Specifikace technických požadavků pro potřeby zadávací dokumentace VZ

Předmět VZ: „Nasazení systému pro sběr a uchovávání záznamů technických aktiv MěÚ Litomyšl“

Projekt: „Zavedení nástrojů kybernetické bezpečnosti MěÚ Litomyšl“,

NPO, výzva č. 41, Kybernetická bezpečnost – obce

Dílčí výstup: „Log Management (LM) - centrální sběr a správa logů“

Obsah

[1 Předmět veřejné zakázky 3](#_Toc195536819)

[2 Technické požadavky LM systému 4](#_Toc195536820)

[3 Požadavky na dodávku a podporu LM systému 6](#_Toc195536821)

[4 Požadavky na Výrobce a Uchazeče 8](#_Toc195536822)

[5 Požadovaná struktura nabídky 9](#_Toc195536823)

# Předmět veřejné zakázky

Dodávka a zprovoznění LM (Log Management) systému zajišťujícího centrálně sběr, uchovávání a vizualizaci záznamů událostí (provozní, systémové, chybové, bezpečnostní, auditní atd.) a záznamů činností administrátorů a uživatelů všech technických aktiv MěÚ Litomyšl, které tyto logy, záznamy generují a předávají LM systému k jejich uložení, příp. dalšímu zpracování.

Výčet technických aktiv MPZ generující záznamy (logy):

|  |  |
| --- | --- |
| **Typ technického aktiva** | **Počet** |
| Fyzický server (HP, Fujitsu) | 4 |
| Virtuální platforma (VMware) | 1 |
| Windows server | 32 |
| Linux 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** |

LM systém bude umístěn a zprovozněn v serverovně, v budově MěÚ Litomyšl, Bří Šťastných 1000, Litomyšl.

# Technické požadavky LM systému

|  |  |
| --- | --- |
| **Kategorie požadavků** | **Požadavky** |
| Služby, funkce | Sběr a automatické ukládání a zpravování záznamů (logů) událostí a činnosti administrátorů a uživatelů technických aktiv.  Šifrovaný přenos (TLS, včetně v. 1.3.) záznamů (logů).  Bezpečné (šifrované) ukládání logů.  Deduplikace a komprimace ukládaných záznamů.  Způsoby, metody sběru záznamů (logů) z technických aktiv:   * syslog (RFC3164, RFC5424), * WEC/WEF (Windows Event Collector / Windows Event Forwarding), * vyčítání záznamů ze souboru, * vyčítání záznamů z databáze, * SW agent, konektor zprovozněný na technickém aktivu.   Podporované formáty zpracovávaných log zpráv:   * syslog (RFC3164, RFC5424), * Common Event Format (CEF), * Common Log Format (CLF), * Log Event Extended Format (LEEF), * Windows Event Log (EVT, EVTX). * JavaScript Object Notation (JSON), * eXtensible Markup Language (XML), * binární, * jiný, standardy nedefinovaný textový formát.   Agregace záznamů dle zdroje nebo typu logů.  Normalizace a parsování (syntaktická analýza) přijatých logů.  Definování politik (zásad) notifikačních služeb a výstrah LM systému v případě vzniku kritických, chybových a bezpečnostních událostí systému.  Definování politik (zásad) notifikačních služeb na základě informací obsažených v záznamech technických aktiv.  Vizualizace, filtrování a třídění nebo slučování logů z více zdrojů.  Vyhledávání logů na základě definovaných podmínek podle hledaného údaje, informace nebo části textu, binárního kódu obsaženého v logu.  Zálohování / obnova nastavení systému.  Export, archivace / obnova záznamů (logů).  Definování reportů vytvářených nad pořízenými záznamy (logy).  Integrace, přeposílání (předávání) záznamů dalším LM systémům, SIEM a SOC.  LM nebude zajišťovat a poskytovat služby SIEM. |
| 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 kapacity úložiště logů, počtu zdrojů logů (připojených technických aktiv) a zpracovávaných EPS minimálně o třetinu požadovaného počtu, kapacity.  HA cluster typu active/active, příp. active/passive. |
| Konektivita | Min. 2x Virtual Network Interface (VIF) |
| Kapacita, výkon, parametry | Min. počet technických aktiv: 100. *(86 aktuálních + 14 rezerva)*  Předpokládaný počet EPS: 2535.  Předpokládaný objem logů za jeden den: 150 GB.  Odhad min. kapacity úložiště logů (na 3 měsíce): 14 TB. |
| Bezpečnostní parametry | Bezpečné (šifrované) ukládání konfigurace a dat (záznamů, logů).  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 LM 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 8 hodin, a to buď elektronicky, telefonicky přes helpdesk Uchazeče, nebo zasláním na jeho e-mailovou adresu.  Zahájení řešení problému nejpozději následující pracovní den 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. |