Specifikace technických požadavků

Předmět VZ:

Systém pro řízení přístupu privilegovaných uživatelů k technickým aktivům MěÚ Hodonín

Projekt:	„Zavedení nástrojů kybernetické bezpečnosti MěÚ Hodonín“, NPO, Výzva č. 41- Kybernetická bezpečnost – obce
Dílčí výstup projektu:	Nástroj pro řízení přístupových oprávnění – Privileged Access Management (PAM)

1. Předmět veřejné zakázky

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

Dodávaný systém PAM musí splňovat požadavky Zadavatele, viz kapitola 2 a 3 níže.

Výčet technických aktiv města spravovaných pracovníky MěÚ Hodonín nebo jejich dodavateli:

Typ technického aktiva	**Počet**
Fyzický server	3
Virtuální platforma	2
Windows server	25
Linux, Unix server	1
Datové úložiště SAN	1
SAN switch	4
Datové úložiště NAS	3
Firewall (FW, NGFW)	1
Aktivní síťový prvek (router, switch, WiFi)	15
Webový server	2
Databázový server	2
Aplikace, IS	34
Poštovní, spam Server	2
Antivirový server	2
Další zařízení, systém, server	3
Počet technických aktiv MěÚ Hodonín celkem	**100**

Systém PAM bude umístěn a zprovozněn v serverovně v budově MěÚ Hodonín, Národní třída 373/25, Hodonín.

2. Požadavky Zadavatele na systém

Kategorie požadavků	**Požadavek**
Služby, funkce systému	Správa a řízení privilegovaných účtů a přístupu a relací privilegovaných uživatelů technických aktiv: - OS Windows, Linux, Unix server, - virtualizační platformy VMware, Hyper-V, KVM, - 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, Tomcat, atd.), - databázové servery (MSSQL, Oracle atd.) - aplikace a aplikační IS, - webové aplikace a IS (portály), - cloudové služby, aplikace a IS.
	Automatické vyhledávání, načítání a správa technických aktiv.
	Automatické vyhledávání, načítání a správa privilegovaných (lokálních, AD, LDAP) účtů aktiv.
	Automatická správa a řízení hesel a SSH klíčů privilegovaných účtů, včetně obměny hesel a SSH klíčů, změny po jejich použití nebo dle časového plánu.
	Automatická správa a řízení přístupu privilegovaného uživatele k aktivu, včetně časově omezeného přístupu privilegovaných uživatelů k aktivu.
	Automatická správa a řízení relace privilegovaného uživatele aktiva, 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.
	Dočasné poskytnutí hesla privilegovaného účtu aktiva.
	Hromadné přidělování/odebírání aktiv a jejich privilegovaných účtů privilegovaným uživatelům (administrátorům).
	Definování a správa skupinových politik (zásad) pro vytváření hesel privilegovaných účtů technických aktiv.
	Definování a správa skupinových politik (zásad) pro přístupy privilegovaných uživatelů k technickým aktivům.

	Lokálních, externí (AD / LDAP) účty privilegovaných uživatelů PAM.
	2FA ověření 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.
	Připojení privilegovaných uživatelů k technickým aktivům pomocí protokolů (klientů): - RDP, - SSH, telnet, - HTTP/S
	Integrace se systémy ServiceDesk a HelpDesk.
	Přeposílání, předávání záznamů LM systémům, SIEM a SOC.
Provedení, způsob nasazení systému	Virtuální zařízení (Hyper-V, VMware, KVM).
	Dlouhodobá (min. na 5 let) licence pro provoz všech požadovaných komponent a funkcí systému.
Rozšiřitelnost, škálovatelnost systému	Zapojení v HA.
	Navyšování kapacity (licencí) a výkonu.
Konektivita systému	Min. 1x Virtual Network Interface (VIF)
Kapacita, výkon, parametry systému	Min. počet technických aktiv: 100. Min. počet privilegovaných uživatelů: 30. Min. počet souběžných relací: 15.
Bezpečnostní parametry systému	Bezpečné ukládání konfiguračních dat, aktiv, privilegovaných účtů a hesel a pořízených záznamů událostí a činností provedených privilegovanými uživateli.
	Bezpečná správa (přes RD, CLI nebo web GUI).
	V případě web GUI musí webová aplikace využívat aktuální technologie s minimálním použitím dalších, nadbytečných technologií na straně klienta s ošetřením bezpečnostních rizik dle OWASP Top 10.

3. Požadavky Zadavatele na dodávku systému

Kategorie požadavků	**Požadavky**
Dokumentace Výrobce	Technický popis (specifikace) systému Nasazení (instalace) systému Administrace systému Údržba systému Příručka pro uživatele systému
Dokumentace vypracovaná Uchazečem	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 jeho emailovou 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.
Předpoklady Uchazeče	Znalost licencování a procesů spojených s dodávkou produktů. Detailní znalost produktu (systému) v rozsahu architektury, návrhu řešení, implementace, správy a provozu systému. Technická podpora produktu v českém jazyce.