzel KVM/Proxmox
- Instalace potřebných licencí, aktualizací a patchů
    - licence musí zahrnovat všechny zde zmiňované vlastnosti a funkce NAC
- Základní systémová konfigurace
    - konfigurace IPv4 a IPv6 adresy, masky, brány
    - konfigurace DNS serverů
    - konfigurace NTP serverů
    - konfigurace SMTP serverů
    - konfigurace HTTPS grafického rozhraní kompatibilního s prohlížeči Google Chrome, Firefox, Safari, Microsoft Edge
    - konfigurace rozhraní příkazové řádky, SSH
    - konfigurace logování na 2 Syslog servery - zasílání veškerých logů
    - konfigurace zálohování konfigurace NAC na externí server
    - konfigurace veřejných SSL certifikátů a CA
    - blokace nezabezpečených a nepotřebných protokolů, služeb
- Konfigurace systému vysoké dostupnosti - High Availibility, minimálně v režimu Active-Passive
- Konfigurace self-monitoringu NAC, triggerů, odesílání notifikací prostřednictvím SMTP
- Konfigurace monitoringu NAC, jeho nejdůležitějších komponentů prostřednictvím webového API, SNMP či skriptů z externích monitorovacích systémů Nagios a Zabbix
    - síťová dosažitelnost IPv4 a IPv6
    - využití RAM
    - využití CPU
    - místo na disku

    - funkčnost databáze
    - funkčnost napojení na externí autentizační zdroje LDAP, AD, SQL
    - funkčnost RADIUS serveru, ověření RADIUS dotazem
    - platnost SSL certifikátů
    - existence aktualizace
- Konfigurace administrátorských účtů s různými úrovněmi oprávnění
    - host – kontrola průběhu ověření a registrace
    - operátor – zřizování hostovských účtů, registrace MAC, registrace stanic
    - administrátor – pokročilá správa účtů, registrací, BYOD
    - superadmin – kompletní správa NAC
- Konfigurace generování záznamů o činnosti systému, ověřování, účtovacích informací
- Konfigurace generování základních statistik a reportů, jejich pravidelné zasílání emailem
- Konfigurace propojení s LDAP servery OU
    - OpenLDAP servery OU
    - AD servery OU včetně zařazení do MS Windows domény
- Konfigurace propojení NAC se síti OU
    - management VLAN
    - registrační VLAN
    - izolační VLAN
    - VLAN – OU zaměstnanci
    - VLAN – OU studenti
    - VLAN – OU hosté
    - VLAN – OU technologie
    - VLAN – OU support
    - VLAN – komerční hosté
- Konfigurace RADIUS serveru a klientů
    - Authentication + Authorization + Accounting
    - Change of Authority
    - dodání šablon konfigurace RADIUS klientů
        - WLC kontroléry Aruba 7210, 7205
        - switche Aruba CX 6300, 6200, 6100, 6000
        - switche Aruba 2530
        - switche HPE 5510, 5500
        - switche HPE 5130, 5120
        - switche HPE 1920, 1910
        - switche Cisco 2960, 2960G
    - metody ověřování
        - 802.1x
        - MAC autentizace
        - Captive Portal
    - priorita metod ověřování a způsobů přístupu k síti
        1. 802.1x
        2. MAC autentizace
        3. Guest VLAN
        4. Critical VLAN
- Konfigurace ověřování v zaměstnanecké síti (OU zaměstnanci)
    - všichni zaměstnanci OU
    - na drátové síti se zachováním access VLAN dané konfigurací switche
    - vyhrazená WiFi sít, samostatné SSID, zabezpečení WPA2/3 Enterprise
    - autentizační zdroj AD, OpenLDAP
    - autentizační protokol EAP-TLS, EAP-PEAP, EAP-TTLS

    - včetně autentizace stanic s MS Windows v doméně – Machine Authentication
    - pouze známé stanice (známé MAC), pokud stanice není v MS Windows doméně
    - v případě neúspěšného ověření přepnutí na self-service portál s možností stáhnout konfigurační profil pro připojení k síti
    - jakékoliv stavové informace jsou platné pouze pro danou síť
- Konfigurace ověřování ve studentské síti (OU studenti)
    - všichni zaměstnanci OU, studenti OU, externisté OU
    - vyhrazená WiFi sít, samostatné SSID, zabezpečení WPA2/3 Enterprise
    - autentizační zdroj AD, OpenLDAP, lokální databáze
    - autentizační protokol EAP-TLS, EAP-PEAP, EAP-TTLS
    - v případě neúspěšného ověření přepnutí na self-service portál s možností stáhnout konfigurační profil pro připojení k síti
    - jakékoliv stavové informace jsou platné pouze pro danou síť
- Konfigurace ověřování v hostovské síti pro hosty OU (OU hosté)
    - všichni zaměstnanci OU, studenti OU, externisté v OpenLDAP, hosté OU
    - vyhrazená WiFi sít, samostatné SSID, otevřená síť
    - autentizační zdroj AD, OpenLDAP, lokální databáze
    - ověření přes Captive Portal (instance 1, odlišná od instance 2)
        - uživatelské jméno a heslo v OpenLDAP
        - SMS s PINem na zadané telefonní číslo hosta
        - voucher kód
        - schválení sponzorem OU
        - externí ověření: eduID
    - jakékoliv stavové informace jsou platné pouze pro danou síť
- Konfigurace ověřování v technologické síti (OU technologie)
    - speciální technologická zařízení, která nepodporují WPA2/3 Enterprise
    - vyhrazená WiFi sít, samostatné SSID, zabezpečení WPA2/3-MPSK
    - autentizační zdroj lokální databáze
    - jakékoliv stavové informace jsou platné pouze pro danou síť
- Konfigurace ověřování v podpůrných drátových sítích (OU support)
    - speciální koncové stanice OU (tiskárny, MaR, UPS, kamery apod.)
    - obvykle nepodporují 802.1X
    - autentizace pomocí MAC
    - autentizační zdroj lokální databáze
    - jakékoliv stavové informace jsou platné pouze pro danou síť
- Konfigurace ověřování v hostovské síti pro komerční hosty skrze komerční konektivitu (komerční hosté)
    - komerční hosté
    - vyhrazená WiFi síť, samostatné SSID, otevřená síť
    - autentizační zdroj lokální databáze
    - ověření přes Captive Portal (instance 2, odlišná od instance 1)
        - SMS s PINem na zadané telefonní číslo hosta
        - voucher kód
        - externí ověření: MojeID, Google, Facebook, MicroSoft
    - jakékoliv stavové informace jsou platné pouze pro danou síť
- Konfigurace TACACS+ serveru a klientů
    - plná podpora Aruba CX VSF/VXF switchů
    - dodání šablon konfigurace TACACS+ klientů
        - WLC kontroléry Aruba 7210, 7205
        - switche Aruba CX 8325
        - switche Aruba CX 6300, 6200, 6100, 6000
        - switche HPE 5710, 5700

        - switche HPE 5510, 5130
        - switche HPE 5500, 5120
        - switche Aruba 3810, 2530
        - switche HPE 1920, 1910
        - switche Cisco 2960, 2960G
- Konfigurace konfiguračních profilů pro připojení k dané síti pro dané OS:
    - MS Windows 11 mimo doménu (User Authentication)
    - MS Windows 11 v doméně, dodání šablony nastavení GPO, Machine x User ověřování
    - Android
    - MacOS/iOS
    - Linux(Ubuntu)
- Konfigurace příkladu vlastní privátní certifikační autority
    - vytvoření CA a uživatelských certifikátů
- Konfigurace příkladu lokálních uživatelských účtů
- Vzorová konfigurace stanic
    - stanice s OS MS Windows mimo doménu
    - stanice s OS MacOS/iOS
    - stanice s OS Android
    - stanice s OS Linux
- Konfigurace napojení na SMS bránu skrze webové API
- Konfigurace samoobslužného portálu a Captive Portal (CP)
    - dodání šablon podpůrné konfigurace WLC a switchů
    - komunikace protokolem HTTPS
    - redirect z HTTP na HTTPS
    - automatická detekce CP v prohlížeči
    - automatický redirect po úspěšném přihlášení na definované URL
    - funkční grafické rozhraní v prohlížečích
        - Google Chrome
        - Firefox
        - Microsoft Edge
        - Safari
    - jazykové mutace portálu dle nastavení prohlížeče
        - česky
        - anglicky
    - přizpůsobení vzhledu a funkcionality CP individuálně pro hostovskou síť OU a pro komerční hostovskou síť
    - vynucení akceptace podmínek užití dle jazyku CP
    - komunikace v SMS či emailu s hostem dle jazyku CP
    - ověření pomocí SMS s PINem na zadané telefonní číslo hosta
    - ověření pomocí emailu sponzorovi z OU z AD, OpenLDAP, lokální databáze
    - ověření pomocí voucheru, automatizace vydávání voucherů elektronicky i v tištěné podobě, generování QR kódu
    - ověření pomocí externího zdroje: EduID, MojeID, Google, Facebook, X, MicroSoft
    - omezení platnosti hostovské registrace dle kontextových informaci
        - časové délky, např. 10 dní
        - časového rámce, např. od-do
        - objemu přenesených dat, např. 1GB
        - počtu přihlášení, např. max. 3 přihlášení
- Konfigurace příkladu vícefaktorové autentizace
- Konfigurace příkladu webového API pro jednoduchou webovou aplikaci, která bude umožňovat

    - zřízení hostovského účtu s ověřením pomocí voucheru s rozlišením pro hosty OU a pro komerční hosty
    - registrace zaměstnaneckých stanic v OU zaměstnanci
- Konfigurace klasifikace připojovaných stanic
- Konfigurace detekce anomálního chování stanice při ověřování a registraci, přepojení do karantény, izolace v izolační VLAN
- Akceptační testy
    - akceptační testy dle jednotlivých bodů specifikace implementace
    - testy neočekávaných výpadků
        - přechod na sekundární server do 10s
        - přechod zpět na primární server po zotavení z výpadku – bezvýpadkově
    - testy dopadu ručního vypnutí nebo aktualizace jednoho uzlu v clusteru na provoz – bezvýpadkově
    - testy vzdáleného přístupu na stanici RDP, VNC
    - testy odesílaných dat mimo síť OSU
        - systém jako celek nesmí bez plné kontroly provozovatele předávat jakákoliv data, např. telemetrie
        - systém jako celek nesmí bez plné kontroly provozovatele umožnit lokální nebo vzdálený přístup, např. automaticky připojované asistenční služby
    - provozní testy na vybraných skupinách koncových stanic
    - provozní testy na vybraných skupinách síťových prvků
    - provozní testy na vybraných skupinách uživatelů AD, OpenLDAP
    - provozní testy všech daných sítí
- Dokumentace skutečného provedení v českém jazyce
- Zaškolení administrátorů OU v rozsahu min. 8h, vytvoření základních návodů pro administrátory v českém jazyce
- Zaškolení techniků OU v rozsahu min. 4h, vytvoření základních návodů pro techniky v českém jazyce