**Tehnička specifikacija – Grupa 2. Programska podrška za upravljanje i auditing AD servisa**

Predmet nabave je nabava sustava za upravljanje i auditing poslovno kritičnih podataka koji se nalaze na IT korisničko serverskoj infrastrukturi. Sustavom mora biti obuhvaćen nadzor Naručiteljeve Microsoft Active Directory i Microsoft Exchange Serverske okoline.

Predmet nabave su i usluge vođenje projekta i implementacija sustava sigurnosnog nadzora dnevničkih

zapisa.

**Vođenje projekta**

Zahtjeva se usluga vođenje projekta koji uključuje sve točke infrastrukturnih usluga. Isporučitelj će odraditi slijedeće usluge:

* + Dokumentiranje projekta i isporuka
  + Komunikacija na projektu
  + Upravljanje projektom
  + Upravljanje rizicima na projektu
  + Upravljanje promjenama tijekom projekta
  + Upravljanje incidentima tijekom projekta
  + Upravljanje resursima i komuniciranje potrebnih resursa prema Naručitelju

**Implementacija sustava**

* + Analiza postojećeg stanja i definiranje preduvjeta
  + Dimenzioniranje infrastrukture naručitelja
  + Dizajn implementacije sustava za sigurnosnog nadzora dnevničkih zapisa
  + Izrada rulova za implementaciju
  + Konfiguracija postavki sustava
  + Implementacija rulova naručitelja
  + Testiranje i analiza
  + Prijenos znanja i edukacija osoblja naručitelja

|  |  |
| --- | --- |
| **2. Programska podrška za upravljanje i auditing AD servisa** |  |
| **Tražena funkcionalnost** | **Zadovoljava (DA/NE)** |
| Rješenje pruža jednostavnu instalaciju unutar virtualiziranog okruženja (on- prem ili cloud) te skalabilnost radi zadovoljavanja eventualnih budućih  proširenja opsega nadzora. |  |
| Rješenje ne zahtjeva distribuciju dodatnih agenata za potrebe prikupljanje podataka (tzv. agentless), a samo prikupljanje podataka neće koristiti nedokumentirane metode. Istovremeno, prikupljeni podaci se mogu  arhivirati na višegodišnji period u slučaju potrebe revidiranja istih. |  |
| Prikupljanje podataka lišenih viška sirovih podataka:  Rješenje mora prikupljati sirove, strojne podatke i pretvarati ih u precizne i jasne informacije o svakoj korisničkoj transakciji. Ne smiju se pojavljivati nečistoće iz sirovih podataka. |  |
| Pouzdani audit podaci:  Rješenje mora konsolidirati podatke iz više različitih izvora (evidencija događaja- eng. "event logs", konfiguracijski podaci, povijest promjena zapisa itd.) kako bi se dobili pouzdani audit podaci. |  |
| Konsolidirani pristup za hibridnu IT infrastrukturu:  Rješenje mora prikupljati audit podatke iz lokalnih aplikacija kao i onih u oblaku te ih čuvati u sigurnom, centralnom repozitoriju za potrebe uzbunjivanja, pretraživanja i za analizu sigurnosnog rizika. |  |
| Detaljne informacije o svakom pristupu ili mijenjanju informacija:  Rješenje mora pratiti i isporučiti sve pojedinosti o promjenama i pokušajima pristupa podacima, uključujući i informacije kada i gdje je pokušaj promjene ili pristupa nastao, tko je to napravio i što je točno promijenjeno ili čemu se pristupilo. Za vrijednosti prije i poslije promjene objekta, rješenje mora dati paralelnu usporedbu vrijednosti atributa objekta prije i nakon izmjene. |  |
| Rješenje mora pohranjivati podatke na dva načina (SQL bazu podataka za izvještavanje i komprimirane datoteke za dugoročnu pohranu). Na ovaj način sustav mora nuditi pohranu podataka na više od 10 godina bez degradacije performansi i osigurati jednostavan pristup podacima za cijelo vrijeme čuvanja. |  |
| Mogući nadzor Imeničkih servisa (Microsoft Active Directory Domain Services, skraćeno AD DS on premise) te domenske grupne politike.  Izvještavanje te pretraživanja konfiguracije na određen datum kao i  promjena unutar imeničkog servisa i grupnih politika (što, tko, kada i gdje); nadzor korisničkih prijava na nadzirane sustave (uspješne i neuspješne) uz podršku za domene kojima se vjeruje (trusted) te domenama s kojima postoji uspostavljeno povjerenje kao i nadzor korisničkih prijava korištenje Microsoft Active Directory Federation Services (AD FS) servisa. |  |
| Exchange server (hybrid licenca) - Nadziranje i izvještavanje o promjenama sigurnosnih prava na Exchange poslužiteljima i poštanskim sandučićima, promjene quota poštanskih sandučića, promjena nad bazom podataka Exchange-a, promjena grupa politika za Exchange. |  |
| Jedinstvena upravljačka konzola za potrebe dohvata, pregleda,  pretraživanja, izvještavanja i kreiranja alarma te konfiguracije rješenja. Rješenje mora posjedovati nadzorne ploče koje korisnicima omogućuju da identificiraju i procjenjuju rizike u tri ključna područja: upravljanje računima, sigurnosne dozvole i upravljanje podacima. |  |
| Nadzorna ploča za otkrivanje anomalija u sustavu:  Rješenje mora imati nadzornu ploču koja pomaže kod otkrivanja zlonamjernih korisnika u IT okruženju tako što daje agregirane podatke o anomalijama korisničkih aktivnosti s pridruženim vrijednostima rizika za svaku anomaliju. |  |
| Izvješća o ponašanju korisnika i analizi slijepe točke (eng. Blind spot analysis):  Rješenje mora imati analitiku sigurnosnih incidenata, kao što su aktivnosti van radnog vremena, neobične prijave na sustav, kratkotrajan povišen broj neuspjelih pokušaja prijave na sustav, pristup arhivskim podacima, akcije prethodno neaktivnih korisnika kao i potencijalno štetne datoteke na poslužiteljima. |  |
| Izrada pretplata za specijalizirana izvješća:  Rješenje mora podržavati sustav pretplate na način da je moguće zakazivanje dostave raznih izvješća ili skupa specifičnih kriterija pretraživanja putem e-pošte. Mora se moći kreirati pretplata za minimalno sljedeće stavke:  - Izvješća  - Rezultate pretraga  - Pregled rizika u sustavu |  |
| Osim već predefiniranih izvještaja, rješenje mora podržavati i kreiranje novih izvještaja na koje se može predbilježiti (npr. dnevno, tjedno i sl.) te ih  dobivati elektroničkom poštom ili na mrežno dijeljenoj lokaciji, ali i mogućnost izvoza sadržaja generiranih izvještaja (npr. pdf, csv, xls, doc, docx).  Također, rješenje mora pružiti mogućnost izvještavanja o usklađenosti  nadziranog okruženja ovisno o različitim standardima (GDPR, ISO 27001, SOX, NIST800-53 i sl.). |  |
| Upozorenja: rješenje mora obavještavati osoblje o sumnjivom ponašanju ili događajima koji se mogu pretvoriti sigurnosne incidente, uključujući aktivnosti koje odskaču od standardnih sigurnosnih praksi (eng. Threshod-based alerts), putem elektronske pošte ili SMS poruka.  Izvještavanje korištenjem SQL SRS-a:  Rješenje mora koristiti SQL Server Reporting Services (uz uključenu podršku za besplatni SQL Server Express) koji predstavlja industrijski standard, za pružanje širokog spektra revizorskih izvještaja. Ne smiju se koristiti vlastiti servisi (eng. proprietary engines) za izradu izvješća. |  |
| IZVJEŠĆA - rješenje mora omogućiti jednostavan pregled i analizu prikupljenih podataka nadziranih komponenti sustava te dati konsolidirani uvid o obavljenim izmjenama (tko, što, kada i gdje), kao i pregled uočenih sigurnosnih rizika vezano za ponašanje korisnika IT okruženja. Isto tako,  mora omogućiti povijesni pregled konfiguracijskih parametara (Imeničkog servisa, grupnih politika, datotečnih poslužitelja, sustava elektroničke pošte) na željeni datum. |  |
| Unaprijed definirana (već gotova) izvješća vezana za nadzor Active Directory-a:  Promjene u AD-u  • Pregled stanja AD-a  • Pregled svih promjena u AD-u  • Pregled promjena u AD-u grupirane po:  o Domenskom kontroleru  o Grupama u AD-u  o Tipovima objekata  o Korisnicima  • Pregled promjena nad kontejnerima  AD izvješća u određenom trenutku u vremenu  • Pregled dozvola po korisničkim računima u AD-u  • Pregled dozvola po objektima u AD-u  • Pregled AD grupa  • Pregled članstva u AD grupama  • Pregled administratorskih grupa  • Pregled članstva u administratorskim grupama  • Pregled korisničkih računa:  o Istekli računi  o Zaključani računi  o Računi kojima lozinka nikad ne ističe  o Računi za koje lozinka nije potrebna  o Zadnja prijava korisničkim računom  Promjene grupnih politika  • Pregled svih promjena na grupnim politikama  • Pregled promjene imena administratorskih i privremenih računa  • Promjena grupnih politika za lozinke  • Promjene grupnih politika za pristup registry-u  • Pregled promjena u postavkama Windows operativnog sustava  • Pregled postavki za bežični pristup mreži  Praćenje prijava na AD  • Pregled korisničkih računa s najvećim brojem prijava  • Pregled svih prijava na sustav  • Pregled neuspjelih prijava  • Pregled prijava i odjava s domenskog kontrolera |  |
| Za potrebe nadzora nad poslužiteljima, rješenje mora sadržavati opciju snimanja akcija korisnika na istima uz mogućnost pretrage pohranjenih video zapisa. |  |
| Sustav mora omogućiti jednostavno, ali i napredno pretraživanje  prikupljenih podataka korištenjem višestrukih filtera, a na rezultate pretrage se može predbilježiti (i iste dobivati u obliku izvještaja) ili definirati vlastite. |  |
| Povrat (eng. Rollback) promjena nad AD-om:  Rješenje mora omogućiti povrat promjena nad AD-objektima, u stanje prije promjene, bez zastoja ili obnavljanja iz sigurnosne kopije.  Obavijest o isteku zaporke:  Rješenje mora omogućiti automatsko podsjećanje korisnika AD-a da promijene svoje zaporke prije nego isteknu.  Praćenje neaktivnih korisnika:  Sustav mora moći automatski otkriti i deaktivirati neaktivne korisničke i računalne račune na temelju prilagođenih kriterija.  Upravljanje zapisima događaja (eng. Event log):  Rješenje mora moći automatski prikupljati, objedinjavati i arhivirati podatke dnevnika događaja kako bi korisnici mogli kontrolirati generičke događaje, događaje koje generiraju servisi, prijave korisnika i prijave na udaljeno računalo (eng. Remote desktop connections). |  |
| Sustav mora imati mogućnost integracije sa drugim sigurnosnim rješenjima korištenjem dokumentiranih RESTful API integracijskih opcija (npr. SIEM, helpdesk/ticketing sustavi i sl.). Rješenje mora nuditi besplatne, unaprijed pripremljene, dodatke koji pojednostavnjuju integraciju proizvoda s aplikacijama kao što su SIEM, ServiceNow ITSM, Cisco mrežni uređaji i Linux sustavi. |  |
| Uključene jednogodišnje pretplatne Active Directory on premise licence za 300 AD korisnika i 300 servisnih računa te Exhange hybrid licence za 300 AD korisnika i 300 servisnih računa. |  |
| Uključeno proizvođačko održavanje u trajanju od 12 mjeseci. |  |
| **Proizvođač** |  |
| **Naziv** |  |

Podrška proizvođača mora uključivati pravo na nove verzije softvera, otklanjanje bugova i grešaka u softveru te pravo na tehničku podrška proizvođača putem otvaranja servisnih prijava u sustavu proizvođača tokom cijelog trajanja ugovora. Ponuditelj mora ponuditi i isporučiti uslugu implementacije programskog rješenja te usluge podrške prema slijedećoj specifikaciji:

* Priprema, snimka stanja i planiranje
* Implementacije programske podrške na serverima
* Testiranje i podešavanje rješenja (fine tuning)
* Usluge reaktivnog održavanja

**Reaktivno održavanje**

Reaktivno održavanje podrazumijevaju pružanje podrške za održavanje funkcionalnosti sustava. Reaktivno održavanje uključuje otklanjanje uzroka zastoja u radu sustava, a obavlja ga se po prijavama od strane Naručitelja ili ako se i bez prijave zastoja utvrdi neispravnost istog.

Poslovi održavanja sastoje se od:

* Dostupnost Service Desk sustava i pozivnog centra Ponuditelja za prijavu incidenata
* Rješavanje incidenta
* Rješavanje (otklanjanje) uzroka kvara
* Eskalaciju incidenta prema proizvođaču opreme prema potrebi (Naručitelj osigurava licence softverske licence, proizvođačko održavanje i pristup portalu proizvođača)

**Preduvjeti koje osigurava Naručitelj, a nisu predmet nabave**

* Sve nužne informacije i odluke potrebno za realizaciju projekta
* Dostupnost i angažman djelatnika Naručitelja nužnih za realizaciju projekta
* Hardverske, sklopovske i programske preduvjete za pružanje usluga koja su predmet nabave (virtualnu okolinu sa potrebnim resursima)
* Potrebne Microsoft licence Windows Server licence i MS SQL licence
* Backup & restore sustav sa pripadajućim licencama koji će pokriti sustav iz predmeta nabave.
* Naručitelj osigurava mogućnosti udaljenog pristupa gospodarskom subjektu koji će pružati uslugu održavanja rješenja.