PRÍLOHA Č. 1 SÚŤAŽNÝCH PODKLADOV – FÁZA 1.

OPIS PREDMETU ZÁKAZKY

1. DIELO

Dielom je kyberneticko-bezpečnostný systém na zvýšenie úrovne kybernetickej a informačnej bezpečnosti pre Objednávateľa. Systém musí zohľadňovať aktíva Objednávateľa, požadované zariadenia a riešenia a všetky požiadavky na riešenie špecifikované v tejto Prílohe č. 1 Zmluvy.

Aktíva Objednávateľa:

- 750 užívateľov Microsoft Office 365
- 750 užívateľov Microsoft Sharepoint
- 750 pracovných staníc
- 2 Active Directory serverov
- 2 Exchange servery
- 12x fyzický a 104x virtuálny Windows Server
- 2 + 2 virtualizačných / HCI serverov
- fyzicky oddelená LAN 4x10 ks
- 4 wifi Controller
- 40 sieťových prepínačov
- 4 sieťové smerovačov
- 6 firewallov
- 2 proxy servery
- 1+1 EOL Network Access Control zariadenia
- 2 DNS servery
- 2 DHCP serverov
- 2 loadbalancing zariadenia
- 2 databázových inštancií
- 20 webových serverov
- 20 aplikačných serverov
- 1 systém pre správu zraniteľností pre 1500 IP zariadení
- 2 zariadenia pre behaviorálnu analýzu siete
- 1 EDR systém pre 750 zariadení
- 400 VPN používateľov
- 10 pracovníkov s právami pre: (IT admin, bezpečnosť, audit, schvaľovateľ prístupov)
- 30 informačných systémov alebo aplikácii na samostatných serveroch alebo VPNkách
- 750 ks koncových staníc
- monitoring siete: Microsoft endpoint configuration manager - Microsoft Systém Center Configuration Manager

Požadované zariadenia a riešenia:

A. **Komplexná bezpečnostná platforma pozostávajúca z nasledujúcich modulov**:
   - modul pre ochranu kritických serverov
   - modul pre monitorovanie sieťovej komunikácie
   - modul pre ochranu sieťovej komunikácie
   - modul pre ochranu emailovej komunikácie
   - modul pre ochranu prístupu do internetu
   - modul pre správu IT aktív a ich rizík
   - modul pre threat inteligence
   - modul pre bezpečnostné testovanie
B. **Vulnerability_Management**
C. **SW nástroj pre manažment IT aktív a sietí**
D. **Nástroj SIEM**
E. **Systém pre behaviorálnu analýzu dátových tokov**
F. **SW nástroj pre pokročilú ochranu koncových bodov**
G. **Nástroj pre správu a riadenie prístupov k IT systémom – pre správcov systémov a privilegovaných používateľov informačných systémov**
H. **HW platforma a SW pre potreby prevádzkovania systému kybernetickej a informačnej bezpečnosti (KIB)**

Dodávaný materiál musí byť dodávaný iba nový, nepoužitý od výrobcu konkrétneho HW alebo SW so zárukou výrobcu.

Inštalácia systému

Požaduje sa v rámci inštalácie dodať zariadenia, umiestniť ich v Dátovom centre, zrealizovať základné spustenie, otestovať funkčnosti komponentov a vypracovať kompletnú dokumentáciu.

Fyzické dodanie zahŕňa dopravu, rozbalenie a skompletovanie komponentov, ekologickú likvidáciu odpadov. Umiestnenie do technologických stojanov zahŕňa inštaláciu do technologických stojanov, drobné elektroinštalačné práce spojené s pripojením do siete (nakáblovanie). Základné spustenie do prevádzky zahŕňa spustenie napájania zariadení a zariadení, aktiváciu prístupových portálov výrobcu, aktiváciu softvérových a hardvérových licencií u výrobcu, aktualizáciu firmvérov komponentov, aplikovanie základných nastavení firmvérov komponentov. Celkové testovanie funkčnosti zahŕňa testovanie redundantného pripojenia na elektrickú sieť, testovanie redundantného pripojenia na LAN sieť, testovanie funkčnosti výmeny redundantných komponentov počas prevádzky, spustenie diagnostických nástrojov, ktoré zariadenie obsahuje. Dokumentácia pozostáva z dokumentu, ktorý podrobne popíše konfiguráciu, vrátanie nastavenia firmvérov, umiestenie a káblovanie zariadení.

Realizáciou Predmetu Zmluvy sleduje Objednávateľ splnenie nasledovných cieľov:

- **Holistický prístup k ochrane pred externými aj internými hrozbami**, ktorý kombinuje rôzne bezpečnostné technológie a prístupy.

- **Nástroje pre efektívny manažment IT aktív a ich rizík vrátane konfigurácií,** ktoré pomôžu identifikovať IT aktíva, bezpečnostné riziká a opatrenia na ich mitigáciu. Pre Manažéra kybernetickej bezpečnosti poskytuje prehľadné reporty o bezpečnostnej situácii organizácie, ktoré sa dajú ľahko prezentovať vedeniu.
- **Pokročilé riešenia pre detekciu a reakciu na hrozby**, ktoré využívajú technológie EDR (Endpoint Detection and Response) a XDR (Extended Detection and Response) na identifikáciu a mitigáciu sofistikovaných kybernetických útokov.
- **Komplexná ochrana koncových bodov**, ktorá zahŕňa antimalvérovú ochranu, prevenciu ransomvéru, kontrolu aplikácií a ďalšie pokročilé bezpečnostné funkcie.
- **Zabezpečenie sieťovej komunikácie** s dôrazom na ochranu prístupu k internetu, ochranu emailovej komunikácie a monitorovanie sieťovej prevádzky.
- **Systematický prístup k manažmentu zraniteľností** a riadeniu záplat, ktorý pomáha udržiavať systémy aktualizované a odolné voči známym hrozbám.
- **Virtuálne patchovanie prinesie** kľúčovú úlohu v správe zraniteľností tým, že poskytuje rýchlu ochranu proti akútnym hrozbám, Tento prístup je obzvlášť cenný v situáciách, kedy organizácie nemôžu okamžite aplikovať oficiálne záplaty kvôli časovým obmedzeniam alebo potrebe testovania v produkčnom prostredí.
- **Ochrana dát pri** spracovaní, prenose a ukladaní s využitím princípov Zero Trust architektúry a pokročilej ochrany emailovej komunikácie

Monitoring a management
Kyberneticko-bezpečnostný systém musí umožňovať vzdialený monitoring a manažment prostredníctvom štandardného webového prehliadača.

Dodaný systém/bezpečnostné riešenie musí predstavovať jeden integrovaný celok, ktorý v sebe spĺňa všetky požadované funkčné a nefunkčné špecifikácie, vrátane ochrany koncových bodov, sieťovej komunikácie, emailov, správu IT aktív a ich rizík a threat inteligence.

A. Komplexná bezpečnostná platforma

1. Všeobecné požiadavky

Bezpečnostná platforma musí:

1) byť dostupná ako cloudová služba (SaaS) s možnosťou on-premise nasadenia pre vybrané komponenty.
2) poskytovať jednotné správcovské rozhranie pre správu všetkých komponentov platformy

3) poskytovať možnosť konfigurácie politík pre všetky moduly z jedného miesta
4) umožňovať pridávať alebo odoberať funkcionality podľa potrieb organizácie
5) umožňovať integráciu nových modulov bez potreby komplexných zmien v existujúcej infraštruktúre
6) správa poskytovateľov identít
7) správa účtov
8) správa užívateľských účtov a rolí
9) umožňovať správu aktív v rôznych bezpečnostných doménach (email, cloud, sieť, mobil, identita a dáta), poskytovať centralizovaný monitoring a reportovanie
10) poskytovať jednotné rozhranie pre sledovanie bezpečnostných udalostí zo všetkých zdrojov
11) umožňovať vytvárať a spúšťať automatizované workflow pre bežné bezpečnostné operácie (automatická reakcia na incident, pravidelné spustenie skriptu,..)
12) poskytovať centralizovaný prehľad všetkých spravovaných zariadení a systémov
13) poskytovať automatickú detekcia a kategorizáciu nových zariadení v sieti
14) Integrácia s Microsoft Information Protection (MIP) pre dešifrovanie a skenovanie šifrovaných emailov a súborov
15) Integrácia s Microsoft Identity Protection (MS Entra ID) pre riadenie prístupu rizikových používateľov
16) Integrácia s bežnými SIEM a SOAR produktmi

2. **Modul pre ochranu kritických serverov**
3. **Modul pre ochranu koncových bodov**
4. **Modul pre monitorovanie sieťovej komunikácie**
5. **Modul pre ochranu sieťovej komunikácie**
6. **Modul pre ochranu emailovej komunikácie**
7. **Modul pre ochranu prístupu do internetu**
8. **Modul pre zabezpečenie riadenie IT aktív a ich rizík**
9. **Modul pre bezpečnostné testovanie**

B. Vulnerability_Management

C. SW nástroj pre manažment IT aktív a sietí

D. Nástroj SIEM

E. Systém pre behaviorálnu analýzu dátových tokov

F. SW nástroj pre pokročilú ochranu koncových bodov

G. Nástroj na správu a riadenie prístupov k IT systémom – pre správcov systémov a privilegovaných používateľov informačných systémov

H. HW platforma a SW pre potreby prevádzkovania systému kybernetickej a informačnej bezpečnosti (KIB)

2. PODPORA

Nepretržitá podpora v režime 24 hodín denne 7 dní v týždni s možnosťou zadať problém alebo incident priamo výrobcovi softvéru, alebo jeho certifikovanému partnerovi, s garantovanou dobou odozvy na kritické incidenty do 2 (dvoch) hodín, po dobu 36 (tridsaťšesť) mesiacov od riadneho odovzdania Diela. Detailný popis požadovanej Podpory je zadefinovaný v Prílohe č.2 Zmluvy, bod 7. Prevádzka a údržba.

Nepretržitá podpora v režime 24 hodín denne 7 dní v týždni s garantovanou dobou hardvérovej opravy do 24 (dvadsiatich štyroch) hodín, po dobu 36 (tridsaťšesť) mesiacov od riadneho odovzdania Diela, pričom oprava aj výjazd technika na opravu je pokrytý touto podporou. Oprava zariadenia musí byť realizovaná priamo výrobcom, alebo jeho lokálnym autorizovaným servisným partnerom (zastúpením).

Počas doby Podpory musí byť poskytnutý prístup k aktuálnym verziám strojových kódov a k aktuálnym verziám licenčného softvéru a jeho súčastí, ktorý tvorí neoddeliteľnú súčasť ponúkaných zariadení.

Aktualizácia (fixy a patche)
Aktualizácia sa požaduje realizovať pravidelne 1 (jeden) krát za kalendárny štvrťrok aktualizáciu strojového kódu a softvéru zariadení. Aktualizácia bude realizovaná v rámci patchovacieho okna v čase pracovného voľna od 22:00 do 6:00.

3. SLUŽBY NA OBJEDNÁVKU

Služby na objednávku sú služby definované Objednávateľom v čase dodávky Diela. Ide o jednoduché služby IKT, ktoré vyplynuli z potreby realizácie Diela a nebolo ich možné špecifikovať pred začatím realizácie Diela. Ide o služby ako napr.:

- zmena konfigurácie nastavenia systému alebo jednotlivých modulov v súvislosti so zmenou pripojenej kritickej infraštruktúry počas inštalácie systému,
- doplnenie konfigurácie systému o nové zariadenia doplnené do infraštruktúry počas inštalácie systému,
- integrácia nových funkcionalít systému, ktoré boli ohlásené počas implementácie systému a počas celej doby zmluvnej podpory,
- doplnenie a aktualizácia bezpečnostnej dokumentácie a užívateľskej dokumentácie o nové funkcionality, ktoré boli ohlásené a dodané počas implementácie systému.

Súčasťou prílohy č. 1 – Opis predmetu zákazky je zároveň príloha č. 1a – Opis predmetu zákazky – Konfigurácia HW.