# Město Kroměříž

Název projektu: Kroměříž - zlepšení kybernetické bezpečnosti infrastruktury

Registrační číslo projektu: CZ.31.2.0/0.0/0.0/23\_093/0008490

# Obecné požadavky

Část 3:

* Řízení přístupů a identit.

**Důležité upozornění:**

Dodavatel, který se stane vybraným dodavatelem této veřejné zakázky, je vyloučen z možnosti ucházet se o plnění audit kybernetické bezpečnosti.

|  |
| --- |
| **Požadavek** |
| Pokud je k provozu níže uvedených informačních systémů nutné další zařízení, licence nebo prvek podle povahy zvoleného technického řešení s výjimkou nově nakupovaných nebo stávajících, uchazeč ho výslovně uvede a zahrne do ceny svého plnění včetně nutných upgrade a update po dobu udržitelnosti. |
| Dodavatel vždy dodrží uvedené požadavky na instalaci a konfiguraci. |
| Dodavatel zajistí instalaci a konfiguraci dodaných HW a SW komponent v návaznosti na stávající infrastrukturu organizace, a to včetně instalace a implementace do stávající IT infrastruktury v sídle zadavatele |
| V případě dodání více kusů zboží u téhož zboží budou dodány identické kusy. Např. server 3x znamená, že zadavatel požaduje 3x identický server. |
| Dodávané zboží bude, tam kde to je možné, od jednoho výrobce z důvodu zajištění maximální kompatibility a jednotného servisního místa a managementu. |
| **Požadavky na certifikaci dodavatele HW a původ zboží** |
| U zařízení, u kterých je výslovně uveden požadavek na certifikaci, musí být Dodavatelem doložena certifikace nebo čestné prohlášení a garance výrobce nabízeného HW, že nabízené zboží je určené pro český trh, je nové, nepoužité a pochází z oficiálního distribučního kanálu v ČR. Dodavatel dodrží uvedené požadavky na certifikaci dodavatele (subdodavatele) HW a původ zboží. |

# Část 3 Řízení přístupů a identit

Stávající infrastruktura města Kroměříže obsahuje 4 produkčních serverů, na kterých je provozována virtualizace VMware vSphere 8. Virtualizační platforma je centrálně spravována přes vCenter 8.

Pro správu identit využívá MS Active Directory, verze OS Windows Server 2019 a identity management EOS4.

Objednavatel provozuje, či spravuje zařízení (HW + VMs Windows/Linux/appliance) a webových aplikací k zajištění správného chodu organizace. O správný běh těchto zařízení a aplikací se stará 15 interních uživatelských účtů, 35 externích uživatelských účtů, z toho může být cca 20 konkurenčních účtů.

|  |  |  |
| --- | --- | --- |
| Zdroje | Výrobce | Kusy |
| HW + VMs Linux servery |  | 10 |
| HW + VMs Windows servery |  | 60 |
| Virtualizační nody | 3x Dell, 1x Lenovo | 4 |
| Switche | HPE | 35 |
| WiFi AP | Ubiquiti UniFi | 40 |
| SAN + NAS | Dell, Synology | 4 |

Implementace

Součástí dodávky je:

1. Poskytnutí veškerých potřebných licencí – zahrnuje všechny potřebné softwarové a provozní licence pro správný chod nástroje, včetně licencí pro všechny moduly a funkce, které budou součástí implementace.
2. Předimplementační analýza a návrh řešení.
3. Analýza privilegovaných účtů, způsob užití a návrh implementace nástroje.
4. Instalace nástroje a veškerých potřebných SW komponent, popřípadě zprovoznění přístupu na cloud (pokud bude součástí řešení) – zahrnuje kompletní instalaci Nástroje, konfiguraci cloudového prostředí, nastavení přístupu pro administrátory.
5. Zprovoznění, nastavení a optimalizace provozu Nástroje – provedení všech potřebných nastavení pro plně funkční provoz Nástroje, včetně optimalizace výkonu, konfigurace parametrů a zajištění správného chodu všech procesů, aby bylo dosaženo maximální efektivity.
6. Předání instalační a provozní dokumentace – dodání podrobné dokumentace v českém jazyce, která obsahuje kompletní výčet všech potřebných úkonů pro správnou instalaci, konfiguraci a údržbu Nástroje. Dokumentace také zahrnuje návody pro administrátory.
7. Proškolení obsluhy – realizace školení pro administrátory Nástroje, které zahrnuje jak základní, tak pokročilé funkce Nástroje. Školení bude zaměřeno na efektivní využívání Nástroje a jeho správu.

## Řízení přístupů a identit

|  |  |  |
| --- | --- | --- |
| **Požadavek** | **Minimální plnění** | **Dodavatel uvede, jestli splňuje požadavky (ano/ne) a navíc popíše jakým způsobem** |
| Výrobce a licenční program |  |  |
| Licence | * nevýhradní licence minimálně na 5 let |  |
| Základní vlastnosti | * Licence pro technologii určenou pro správu přístupů ke kritické infrastruktuře * Nástroj je dodáván jako fully packaged software (obsahuje i OS) s podporou pro virtuální prostředí jako Hyper-V/VMWARE či možností instalace do cloudové infrastruktury (Amazon Web Services, Microsoft Azure). Možnost instalace do cloudové infrastruktury (Amazon Web Services, Microsoft Azure) * Podpora instalace v režimu vysoké dostupnosti. * Systém dokáže fungovat jako jednotný přístupový bod pro několik instancí v necentralizované infrastruktuře. * Nástroj funguje jako přístupová proxy. * Nástroj podporuje protokoly SSH a RDP protokoly pro primární spojení, tedy mezi privilegovaným účtem a proxy. * Nástroj podporuje protokoly SSH, RDP, VNC, RLOGIN a TELNET pro sekundární spojení, tedy mezi proxy a monitorovaným systémem. * Nástroj u nepodporovaných protokolů umožňuje spuštění klientské aplikace na Jump serveru tak, aby uživateli byla přístupná pouze daná klientská aplikace. * Nástroj podporuje integraci s externími uživatelskými databázemi v minimálním rozsahu LDAP/LDAPS/Microsoft Active Directory/RADIUS/KERBEROS/TACACS+ * Nástroj nevyžaduje žádné instalace software agentů na monitorovaný systém. * Nástroj umožňuje uživatelskou autentizaci pomocí jména / hesla, X.509 certifikátu či SSH klíče. * Integrace nástroje s LDAP či Active Directory nezávisí na periodických synchronizacích. Systém mapuje schémata uživatelských skupin z LDAP/AD do lokálních PAM skupin. * Nástroj umožňuje tvorbu účtů s rozdílnými rolemi – minimálně správce, uživatel a auditor. * Nástroj umožňuje definici uživatelů, spravovaných zařízení a jejich skupin, u kterých bude jednotlivým auditorským účtům uděleno oprávnění prohlížet záznamy. * Nástroj umožňuje konfigurace uživatelských profilů se zahrnutím možnosti filtrovat příchozí připojení na základě zdrojové IP adresy, síťové adresy a masky sítě či FQDN. * Nástroj umožňuje definování cílových systémů zadáním IP adresy, DNS nebo zadáním IP adresy a masky. * Nástroj umožňuje definování přístupových politik přiřazováním uživatelských účtů či skupin k cílovým systémům či jejich skupinám. * Nástroj podporuje integraci se SIEM/SYSLOG. * Nástroj umožňuje zaznamenávání všech zprostředkovaných relací formou videozáznamu s doplňujícími metadaty. * Nástroj umožňuje aktivaci / deaktivaci zaznamenání relací dle jednotlivých uživatelských skupin. * Nástroj umožňuje shlédnutí záznamů relací prostřednictvím webového rozhraní. * Nástroj umožňuje následný export videozáznamu do běžně podporovaného typu souboru (.mp4 či .flv) * Nastroj umožňuje ukládání zaznamenaných relací lokálně či na externí úložiště CIFS/NFS. * Nástroj zaznamenává a uchovává všechny uživatelem zadané příkazy v průběhu SSH relací. * Nástroj zaznamenává a uchovává názvy všech oken a procesů otevřených v průběhu RDP relace. * Nástroj umožňuje sběr metadata v průběhu RDP relace. * Nástroj u relací SSH umožňuje definovat vzory regulárních výrazů pro prováděné příkazy, a pokud je takový vzor detekován, umožní nastavit jednu z akcí: ukončení relace nebo odeslání oznámení o detekci vzoru. * Nástroj umožňuje přiřazení definovaných vzorů k monitoringu / ukončování relací k vybraným skupinám uživatelů či systémů. * Nástroj poskytuje ochranu hesel zadávaných v průběhu RDP relace prostřednictvím detekce vstupu kurzoru do pole pro vyplnění hesla či UAC (User Account Control) okna. * Nástroj umožňuje schvalování přístupu privilegovaného uživatele k určitým monitorovaným systémům. Schvalování přístupu musí fungovat minimálně v následujícím rozsahu:   + Privilegovaný uživatel požádá o přístup   + Definovaní uživatelé obdrží žádost o schválení přístupu.   + Minimální definovaný počet uživatelů schválí žádost.   + Privilegovaný uživatel po schvalovacím procesu automaticky získá přístup k monitorovanému systému. * Nástroj umožňuje vyžadování výše uvedených schvalování v určitých časových rámcích- např. Pondělí-pátek, 9:00-16:00 bez potřeby schválení, v jiných časech pouze po schválení. * Správce nástroje/auditor má možnost pozorovat probíhající relace v reálném čase, včetně možnosti pozorovanou relaci ukončit. * Při auditu či kontrole proběhlé relace má nástroj možnost zobrazit metadata a videozáznam relace na jedné stránce s časovou osou propojující metadata s vizuální reprezentací. * Nástroj dokáže pracovat se sdílenými účty s možností určení, kdo v daný moment tento účet využíval. * Nástroj poskytuje různé metody autentizace privilegovaných uživatelů na monitorovaných systémech, minimálně:   + Autentizace privilegovaného uživatele na monitorovaném systému pomocí stejných přihlašovacích údajů, které byly využity pro autentizaci na proxy.   + Autentizace privilegovaného uživatele na monitorovaném systému pomocí statických a bezpečně uložených přihlašovacích údajů. (např. root, admin, privilegovaný lokální účet).   + Vyzváním uživatele k opětovnému zadání přihlašovacích údajů k monitorovanému systému, bez jejich zaznamenání. * Nástroj umožňuje vyhledávání systémů a privilegovaných účtů formou scanování RDP + SSH portů a importů z AD. * Nástroj disponuje mechanismem pro plnou či částečnou automatizaci onboardingu nově nalezených zařízení / účtů. * Nástroj lze rozšířit o modul umožňující centralizaci přístupu k několika odděleným instancím prostřednictvím jednotného webového HTML5 rozhraní s integrovaným RDP a SSH klientem pro primární spojení. * Modul pro centralizaci přístupů podporuje prohlížeče Internet Explorer, Microsoft Edge, Google Chrome a Mozilla Firefox bez potřeby instalace pluginů (java, flash) * Modul pro centralizaci přístupů je dodán jako aplikace běžící na jednom z těchto OS: Microsoft Windows Server 2012 R2, Microsoft Windows Server 2016 (x64), Red Hat Enterprise Linux, CentOS 6.6, Red Hat Entreprise Linux, CentOS 7.1, Debian 8 (amd64). * Modul pro centralizaci přístupů umožňuje auditorským účtům globální vyhledávání napříč metadaty ze všech realizovaných relací všech instancí nástroje. * Technologie umožňuje automatické rotace hesel a SSH klíčů. * Technologie umožňuje vytvářet různé plány automatické změny hesel a SSH klíčů na cílových systémech. * Technologie podporuje přístup pomocí jednorázových hesel s omezenou platností pro RDP a SSH relace * Technologie podporuje vlastní zásady/požadavky na změnu hesla:   + Požadovaný minimální počet znaků,   + Vyloučení znaků určených správcem,   + Povinná velká a malá písmena,   + Požadované speciální znaky |  |

## Požadavky na záruky

Zadavatel požaduje záruku na veškeré dodané technologie v délce trvání minimálně **24 měsíců** od okamžiku předání díla, není-li u konkrétního zařízení či komponenty požadováno jinak v specifikaci ZD

Veškeré opravy po dobu záruky budou provedeny bez dalších nákladů pro zadavatele. Veškeré komponenty, náhradní díly a práce, poskytnuté v rámci záruky budou poskytnuty bezplatně.

## Požadavky na technickou podporu

Dodavatel nacení i potřebnou technickou podporu - je proces pravidelného udržování, vylepšování a opravování softwarových aplikací po jejich prvotním vývoji a nasazení. Zadavatel v rámci stanovení nabídkové ceny nacení veškerou potřebnou technickou podporu k řádnému provozovaní dodaného řešení. Potřebnou technickou podporu dodavatel nacení po dobu udržitelnosti projektu 5let. Technická podpora bude dle povahy dodaného řešení pokrývat minimálně níže uvedené scénáře:

* **Technická podpora:** Oprava chyb a problémů, které se objeví po nasazení softwaru. To může zahrnovat opravy bezpečnostních zranitelností, chyb v kódu nebo jiné problémy, které ovlivňují funkčnost softwaru.
* **Nové verze a aktualizace:** Úpravy a změny softwaru, aby zůstal kompatibilní s měnícím se prostředím. To může zahrnovat aktualizace pro nové operační systémy, hardware nebo jiné softwarové závislosti. Soulad SW s platnou legislativou.
* **Optimalizace provozu:** Vylepšení softwaru za účelem zvýšení jeho výkonu nebo použitelnosti. To může zahrnovat optimalizaci kódu, zlepšení uživatelského rozhraní nebo zavádění nových funkcí.

Údržba softwaru je klíčová pro zajištění, že software zůstane funkční, bezpečný a relevantní i po dlouhou dobu po jeho původním nasazení.

**Garantovaná doba reakce Poskytovatele od nahlášení požadavku na poskytnutí technické podpory**

1. Služba je poskytována Pracovníky Poskytovatele v okamžiku, kdy dojde k zadání Požadavku.
2. Obsahem této služby je reakce Poskytovatele na Požadavky dle jejich priority a zahájení řešení v rámci **Servisního kalendáře, tj. pracovní dny od 7:00 do 17:00**.
   1. Je-li požadavek nahlášen mimo pracovní dobu, je počátkem uvedené doby 7:00 hodin nejbližšího pracovního dne.
   2. Dodavatel je povinen zahájit řešení požadavku bezodkladně, nejpozději však do níže uvedených časů, viz tabulka Klasifikace požadavku a stavů.
3. Požadavek na provedení této služby zadávají Kontaktní osoby Objednatele nebo Poskytovatele zadáním Požadavku na Helpdesk Poskytovatele.
4. Zahájení řešení je primárně poskytováno Vzdáleným připojením pracovníka Poskytovatele. Pokud to technická povaha řešení Požadavku vyžaduje, bude realizován fyzický zásah pracovníka Poskytovatele v místě technologických center města Kroměříže, přesné místo bude vždy specifikováno v zadaném požadavku.

**Klasifikace požadavku a stavů**

|  |  |  |  |
| --- | --- | --- | --- |
| **Klasifikace** | **Definice** | **SLA zahájení řešení** | **Předpokládané vyřešení požadavku** |
| 1. Nahlášení požadavku | Potvrzení přijetí nahlášeného požadavku jedním z výše uvedených způsobů hlášení požadavku. | Nejpozději do 15 minut | Není specifikováno |
| 1. Kritický požadavek (A) | Události, které znemožňují přístup ke službám a datům poskytovaných Prvky IT, nebo jejich využívání, vážně ovlivňují plnění termínů nebo ziskovost, případně mají vliv na většinu uživatelů a služeb. | Nejpozději do 2 hodiny od nahlášení požadavku v rámci Servisního kalendáře | Do 8 hodin od zahájení řešení, dle servisního kalendáře |
| 1. Závažný požadavek (B) | Události, které významným způsobem degradují, nebo silně omezují funkcionalitu nebo službu Prvku IT, ale existuje náhradní řešení (činnost pokračuje v omezeném provozu). | Nejpozději do 5 hodin od nahlášení požadavku v rámci Servisního kalendáře | Do 16 hodin od zahájení řešení, dle servisního kalendáře |
| 1. Ostatní požadavky (C) | Všechny ostatní požadavky, neomezující řádné používání Informačního systému, které tvoří Prvky IT. | Nejpozději do druhého pracovního dne od nahlášení požadavku | Do 32 hodin od zahájení řešení, dle servisního kalendáře |
| 1. Změnové požadavky | Součinnost při implementaci změn a činnostech při nasazovaní nových prvků IT či jejich částí. | Nejpozději do 7 pracovních dní | Stanoveno dohodou |
| 1. Konzultace a návrh řešení, programátorské práce | Konzultace při řešení problémů nebo při úpravách prvků IT. | Nejpozději do 5 pracovních dní | Stanoveno dohodou |

Pro případ, že bude zadavatel požadovat služby rozšířené technické podpory podle písmena e) a f), budou tyto služby vyúčtovány po skončení kalendářního měsíce, ve kterém byly čerpány, v hodinové sazbě uvedené v Kalkulaci ceny, dle skutečně realizovaných hodin rozšířené servisní podpory. Předpokládaný rozsah služeb rozšířené technické podpory pro účely přípravy nabídky je 100 hodin / na 5 let.

# Společné požadavky

|  |
| --- |
| **Požadavek** |
| Dodavatel bere na vědomí, že součástí akceptace plnění jsou výsledky auditu, který bude prověřovat, zda jím implementovaná bezpečnostní opatření jsou funkční. Dodavatel pak poskytne součinnost nebo napraví nalezené chyby vysoké závažnosti v implementaci technických opatření. |
| Součástí je zajištění instalace a konfigurace veškerých komponent v návaznosti na stávající infrastrukturu úřadu (tj. včetně dopravy, montáže, instalace a implementace do stávající IT infrastruktury) v sídle zadavatele. |
| Součástí instalace musí být i zaškolení IT administrátorů minimálně v rozsahu nutném pro samostatnou administraci všech komponent zakázky. Administrací se rozumí zejména: konfigurace, monitoring činnosti, aktualizace, řešení problémů, zálohování konfigurace. |
| Zákaznická dokumentace bude zahrnovat:   * popis všech prvků/zařízení, * popis způsobu zálohy a obnovy konfigurace všech prvků/zařízení * veškeré požadavky na zachování záruky/podpory (např. environmentální, kompatibilita, …) * informaci o způsobu řešení servisních požadavků |
| Dodavatel do své nabídky zahrne veškerý instalační materiál a kabeláž nutnou k plnohodnotnému zprovoznění dodané technologie jako logického a funkčního celku. |
| Dodavatel zajistí instalaci a konfiguraci dodaných HW a SW komponent v návaznosti na stávající infrastrukturu organizace, a to včetně instalace a implementace do stávající IT infrastruktury v sídle zadavatele:   * instalace zařízení do standardní RACK skříně 19“ * implementace Best Practice scénářů pro dané konfigurace * kontroly kompatibility verzí ovladačů a firmware jednotlivých zařízení a jejich aktualizace * registrace záruk u výrobců * umístění do racku a zapojení kabeláže vč. jejího označení, * inicializace a konfigurace všech dodaných zařízení * nastavení IP adres * nastavení vysoké dostupnosti * konfiguraci datových prostor polí, integrace s hypervizorem, nastavení dohledu a instalace SW pro monitoring výkonu * zapojení do stávající SAN |
| Dodavatelé za všechny části si budou poskytovat vzájemnou součinnost při zprovoznění nebo implementaci všech částí zakázky v nezbytném rozsahu. Předpokládaná součinnost pro každého dodavatele v každé části je 1 člověkoden celkem pro všechny části. |

# Provozní podpora

|  |
| --- |
| **Požadavek** |
| Podpora a servis pro dodaný HW a SW budou poskytovány minimálně po celou dobu udržitelnosti projektu (tj. 60 měsíců od předání díla), pokud není specifikováno jinak. |
| Bude zajištěna udržitelnost HW a SW včetně třetích stran, dodaných v rámci veřejné zakázky. |
| Technická podpora a servis zařízení HW a SW budou realizovány dodavatelem, případně prostřednictvím odpovídajícího servisního kanálu výrobce. |
| Technická podpora a servis budou realizovány v místě zadavatele. Výjimku tvoří činnosti realizovatelné vzdáleným připojením. |
| Technická podpora bude zajišťována těmito způsoby:   * Telefonicky prostřednictvím přiděleného tel. kontaktu. * Prostřednictvím elektronické oznamovací služby (tzv. helpdesku). * Prostřednictvím vzdáleného připojení na PC uživatele / server. |
| Telefonická, e-mailová podpora a podpora prostřednictvím vzdáleného připojení bude k dispozici minimálně v pracovních dnech od 7 do 17 hod. |
| Služba HelpDesk umožní příjem požadavku na servisní zásah v českém jazyce prostřednictvím webového rozhraní v režimu 7x24 hod (s výjimkou předem nahlášených servisních zásahů při správě systému HelpDesk). |