Název veřejné zakázky: **KYBEZ města Litvínov - Redundantní infrastruktura; §27 Zajišťování úrovně dostupnosti informací č. 82/2018 Sb., o kybernetické bezpečnosti**

systémové číslo: P25V00000064

# Předmět veřejné zakázky

Předmětem veřejné zakázky je dodávka a implementace technologií ke zvýšení úrovně kybernetické bezpečnosti informačních systémů (IS) a komunikačních systémů (KS) zadavatele. Dodavatel, se kterým bude uzavřena smlouva, poskytne zadavateli požadované dodávky a související služby specifikované v této příloze.

Přehled oblastí, které jsou předmětem dodávky:

| **Zajišťovaná oblast** | **Stručný popis položky** |
| --- | --- |
| Zajišťování úrovně dostupností informací a kontinuity provozu | * Zajištění kontinuity provozu v případě selhání primární infrastruktury (ochrana dostupnosti). * Replikace virtuálních serverů k možnosti obnovení provozu * Zálohování se zabezpečením za účelem zajištění integrity a nedotknutelnosti záloh (ochrana proti ransomware apod.) * Provoz zálohovacího serveru a DC řadiče v DR lokalitě pro rychlou obnovu klíčových služeb. |

Dodavatel je povinen navrhovat řešení v souladu s nejlepšími dostupnými technologickými praktikami, doporučeními výrobců a relevantními normami kybernetické bezpečnosti.

Není-li u technického parametru uvedeno, že jde o minimální či maximální hodnotu, lze nabídnout technické řešení, které poskytuje vyšší užitnou hodnotu, pokud tím nebude ohrožena kompatibilita, interoperabilita nebo integrace v rámci cílového prostředí.

# Stávající a cílový stav

V současnosti Městský úřad Litvínov poskytuje služby ve třech hlavních lokalitách:

* budova nám. Míru 11 (RADNICE),
* budova Vodní 871 (VODNÍ),
* budova Tržní 2042 (TRŽNÍ).

Budovy jsou propojeny následovně:



Serverová vysoce dostupná virtualizovaná infrastruktura je tvořena 3 nodovým ESX vSAN clusterem.

Lokality jsou osazeny centrálními přepínači Aruba 6300M (dvojice na lokalitu), které jsou spojeny do kruhu, v tzv. stacku, chovají se a spravují jako jeden.

Zadavatel má virtualizované prostředí pokryté licencemi Windows Server Datacenter 2022.

Pro monitoring prostředí Zadavatel využívá nástroj PRTG.

Zadavatel plánuje v lokalitě náměstí Míru 11 vybudovat tzv. disaster recovery (DR) lokalitu, ve které bude umístěn dostatečně výkonný server pro provoz klíčových technologií v případě nedostupnosti primární lokality Tržní 2042.

Zároveň na tomto serveru bude provozován zálohovací server a doménový řadič jako virtuální server. Na server budou prováděny repliky virtuálních serverů z primárního VMware clusteru. Dále bude na serveru prováděna testovací obnova záloh apod.

V této lokalitě bude umístěno i nové zálohovací úložiště s možností využití časových zámků na uložené zálohy. Zařízení musí být plně kompatibilní se stávajícím zálohovacím řešením Veeam Backup&Replication ve verzi Enterprise, na kterou má Zadavatel platnou maintenance.

Dále Zadavatel vlastní licenci ESX Standard s platnou maintenance pro celkem 32 jader.

# Implementační služby

## Obecné požadavky

Zadavatel požaduje provedení následujících implementačních činností na dodaných komponentech a případně dalších zařízeních. Rozsah služeb zahrnuje minimálně tyto kroky:

* **Zpracování prováděcí dokumentace**, která musí být před zahájením realizace dodávek schválena zadavatelem. Tato dokumentace bude zahrnovat:
  + předimplementační analýzu,
  + návrh cílového konceptu řešen.
* **Dodávku a implementaci řešení** v souladu se schváleným cílovým konceptem.
* **Zajištění projektového řízení** po celou dobu realizace zakázky.
* **Zpracování školicích materiálů a realizaci školení** pro 3 administrátory v sídle zadavatele v rozsahu 2 pracovních dnů.
* **Zajištění zkušebního provozu** v délce minimálně 14 kalendářních dnů. Během tohoto období musí být k dispozici technická podpora alespoň dvou specialistů na dodané řešení, s maximální dobou dojezdu 3 hodiny od nahlášení požadavku v pracovních dnech mezi 8:00 a 17:00.
* **Předání systému do ostrého provozu**. Akceptace bude provedena pouze v případě úspěšného ukončení bezproblémového zkušebního provozu.

Veškeré náklady spojené s implementačními službami a školením musí být zahrnuty v nabídkové ceně (neuvádějí se samostatně).

Všechny dodané dokumenty musí být vyhotoveny výhradně v českém jazyce a předány v elektronické podobě ve standardních formátech používaných zadavatelem (např. MS Office).

## Požadavky na zpracování prováděcí dokumentace

Dodavatel před zahájením implementačních prací zpracuje prováděcí dokumentaci, která bude vycházet z předimplementační analýzy a bude obsahovat veškeré aktivity nezbytné pro úspěšnou realizaci předmětu plnění.

Předimplementační analýza bude reflektovat aktuální prostředí zadavatele a navrhované řešení dodavatele. Minimálně bude zahrnovat tyto oblasti:

* Analýzu stávající konfigurace a vazeb na související systémy,
* Identifikaci požadované součinnosti ze strany zadavatele.

Na základě této analýzy bude vytvořen cílový koncept, který zohlední výchozí stav i technické parametry nabízeného řešení. Cílový koncept bude obsahovat minimálně:

* podrobný popis cílového stavu a funkcionality jednotlivých částí řešení,
* přehled nutných a doporučených optimalizačních a konfiguračních změn navázaných systémů,
* způsob zajištění jednotlivých dodávek a služeb, včetně časového harmonogramu,
* způsob zajištění jednotlivých dodávek a služeb, včetně časového harmonogramu,
* detailní návrh implementačního postupu,
* způsob zajištění informační bezpečnosti,
* projektový harmonogram s vyznačením klíčových milníků,
* popis vazeb na stávající systémy a jejich konfiguraci,
* návrh akceptačních kritérií a testovacích scénářů,
* specifikaci školení, jejich obsahu a rozsahu,
* přehled a strukturu provozní dokumentace.

V návrhu akceptačních kritérií a testovacích scénářů budou minimálně tyto kritéria:

* Na DR serveru je provozován zálohovací server a jeden doménový řadič.
* Klíčové servery jsou replikovány na DR server.
* Zálohovací řešení obsahuje nové uložiště a zálohy na něj ukládané jsou označeny časovými zámky.
* Pokus o smazání zálohy byl neúspěšný.
* Byla provedena testovací obnova ze zařízení (soubor, virtuální server).
* Byla provedena revize zálohovacích plánů.
* Byla předána dokumentace skutečného provedení.

Po předání dokumentace bude mít zadavatel lhůtu 10 pracovních dnů na její připomínkování. Dodavatel je povinen všechny připomínky vypořádat – buď jejich zapracováním, nebo formou písemného a odůvodněného odmítnutí v případě, že je považuje za nevalidní. Zadavatel nebude dokumentaci opravovat, ale pouze vyznačí věcné nebo formální nedostatky.

Prováděcí dokumentace musí být výslovně schválena zadavatelem před zahájením dalších etap plnění.

Po realizaci implementace bude dokumentace aktualizována dle skutečně provedeného stavu, včetně všech konfigurací, nastavení a analytických výstupů. Tato aktualizovaná dokumentace bude nedílnou součástí dokumentace předávané v rámci akceptačního protokolu.

# Požadované parametry technického řešení

## Obecné požadavky

Zadavatel při výstavbě, správě a provozu technologií důsledně uplatňuje princip technologické neutrality. To znamená, že využívá taková řešení, která neomezují možnost nasazení technologií od různých výrobců. Stejný přístup musí dodržovat i řešení nabízené v rámci této veřejné zakázky.

Nabízené řešení nesmí být závislé na jediné technologii nebo komponentě, která by omezovala jeho budoucí rozšiřitelnost nebo interoperabilitu.

U každého softwarového produktu, který uchazeč zahrne do nabídky, musí být výslovně uvedeny veškeré licenční a výkonové požadavky spojené s jeho instalací a provozem. Součástí nabídky musí být rovněž specifikace hardwaru, na kterém bude řešení provozováno.

Účastník ve své nabídce přehledně a srozumitelně popíše, jakým způsobem splňuje každý z požadovaných parametrů, a to včetně uvedení konkrétní značky a specifikace nabízených položek. Tyto údaje může účastník uvést přímo do přiložené tabulky, nebo je doložit jinou vhodnou formou (např. katalogovými listy). V takovém případě však musí být v tabulce jednoznačně uvedeno, kde přesně se tyto informace v nabídce nacházejí.

Dodavatel, se kterým bude uzavřena smlouva na plnění veřejné zakázky, před podpisem akceptačního protokolu bez výhrad zadavateli doloží, že všechny dodávky, které dodá zadavateli:

* jsou nové, byly oprávněně uvedeny na trh v EU nebo pochází z autorizovaného prodejního kanálu výrobce,
* mají plnou záruku od výrobce,
* obsahuji licenci na používání příslušného softwaru,
* jsou určeny pro provoz v České republice,
* z databází výrobce, distributora či prodejce bude možné výše uvedené skutečnosti doložit.

Tyto skutečnosti dodavatel, se kterým bude uzavřena smlouva na plnění veřejné zakázky doloží, čestným prohlášením výrobce, distributora (prodejce), popř. uchazečem samotným, nelze-li prohlášení výrobce nebo distributora (prodejce) získat. Zadavatel si vyhrazuje právo na zjištění původu výrobku při jejich převzetí, a to dle příslušných sériových čísel a právo podpisu akceptačního protokolu bez výhrad, osvědčujícího převzetí dodávky, až po ověření původu výrobku.

Součástí plnění je poskytování standardní podpory a záruky po dobu minimálně 60 měsíců od data převzetí předmětu plnění, potvrzeného bez výhrad akceptačním protokolem. Tato podpora zahrnuje zejména nárok Zadavatele na bezplatné dodání všech nových verzí dodaného softwaru a bezplatné provedení veškerých oprav dodaného hardwaru i softwaru.

## Technické požadavky

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Část** | **Parametr** | **Popis povinného parametru** | **Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek** | **Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru** |
| **Server** | Identifikace nabízeného řešení | Jednoznačná identifikace serveru (název, typ, označení výrobce apod.) |  |  | |
| Provedení | Umístitelné do racku, včetně montážního materiálu, max. 2U.  Barevně označené hot-plug komponenty.  Pro přístup ke všem komponentám není nutné nářadí.  Zásuvné ližiny s managementem kabeláže. |  |  | |
| CPU | Max. 2x CPU, z licenčních důvodů maximálně celkový počet 16 jader.  Výkon serveru dle https://spec.org: SPECrate®2017\_int\_base min. 171 bodů SPECrate®2017\_fp\_base min. 256 bodů |  |  | |
| RAM | Min. 16 slotů pro DDR5 RDIMM.  Min. 1024 GB RAM ECC, min. 4800 MT/s.  Počet paměťových modulů a rozmístění musí být zvoleno pro optimální výkon s CPU. |  |  | |
| Diskový subsystém | Šasi serveru musí pojmout min. 24 disků formátu 3.5", přístupných v hot-swap rámečcích a min. další 4 NVMe disky rovněž v hot-swap rámečcích.  Řadič min. 4GB Cache, SATA / SAS / NVMe, podpora RAID 0, 1, 5, 6, 10, 50, 60.  Rozhraní disků: SAS/SATA/NVMe  Osazení: 16x 2,4 TB SAS 10K, 4x 6.4TB NVME Read Intensive |  |  | |
| Boot Drive | Musí být zajištěna dvojicí SSD disků v RAID1 s kapacitou min. 480 GB.  Disky musí být připojeny na samostatný RAID řadič mimo Diskový subsystém.  Disky nesmí zabírat pozici v 28 diskovém šasi vyhrazeném pro Diskový subsystém.  Disky musí být hot-swap, přístupné z přední nebo zadní strany serveru. |  |  | |
| Interface | Min. 3x externí USB, z toho min. 1x USB 3.0.  Min. 1x VGA port (na přední nebo na zadní straně serveru). |  |  | |
| Napájecí zdroje | 2x napájecí zdroj max. 1100 W, redundance, min. Platinum energetická účinnost dle certifikace 80 PLUS. |  |  | |
| Síťové porty | Min. 2x 10/25GbE SFP28 |  |  | |
| TPM | Integrovaný TPM čip verze min. 2.0 |  |  | |
| Kompatibilita | Microsoft Windows Server®  VMware® ESXi |  |  | |
| Kompatibilita s centrálním managementem | Management serveru musí být integrovatelný do centrálního managementu, který podporuje i další produkty stejného výrobce, jako např. disková pole a switche. |  |  | |
| Automatická aktualizace managementu serveru | Management serveru musí umožňovat aktualizaci firmware managementu serveru automaticky při vydání nové verze, např. v časech nižší zátěže serveru. Management musí být restartován odděleně od serveru.V případě, že je restart serveru vyžadován z důvodu aktualizace je administrátor upozorněn min. emailovou notifikací předem. – možnost nastavení upozornění min. emailovou notifikací |  |  | |
| Management a vzdálená správa | Vzdálená správa – dostupnost centrálního management prostředí serveru, nezávislého na spuštěné virtualizační platformě, či spuštěném operačním systému, vč. monitoringu, chybových hlášení emailem, vzdáleného a lokálního připojení (KVM) prostřednictvím dedikovaného LAN portu s podporou IPv4 a IPv6. Vzdálená správa musí disponovat vlastním management GUI, přístupným z běžných www prohlížečů. |  |  | |
| Přehled zabezpečení | Management serveru musí disponovat přehledem zabezpečení serveru, pro možnost rychle identifikovat potenciální bezpečnostní rizika a snadnou kontrolu nad klíčovými bezpečnostními prvky, jako je např. uzamčení konfigurace serveru, detekce složitosti hesel, zapnutí/vypnutí logování neúspěšných přihlašování apod. Přehled zabezpečení musí být jednoznačně barevně identifikovatelný min. v režimu rizika vysoký, střední. |  |  | |
| Efektivní řízení spotřeby/výkonu | Management serveru musí disponovat funkcí doporučení k optimalizaci výkonu serveru. |  |  | |
| Compliance | Z bezpečnostních důvodů musí být možné naplánovat pravidelné provedení porovnání aktuálního stavu firmware serveru a jeho konfigurace s aplikovanou šablonou automatizovaným způsobem, s automatickým zasláním reportu o výsledku porovnání emailem. je-li tato vlastnost licencována, požadujeme plnou licenci v ceně serveru. |  |  | |
| Bezpečné vymazaní | Management serveru musí disponovat jednoduchou (na jedno kliknutí) možností kompletního smazání serveru dle standardu NIST 800-88R1 tak, aby na serveru nezůstala žádná data, nebo informace o vlastnických informací. |  |  | |
| Zámek konfigurace | Management serveru musí umožnovat tzv. zámek konfigurace celého serveru nebo specifických komponent. Digitální otisk konfigurace serveru musí být bezpečně uložen jako logovací soubor např. na serverovém integrovaném TPM čipu. Jakýkoliv pokus o vniknutí musí být detekován a server pak není možné, do zadání hesla tohoto zámku a revizi změn, nabootovat. |  |  | |
| Bare metal | Centrální management serverů musí umožňovat „server bare metal“ deployment založený na šablonách (předdefinovaných konfiguracích pravidel, jejichž součástí je kromě samotného OS i konfigurace BIOS, RAID). |  |  | |
| Záruka a technická podpora výrobce | Standardní záruka min. 60 měsíců  Servis je poskytován přímo výrobcem hardware.  Oprava v místě instalace hardware.  Možnost automatického generování servisního incidentu přímo u výrobce hardware (server musí být schopen automatizovaného předávání závad a otevírání servisních požadavku na helpdesk výrobce).  Podpora musí zahrnovat i nárok na aktualizace software a firmware pro komponenty serveru. Podpora prostřednictvím internetu musí umožňovat ověření typu a délky záruky a stahování aktuálních ovladačů, firmware, software a manuálů z internetu adresně pro konkrétní zadané sériové číslo zařízení. |  |  | |
| **Úložiště záloh** | Identifikace nabízeného řešení | Jednoznačná identifikace serveru (název, typ, označení výrobce apod.) |  |  | |
| Provedení | Umístitelné do racku, včetně montážního materiálu, max. 2U.  Barevně označené hot-plug komponenty. |  |  | |
| Kompatibilita | Nabízené zařízení pro zálohování musí být certifikováno pro spolupráci se stávajícím zálohovacím řešením Veeam Backup&Replication |  |  | |
| Kapacita | Nabízené zařízení musí být nabízeno s minimálně 80 TB hrubé (raw) kapacity |  |  | |
| RAID | Nabízené zařízení musí mít data chráněna na hardwarové úrovni pomocí RAID6. |  |  | |
| HotSpare | Nabízené zařízení musí být vybaveno nejméně jedním hotspare diskem. |  |  | |
| Disky pro operační systém | Nabízené zařízení musí mít samostatné vyhrazené disky pro operační systém zařízení a nesmí být součástí kapacity na zálohování dat. |  |  | |
| Virtual Tape Library | Nabízené zařízení musí podporovat emulaci VTL i NAS cíle, jako je NFS a CIFS. |  |  | |
| Škálovatelnost | Nabízené zařízení má být rozšiřitelné na minimálně 200 TB využitelné (usable) kapacity v nativním režimu (bez deduplikace a komprese) a o dalších 400TB nativní využitelné kapacity s využitím úložiště v cloudu, jako je AWS, Azure nebo v objektovém úložišti. |  |  | |
| Parametry VTL | Nabízené zařízení musí mít schopno v jednom zařízení kombinovat 64 páskových knihoven a NAS cílů spolu s minimálně 100.000 sloty pro média. |  |  | |
| Selektivní obnova | Nabízené zařízení musí být schopno provádět selektivní obnovu přímo z vlastní diskové knihovny. |  |  | |
| Deduplikace | Nabízené zařízení musí mít integrovanou licenci pro deduplikaci, licenci pro replikaci s malou šířkou pásma (low bandwidth) tak, aby do DR lokality byly přenášeny pouze jedinečné neduplikované datové bloky. |  |  | |
| Práce s deduplikací dat | Nabízené zařízení musí být schopno pracovat s deduplikací dat založené na zdroji (source based) i na cíli (target based), a musí být integrována se všemi běžnými výrobci backup softwaru. |  |  | |
| Emulace páskové jednotky | Schopnost flexibilně emulovat páskové jednotky/formáty LTO-5, LTO-6 a LTO-7 atd. |  |  | |
| LAN | Nabízené zařízení musí mít minimálně 2x 10/25 Gbps SFP+ porty. |  |  | |
| Šifrování | Nabízené diskové zálohovací zařízení musí podporovat funkci šifrování. |  |  | |
| Zabránění neautorizovaným operacím | Nabízené diskové zálohovací zařízení musí podporovat dvojitou autorizaci pro zabránění neautorizovaným operacím, které znemožní útočníkovi provést nebo dokončit všechny kritické operace, jako je vymazání úložiště záloh, změna systémového času atd. |  |  | |
| Dvojitá autorizace | Dvojí autorizace musí být schválena dvěma samostatnými účty nebo subjekty namísto jednoho odpovědného účtu / subjektu, aby bylo možné účinně zabránit všem škodlivým akcím, jako jsou útoky ransomware. |  |  | |
| Nezávislost duální autorizace | Duální autorizace musí být nezávislá na použití a výrobci zálohovacího software v daném prostředí. |  |  | |
| Bezpečné mazání | Nabízené diskové zálohovací zařízení musí také podporovat funkci bezpečného mazání pro ochranu před neoprávněným obnovením smazaných dat. |  |  | |
| Podpora VLAN | Nabízené diskové zálohovací zařízení musí podporovat označování sítí VLAN. Nabízené IP porty stejného typu musí také podporovat propojení portů v adaptivním vyrovnávání zátěže i v režimu aktivního zálohování. |  |  | |
| Výkon | Nabízené zařízení musí podporovat jmenovitý výkon zápisu alespoň 24 TB/hodinu |  |  | |
| Záruka a technická podpora výrobce | Standardní záruka min. 60 měsíců  Servis je poskytován přímo výrobcem hardware.  Oprava v místě instalace hardware.  Možnost automatického generování servisního incidentu přímo u výrobce hardware. Podpora musí zahrnovat i nárok na aktualizace software a firmware pro komponenty úložiště. Podpora prostřednictvím internetu musí umožňovat ověření typu a délky záruky a stahování aktuálních ovladačů, firmware, software a manuálů z internetu adresně pro konkrétní zadané sériové číslo zařízení. |  |  | |