Státní tiskárna cenin, s. p.
Růžová 943/6, Nové Město, 110 00 Praha 1, Česká republika
Zastoupený: Tomášem Hebelkou, MSc, generálním ředitelem
(dále jen „zadavatel“)

VYSVĚTLENÍ, DOPLNĚNÍ A ZMĚNA ZADÁVACÍ DOKUMENTACE – I.

(dále jen „toto vysvětlení ZD“)

Zadavatel veřejné zakázky **„Pořízení, implementace a provoz systému pro řízení privilegovaných účtů (PAM)“** zadávané v otevřeném nadlimitním řízení dle zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „zákon“), tímto v souladu s ustanovením § 98 a 99 zákona vysvětluje, doplňuje a mění zadávací dokumentaci.

Dotaz č. 1:

Zadavatel v Příloze 1 - P1aSML - Technická specifikace_Technické řešení.docx v čl. 2 odst. 2.1 uvádí mezi typy aktuálně používaných privilegovaných účtů SSH klíče.

Pro řádnou přípravu nabídky si dovolujeme požádat o uvedení počtu SSH klíčů využívaných Zadavatelem.

Odpověď na dotaz č. 1:

Nabídka musí být jak z pohledu implementace, tak z pohledu licencování zcela nezávislá na počtu používaných SSH klíčů. Aktuálně uvažujeme o plném převodu na SSH klíče a jejich počet tak v tuto chvíli nejsme schopni detailně specifikovat.

Dotaz č. 2:

Zadavatel v Příloze 1 - P1cSML - Technická specifikace_Koncové systémy a počet uživatelů.docx v čl. 1 odst. 1.2 uvádí přehled počtu uživatelů, kteří budou využívat PAM řešení, přičemž administrátorů je v tabulce tohoto odstavce uvedeno celkem 80 (Infrastrukturní administrátoři (interní): 5, Infrastrukturní administrátoři (externí): cca 70, Aplikační administrátoři (interní/externí): 5) Dodavatelem zamýšlené řešení PAM je licencováno primárně podle počtu administrátorů samotného systému PAM, tzn. podle počtu adminů/techniků či dalších pověřených osob, které v rámci nástroje vykonávají konfigurační/administrační činnosti, zejména činnosti spojené s přidáváním zdrojů do PAM, přidělování přístupů uživatelům k jednotlivým zdrojům (privileg. účtům atp.), nastavují pravidelné rotace hesel atd. Jedná se v zásadě o tzv. „superadminy“.

Běžní technici/uživatelé, kteří se přes PAM připojují k jim přiděleným privilegovaným účtům se v rámci Dodavatelem zamýšleného řešení nelicencují, zároveň není licencován ani počet zdrojů (např. serverů s privilegovanými účty atp.)

Pro řádné nacenění počtu licencí si dovolujeme požádat Zadavatele o uvedení počtu osob, které budou dle výše uvedeného popisu patřit do kategorie „superadminů“, resp. správců vlastního PAM řešení.

Odpověď na dotaz č. 2:

Předpokládáme, že skupina Vámi zmiňovaných “superadminů” bude mít velikost 10 osob.

Dotaz č. 3:

V dokumentu "Část 1a – Technické požadavky" je v bodě B9 výslovně uvedeno, že „Druhý faktor autentizace bude vůči existujícímu 2FA řešení Microsoft MFA nebo SMS“. Ověření proti jedinému MFA/2FA řešení tak vytváří Single Point Of Failure (SPOF), který neumožňuje plné zajištění požadované vysoké dostupnosti řešení. Rozumíme tedy správně zadání, že nedílnou součástí řešení je dodávka a implementace alternativního MFA/2FA řešení, které výše zmíněný SPOF účinně eliminuje?

Odpověď na dotaz č. 3:

Ano, pro zajištění vysoké dostupnosti s eliminací hrozby nefunkčnosti existujícího 2FA řešení požadujeme v rámci dodávky také alternativní MFA/2FA řešení.

Dotaz č. 4:

V dokumentu "Část 1a – Technické požadavky" je v bodě C1 výslovně uvedeno, že: „Musí být zajištěno nahrávání relací, uskutečněných prostřednictvím PAM řešení“. Rozumíme tedy zadání správně, že veškeré činnosti privilegovaných uživatelů, tedy včetně právě všech správců řešení, musí být uskutečňovány výhradně prostřednictvím vlastního PAM řešení a všechny tyto události taktéž nahrávány? Jinými slovy, že nebude možné provést přihlášení jakéhokoliv administrátora systému, aniž by tato událost byla nahrána?

Odpověď na dotaz č. 4:

Ano, požadujeme, aby veškeré činnosti privilegovaných uživatelů, tedy včetně všech správců řešení, byly uskutečňovány výhradně prostřednictvím vlastního PAM řešení a aby všechny tyto události byly taktéž nahrávány. Nebude tedy možné provést přihlášení jakéhokoliv administrátora systému, aniž by tato událost byla nahrána.

Dotaz č. 5:

V dokumentu "Část 1b – Obecné požadavky na dodávku" je v bodě 1.1 uvedeno, že dodavatel provede „analýzu nezbytnou pro instalaci a konfiguraci komponent PAM řešení, integraci

všech typů koncových systémů“. Rozumíme tomu správně, že má tato bezpečnostní analýza obsahovat i detailní popis současného stavu prostředí zákazníka tedy například dlouhodobě neměněná hesla privilegovaných účtů (administrátorských, servisních, aplikačních), Pass-the-Hash vulnerability, přístupová oprávnění ve formátu prostého textu a další?

Odpověď na dotaz č.5:

Ano, požadavkem je, aby tato bezpečnostní analýza obsahovala i detailní popis současného stavu prostředí zákazníka včetně například dlouhodobě neměněných hesel privilegovaných účtů (administrátorských, servisních, aplikačních), Pass-the-Hash vulnerabilit a přístupových oprávnění ve formátu prostého textu.

Dotaz č. 6:

V dokumentu "Část 1c – Koncové systémy a počet uživatelů" je v bodě 1.1 uvedeno, že připojení pro „BNS – a Manažerský systém pro finanční plánování“, „Telefonní ústředna – Unify“, „Cicero“ a „MetaServer“ bude prováděno prostřednictvím nativního aplikačního (tedy „tlustého“) klienta. Rozumíme tedy zadání správně, že řešení má poskytovat nativní podporu pro vývoj a následnou integraci libovolných aplikačních klientů, kteří umožní připojení k dané aplikaci a případnou rotaci přístupových oprávnění daného uživatele?

Odpověď na dotaz č. 6:

Ano, poptávané řešení má poskytovat nativní podporu pro vývoj a následnou integraci libovolných aplikačních klientů, kteří umožní připojení k dané aplikaci a případnou rotaci přístupových oprávnění daného uživatele.

Dotaz č. 7:

V dokumentu "Část 1c – Koncové systémy a počet uživatelů" je v bodě 1.1 uvedeno, že připojení pro například „MS SQL“ bude prováděno prostřednictvím RDP, tedy nikoliv prostřednictvím nativního aplikačního (tedy „tlustého“) klienta. Jedná se o záměr, či administrativní chybu zadání?

Odpověď na dotaz č. 7:

MS SQL může být připojeno prostřednictvím nativního aplikačního klienta.

Zadavatel přikládá upravenou přílohu č. 1 Návrhu smlouvy – **Část 1c – Koncové systémy a počet uživatelů**, ve které je výše uvedená informace také doplněna a zvýrazněna revizním módem.

Předložením krycího listu nabídky (příloha č. 2 zadávací dokumentace) ve své nabídce tak budou účastníci akceptovat tuto novou verzi dnes zveřejněné přílohy č. 1 Návrhu smlouvy – Část 1c – Koncové systémy a počet uživatelů.

Dotaz č. 8:

Ze zadání není zcela zřejmé, zdali má být součástí řešení také bezpečný přístup k PAM řešení z externího prostředí bez využití VPN. Můžeme požádat o jednoznačné stanovisko ohledně zajištění takového přístupu?

Odpověď na dotaz č. 8:

Ano, součástí dodávky má být také zajištění možností pro bezpečný přístup k PAM řešení z externího prostředí bez využití VPN.

Zadavatel přikládá upravenou přílohu č. 1 Návrhu smlouvy – **Část 1a – Technické požadavky**, ve které je výše uvedená informace také doplněna a zvýrazněna revizním módem.

Účastník je povinen využít tuto verzi dané přílohy pro účely podání své nabídky.

Dotaz č. 9:

Má být součástí řešení i možnost bezpečného připojení privilegovaných uživatelů k externím zdrojům prostřednictvím MFA/2FA (například administrace Microsoft MFA/2FA řešení, umístěné v MS Azure)?

Odpověď na dotaz č. 9:

Ano, řešení musí umožňovat bezpečné připojení privilegovaných uživatelů k různým typům a různě umístěním systémům a aplikacím, tedy včetně bezpečného připojení privilegovaných uživatelů k externím zdrojům prostřednictvím MFA/2FA (například administrace Microsoft MFA/2FA řešení, umístěné v MS Azure).

Zadavatel přikládá upravenou přílohu č. 1 Návrhu smlouvy – **Část 1a – Technické požadavky**, ve které je výše uvedená informace také doplněna a zvýrazněna revizním módem.

Účastník je povinen využít tuto verzi dané přílohy pro účely podání své nabídky.

Na základě výše uvedeného zadavatel přiměřeně prodlužuje lhůtu pro podání nabídek, a to o 3 pracovní dny:

- Původní lhůta pro podání nabídek: do 14.08.2024, 09:00

- Nová lhůta pro podání nabídek: do 19.08.2024, 09:00
- Otevírání nabídek: po uplynutí lhůty pro podání nabídek

Přílohy:

1) Příloha 1 - P1aSML - Technická specifikace_Technické řešení_rev20240805
2) Příloha 1 - P1cSML - Technická specifikace_Koncové systémy a počet uživatelů_rev20240805

Zpracoval/a: Mgr. Zuzana Drahokoupil Šenoldová
Uveřejněno prostřednictvím elektronického nástroje EZAK
V Praze, dne *dle elektronického podpisu*

Podepsal(a): Mgr. Zuzana Drahokoupil Šenoldová
Datum: 05.08.2024 15:28:27

_____

Mgr. Zuzana Drahokoupil Šenoldová
vedoucí útvaru veřejných zakázek
za zadavatele Státní tiskárna cenin, s. p.