GENERÁLNA PROKURATÚRA SLOVENSKEJ REPUBLIKY
Štúrova 2, 812 85 Bratislava
Ekonomický odbor

Príloha č. 1

Podrobný opis predmetu zákazky

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.

Riešenie má pokryť hlavne centralizovanú správu, 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, vyhodnotiť rizikové bezpečnostné udalosti a pomáhať pri odhaľovaní prístupov, ktoré môžu ohroziť prevádzku informačných systémov a tým obmedziť, prípadne znemožniť poskytovanie služieb.

Riešenie má 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.

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 exspiráciu platnosti politiky. Má zahŕňať taktiež schvaľovanie požiadaviek na heslo.

Riešenie musí zabezpečiť hlavne:

- 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.

GENERÁLNA PROKURATÚRA SLOVENSKEJ REPUBLIKY
Štúrova 2, 812 85 Bratislava
Ekonomický odbor

Funkčná špecifikácia

ŠPECIFIKÁCIA POŽIADAVIEK	
Základné požiadavky	
1	- riadenie, správa, skenovanie, identifikácia a enrolment privilegovaných účtov zariadení a aplikácií, - riadenie prístupov k týmto účtom, monitoring všetkých aktivít
2	- jednotná centrálna správa, riešenie musí umožňovať konfiguráciu pomocou RestAPI - správa užívateľov, zakladanie a editácia účtov, zmeny prihlasovacích údajov, terminácia spojení atď.
3	- automatická zmena/rotácia hesiel na základe definovaných politík a komplexity hesla, úložisko hesiel
4	- auditné záznamy o prístupoch k heslám o operáciách nad spravovanými privilegovanými prístupmi
5	- delegovanie správy prístupov, členenie na logické celky s vymedzenými oprávneniami
6	- monitoring, správa a nahrávanie používateľských (administrátorských) session počas prístupu pod privilegovaným účtom
7	- spracovanie metadát o nahrávaných session tak aby bolo možné v nahrávkach vyhľadávať napr. spustené aplikácie a príkazy
8	- správa SSH kľúčov v prostredí UNIX a Linux
9	- podpora využitia jump host (Windows RDP, Unix SSH) na nadviazanie spojenia s koncovým zariadením
10	- zabezpečenie prístupu tak, aby administrátor nevedel heslo k privilegovaného účtu ku koncovému zariadeniu
11	- podpora dvojfaktorovej autentifikácie (2fa nie je predmetom obstarávania)
12	- centrálna autentizácia a riadenie prístupu
13	- full-textové vyhľadávanie v záznamoch
14	- automatická výmena hesiel a SSH kľúčov uložených účtov po ukončení relácie (jednorazové heslo) alebo opakovane
15	- heslá k privilegovaným účtom musia spĺňať požiadavky politiky hesiel
16	- uloženie hesiel v šifrovanej forme (šifrované úložisko)
17	- podpora pravidelného (ročného) auditu privilegovaných prístupov
18	- vysoká bezpečnosť prenášaných a uložených dát (dôvernosť, dostupnosť, integrita)

GENERÁLNA PROKURATÚRA SLOVENSKEJ REPUBLIKY
Štúrova 2, 812 85 Bratislava
Ekonomický odbor

Password Management, riadenie prístupu	
1	- pokročilé metódy pre zabezpečenie prístupu k samotnému heslu. Možnosť zmeniť heslo pre uložený účet po každom jeho použití. Možnosť zažiadanie o prístup k heslu (zo strany používateľa) a následné schválenie (zo strany vlastníka).
2	- Workflow Engine - ktorý podporuje riadenie časových reštrikcií, prehliadačov, viacnásobné schvaľovanie, núdzový prístup a exspiráciu politík. Požiadavka na pridelenie hesla môže byť schválená automaticky alebo môže vyžadovať viacúrovňové schvaľovanie. Na základe analýzy v rámci riešenia implementovať päť workflow.
3	- v prípade potreby systém umožňuje rozšírenie o aplikovanie princípu štyroch očí - napr. prístup k definovanému reportu, vytvorenie reportu, prístup k aktívnej/nahranej relácii
4	- možnosť automatickej zmeny hesla a periodického overovania platnosti hesla, vzdialenej zmeny hesla, nastavenia frekvencie zmeny hesla, zložitosť hesla...
5	- funkcie logovania a reportovania pre podporu monitoringu aktivity správy hesiel a prípadnú opravu abnormalít
6	- prispôsobiteľné pracovné postupy a činnosti, umožňujúce prispôsobiť politiky hesiel a obnoviť pracovné postupy tak, aby zodpovedali potrebám a požiadavkám
7	- v prípade potreby má systém umožňovať rozšírenie o povolenie prístupu na vyžiadanie
8	- v prípade potreby má systém umožňovať rozšírenie o povolenie prístupu na vyžiadanie - načasovaný prístup
9	- podpora viacerých domén
10	- obsluha používateľov z viacerých domén - s dôverou alebo bez nej
11	- integrácia so systémom Windows, šifrovanie údajov a bezpečná komunikácia
12	- podpora SSL/TSL a CryptoAPI spoločnosti Microsoft
13	- samoobsluha používateľa, samoobslužné funkcie na zvládnutie základných úloh s heslom
14	- možnosť zaregistrovať a používať samoobslužné služby na resetovanie svojich hesiel alebo na odomknutie účtov a na resetovanie hesiel, keď je systém offline
15	- správa hesiel, založená na AD, rozšírená aj na operačné systémy iné ako Microsoft - ako napríklad Unix a Linux
16	- vyhľadávanie privilegovaných účtov, servisných účtov v operačných systémoch / LDAP / AD
17	- automatická výmena hesiel privilegovaných účtov na koncových systémoch s OS MS Windows
18	- riešenie musí byť schopné riadiť prístupy v rámci „session" podľa overenia voči LDAP / RADIUS
19	- riešenie podporuje možnosť dvojfaktorovej autentizácie pre „session" (reláciu)
Vytváranie a správa auditných záznamov, monitorovanie	

1	- riešenie zaznamenáva udalosti, aktivity užívateľa na cieľovom systéme (prihlásenie, prístup k heslu, zmena konfigurácie, prístup k nahranej session, atď.)
2	- riešenie umožňuje logovanie ako interných akcií, tak aj informácií o „sessions" pomocou syslog protokolu, podpora TLS nad syslog protokolom
3	- riešenie umožňuje prehrávať všetky užívateľské aktivity
4	- riešenie umožňuje prehrávať zaznamenané aktivity. Všetky akcie užívateľov sú viditeľné tak, ako boli zobrazované na ich monitore
5	- riešenie umožňuje rýchle prehrávania, vyhľadávanie udalostí (napr. napísané príkazy alebo stlačenie "Enter") a textov, prehliadaných užívateľom
6	- riešenie dokáže monitorovať sieťovú prevádzku v reálnom čase a vykonávať rôzne akcie v prípade, že sa na obrazovke objaví určitá kombinácia (napr. podozrivý príkaz, názov okna alebo text). V prípade, že zaregistruje podozrivú akciu, môže poslať e-mailovú a syslog notifikáciu, alebo okamžite ukončiť spojenie.
7	- riešenie umožňuje vyhľadávanie udalostí s využitím indexov, alebo inej podobnej funkcionality
8	- riešenie umožňuje konfigurovať a využívať nezávislé zálohovacie politiky tak na konfiguráciu, ako aj pre jednotlivé politiky prístupu
9	- riešenie umožňuje konfigurovať a využívať nezávislé archivačné (data retention) politiky pre jednotlivé politiky prístupu
10	- riešenie umožňuje export dát v originálnom formáte
11	- zabezpečenie logov, zaznamenaných dát proti možným úpravám/zmazaniu
12	- ukladanie relácie a histórie hesiel, logov po dobu 12 mesiacov
Reporting a notifikácie	
1	- poskytuje webové užívateľské rozhranie pre reporting - umožňuje vygenerovať report všetkých aktivít administrátora/účtu
2	- rýchly a jednoduchý náhľad na všetky aktivity s použitím query buildera. V závislosti na tom, kto požaduje report – napr. IT administrátori alebo IT manažéri – je možné pridávať a odstraňovať dáta podľa potreby a požiadaviek na informácie
3	- poskytuje rozhranie pre reporting, pomocou ktorého je možné vytvárať nové zostavy bez nutnosti použiť SQL dotazy,
4	- umožňuje poskytovať preddefinované reporty s možnosťou ich parametrizácie, ako aj s možnosťou vytvárať reporty na základe aktuálnych požiadaviek
5	- umožňuje vytváranie štandardných reportov nad prístupmi, účtami, aktivitami, udalosťami, stave prístupových práv, atď.
6	- poskytuje Dashboardy/Štatistiky o „sessions"
7	- umožňuje exportovať reporty do niektorých z formátov: CSV, XLSX, XML
8	- umožňuje nastaviť upozornenia na základe vybraných udalostí (napr. prístupu na systém, použitie určitého účtu, atď.)
9	- umožňuje nastavenie prístupov k reportom pre vybraných používateľov

Kapacitné a výkonové požiadavky (licenčné)	
1	- riešenie umožňuje licenčné pokrytie 103 zariadení (serverov, ...)
2	- riešenie umožňuje pokrytie min. 50 privilegovaných externých užívateľov
3	- riešenie umožňuje pokrytie min. 15 privilegovaných interných užívateľov
4	- riešenie umožňuje pokrytie architektúry s dostupnosťou na úrovni aktiv - pasiv
Bezpečnostné požiadavky	
1	- riešenie nevyžaduje inštaláciu, klienta na pracovné stanice, ani na cieľové systémy/zariadenia
2	- riešenie umožňuje šifrovanú komunikáciu, vrátane externých užívateľov
3	- riešenie umožňuje bezpečný vzdialený prístup - vrátane vytvárania užívateľov, priradenia oprávnení, ...
4	- riešenie plne podporuje multi-tenant prostredia. Užívatelia / skupiny užívateľov majú prístup iba k vybraným účtom, systémom, auditným záznamom, konfiguráciám atď.
5	- riešenie umožňuje vysokú bezpečnosť prenášaných a uložených informácii v centrálnom a vysoko bezpečnom úložisku
6	- certifikácie riešenia bezpečnostným štandardom napr. "Common Criteria" alebo FIPS alebo ekvivalent
Ďalšie funkčné a technické požiadavky, ktoré sú očakávané od riešenia	
1	- všetky komponenty by mali spĺňať nároky na vysoké zabezpečenie a dostupnosť, vrátane databáz
2	- podpora nasadenia vo vysokej dostupnosti, vlastné technologické možnosti pre zabezpečenie High Availability, Disaster Recovery a zálohovania
3	- API pre integráciu s HelpDesk/ServiceDesk, SIEM systémami
4	- Licencia musí zahrňať podporu výrobcu v trvaní min. 12 mesiacov

Predmet plnenia spĺňa požiadavky uvedené v tomto a ostatných dokumentoch tvoriacich opis predmetu zákazky, ako aj súlad a naplnenie požiadaviek platnej legislatívy a štandardov v oblastiach informačných systémov verejnej správy a bezpečnosti (napr. metodické pokyny, manuály a pod.).

Predmetom plnenia sú implementačné a konfiguračné práce 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.

Z hľadiska kapacitných požiadaviek riešenie zabezpečuje dostatočné licenčné pokrytie pre:

- integráciu 110 systémov a zariadení,
- prístup 30 interných privilegovaných identít – zamestnancov obstarávateľa,
- prístup 150 externých privilegovaných identít – zmluvných partnerov a dodávateľov,
- ukladanie relácie a histórie hesiel, logov po dobu 12 mesiacov.

Minimálna požadovaná úroveň zabezpečenia dostupnosti na úrovni aplikačných komponentov riešenia je Aktiv – Pasiv.

V rámci implementácie riešenia je požadovaná integrácia nasledujúcich systémov:

- 38 ks Windows server 2012
- 16 ks Windows server 2019
- 1 ks Windows server 2022
- 6 ks Centos 6.x
- 19 ks CentOS 7.x
- 1 ks Rocky Linux 8.x
- 3 ks Oracle Linux 8.x
- 3 ks Rocky Linux 9.x
- 7ks Solaris 11 SPARC
- 4x F5 2200s, firmware BIG-IP 12.1.6
- 4x Check Point 6400
- 4x Cisco IronPort ESA C195

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.

Súčasťou riešenia sú perpetuálne (trvalé) licencie systému PAM, t. j. ročný náklad na podporu výrobcu po dodaní riešenia neprevyšuje 30% z ceny licencie.

.....

Ing. Andrej Bališ
Člen predstavenstva