OPIS PREDMETU ZÁKAZKY

Názov zákazky:
Riadenie kybernetickej bezpečnosti – Kontrola privilegovaných používateľov

Verejný obstarávateľ prevádzkuje svoju činnosť vo viacerých lokalitách v rámci Slovenskej republiky. Jednotlivé pracoviská sú prepojené dátovou sieťou WAN, prostredníctvom ktorej zamestnanci pristupujú k aplikáciám, výpočtovým, informačným a komunikačným, zdrojom. V rámci celkového zvýšenia kybernetickej bezpečnosti organizácie je zámerom verejného obstarávateľa, nasadiť, rozšíriť prípadne doplniť systémy, prostredníctvom ktorých je možné spravovať, riadiť a kontrolovať prístup používateľov s tzv. privilegovaný prístupom.

Kontrola prístupu privilegovaných používateľov

Pod pojmom privilegovaný prístup označujeme pre tento účel účet na úrovni operačného systému, ktorý má vysoké oprávnenia, t. j. účty typu/role root v Linux/UNIX systémoch, účty typu/role Administrátor vo Windows systémoch, systémové účty používané aplikáciami alebo zdieľané účty, ktoré nie sú viazané na fyzickú osobu. S týmito účtami pracujú privilegovaní užívatelia. Pojem privilegovaný užívateľ označuje fyzickú osobu, ktorá používa privilegované účty. Ide hlavne o pracovníkov prevádzky, dodávateľov, alebo vývojárov. Cieľový systém označuje systém, na ktorý sa privilegovaný užívateľ pripojuje prostredníctvom privilegovaných účtov.

Úlohou riešenia je predovšetkým centralizovaná správa, bezpečný prístup k heslám a zdieľaným účtom, riadenie prístupu k heslám, riadenie životného cyklu hesiel, riadenie prístupu privilegovaných užívateľov, riadenie prístupu k aktívam, real-time monitoring prístupu k aktívam v ICT infraštruktúre, vyhodnocovanie rizikových bezpečnostných udalosti a pomoc pri odhaľovaní prístupov, ktoré môžu ohroziť prevádzku informačných systémov a tým obmedziť, prípadne znemožniť poskytovanie služieb.

Zároveň má systém zaznamenávať činnosť systémového 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. Úlohou riešenia je taktiež 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 exspiráciu platnosti politiky, pričom zahŕňa taktiež schvaľovanie požiadaviek na heslo.

V prostredí prevádzkovej infraštruktúry verejného obstarávateľa je nasadený a prevádzkovaný nástroj na zabezpečenie kontroly nad privilegovanými účtami výrobcu BeyondTrust. Pre zvýšenie efektivity a bezpečnosti prevádzky je nutné zabezpečiť rozšírenie existujúceho riešenia na všetky prevádzkované systémy tak, aby bola zabezpečená rovnaká úroveň bezpečnosti a kontroly nad prístupmi v rámci prevádzkovej infraštruktúry.

Architektúra aktuálneho riešenia je založená na produkte BeyondTrust Password Safe v konfigurácií s dvomi virtuálnymi serverovými komponentmi BeyondTrust Appliance, ktoré sú prevádzkované v režime Active – Pasive. Kontrola a správa privilegovaných prístupov je nasadená na 103 systémov, ktoré pozostávajú z nasledujúcich typov:

- MS Windows Server (2012,2019,2022),
- Linux Server (napr. Centos, Oracle Linux),
- Solaris 11 Sparc,
- F5 BIG IP,
- CheckPoint 6400,
- Cisco IronPort ESA.

Licenčný model riešenia je postavený na uvedenom počte integrovaných systémov a počte virtuálnych serverových appliance.

Rozšírené riešenie musí spĺňať nasledovné požiadavky:

- skenovanie, identifikáciu a enrolment privilegovaných účtov zariadení a aplikácií,
- automatickú zmenu/rotácia 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.

Riešenie umožňuje konfiguráciu prístupových rolí a oprávnení k samotnému systému minimálne v rozsahu nasledujúcich rolí:

- Správca (administrátor) - riešenie umožní definovať typ používateľa s najvyššími právami, používateľ s touto rolou bude mať možnosť využívať nástroj v jeho plnom rozsahu funkcionality.
- Používateľ - riešenie umožní definovať typ používateľa s právami v rozsahu funkcionality potrebnej pre správu pripojených zariadení a aplikácii.
- Audítor - riešenie umožní definovať typ používateľa s právami na prístup k auditným informáciám a nahrávkam.
- Schvaľovateľ - riešenie umožní definovať typ používateľa s právami na schvaľovanie prístupov k vybraným skupinám účtov.

Z licenčného pohľadu je súčasťou požadovaného predmetu plnenia:

- Dodanie licenčného pokrytia pre rozšírenie riešenia o 127 integrovaných systémov s licenčnou podporou na 3 roky.
- Zosúladenie licenčného pokrytia a podpory existujúcej časti riešenia (aktuálny dátum exspirácie licenčnej podpory 31.8.2025) s rozšírenými licenciami.
- Konfiguračné a implementačné práce pre zabezpečenie rozšírenia riešenia.

Typ licencie	**Popis produktu**	**Množstvo**	**Obdobie**
Rozšírenie počtu systémov	Password Safe Per Asset License	127	Trvalá licencia
Podpora pre rozšírenie počtu systémov	Password Safe Per Asset Maintenance	127	3 roky
Predĺženie licencií aktuálneho riešenia	Password Safe Per Asset Maintenance	103	Rovnaké obdobie exspirácie ako rozšírené riešenie
Predĺženie licencií aktuálneho riešenia	BeyondTrust Appliance U Series-VM - Maintenance	2	

- Požadujú sa perpetuálne (trvalé) licencie v súlade s existujúcim licenčným modelom bez obmedzenia počtu používateľov. V rámci dodávky licencií je nutné zabezpečiť aj licenčné pokrytie a zosúladenie času exspirácie nových aj súčasných licencií z pohľadu technickej podpory v rovnakom dátume.

Konfiguračné a implementačné práce pre zabezpečenie rozšírenia riešenia musia zahrnúť:

- Rozšírenie existujúceho detailného návrhu riešenia v súlade s existujúcou funkcionalitou a architektúrou riešenia, aktualizácia testovacích scénarov.
- Realizácia konfigurácie a implementácie riešenia – konfigurácia integračných rozhraní, konfigurácia politík potrebných pre riadny chod aplikácií.
- Overenie funkčnosti riešenia – realizácia testov na základe pozitívnych a negatívnych testovacích scenárov.
- Rozšírenie existujúcej dokumentácie riešenia – inštalačná a konfiguračná príručka.
- Nasadenie riešenia do prevádzky – inicializácia všetkých požadovaných prístupov.
- Post implementačná podpora v trvaní 1 mesiac – monitoring a ladenie výkonu.