Specifikace technických požadavků pro potřeby zadávací dokumentace VZ

Předmět VZ: „Nasazení systému pro řízení přístupu privilegovaných uživatelů k technickým aktivům MěÚ Litomyšl“

Projekt: „Zavedení nástrojů kybernetické bezpečnosti MěÚ Litomyšl“,

NPO, výzva č. 41, Kybernetická bezpečnost – obce

Dílčí výstup: „Privileged Access Management (PAM)“

Obsah

[1 Předmět veřejné zakázky 3](#_Toc195518234)

[2 Technické požadavky PAM 4](#_Toc195518235)

[3 Požadavky na dodávku a podporu PAM 7](#_Toc195518236)

[4 Požadavky na Výrobce a Uchazeče 9](#_Toc195518237)

[5 Požadovaná struktura nabídky 10](#_Toc195518238)

# Předmět veřejné zakázky

Dodávka a zprovoznění systému PAM (Privileged Access Management) pro řízení přístupu uživatelů (pracovníků města a dodavatelů) s rozšířenými nebo administrátorskými právy k technickým aktivům MěÚ Litomyšl, v rozsahu řízení privilegovaných účtů a relací (Privileged Account and Session Management - PASM) zajišťující automatickou bezpečnou správu a řízení hesel a SSH klíčů privilegovaných účtů technických aktiv MěÚ a řízení přístupů a monitorování relací privilegovaných uživatelů prostřednictvím zabezpečené proxy brány (session gateway), jump serveru.

Výčet technických aktiv města spravovaných pracovníky SMZ nebo jejich dodavateli:

|  |  |
| --- | --- |
| **Typ technického aktiva** | **Počet** |
| Fyzický server (HP, Fujitsu) | 4 |
| Virtuální platforma (VMware) | 1 |
| Windows server | 32 |
| Linux, Unix server | 3 |
| Directory server (AD) | 1 |
| Diskové pole (IBM) | 1 |
| Datové úložiště NAS (Synology) | 2 |
| Firewall, Next Generation Firewall (MikroTik) | 1 |
| Aktivní síťový prvek (ARUBA, HP) | 18 |
| Zálohovací server (Veeam) | 1 |
| Webový server (MS IIS, Apache) | 2 |
| Databázový server (MS SQL, MySQL/Maria DB) | 2 |
| Aplikace, IS | 14 |
| Poštovní Server (IceWarp) | 1 |
| Antivirový, spam server (ESET) | 1 |
| Další zařízení, systém, server (SafeQ, JITSI MEET) | 2 |
| Počet technických aktiv MěÚ Litomyšl celkem | **86** |

Systém PAM bude umístěn a zprovozněn v serverovně, v budově MěÚ Litomyšl, Bří Šťastných 1000, Litomyšl.

# Technické požadavky PAM

|  |  |
| --- | --- |
| **Kategorie požadavků** | **Požadavky** |
| Služby, funkce | Správa a řízení privilegovaných, včetně servisních, účtů a přístupů a relací privilegovaných uživatelů k technickým aktivům:   * OS Windows, Linux * virtualizační platformy VMware, Hyper-V, KVM, Proxmox * kontejnerové platformy Azure, OpenShift, Kubernetes, * síťové zařízení a systémy (FW, SW, LB, WAF, WiFi atd.), * zařízení a systémy datových úložišť (SAN, NAS atd.) * bezpečnostní zařízení a systémy (IPS, NDR, MFA atd.), * management fyzických serverů, * management páskových knihoven, * management WiFi sítí, * webové servery (MS IIS, Apache atd.), * databázové servery (MSSQL atd.) * aplikace a aplikační IS, * webové aplikace a IS (portály), * cloudové služby, aplikace a IS (SOFA, ESET, Sophos).   Připojování privilegovaných uživatelů k technickým aktivům prostřednictvím:   * RDP, * SSH, * HTTP/S.   Automatické vyhledávání, načítání a správa technických aktiv.  Automatické vyhledávání, načítání a správa privilegovaných (lokálních, AD, LDAP) účtů technických aktiv.  Správa a řízení hesel a SSH klíčů privilegovaných účtů, včetně   * změny hesla, SSH klíče na vyžádání, * automatické změny hesla, SSH klíče po jeho použití * automatické změny hesel, SSH klíčů podle časového plánu.   Automatická správa a řízení přístupu privilegovaného uživatele k technickému aktivu, včetně časově omezeného přístupu.  Automatická správa a řízení relací privilegovaného uživatele přistupujícího k technickému aktivu, včetně   * ukončování (terminace) potenciálně nebezpečných relací, * monitorování a nahrávání relace po celou dobu jejich trvání, * zaznamenávání (úhozy, spouštění aplikací) prováděných činností.   Schvalování žádostí o přístup privilegovaného uživatele k technickému aktivu.  Automatické schvalování žádosti o přístup privilegovaného uživatele k technickému aktivu.  Skrytí hesla privilegovaného účtu během spouštění relace, přihlašování k technickému aktivu.  Dočasné poskytnutí hesla privilegovaného účtu technického aktiva uživateli PAM pro přístup k aktivu.  Definování a správa skupinových politik (zásad) pro vytváření hesel privilegovaných účtů spravovaných technických aktiv.  Definování a správa skupinových politik (zásad) pro přístupy privilegovaných uživatelů k technickým aktivům.  Hromadné přidělování, odebírání spravovaných technických aktiv a jejich privilegovaných účtů uživatelům PAM (administrátorům aktiv).  Začleňování aplikací a IS třetích stran pod správu PAM by mělo být řešeno pomocí univerzálního, v maximálně možné míře snadno a automatizovaně konfigurovatelného nástroje, bez nutnosti provádění změn v integrovaných aplikacích a systémem anebo potřeby úzké spolupráce s jejich dodavateli.  Možnost lokálních a externích (AD, LDAP) účtů uživatelů PAM.  Možnost 2FA ověřování uživatelů PAM (SW token, bezpečnostní klíč atd.).  Auditování (zaznamenávání) událostí a činností týkající se správy PAM, s možností jejich vizualizace.  Auditování (zaznamenávání) relací a činností provedených na aktivech privilegovanými uživateli, s možností jejich vizualizace.  Odhalování rizikových účtů a potenciálních bezpečnostních hrozeb.  Zálohování / obnova nastavení systému a spravovaných technických aktiv, privilegovaných účtů a uživatelů.  Integrace se systémy ServiceDesk, HelpDesk.  Integrace, předávání logů a auditních záznamů LM systémům, SIEM a SOC.  Systém PAM nebude zajišťovat a ani využívat služeb správy privilegovaných identit (účtů) neboli Privileged Identity Management (PIM). |
| 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 platformu).  Časově neomezená nebo dlouhodobá (min. na 5 let) licence pro provoz všech požadovaných komponent, služeb a funkcí systému. |
| Rozšiřitelnost, škálovatelnost | Škálovatelný, snadno rozšiřitelný systém umožňující navyšovaní počtu privilegovaných uživatelů, spravovaných technických aktiv a souběžných relací minimálně o třetinu požadovaného počtu.  HA cluster typu active/active, příp. active/passive. |
| Konektivita | Min. 1x Virtual Network Interface (VIF) |
| Kapacita, výkon, parametry | Min. počet privilegovaných uživatelů: 50. *(3 interní + 2x22 externí + 3 rezerva)*  Min. počet souběžných relací: 35. *(3x3 interní + 22 externí + 4 rezerva)*  Min. počet technických aktiv: 100. *(86 aktuálních + 14 rezerva)* |
| Bezpečnostní parametry | Bezpečné (šifrované) ukládání konfiguračních dat, aktiv, privilegovaných účtů a hesel a pořízených záznamů událostí a činností privilegovaných uživatelů.  Bezpečná (šifrovaná komunikace, AAA, 2FA) správa a konfigurace systému (přes RD, CLI nebo web GUI).  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 PAM

|  |  |
| --- | --- |
| Dokumentace Výrobce | Technický popis (specifikace) systému  Instalace (implementace) systému  Administrace systému  Údržba systému  Příručka pro uživatele systému |
| Dokumentace Uchazeče | Předimplementační analýza  Instalační (implementační) dokumentace systému  Provozní dokumentace (implementovaného) systému  Příručka administrátora systému (v českém jazyce)  Příručka uživatele 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 e-mailovou adresu podpory Uchazeče.  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. |