# Specifikace technických požadavků

## Předmět VZ:

## Systém pro sběr a uchovávání záznamů technických aktiv MěÚ Hodonín

| | |
|---|---|
| Projekt: | „Zavedení nástrojů kybernetické bezpečnosti MěÚ Hodonín“, NPO, Výzva č. 41- Kybernetická bezpečnost – obce |
| Název opatření: | Nástroj pro zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů – Log Management (LM) systém |

# 1. Předmět veřejné zakázky

Dodávka a zprovoznění LM (Log Management) systému zajišťující centrálně v rámci organizace sběr, ukládání a vizualizaci záznamů událostí (provozní, systémové, chybové, bezpečnostní, auditní atd.) a činností administrátorů a uživatelů všech technických aktiv MěÚ Hodonín, které tyto logy, záznamy generují.

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

Výčet technických aktiv MěÚ Hodonín:

| **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** |

LM systém 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 | Sběr, přenos a automatické zpravování a ukládání záznamů (logů) událostí technických aktiv a záznamů činností administrátorů a uživatelů. |
| | Sběr, přenos a zpracování záznamů (logů) z technických aktiv:<br>- OS Windows, Linux, Unix server,<br>- kontejnerové platformy Azure, OpenShift, Kubernetes,<br>- virtualizační platformy VMware, Hyper-V, KVM,<br>- síťové zařízení a systémy (FW, SW, LB, WAF, WiFi atd.),<br>- zařízení a systémy datových úložišť (SAN, NAS atd.)<br>- bezpečnostní zařízení a systémy (IPS, NDR, MFA atd.),<br>- management fyzických serverů,<br>- management páskových knihoven,<br>- management WiFi sítí,<br>- webové servery (MS IIS, Apache, Tomcat, atd.),<br>- databázové servery (MSSQL, Oracle atd.)<br>- aplikace a aplikační IS,<br>- webové aplikace a IS (portály). |
| | Šifrovaný přenos (TLS, včetně v. 1.3.) záznamů (logů). |
| | Bezpečné (šifrovaného) ukládání logů. |
| | Deduplikace a komprimace ukládaných záznamů. |
| | Agregace záznamů dle zdroje nebo typu logů. |
| | Normalizace a parsování (syntaktická analýza) přijatých logů. |
| | Zobrazování, filtrování a třídění záznamů (logů). |
| | Vyhledávání záznamů na základě definovaných podmínek (čas, zdroj, typ atd.) podle hledaného údaje, informace nebo části textu obsaženého v logu. |
| | Definování reportů vytvářených nad pořízenými a zpracovanými záznamy. |
| | Definování politik (zásad) notifikačních služeb a služeb výstrah LM systému. |
| | Definování politik (zásad) notifikačních služeb a služeb výstrah LM systému. |
| | Způsoby předávání záznamů (logů):<br>- protokolem syslog (RFC3164, RFC5424),<br>- z platforem a OS Microsoft metodou Windows Event Forwarding (WEF) nebo prostřednictvím SW agenta, konektoru,<br>- vyčítáním záznamů technického aktiva ze souboru, |

| | |
|---|---|
| | - vyčítáním záznamů technického aktiva z databáze,<br>- případně použitím SW agenta (konektoru) zprovozněného na technickém aktivu |
| | Podporované formáty pro zpracování log zpráv:<br>- syslog (RFC3164, RFC5424),<br>- Common Event Format (CEF),<br>- Common Log Format (CLF)<br>- Windows Event Log (EVT, EVTX),<br>- JavaScript Object Notation (JSON),<br>- eXtensible Markup Language (XML),<br>- textový záznam,<br>- binární záznam. |
| | Zálohování, obnova, export a archivace záznamů. |
| | Přeposílání, předávání záznamů externím LM systémům, SIEM a SOC. |
| Provedení, způsob nasazení systému | Virtuální zařízení (Hyper-V, VMware, KVM). |
| | Dlouhodobá (min. 5 let) licence pro provoz všech požadovaných komponent a funkcí systému. |
| Rozšiřitelnost, škálovatelnost systému | Navyšování kapacity (zdrojů logů, úložiště logů) a výkonu (EPS). |
| | Zapojení v HA. |
| Konektivita systému | Min. 1x Virtual Network Interface (VIF) |
| Kapacita, výkon, parametry systému | Min. počet technických aktiv: 100.<br>Předpokládaný počet EPS: 500.<br>Předpokládaný objem logů za jeden den: 20 GB.<br>Min. kapacita úložiště logů na 3 měsíce: 2 TB. |
| Bezpečnostní parametry systému | Bezpečné ukládání konfigurace a dat (logů). |
| | Bezpečný přístup (přes CLI nebo web GUI) ke správě zařízení. |
| | 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<br>Nasazení (instalace) systému<br>Administrace systému<br>Údržba systému<br>Příručka pro uživatele systému |
| Dokumentace vypracovaná Uchazečem | Předimplementační analýza<br>Instalační (implementační) dokumentace systému<br>Provozní dokumentace (implementovaného) systému<br>Příručka administrátora systému (v českém jazyce)<br>Příručka uživatele systému (v českém jazyce) |
| Technická podpora Výrobce | Opravy chyb a závad systému.<br>Řešení problému vzniklých při konfigurací služeb a funkcí.<br>Vydávání aktualizací systému s opravenými chybami a závady systému.<br>Vydávání bezpečnostních aktualizací a záplat systému.<br>Doba trvání podpory min. 5 let. |
| Technická podpora Uchazeče | Opravy chyb a závad způsobených implementací<br>Opravy chyb a závad zjištěných během provozování systému.<br>Změny konfigurace služeb a funkcí systému v důsledku změn ICT infrastruktury.<br>Řešení provozních problémů systému.<br>Provádění aktualizací (update, případně upgrade) a záplat systému.<br>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.<br>Zahájení řešení problému do 12 hodin od okamžiku nahlášení.<br>Vyřešení chyby nebo závady, bránící systému poskytovat požadované služby a funkce, nebo je omezuje, příp. degraduje, do 24 hodin.<br>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.<br>Znalost produktu (systému) v rozsahu architektury, návrhu řešení, implementace, správy a provozu systému.<br>Technická podpora produktu v českém jazyce. |