

Príloha č. 1

k zmluve o dodaní riešenia správy a riadenia privilegovaných prístupov

Predmet plnenia

Implementácia riešenia správy a riadenia privilegovaných prístupov – PAM. Riešenie musí zabezpečiť bezpečný, riadený a kontrolovaný prístup interných ako aj externých pracovníkov prevádzkovej podpory k definovaným systémom prevádzkovej infraštruktúry.

Opis predmetu plnenia

1. Aktuálne prostredie Dodávateľa:

Aktuálne je v prostredí obstarávateľa riadený vzdialený prístup prostredníctvom VPN koncentrátora CISCO ASA5516-x. Riadenie prístupov je zabezpečené prostredníctvom definovaných ACL pre jednotlivé typy prístupových účtov. Správa prístupov je realizovaná prostredníctvom Active Directory security groups. Pre jednotlivé skupiny prístupov je k dispozícii vyhradené pracovné prostredie – jump server, prostredníctvom ktorých prístupujú k spravovaným systémom.

V rámci implementácie riešenia je požadovaná integrácia systémov, ktorých prehľad a spôsob integrácie je v nasledujúcej tabuľke:

Systém/zariadenie	Prístup	Zmena hesla
33ks Windows server 2008 R2 SP1, 2012 R2, 2016	RDP / RDP klient	Štandardný Windows mechanizmus
2 ks CentOS 7 server	SSH / SSH klient	Štandardný SSH / Linux mechanizmus
1ks Check Point Management Server - GAIA R80.30	CLI/SSH/SSH klient Web rozhranie/HTTPS/Web Browser Smart Dashboard/proprietarny protokol/Smart Dashboard Client	CLI/SSH Web rozhranie/HTTPS Smart Dashboard/proprietarny protokol/
1ks VMware vSphere vCenter	Web rozhranie/HTTPS/Web Browser	Web rozhranie/HTTPS/Web Browser Štandardný Windows mechanizmus
1ks Citrix XenApp	RDP / RDP klient	Štandardný Windows mechanizmus
1ks Hyper-V 2016 Cluster	RDP / RDP klient	Štandardný Windows mechanizmus
1ks MS SQL Server	SQL Server Management Studio	Centrálné s využitím MS AD
38 ks sieťové zariadenia CISCO iOS, iOS-XE, ASA OS, FX OS	CLI/SSH/ Web rozhranie/HTTPS/Web Browser	CLI/SSH/
2ks Oracle DB server	SQL Developer/SSH	SQL Developer/SSH
250 ks PC a Nb/užívateľov	RDP / RDP klient	Centrálné s využitím MS AD

2. Požiadavky na riešenie správy a riadenia privilegovaných prístupov

Riešenie musí zabezpečiť hlavne centralizovanú správu, bezpečný prístup k heslám a zdieľaným účtom, riadenie prístupu k heslám, riadenie životného cyklu hesiel, riadenie prístupu privilegovaných používateľov, riadenie prístupu k aktívam, real-time monitoring prístupu k definovaným prvkom prevádzkovej infraštruktúry.

Dôraz musí byť kladený najmä na privilegované účty. Jedná sa o účty, ktoré majú v operačnom systéme vysoké oprávnenia. Jedná sa o účty typu root v Linux/UNIX systémoch, účty typu Administrátor vo Windows systémoch, systémové účty používané aplikáciami alebo zdieľané účty, ktoré nie sú viazané na jedinú fyzickú osobu.

Riešenie má zaznamenávať činnosť používateľa/administrátora, ktorý pristupuje k citlivým dátam alebo vykonáva konfiguračnú činnosť a vytvárať auditnú stopu pre potreby možného sledovať udalosti presne tak, ako sa v skutočnosti odohrali.

Riešenie má automatizovať, kontrolovať a zabezpečovať proces prideľovania privilegovaných poverení (pomocou správy hesiel, čiže privilegovaný užívateľ nepozná heslo do doby než ho potrebuje) so schvaľovateľmi úloh, núdzový prístup a expiráciu platnosti politiky. Má zahŕňať taktiež schvaľovanie požiadaviek na heslo.

Riešenie musí zabezpečiť minimálne:

- skenovanie, identifikáciu a enrolment privilegovaných účtov zariadení a aplikácií,
- automatickú zmenu/rotáciu hesiel na základe definovaných politík a komplexity hesla, úložisko hesiel ,
- auditné záznamy o prístupoch k heslám o operáciách nad spravovanými privilegovanými prístupmi, účtami,
- delegovanie správy prístupov, členenie na logické celky s vymedzenými oprávneniami,
- monitoring, správu a nahrávanie používateľských (administrátorských) session počas prístupu pod privilegovaným účtom,
- spracovanie metadát o nahrávaných session tak, aby bolo možné v nahrávkach vyhľadávať napr. spustené aplikácie a príkazy,
- správu SSH kľúčov v prostredí UNIX a Linux,
- podporu využitia jump host (Windows RDP, Unix SSH) na nadviazanie spojenia s koncovým zariadením,
- zabezpečenie prístupu tak, aby administrátor nevedel heslo k privilegovaného účtu ku koncovému zariadeniu,
- podporu dvojfaktorovej autentifikácie,
- centrálnu autentizáciu a riadenie prístupu,
- full-textové vyhľadávanie v záznamoch,
- tvorba black-listov a white-listov,
- behaviorálnu analýzu správania užívateľov,
- ukladanie relácie a histórie hesiel, logov po dobu 12 mesiacov, od 1.1.2023 do 31.12.2023.

V rámci realizácie očakáva Objednávateľ naplnenie popisu uvedeného v tomto a ostatných dokumentoch tvoriacich opis predmetu plnenia, ako aj súlad a naplnenie požiadaviek platnej legislatívy a štandardov v oblastiach informačných systémov verejnej správy a bezpečnosti (napr. metodické pokyny, manuály a pod.).

3. Dodanie softvéru a jeho licenčného krytia (predmet plnenia podľa článku 1 ods. 2 písm. a) zmluvy):

- Dodanie CyberArk Privileged Access Manager

- Licencie na obdobie od 20.12.2022 do 19.12.2023
- licenčné pokrytie pre:
 - integráciu 100 systémov a zariadení,
 - prístup 10 interných privilegovaných identít – zamestnancov Objednávateľa,
 - prístup 60 externých privilegovaných identít – zmluvných partnerov a dodávateľov,

4. Predmetom plnenia podľa článku 1 ods. 2 písm. b) zmluvy sú implementačné a konfiguračné práce minimálne v rozsahu:

- Vypracovanie detailného návrhu riešenia – naplnenie funkčných požiadaviek, návrh architektúry riešenia zo začlenením do prevádzkovej infraštruktúry, vypracovanie dokumentu detailného návrhu riešenia, testovacie scenáre.
- Realizácia implementácie riešenia – nasadenie centrálnych komponentov, konfigurácia integračných rozhraní, konfigurácia politík potrebných pre riadny chod aplikácií.
- Overenie funkčnosti riešenia – realizácia testov na základe pozitívnych a negatívnych testovacích scenárov.
- Školenie pre rolu – administrátor správca systému.
- Dokumentácia riešenia minimálne v rozsahu – inštalačná a konfiguračná príručka, používateľská príručka pre koncových používateľov.
- Nasadenie riešenia do prevádzky – inicializácia všetkých požadovaných prístupov.
- Post implementačná podpora v trvaní 1 mesiac – monitoring a ladenie výkonu.