Název zakázky: Pořízení systému pro řízení a správu privilegovaných účtů (PIM/PAM)
Číslo zakázky: P25V00000007
Zadavatel: Statutární město Frýdek-Místek, se sídlem Frýdek-Místek, Radniční 1148, PSČ 738 01

1. Cena dodávky

	Cena bez DPH	DPH	Cena včetně DPH
I. PIM/PAM	**=2365000,-Kč**	**=496650,-Kč**	**=2861650,-Kč**
II. Hodinová sazba	**=2000,-Kč**	**=420,-Kč**	**=2420,-Kč**

2. Technická specifikace předmětu plnění veřejné zakázky

Předmětem zakázky je pořízení a implementace systému pro řízení a správu privilegovaných účtů a přístupů, tzv. Privileged Identity and Access Management (dále jen „PIM/PAM"), který zajistí jednotnou centrální správu privilegovaných účtů, řízení přístupů k hardware a software infrastruktury magistrátu města Frýdku-Místku (MMFM), včetně monitorování operací prováděných privilegovanými osobami. Součástí plnění budou veškeré potřebné licence, software, hardware, implementace, technická dokumentace k dodanému řešení a zaškolení IT zaměstnanců objednavatele.

a) Popis prostředí objednavatele

Stávající infrastruktura MMFM obsahuje pět produkčních serverů a dva testovací servery, na kterých je provozována virtualizace VMware vSphere 8. Virtualizační platforma je centrálně spravována přes vCenter 8.

Pro správu identit využívá objednavatel MS Active Directory, verze OS Windows Server 2022 a identity management AC Identita verze 5.4.2.

Objednavatel provozuje, či spravuje 215 zařízení (HW + VMs Windows/Linux/appliance) a webových aplikací k zajištění správného chodu organizace. O správný běh těchto zařízení a aplikací se stará 12 interních uživatelů, 82 externích uživatelů a 32 webmasterů.

Zdroje	Výrobce	Kusy
HW + VMs Linux servery		41
HW + VMs Windows servery		66
VMs appliance (libovolný OS)		8
Virtualizační nody	[redacted]	8
HW Firewall		2 HA
Switche		39
WiFi AP		104
SAN + NAS		2 + 1 + 1
EDR		2 (WS) + 6 (Linux) + cloud
XDR Sensor - Network		1

b) Popis požadovaného řešení

Jednotlivé informační systémy, které objednavatel provozuje, jsou spravovány privilegovanými účty, které jsou využívány pro správu aplikací nebo systémových služeb a jako takové představují

významné bezpečnostní riziko. Dodaný systém bude zajišťovat jednotnou správu a monitoring privilegovaných účtů objednavatele. Řešení bude umožňovat detekci a řízení privilegovaných účtů, automatickou rotaci hesel, bezpečné ukládání hesel, monitorování a zaznamenávání sezení, pořizování a archivování auditních záznamů, reportování a upozornění interních administrátorů na vybrané události a multifaktorovou autentifikaci.

I. Detekce a napojení

PIM/PAM zpracovává přístup k oprávněním prostřednictvím struktury složek v kombinaci s řízením přístupu založených na rolích a integrací s jednotlivými službami Active Directory/LDAP. Minimální výčet rolí, který objednavatel vyžaduje je uživatel, auditor a administrátor. Spravovaná oprávnění musí být uložena v šifrované databázi. Administrátoři PIM/PAM řešení nesmí mít automaticky přístup ke všem datům. Účty a systémy, ke kterým nemají práva přístupu, nejsou pro tyto uživatele viditelné. Nabízené řešení provádí pravidelnou automatickou synchronizaci s MS AD objednavatele v definovatelné frekvenci, kde se minimálně synchronizuje stav účtu (aktivní, zakázaný) a příslušnost ke skupinám. Správce řešení bude mít možnost okamžitého zavedení nových uživatelů do systému, včetně veškerého nastavení daného uživatele, bez ohledu na synchronizaci se službami AD.

II. Schvalování privilegovaných přístupů

Řešení bude umožňovat víceúrovňové schvalování privilegovaných přístupů k cílovým systémům příslušným administrátorům. Určení administrátoři, případně auditoři ze strany objednavatele musí obdržet emailovou notifikaci s žádostí o privilegovaný přístup. Uživatelé, či skupiny uživatelů mají přístup pouze k definovaným privilegovaným účtům a systémům. Přístupy lze omezit dle vybraného uživatelského účtu, nebo na daný časový úsek. Časový úsek, na který bude přístup schválen si volí každý administrátor sám. Během tohoto časového úseku je privilegovaný účet přidělen k užívání vždy pouze jednomu uživateli. Každý schvalovací proces bude možno opatřit komentářem s odůvodněním schválení, či zamítnutí přístupu. Schvalování přístupů bude probíhat přímo v dodaném řešení s provedením auditního záznamu.

III. Přístup na cílový systém

Privilegovaný přístup na cílový systém bude zprostředkován pomocí jump serveru prostřednictvím zvoleného komunikačního protokolu, aplikace a příslušného privilegovaného účtu tak, aby koncový uživatel neměl přístup k přihlašovacím údajům. Přístupová hesla jednotlivých uživatelů se budou pravidelně a automaticky měnit, a to po ukončení relace, nebo v pravidelných intervalech dle bezpečnostní politiky. Rotaci hesla bude moct vynutit i uživatel/administrátor.

Izolace přístupu je možná až na úroveň aplikace (typu webový prohlížeč s konkrétní URL, MMC konzole s vybraným snap-in, konkrétní aplikace jako je např. MS SQL Management Studio, WinSCP, atp.), kdy uživatel nemá možnost přistupovat k jiným službám a aplikacím v rámci dané relace.

Přístup k uživatelskému rozhraní je vyžadován prostřednictvím webového portálu s podporou ověření přes MS AD a druhým faktorem. Vzdálené připojení k relaci lze navázat jak přes prohlížeč, prostřednictvím kterého se otevře okno s příslušnou klientskou aplikací, bez nutnosti její lokální instalace, tak pomocí standardních protokolů RDP a SSH a standardních klientů typu putty a remote desktop manager. U všech možností připojení ke vzdálené relaci musí být podporováno vynucení silné autentizace (LDAP, RADIUS atp.). Řešení musí umožňovat přímé spuštění výchozího RDP/SSH klienta a automatické předání přihlašovacích údajů, bez možnosti uživatele tyto údaje získat.

Systém musí umožňovat větší počet otevřených spojení na jednoho administrátora, a to minimálně 5 SSH a 5 RDP spojení. Dále by měl systém umožňovat alespoň 30 souběžných SSH a 30 souběžných RDP spojení v jeden okamžik.

IV. Monitoring, logování a reporty

Řešení musí umožňovat monitoring a kontinuální nahrávání celé relace a aktivit privilegovaných účtů ve video formátu s možností kontextového vyhledávání, bez nutnosti instalace agentů na koncový systém. Probíhající relaci bude moct administrátor ze strany IT objednavatele sledovat, zastavit, případně ukončit. Aktivní relace půjde monitorovat rovněž v prostředí internetového prohlížeče. V záznamech bude možno zpětně vyhledávat využitím metadat, které budou obsahovat v závislosti na typu relace minimálně jméno uživatele, spuštěné aplikace a události, jednotlivé příkazy, kliky na jednotlivé odkazy, stisky kláves, volba radio buttonu či check boxu v okně, změna obsahu textového pole v okně, start a zastavení procesů. Nahrávky musí být zaznamenávány efektivním způsobem – komprimace, záznam pouze aktivní relace, tak ať je výsledná velikost co nejnižší. Nahrávky musí jít přehrát přímo v dodaném řešení bez nutnosti instalace dalších doplňků s možností exportu do mp4, případně jiného běžně používaného video formátu. Nahrávky budou uchovávány definovanou dobu, či do definované datové velikosti, minimálně však po dobu 30 dní.

Zároveň musí řešení zaručovat auditovatelnost jednotlivých operací, možnost pravidelného generování reportů ve standardních formátech (docx, xlxs, txt atp.) a textové logy. Logy bude možno uchovávat minimálně po dobu 30 dní. Reporting zaměřen na standardní události, nastavené parametry, přehled nevyužívaných účtů, aktuálnost bezpečnostní politiky za zvolené období. Detekce potenciálně škodlivého chování – pokus o připojení z nestandardní IP, pokus o připojení na aplikaci, ke které nemá uživatel přístup, pokus o použití privilegovaného přístupu v nestandardní dobu, případně v nepovolený čas. Auditní záznamy musí být šifrovány s přístupem pouze pro oprávněné uživatele.

Veškeré komponenty systému musí podporovat SNMP, tak aby bylo možné monitorovat dostupnost prostředků, minimálně monitoring vytížení CPU, obsazení disků, paměti a obsazenosti databáze. Možnost napojení na [redacted] objednavatele.

V. Ochrana a bezpečnost

Úložiště dat, kde jsou uloženy jednotlivé účty, přihlašovací údaje, nahrávky relací a auditní záznamy musí být vysoce zabezpečeno a odděleno od ostatních komponent řešení. Databáze dat bude součástí řešení a není nutné využívat nástroje třetích stran.

Dodaný systém musí obsahovat řešení pro bezpečné ukládání hesel, tak aby bylo možné ukládat hesla i do ostatních systémů objednavatele, které nejsou integrovány do systému PIM/PAM.

Řešení musí umožňovat alespoň dvou faktorovou autentizaci uživatelů pro přístup k uloženým údajům i pro bezpečné vzdálené připojení. Podpora integrace s MFA nástroji třetích stran ([redacted] MS Authenticator, Google Authenticator atp.). Objednavatel v současnosti využívá [redacted].

Řešení musí být nasazeno v režimu vysoké dostupnosti (HA), minimálně v režimu Active-Passive a Disaster Recovery tak, aby citlivá data byla stále vysoce zabezpečená a dostupná. Jedna instance musí běžet ve virtuálním prostředí objednavatele a druhá na dodaném HW. HA proces musí být plně automatický.

Systém musí zahrnovat řešení pro případ selhání systému – Disaster Recovery, tzn. nouzové scénáře s postupy, jak jednat v situacích s fatálním dopadem na PIM/PAM systém. Musí existovat jeden lokální super-admin účet s odpovídajícím oprávněním, který bude chráněn dostatečně bezpečným heslem uloženým u objednavatele v trezoru, nebo na jiném zabezpečeným místě. Tento účet bude sloužit k obnově v případě selhání systému. K dispozici musí být možnost exportu a pravidelného zálohování kompletní konfigurace a nastavení celého systému pro případ obnovy.

VI. Licencování

Žádná z nabízených technologií nesmí být v okamžiku podání nabídky označena výrobcem jako končící. Všechny požadované funkce musí být v době podání nabídky součástí stabilní verze dodávaného softwaru. Součástí dodávky je také dodání všech potřebných SW/HW produktů a licencí, včetně licencí třetích strat, pro bezproblémový provoz navrhovaného řešení.

Z pohledu licenční politiky jsou požadovány licence perpetuální, buď na uživatele, nebo spravované zařízení/aplikaci s příslušnou maintenance, s minimálně 150 uživateli a 230 zařízeními.

Řešení musí být dimenzováno na minimální počet souběžných relací v počtu 30 SSH a 30 RDP.

c) Implementace

Dodavatel musí dodat plně funkční systém, kompletně zprovozněný, nainstalovaný, nakonfigurovaný, integrovaný do prostředí objednavatele (integrace s AD, OS serverů provozovaných objednavatelem), dle svých nejlepších znalostí a svědomí.

Řešení bude dodáno ve formě HW appliance (19" rack mount) a VM appliance, tak aby byla zajištěná vysoká dostupnost, včetně všech licencí nezbytných pro provoz a správu. Objednavatel požaduje redundantní zapojení do 1/10/25 Gbps switchů včetně potřebných trancieverů a kabelů.

V rámci implementace poskytne dodavatel konzultace a best practices ohledně nasazení sytému a zabezpečení privilegovaných účtů. Způsob implementace bude vycházet z před implementační analýzy zpracované dodavatelem před započetím instalace a konfigurace (náklady na provedení před implementační analýzy musí být zahrnuty v nabídkové ceně). Analýza bude obsahovat mimo jiné harmonogram realizace projektu, konkrétní popis postupu nasazení dodaného řešení u objednavatele, upřesnění parametrizace, definování workflow, popis realizace integrace s navazujícími systémy provozovanými v prostředí objednavatele. Před implementační analýza musí být konzultována se zaměstnanci objednavatele z odboru IT a následně odsouhlasena objednavatelem.

d) Technická podpora

Technická podpora je požadována v délce 60 měsíců. Tato podpora musí zahrnovat update a upgrade, jak OS appliance, tak samotného softwaru, v důsledku samostatné inovační činnosti výrobce, případně z důvodu změny právních předpisů, či zjištěných zranitelností. Zpracování změn a nařízení dle platné legislativy bude vyřešeno nejpozději k datu účinnosti změny. Technologický update a upgrade v důsledku vývoje hardwarových a softwarových prostředků, popřípadě změny technologických postupů objednavatele, které mají vliv na funkčnost dodaného řešení. Záruka na dodaný HW a technická podpora bude poskytnuta přímo výrobcem po dobu min. 60 měsíců s reakční dobou opravy NBD a vyřešením závady do 30 dnů.

Objednavatel požaduje technickou podporu výrobce v režimu 8x5. Objednavatel bude mít permanentní možnost nahlášení závady.

Nadstandardní požadavky objednavatele, které nespadají pod běžnou technickou podporu budou účtovány podle hodinové sazby uvedené v bodě 1 tohoto dokumentu. Jedná se o dodatečné práce objednané objednavatelem samostatnými objednávkami.

e) Harmonogram, plán odstávek a termíny

Objednavatel vyžaduje dodání harmonogramu plnění v předimplementační analýze. Dílo musí být předáno do 70 dnů od začátku plnění. Plnění začíná v čase T, což je datum zveřejnění smlouvy v Registru smluv. Harmonogram musí schválit obě strany.

Zahájení	T + 0 dní
Akceptační testy + předání díla	T + 70 den (70 dní)

Bez odstávkové instalace a konfigurace můžou probíhat za provozu. Práce, které vyžadují odstávku je možno provádět po pracovní době. Veškeré práce musí probíhat po předešlé domluvě.

Odstávky je možno provádět po domluvě v těchto časech:

- pondělí a středa od 17:00
- úterý a pátek od 14:00
- čtvrtek od 15:00
- odstávky po 20 hod. a o víkendu je možno realizovat jen po individuální domluvě

f) Akceptační testy a zkušební provoz

Součástí akceptačních testů, které navrhne dodavatel, musí být pro každou jednu část systému minimálně:

- prokázání kompletnosti dodávky a splnění všech povinných požadavků
- prokázání aktivací hardware i software aktivačními nebo jinými klíči či prostředky v případě, že je aktivace potřebná
- před akceptací a předáním díla proběhne 15denní zkušební provoz. Pokud se vyskytnou během testování ve zkušebním provozu závady, dodavatel je povinen závady odstranit do 48 hodin od nahlášení, nejpozději však do konce zkušebního provozu.

g) Školení zaměstnanců objednavatele

Dodavatel zajistí školení zaměstnanců objednavatele z odboru IT na veškeré součásti nabízeného řešení

- školení musí probíhat v místě plnění a v rozsahu potřebném pro využívání nabízeného řešení (ukázka, popis, nastavení a vysvětlení jednotlivých součástí systému) minimálně v rozsahu 8 hodin
- školení se zúčastní 11 administrátorů (k dispozici je školící místnost s prezentační technikou v místě plnění)
- náklady na školení musí být zahrnuty v nabídkové ceně
- dodavatel po úspěšné instalaci, konfiguraci a integraci vypracuje a dodá objednavateli veškerou (provozní, technickou a uživatelskou) dokumentaci