**Příloha č. 2 - Technická specifikace řešení řízení přístupu do sítě LAN**

V současné době není v datové síti objednatele implementováno řešení pro ochranu síťových segmentů. Objednatel požaduje, aby zhotovitel navrhl řešení, které splňuje požadavky současných bezpečnostních požadavků.

Objednatel požaduje dodat a naimplementovat nástroj, který zajistí správu a zabezpečení přístupu zařízení k lokální síti a vytváření bezpečnostních politik. Ta, aby znemožnilo přístup neoprávněných osob a vzniku případných škod z hlediska úniku dat či poškození systému.

**Popis**

Cílem celého řešení je v budoucnu zajistit zabezpečený a kontrolovaný přístup zařízení do lokální sítě a umožnit z centrálního místa řídit politiky pro jednotlivé skupiny zařízení a uživatelů. Tento proces 2 bude založen na připojení koncových zařízení a konkrétních uživatelů na základě autentizace (rozpoznání identity zařízení a uživatele) a autorizace (zpřístupnění konkrétních datových zdrojů podle uživatelské role, stavu koncového zařízení) a dalších atributů v rámci kontextu uživatele.

Integrované funkce zajišťují komunikaci s AAA serverem (RADIUS) a nastavují komplexní, přitom unifikované, bezpečnostní politiky pro autentizaci a autorizaci koncových bodů.

Řešení musí zajistit, že bezpečný přístup k chráněným datům bude zajištěn pouze uživatelům, kteří na něj mají na základě daných politik nárok. Toto řízení je založeno na přidělených, předem definovaných, rolích uživatelů, kterými jsou všichni zaměstnanci, dodavatelé a další skupiny uživatelů, jejichž identita je vždy jednoznačně ověřena.

Správa bezpečnostních opatření vyžaduje, aby se zjednodušila administrace bezpečnostních politik, což umožní jejich jednotné uplatňování napříč sítí. To zahrnuje kontrolu nad politikami pro přístup v LAN, WLAN sítích (včetně přístupu pro hosty), přes VPN a potenciálně i 5G sítě pro IoT. Při vytváření těchto politik systém vezme v úvahu řadu faktorů, jako jsou identita uživatele, skupina, kde pracuje, umístění, čas, typ připojeného zařízení atd. V závislosti na těchto faktorech budou stanoveny různé úrovně přístupových práv, které se promítnou do nastavení politik.

Je také nezbytné, aby systém umožňoval flexibilní přesun komunikace koncových zařízení do různých segmentů práce nebo do karantény, a to na základě dynamické aplikace přístupových filtrů prostřednictvím procesu změny autorizace (CoA), což je proces definovaný v RFC protokolu RADIUS, založený na analýze aktuálních vstupních dat jako jsou typ a stav zařízení.

Rozšiřitelnost systému by měla zahrnovat také řízení bezpečného přenosu dat skrze síť, včetně šifrování na rozhraních přepínačů, a schopnost uplatňovat filtraci přístupů na základě bezpečnostních rolí uživatelů.

Centrální komponenty pro správu bezpečnosti, které jsou propojeny s externími autentizačními databázemi, jako je AD nebo LDAP, by měly podporovat aplikaci bezpečnostních politik i na další zařízení, jako jsou firewally, na základě identit uživatelů nebo jejich skupinových rolí.

Klíčové je zajistit vysokou dostupnost celého systému, včetně jeho redundance, centrální správy a dohledu, a také možnosti analýzy a reportování událostí z jediného místa.

**Technické specifikace**

Následuje seznam technických specifikací, které jsou minimálně vyžadovány a je s nimi počítáno i pro případné další rozšíření bezpečnostního řešení formou nákupu vyšších licencí. Dodané řešení musí podporovat tyto funkce již v základní verzi a je možné je implementovat postupně.

| Specifikace minimálních požadavků | Splněno [ano/ne] | Poznámka |
|---|---|---|
| **Obecná charakteristika ověřovacího řešení** | ANO | |
| Centralizovaný systém pro ověřování uživatelů, klasifikaci zařízení, řízení přístupu k síti a guest přístup definující pravidla přístupu k síti v závislosti na kontextu připojení (uživatel, typ zařízení, stav zařízení, místo připojení apod.). | ANO | |
| Ve spolupráci s aktivními prvky (LAN přepínači, bezdrátovými AP nebo řídícími moduly, VPN branami) poskytuje ochranu před neoprávněným přístupem k pevné LAN síti, bezdrátové wifi síti (metodou 802.1x) a pro VPN přístup. | ANO | |
| V rámci ekosystému vytvořenému pomocí integrační platformy musí být možno použít adaptivní řízení síťových prvků organizace, které umožnuje rychle reagovat na útoky metodou přímého využití sítě jako vynucovacího prostředku (konkrétní scénáře odpojení uživatele). V praxi toto může znamenat odpojení problematického koncového zařízení přímo od rozhraní LAN přepínače nebo od WiFi přístupového prvku na základě signalizace od detekčního bezpečnostního systému umístěného uvnitř sítě. | ANO | |
| Integrace s NGFW, kde nástroj pro kontrolu přístupu do sítě na základě sdílených informací může infikované koncové zařízení pozorovat, omezit jim přístup, nebo napomoci v remediačním procesu. | ANO | |
| Poskytuje AAA funkce (viz níže). | ANO | |
| Podporuje klasifikaci připojených zařízení a řízení přístupu na základě této klasifikace (Network Admission Control). | ANO | |
| Podporuje centralizované nebo distribuované nasazení pro vysokou odolnost a rozšiřování capacity. | ANO | |
| Umožňuje snadné zálohování, rychlou a úplnou obnovu konfigurace. | ANO | |
| Je dostupné ve formě Appliance (hardware i software podporovaný jedním výrobcem). | ANO | |
| Je dostupné ve formě Virtuálního stroje na platformách Vmware, Linux KVM a Microsoft Hyper-V. | ANO | |
| Je dostupné ve formě cloudového řešení (AWS, Azure, Oracle). | ANO | |
| **AAA funkce (ověřování, autorizace a záznamy o průběhu připojování uživatelů a zařízení k síti)** | ANO | |
| ***Podporované protokoly*** | ANO | |
| RADIUS pro autentizaci, autorizaci a accounting | ANO | |
| proxy funkce pro externí RADIUS | ANO | |
| PAP, MS-CHAP, MS-CHAPv2, EAP – MD5, Protected EAP (PEAP), EAP-TLS, EAP-TTLS, EAP-FAST, EAP-TEAP | ANO | |
| podpora TACACS+ pro centrální řízení administrativního přístupu na zařízení | ANO | |
| ***Podporované databáze uživatelů (s možností definovat pořadí autentizace*** | ANO | |
| Interní (pro uživatele i koncová zařízení) | ANO | |
| Active Directory – více nezávislých domén | ANO | |
| Azure Active Directory | ANO | |
| LDAP (RFC 2251) | ANO | |
| RADIUS Token indentity source (RFC 2865) | ANO | |
| RSA RADIUS token server | ANO | |
| Autentizace pomocí údajů obsažených v certifikátu | ANO | |
| ***Ověřování uživatelů a zařízení*** | ANO | |
| Ověření uživatelů/zařízení heslem nebo certifikátem (různé kombinace) | ANO | |
| Ověření MAC adresou připojovaného zařízení | ANO | |

| Specifikace minimálních požadavků | Splněno [ano/ne] | Poznámka |
|---|---|---|
| ***Autorizace: pružný systém pro definici pravidel pro přístup k síti*** | ANO | |
| Řízení přístupu k síti pomocí filtrů nebo přiřazením do VLAN sítě podle<br>• uživatele (role, skupiny),<br>• stavu a typu koncového zařízení (viz výše),<br>• místa připojení,<br>• historie připojení | ANO | |
| Omezení přístupu k síti pomocí filtrů aplikovaných na vstupu do sítě | ANO | |
| Omezení přístupu k síti pomocí filtrů aplikovaných na výstupu ze sítě | ANO | |
| Podpora Change of Authorization (CoA, RFC 3576) pro změny vynucovaných politik „za běhu“ | ANO | |
| Možnost jednoduše identifikovat/označit přenášená data uživatele (rámce) v chráněné oblasti | ANO | |
| Řízení autentizace a založení důvěryhodné infrastruktury mezi jednotlivými prvky sítě, pro bezpečný a šifrovaný transport dat | ANO | |
| ***Accounting*** | ANO | |
| Zaznamenávání aktivity uživatelů a zařízení připojených k síti | ANO | |
| Dotazovací systém, korelace záznamů, centralizované výkazy | ANO | |
| Systém pro sledování výstrah (úspěšná/neúspěšná přihlašování, neaktivita, stav systému AAA, dostupnost externích databází, aktivita filtrů) | ANO | |
| ***Funkce GUEST serveru*** | ANO | |
| Vytváření časově omezených oprávnění pro přístup k síti nebo do internetu pro hosty, externí spolupracovníky apod. ve fixních LAN i WiFi | ANO | |
| Oprávnění přidělovaná správcem přístupu přes portál pro snadné vytváření dočasných účtů | ANO | |
| Samoobslužný portál pro uživatele | ANO | |
| Ověření přes HTTP a HTTPS | ANO | |
| Rozhraní pro integraci s externími operátory pro zasílání SMS zpráv s autentizačními údaji | ANO | |
| Propojení s email serverem pro zasílání Guest účtu | ANO | |
| ***Rozpoznávání typu koncových zařízení a jejich stavu*** | ANO | |
| Automatické rozpoznávání a klasifikace připojených zařízení (PC, telefonů, tabletů, mobilních telefonů apod.) ve spolupráci se síťovou infrastrukturou | ANO | |
| Předdefinované profily pro běžná mobilní zařízení (zařízení s OS Android, Apple, a další) | ANO | |
| Předdefinované profily pro síťová zařízení NAD od různých vendorů | ANO | |
| Podpora pro IPv6 koncová zařízení | ANO | |
| ***Podpora BYOD*** | ANO | |
| Onboarding (registrace, provisioning, nastavení klientských zařízení) | ANO | |
| Onboarding/provisioning proces formou samoobsluhu | ANO | |
| Specifické politiky pro BYOD zařízení | ANO | |
| Možnost nastavení limitu BYOD zařízení pro jednoho uživatele | ANO | |
| Interní CA, pro vydávání certifikátů BYOD zařízením | ANO | |
| Interní CA lze řetězit jako subordinate pod firemní CA | ANO | |
| ***Podpora MDM*** | ANO | |
| Workflow pro registrace do MDM | ANO | |
| Výměna informací z MDM platformy a využití v politikách (např. pokud zařízení je „compliant“) | ANO | |
| Ovládání MDM přímo z prostředků bezpečnostního managementu (zamykání, mazání, apod.) zařízení | ANO | |
| Uživatelská samoobsluha přes web portál (např. zamknutí přístupu pro ztracené zařízení) | ANO | |
| ***Rozpoznávání stavu koncových zařízení a jeho náprava*** | ANO | |
| Ověření stavu koncových zařízení pomocí softwarovéha agenta nebo web agenta na koncovém zařízení. Systém musí rozpoznat:<br>· instalovaný operační systém<br>· opravy instalované v operačním systému | ANO | |

| Specifikace minimálních požadavků | Splněno [ano/ne] | Poznámka |
|---|---|---|
| · verze instalovaných programů<br>· hodnoty položek v registry databázi systémů Windows<br>· stav aplikací, zajména antivirů, antispyware, antimalware a firewall | | |
| Ověření stavu koncových stanic pomocí skriptů PowerShell (WIN), nebo shell (MacOS, Linux) | ANO | |
| Spolupráce na uvedení stanic do požadovaného stavu (informací, odkazem,spuštěním programu, aktualizací antiviru, aktualizací OS, stažením souboru) | ANO | |
| ***Další vlastnosti*** | ANO | |
| Aktivace šifrování MACSec (IEEE 802.1ae) pro připojená zařízení (pokud MACSec podporují) | ANO | |
| Možnost vyčítání informací o uživateli z Active Directory (Passive Fingerprint) nebo z logů jiných síťových zařízení | ANO | |
| Podpora SXP (Exchange Protocol) dle IETF | ANO | |
| Otevřené API pro podporu propojení se zařízeními třetích stran | ANO | |
| **Funkce pro správu ověřovacího systému** | ANO | |
| Centralizovaná správa | ANO | |
| Definice rolí administrátorů a úrovní přístupu k ověřovacímu systému | ANO | |
| Zjednodušení správy vytvářeními skupin uživatelů, koncových a síťových zařízení | ANO | |
| Grafické rozhraní pro definici pravidel přístupu k síti | ANO | |
| Grafické rozhraní pro monitorování, definici výkazů, řešení problémů | ANO | |
| Diagnostika problémů (systémová, údaje o chybách přihlašování, TCP dump, packet capture) | ANO | |
| Zaznamenávání událostí na externí syslog server | ANO | |
| Čtení monitoring dat pomoci analytických aplikací třetích stran (PowerBI, Tableau, Kibana) | ANO | |
| Podpora SNMPv3 | ANO | |
| NTP pro synchronizaci času | ANO | |
| SMTP pro zasílání zpráv a výstrah přes e-mail | ANO | |

Součástí dodaného řešení je nezbytný hardware pro běh celého systému formou dedikované fyzické Appliance v režimu vysoké dostupnosti Active/Active. Dodaný HW musí zvládnout ověřování pro cca 1300 zařízení v rámci implementace s rezervou pro možné rozšíření až na cca 8000 zařízení. V první fázi implementace je počítáno pouze se základním ověřováním uživatelů a zařízení do sítě LAN, a poskytnutí Guest portálu pro mobilní zařízení.

Nezbytnou součástí nabídky musí být vypracování dokumentace o současném stavu prostředí (analýza prostředí) s doporučeními a postupem implementace řešení. Součástí dokumentace bude i popis celého nabízeného řešení s ohledem na současný stav prostředí a na požadované funkcionality. Na základě této analýzy bude možné odhadnout náročnost implementace řešení a naplánovat jednotlivé kroky implementace.

Součástí nabídky musí být implementační práce spojené s instalováním fyzických serverů a jejich uvedením do prostředí, implementace a nastavení politik vydefinovaných v dokumentaci z analýzy prostředí a vytvoření dokumentace o implementovaném řešení.

V rámci předání díla musí dodavatel zajistit potřebné školení pro min. 2 zaměstnance objednatele v rozsahu vzájemně odsouhlasené best-practices.

Součástí předání díla musí dodavatel zajistit provedení testovacích procedur a seznámit objednatele s jejich úspěšným provedením.

Na poskytnuté řešení musí být poskytnuta záruka a podpora výrobce v délce 24 měsíců.