# 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 4:

* Pořízení a implementace nástroje pro analýzu a monitoring síťového provozu.

**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 4 Pořízení a implementace nástroje pro analýzu a monitoring síťového provozu

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 variant řešení.
3. 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.
4. 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.
5. 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.
6. 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.

## Pořízení a implementace nástroje pro analýzu a monitoring síťového provozu

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Minimální požadavek** |  |
| Výrobce, název, verze a licenční program | (doplnit) |  |
| Licence | * Nevýhradní licence v délce trvání minimálně 5 let |  |
| Data | * Minimální doba uložení dat pro analýzu bude 6 měsíců. Požadavek musí odpovídat platné legislativě. |  |
| Funkce | * HW appliance * Počet monitorovacích portů minimálně 2 x 1000 MbE * Pasivní zapojení bez vlivu na monitorovanou síť (zapojení pomocí TAPů, případně v kombinaci se SPAN/mirror porty). * Cache minimálně 0,5 M * Podpora flow dat minimálně - NetFlow v5/v9, IPFIX, NetStream, jFlow, cflowd * Podpora IPv4, IPv6, VLAN, MPLS, Ethernet 10Mb/s až 100Gb/s * Sběr síťových statistik ze vzdálených lokalit s centrálním přístupem k reportům, incidentům a síťovým statistikám a centrální správou systému. * Bezztrátový sběr dat na kolektorech z různých datových zdrojů, podpora standardizovaných protokolů pro výměnu dat o IP tocích (NetFlow v5, NetFlow v9 – RFC3954, IPFIX, jFlow, cflowd, NetStream). * Dlouhodobé ukládání statistik IP toků a jejich centrální sledování a vyhodnocování bezpečnostních hrozeb v síti, prokazování bezpečnostních incidentů. * Reporty a alerty minimálně - e-mail, PDF/CSV, syslog, SNMP, packet capture trigger, script trigger * Otevřené rozhraní a dokumentované API s možností integrace nástrojů i třetích stran. * Podpora pro nativní nasazení v prostředí Microsoft Azure. Podpora pro zpracování dat zrcadleného provozu v Microsoft Azure. * Zabezpečená vzdálená správa, dohled a konfigurace – SSH, HTTPS. * Správa uživatelů a přístupových práv na zařízení prostřednictvím uživatelských rolí. * Vestavěný kolektor pro dočasné ukládání flow statistik (zajištění redundance), který zahrnuje plnohodnotnou funkcionalitu flow kolektoru. * Podpora autentizace vůči LDAP (Active Directory). * Použití DNS cache na zařízení pro rychlejší překlad IP adres na doménová jména. * Zpracování datového provozu IPv4 a IPv6, VLAN, MPLS a jejich reportování na kolektor. * Monitorování provozu v tunelu (dekapsulace) GRE, VxLAN, ESP a OTV. * Uživatelsky definovatelné šablony pro protokoly NetFlow v9 a IPFIX. * Monitorování a reportování MAC adres ve flow statistikách. Možnost použít MAC adresu jako položku klíče flow záznamu. * Reportování RTT, SRT, delay, jitter, retransmise, out-of-order pakety jako součást flow statistik. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX). * Monitorování a analýza HTTP provozu - včetně položek typu URL, hostname, stavový kód HTTP, dotazovací metoda. Pro HTTPS reportování hostname jako SNI. Použití standardní technologie reportování těchto rozšiřujících statistik (IPFIX). * Identifikace operačního systému vč. jeho verze. Identifikace internetového prohlížeče vč. jeho verze. Použití standardní technologie reportování těchto rozšiřujících statistik (IPFIX). * Monitorování VoIP statistik, protokol SIP – položky typu SIP URI, jitter, latence, ztrátovost paketů. Použití standardní technologie reportování těchto rozšiřujících statistik IPFIX). * Monitorování a analýza DNS provozu - položky jako typ dotazu, dotazovaná doména, návratová hodnota, odpověď. Použití standardní technologie reportování těchto rozšiřujících statistik (IPFIX). * Monitorování a analýza SMB/CISF provozu – položky typu síťová cesta, název souboru, typ operace. Použití standardní technologie reportování těchto rozšiřujících statistik (IPFIX). * Monitorování DHCP provozu – položky jako typ DHCP požadavku, originální MAC adresa. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX). * Monitorování e-mailového provozu – protokolů SMTP, POP3, IMAP a položek jako uživatelské jméno, jméno odesílatele, selhání autentizace a další. Použití standardní technologie reportování těchto rozšiřujících statistik (IPFIX). * Monitorování Microsoft SQL provozu (TDS protokolu) – položky jako typ dotazu, verze klienta a serveru, uživatelské jméno a další. Použití standardní technologie reportování těchto rozšiřujících statistik (IPFIX). * Schopnost monitorování a reportování různých charakteristik provozu šifrovaného pomocí SSL/TLS. To zahrnuje verzi protokolu, šifrovací algoritmus, cipher suite, detaily certifikátu a další. * Monitorování rozšířených L3/L4 informací - TTL (Time to live), TCP Window size, TCP SYN packet size umožňujících detekci NATů. * Podpora vzorkování na úrovni paketů. Podpora vzorkování na úrovni toků. * Podpora filtrování dat na sondě na základě IP prefixů, VLAN, AS (pro různé cíle exportu různé statistiky). * Podpora vyplňování AS na základě vestavěného či dodaného seznamu. * Podpora pro nastavení hodnoty interface index pro exportované flow statistiky per monitorovací port. * Sonda umožňuje rozšíření o funkcionalitu záznamu provozu v plném rozsahu na základě pravidla záchytu definovaného uživatelem. * Rozšíření je řešeno formou licence/instalace SW bez nutnosti změny HW konfigurace. * Architektura systému umožňuje streamové zpracovávání flow dat pro rychlou detekci bezpečnostních nebo provozních anomálií. * Systém umožňuje deduplikovat flow statistiky před jejich vlastní analýzou. * Systém umožňuje korelovat toky před a za proxy serverem před jejich vlastní analýzou s cílem identifikovat provoz procházející proxy serverem a tento provoz přiřadit koncovému uživateli. * Systém podporuje vzorkování na úrovní toků před jejich vlastním zpracováním. * Systém umožňuje spravovat zdroje síťových toků, umožňuje dočasně pozastavit příjem toků a indikovat poruchu zdroje síťových toků. * Systém zobrazuje informace o identitě uživatelů obsaženou ve flow datech jako součást události. * Systém podporuje persistenci doménových jmen, tedy uložení doménové jména původce události v okamžiku zaznamenání výskytu této události. * Systém obsahuje předdefinovanou sadu detekčních metod a algoritmů pro analýzu flow statistik, detekci bezpečnostních incidentů, provozních problémů a síťových anomálií. * Detekce skenování portů, slovníkové útoky, útoky odepření služeb (DoS), útoky na síťové protokoly SSH, RDP, Telnet a další obdobné služby. * Detekce anomálií v DNS, DHCP, SMTP, multicast provozu a nestandardní komunikace. * Detekce P2P sítí, a VPN komunikace * Systém umožňuje identifikovat bezpečnostní události (např. komunikaci s botnet command & control centry, přístup na phishing servery, apod.) * využíváním zdrojů IP a host reputačních databází poskytovaných * výrobcem a aktualizovaných nejméně každých 24 hodin. Systém umožňuje zapojit další zdroje IP a host reputačních dat pro automatickou detekci. * Detekce nadměrné zátěže sítě, výpadků služeb, nových a cizích zařízení připojených k síti. * Detekce síťových anomálií na základě predikce budoucího chování sítě s využíváním znalosti historie komunikace. * Systém je schopen k jednotlivým detekcím vytvářet a evidovat události a umožňuje jejich analýzu v uživatelském prostředí * Systém obsahuje konfiguračního průvodce pro nastavení systému při prvním spuštění podle parametrů sítě, do kterého je systém nasazen. * Jednotlivé detekční schopnosti je možné konfigurovat a parametrizovat tak, aby bylo dosaženo maximální efektivity a minimálního počtu falešných poplachů. Detekční mechanismy je možné konfigurovat různým způsobem (např. s různou citlivostí) pro statistiky z různých segmentů sítě (např. LAN nebo DMZ). * Systém umožňuje spravovat detekční metody z uživatelského prostředí, vytvářet kopie detekčních metod a nastavit jejich individuální parametry. * Systém umožňuje definovat vlastní detekční metody pomocí poskytnutých příkazů, které vyhledávají ve flow statistikách (včetně informací z aplikační vrstvy) specifické vzory chování. Události detekované vlastními metodami jsou zpracovávány standardně jako události z dostupných detekčních metod (notifikace, reportování, atd.). * Detekce NATů v síti s využitím rozšířených informací z L3/L4. * Systém umožňuje definovat filtry vč. komplexních filtrů složených z dílčích filtrů. Pro zjednodušení definice filtrů je možné používat operace jako inverze nebo rozdíl filtrů. Filtry je možné exportovat do formátu XML nebo z tohoto formátu importovat. K jednotlivým záznamům a filtrům lze připojit uživatelský popis účelu. * Případné události, které představují falešné poplachy (false positives) je možné odstranit prostřednictvím jednoduché konfigurace pravidel pro vyloučení falešných poplachů dostupné v uživatelském rozhraní. * Systém umožňuje zastavit a opět spustit pravidla falešného poplachu, aby bylo možné ověřit jejich požadovanou funkčnost při běžném provozu * Systém umožňuje při vytváření pravidel pro falešné poplachy smazat již detekované falešné události. * Předdefinované priority událostí s možností uživatelského nastavení závažnosti událostí na základě IP adresních rozsahů, typů událostí, míst výskytu nebo detailů události. Jedna událost může mít v závislosti na konfiguraci přiřazeno více priorit. * Systém umožňuje předdefinovat uživatelské pohledy na události a prioritu dle uživatelských rolí. * Správa uživatelů a přístupových práv k událostem prostřednictvím uživatelských rolí. Separace událostí s omezením přístupu pro jednotlivé role/uživatele. * Události je možné reportovat do dohledových systémů prostřednictvím funkcionality SNMP trap. * Notifikace o detekovaných událostech prostřednictvím e-mailu s podporou různých formátů (HTML, incident handling systém, úsporný textový formát). Možnost připojit vzorek flow dat, na základě kterých byla událost detekována k e-mailovému reportu. * Systém integruje informace ze služeb DNS, WHOIS, geolokační služby. * Uživatelsky definované externí služby fungující na protokolu HTTP. * Systém je schopen za pomoci zabezpečeného komunikačního rozhraní získat další informace k IP adrese z adresářových služeb AD/LDAP. * Systém zaznamenává na základě definovaného pravidla záchytu síťový provoz v plném rozsahu (vrstvy L2-L7) a záznamy zachyceného síťového provozu ukládá v souboru s formátem PCAP, který je možno stáhnout z webového uživatelského prostředí pro následnou analýzu v programu třetí strany (např. Wireshark). * Systémem je možné provozovat celý na monitorovací sondě včetně webového rozhraním pro manuální zadávání požadavků na záchyt síťového provozu. Webové rozhraní sondy umožňuje definovat, na jakých monitorovacích rozhraních sondy bude prováděn záchyt. * Systém umožňuje pro jednotlivé záznamy definovat filtry a zachytávat tak část síťového provozu. Kritéria filtrace jsou parametry z vrstev L2-L4 a L7. * Systém umožňuje filtrovat síťový provoz podle VLAN tagu, MPLS značky. * Systém umožňuje filtrovat síťový provoz podle IPv4, IPv6 adresy, čísla sítě a masky. * Systém umožňuje filtrovat síťový provoz podle portů TCP, UDP a SCTP * Systém umožňuje filtrovat síťový provoz VoIP hovorů používající SIP a H.323 protokoly * Záchyt síťového provozu je možné spustit automaticky na základě detekce události systémem pro automatické vyhodnocování NetFlow dat. * Systém umožňuje analyzovat síťový provoz a výsledky analýzy prezentuje ve srozumitelné podobě v rámci událostí, které popisují, jak jednotlivé komunikace v záznamu provozu probíhaly. Události jsou rozlišovány podle závažnosti do několik úrovní a indikují problémy vzniklé v síťovém provozu na podporovaných protokolech. * Systém umožňuje analyzovat vlastní záznamy provozu nebo externí záznamy nahrané do systému ve formě souboru PCAP. * Systém podporuje nejčastěji používané protokoly v podnikových sítích včetně protokolů pro konfiguraci sítě (DHCP, DNS), e-mailovou komunikaci (IMAP, POP, SMTP), síťové úložiště a posílání dat (SMB, FTP), protokoly HTTP s SSL/TLS. Systém umožňuje analýzu i na nižších vrstvách a diagnostikuje chyby v protokolech TCP, IP. * Sondu je možné integrovat do dohledového systému pro kontrolu dostupnosti a vytížení zdrojů technologií SNMP. * SIEM podpora minimálně - Using CEF (over syslog), SNMP * Stream data processing minimálně 1000 (flows/s) * Behavior patterns processing minimálně 1000 (flows/s) * Data feeds minimáně 3 * Kompletní záznam síťového provozu L2-L7 na vyžádání a při konkrétní události (packet sniffing). * Vestvaěné expertní znalosti - Rozkliknutím výsledků analýzy lze procházet jednotlivé kroky a zobrazit vysvětlení možných příčin problémů a to včetně doporučení, jak daný problém řešit. * Provádění automatické analýzy rozhodovacího stromu síťových protokolů, jejich závislosti, RFC specifikací, chyb a okamžité informování o nalezených problémech a jejich závažnosti. * Systém umožňuje postupné rozšiřování řešení pro automatické vyhodnocení přidáním dalších instancí systému při zachování jednoho uživatelského rozhraní pro dané řešení bez ohledu na počet zapojených instancí. * Systém detekce anomálií poskytuje dokumentované API pro získávání a zpracování událostí. Prostřednictvím API je možné systém detekce anomálií rovněž konfigurovat (např. vytvářet filtry, měnit nastavení detekčních metod, apod.). * Události je možné exportovat do formátu CSV pro další zpracování. * Předdefinovaná sada reportů s možností plné konfigurace uživatelem. Reporty dostupné prostřednictvím webového uživatelského rozhraní, ve formátu PDF. Automatická distribuce reportů e-mailem. * Systém umožňuje interaktivní vizualizaci detekovaných událostí formou grafické reprezentace flow statistik, na základě kterých byla událost rozpoznána. * Systém nabízí flexibilní uživatelské rozhraní pro vyhledávání událostí dle různých parametrů (typ události, IP adrese původce události, filtr, přiřazení události do kategorie, ID události apod.). Události je možné prezentovat různým způsobem (prostý seznam, agregace dle zdrojů, dle cílů apod.). * Webové uživatelské rozhraní v českém jazyce. Uživatelsky definovatelný dashboard (konfigurace per uživatel). Vizualizace průběhu provozu s vyznačením detekovaných událostí v závislosti na nastavené závažnosti událostí. * Plná zákaznická podpora v českém jazyce. |  |
| Implementace | * Instalace sondy a propojení se sběrnými porty - flowdata * Sběr dat, vyhodnocení a analýza provozu * Konfigurace bezpečnostních pravidel a alertů * Propojení na dohledové centrum |  |
| Podpora | * Propojení na dohledové centrum zajišťující komplexní monitoring infrastruktury v pracovní dny od 6h do 18h. * Fyzický operátor zajišťující okamžitou komunikaci směrem k servisní podpoře na straně objednavatele, bezpečnostní specialista, garantující správné vyhodnocení bezpečnostní události a garanci následného řešení. * Konzole pro dohled k dispozici 24x7 pro správce na straně objednatele služby * Automatizované vyhodnocování událostí a korelace událostí * Měsíční zasílání reportů a statistik monitorovaných dat * Pravidelná správa a dohled nad provozem monitorovacího zařízení včetně všech provozních i bezpečnostních aktualizací na denní bázi |  |

## Požadavky na záruky

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

Veškeré záruční 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.
* **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 6 hodiny od nahlášení požadavku v rámci Servisního kalendáře | Do 12 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 10 hodin od nahlášení požadavku v rámci Servisního kalendáře | Do 24 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 14 hodin od nahlášení požadavku v rámci Servisního kalendáře | 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). |