Specifikace technických požadavků pro potřeby zadávací dokumentace VZ

Předmět VZ: „Nasazení systému pro ověřování a řízení přístupu uživatelů, síťových zařízení ke komunikační síti MěÚ Litomyšl“

Projekt: „Zavedení nástrojů kybernetické bezpečnosti MěÚ Litomyšl“,

NPO, výzva č. 41, Kybernetická bezpečnost – obce

Dílčí výstup: „Network Access Control (NAC) - RADIUS server (IEEE standard 802.1x)“

Obsah

[1 Předmět veřejné zakázky 3](#_Toc196899306)

[2 Technické požadavky NAC 4](#_Toc196899307)

[3 Požadavky na dodávku a podporu NAC 6](#_Toc196899308)

[4 Požadavky na Výrobce a Uchazeče 8](#_Toc196899309)

[5 Požadovaná struktura nabídky 9](#_Toc196899310)

# Předmět veřejné zakázky

Dodávka a zprovoznění systému NAC (Network Access Control) – Network Access Serveru (NAS) neboli RADIUS serveru, zajišťujícího ověřování a řízení přístupu uživatelů, síťových zařízení (klientů) ke komunikační síti MěÚ Litomyšl.

NAC (RADIUS server) bude umístěn a zprovozněn v serverovně, v budově MěÚ Litomyšl, Bří Šťastných 1000, Litomyšl.

# Technické požadavky NAC

|  |  |
| --- | --- |
| **Kategorie požadavků** | **Požadavky** |
| Služby, funkce | Autentizace a autorizace uživatele, síťového zařízení (síťového klienta) při přístupu k (bez)drátovým, virtuálním nebo VPN sítím.  Autentizace a autorizace klienta RADIUS protokolem splňující aktuálně platné standardy IETF RFC.  Autentizace a autorizace klienta protokolem IEEE 802.1X.  Metody pro autentizaci klienta:   * PEAP-MSCHAPv2, * EAP-TLS, * EAP-TTLS, * MAC.   Podpora autentizace a autorizace pomocí dalších externích zdrojů   * LDAP, * MS AD, * Token, * MAC auth, * generické SQL databáze, * HTTPS web autentizace.   Podpora Single Sign-On autentizace, minimálně pomocí:   * SAML 2+ IdP a SP, * OAuth.   Podpora vícefaktorové autentizace (Multifactor Authentication – MFA), minimálně pomocí   * HW / SW tokeny (HOTP, TOTP, OATH), * bezpečnostní klíče (FIDO2, FIDO U2F), * e-mail, SMS tokeny, * X.509 certifikáty, * PUSH notifikace.   Podpora autorizace uživatelů na základě kontextových informací jako čas, místo připojení, osobní profil či skupina v AD.  Podpora TACACS+ autentizace.  Automatická správa registrace a obnovy přístupu samotnými uživateli.  Příjem a zpracovávání hlášení (záznamů událostí) z externích zdrojů, vyhledávání klíčových událostí a automatizované reakce na ně.  RESTful API pro zpracování autentizační, autorizační událostí, událostí zaslaných z externích zdrojů a konfiguraci, správu systému.  Zálohování / obnova nastavení systému a spravovaných el. identit a jejich přístupových oprávnění a práv.  Integrace s systémy MDM (Mobile Device Management) třetích stran.  Integrace se systémy ServiceDesk, HelpDesk třetích stran.  Integrace, předávání logů a auditních záznamů LM systémům, SIEM a SOC. |
| Provedení, způsob nasazení | Bezpečný, sofistikovaný systém s jednotným, přehledným, uživatelsky srozumitelným rozhraním, využívající proprietární nebo komerčně podporované open-source technologie, jejichž výrobci, dodavatelé zaručují jejich dlouhodobý (min. po dobu 5 let), udržitelný rozvoj a podporu, zahrnující vydávání opravných a bezpečnostních balíčků a aktualizací.  Virtuální zařízení (jak pro Hyper-V, tak VMware).  Časově neomezená nebo dlouhodobá (min. 5 let) licence pro provoz všech požadovaných komponent a funkcí systému. |
| Rozšiřitelnost, škálovatelnost | Škálovatelný, snadno rozšiřitelný systém umožňující navyšovaní počtu připojovaných koncových zařízení uživatelů minimálně o třetinu požadovaného počtu.  HA cluster typu active/active, příp. active/passive. |
| Konektivita | Min. 2x Virtual Network Interface (VIF) |
| Kapacita, výkon, parametry | Min. počet síťových klientů (uživatelů, zařízení): 300. *(200 interní + 2x22 externí + 6 rezerva)*  Min. počet uživatelů ověřovaný 2FA: 50. *(3 interní + 2x22 externí + 3 rezerva)* |
| Bezpečnostní parametry | Bezpečné (šifrované) ukládání konfigurace, identit a přístupových práv.  Bezpečný (šifrovaná komunikace, AAA, 2FA) přístup (přes CLI nebo web GUI) ke správě a konfiguraci systému.  V případě webové aplikace pro správu systému použití HTML5 s minimálním využitím dalších technologických doplňků a komponent na straně klienta, splňující OWASP Top 10 Client-Side Security Risks. |

# Požadavky na dodávku a podporu NAC

|  |  |
| --- | --- |
| **Kategorie požadavků** | **Požadavky** |
| Dokumentace Výrobce | Technický popis (specifikace) systému.  Instalace (nasazení) systému.  Administrace systému.  Údržba systému. |
| Dokumentace vypracovaná Uchazečem | Předimplementační analýza.  Instalační (implementační) dokumentace systému.  Provozní dokumentace (implementovaného) systému.  Příručka administrátora systému (v českém jazyce).  Příručky pro uživatele (klienty) systému (v českém jazyce). |
| Technická podpora Výrobce | Opravy chyb a závad systému.  Řešení problému vzniklých při konfigurací služeb a funkcí.  Vydávání aktualizací systému s opravenými chybami a závady systému.  Vydávání bezpečnostních aktualizací a záplat systému.  Doba trvání podpory min. 5 let. |
| Technická podpora Uchazeče | Opravy chyb a závad způsobených implementací  Opravy chyb a závad zjištěných během provozování systému.  Změny konfigurace služeb a funkcí systému v důsledku změn ICT infrastruktury.  Řešení provozních problémů systému.  Provádění aktualizací (update, případně upgrade) a záplat systému.  Doba trvání podpory min. 5 let. |
| Podmínky SLA  (Service-Level Agreement) | Hlášení chyb a závad nepřetržitě v režimu 5 dní v týdnu x 12 hodin, a to buď elektronicky, telefonicky přes helpdesk Uchazeče, nebo zasláním na jeho e-mailovou adresu.  Zahájení řešení problému do 12 hodin od okamžiku nahlášení.  Vyřešení chyby nebo závady, bránící systému poskytovat požadované služby a funkce, nebo je omezuje, příp. degraduje, do 24 hodin.  Vyřešení chyby nebo závady, která nedegraduje systém a neomezuje jeho služby a funkčnost, do 5 pracovních dnů. |
| Záruka poskytovaná Uchazečem | Rozšířená záruka na dílo min. 5 let. |

# Požadavky na Výrobce a Uchazeče

|  |  |
| --- | --- |
| Výrobce | Proces bezpečného vývoje softwaru (aplikací).  Podpora systému min. po dobu 5 let, zahrnující opravné a bezpečnostní aktualizace všech SW komponent a aktualizace stávajících, vylepšených a nových služeb a funkcí systému.  Min. 5 let působení na trhu v oblasti poptávaného systému. |
| Uchazeč | Partner Výrobce (vendora).  Detailní, prokazatelná znalost licencování a procesů spojených s vendorem a prodejem jeho produktů.  Detailní, prokazatelná znalost produktů a návrhu architektury řešení.  Detailní, prokazatelná znalost instalace, implementace řešení.  Prokazatelné zkušenosti s implementací a zajištěním technické podpory (správy a provozu) nabízeného řešení.  Technická podpora produktu v českém jazyce. |

# Požadovaná struktura nabídky

|  |  |
| --- | --- |
| 1. | Popis nabízeného řešení zohledňující požadavky Zadavatele. |
| 2. | Popis jednotlivých zařízení, systémů a technologií, platforem (SW komponent) použitých v nabízeném řešení. |
| 3. | Požadavky na provozní prostředí Zadavatele, tj. specifikace dalších podpůrných komponent a vybavení (HW, SW, licencí, aplikací atd.) „nutných“ pro zprovoznění řešení. |
| 4. | Stručný popis provedení implementace, testování a způsobu nasazení do produkčního prostředí. |
| 5. | Požadavky Uchazeče na součinnost Zadavatele, příp. Subdodavatelů nebo Dodavatelů (společností třetích stran) technických aktiv Zadavatele. |
| 6. | Přehled (např. webový odkaz) dostupné dokumentace Výrobce. |
| 7. | Přehled (např. webový odkaz) školení Výrobce (vendora) a Uchazeče určené pro administrátory systému a privilegované uživatele (administrátory) technických aktiv Zadavatele. |
| 8. | Stručný přehled podpory poskytované Výrobcem a Uchazečem. |
| 9. | Stručný popis obsahu a formy akceptačních testů. |
| 10. | Doložení kvalifikačních předpokladů Uchazeče. |
| 11. | Předpokládaná doba realizace, včetně harmonogramu prací (čas, počet MD) zahrnující všechny fáze dodávky (předimplementační analýza, nasazení, testování, akceptace a zaškolení administrátorů systému a privilegovaných uživatelů Zadavatele atd.) s ohledem na požadovanou součinnost Zadavatele, Dodavatelů a Provozovatelů napojovaných IS. |
| 12. | Cena nabízeného řešení rozdělená na ceny za   * SW, licence, * návrh řešení (předimplementační analýzu), * konzultační, návrhové a implementační práce, * požadovanou dokumentaci, * školení administrátorů systému a privilegovaných uživatelů, * roční podporu Výrobce po dobu min. 5 let, * roční podporu Uchazeče po dobu min. 5 let. |