B. OPIS PREDMETU ZÁKAZKY

Mesto Trstená realizuje projekt s názvom Podpora v oblasti kybernetickej a informačnej bezpečnosti v meste Trstená, kód projektu: 401101FMI9, ktorý bol schválený v rámci výzvy : PSK-MIRRI-611-2024-DV-EFRR - Podpora v oblasti kybernetickej a informačnej bezpečnosti na regionálnej úrovni - verejná správa. V rámci projektu mesto vyhlásilo verejné obstarávanie s názvom: **„Technologické riešenie pre oblasť KIB mesta Trstená“**

Výsledky projektu budú plniť nasledujúce špecifické ciele výzvy:

- RSO 1.2 Využívanie prínosov digitalizácie pre občanov, podniky, výskumné organizácie a orgány verejnej správy

Cieľom výzvy je podporiť a realizovať opatrenia KIB definované **najmä v zákonoch č. 69/2018 Z. z.** o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len „zákon č. 69/2018 Z. z.“ resp. „ZoKB“) a č. **95/2019 Z. z.** o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov (ďalej len „zákon o ITVS“).

Realizácia projektu je stanovená nasledujúcimi míľnikmi:

- Dodanie tovarov – do 12 mesiacov od nadobudnutia účinnosti zmluvy;
- Dodanie služieb okrem SLA – najneskôr do 12 mesiacov od nadobudnutia účinnosti zmluvy;
- Dodanie Služby podpory prevádzky/SLA (zabezpečenie podpory SOC/SLA 24/7) sa bude realizovať – po dobu 5 rokov od protokolárneho prevzatia tovarov a služieb.

Pri realizácii zákazky sa bude postupovať v súlade s Vyhláškou Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky č. 401/2023 Z. z. o riadení projektov a zmenových požiadaviek v prevádzke informačných technológií verejnej správy

V rámci projektu sa bude realizovať komplexné technologické riešenie pozostávajúce z nasledovných opatrení:

Položka 1 - Nasadenie informačného systému pre identifikáciu a riadenie rizík v zmysle zákona č. 69/2018 Z. z. a vyhlášky 362/2018 Z. z. (§6) v rovine riadenia, revízie a aktualizácie potrebnej dokumentácie.

Informačný systém pre identifikáciu a riadenie rizík musí spĺňať tieto funkčné vlastnosti:

- správa aktív – vedenie zoznamu aktív subjektu, vrátane ich vlastníkov
- správa zraniteľností – vedenie zoznamu rozpoznaných zraniteľností, vrátane ich vlastníkov
- správa hrozieb – vedenie zoznamu rozpoznaných hrozieb
- správa opatrení – vedenie zoznamu opatrení potrebných na potlačenie zraniteľností
- správa vzťahov – evidencia rozpoznaných vzťahov medzi aktívami a zraniteľnosťami
- správa rizík – identifikácia a ohodnotenie rizík na základe pravdepodobností hrozieb, uplatňovaných opatrení a dopadov na subjekt,
- semikvantitatívna prípadne kvantitatívna metóda hodnotenia významnosti rizík,
- číselné ohodnotenie pravdepodobnosti hrozieb a účinnosti opatrení,
- významnosť rizík vyjadrená číselne a následne kategorizovaná.

Používateľské rozhranie a výstupy musia spĺňať tieto požiadavky:

- pre interakciu s používateľom musí byť k dispozícii webové rozhranie bez špeciálnych nárokov na webový prehliadač v plnej podpore slovenského jazyka,
    - výstupy musia byť realizované vo forme prehľadov a zostáv vo formáte PDF alebo .xlsx vyhotovené v slovenskom jazyku vrátane šablón a komentárov,
    - softvér musí umožňovať riadiť prístup používateľov k obsahu rizikovej analýzy.

Správa používateľov musí umožňovať:

- evidenciu používateľov, oprávnených pristupovať k subjektom a identifikovať resp. manažovať ich riziká,
- širokú integráciu na existujúce systémy správy používateľov,
- prideľovanie rolí oprávneným používateľom s rôznym stupňom oprávnení.

IS pre identifikáciu a riadenie rizík musí umožňovať vykonávať revízie a aktualizáciu rizikovej analýzy, riadiť riziká, aktíva, zraniteľnosti a hrozby systémom, ktorý dokumentuje históriu a je auditovateľný. Verejný objednávateľ požaduje informačný systém typu klient – server nasadený u verejného obstarávateľa na jeho serveri bez závislosti na cloudových službách, aktualizáciách cez internet a inom komerčnom programovom vybavení okrem operačného systému.

Požiadavky na výkon činností manažéra pre riadenie rizík prostredníctvom IS pre identifikáciu a riadenie rizík:

- tvorba analýz rizík podľa potreby a požiadaviek verejného obstarávateľa,
- pravidelné hodnotenie a ošetrovanie rizík,
- tvorba plánu eliminácie rizík,
- správa aktív a ich vlastníkov,
- dohľad nad riadením rizík.

Verejný obstarávateľ požaduje oceniť a implementovať časovo neobmedzenú licenciu informačného systému pre identifikáciu a riadenie rizík pre jedného používateľa, ako aj zrealizovať inštaláciu a na serveroch verejného obstarávateľa, vyškoliť zamestnancov verejného obstarávateľa a zabezpečiť výkon špecialistu na riadenie rizík (manažéra pre riadenie rizík) až do termínu ukončenia realizácie projektu.
Požiadavky na výkon činností špecialistu pre riadenie rizík:

- zabezpečovanie procesu riadenia rizík,
- detailná identifikácia kľúčových aktív (nielen informačných), zraniteľných miest v prevádzkových postupoch i spôsoboch využívania technológií,
- návrh konkrétnych opatrení smerujúcich k náprave zistených nedostatkov členených podľa priority realizácie a náročnosti
- realizácia zmien v štruktúre aktív Mesta Trstená.

Položka 2 - Vypracovanie kontinuity činností v zmysle ZoKB – riadenie kontinuity činností - Business Continuity Management (BCM) v zmysle zákona č. 69/2018 Z. z. a vyhlášky 362/2018 Z. z. (§17)

Kontinuita činností musí zadefinovať scenáre rôznych udalostí, ktoré potenciálne môžu mať negatívny vplyv na bežné činnosti organizácie ako sú napríklad:

- náhla nedostupnosť personálu či nepoužiteľnosť pracoviska/budovy,

- nedostupnosť technologickej infraštruktúry či potrebných médií,
- incident či živelná katastrofa.

V rámci kontinuity činností musia byť stanovené požiadavky na zdroje (adekvátne finančné, materiálno-technické a personálne zdroje), ktoré budú potrebné na implementáciu vybraných stratégií kontinuity činností. V zmysle požiadaviek zákona o kybernetickej bezpečnosti sa musí určiť, čo má byť:

- hlavným cieľom plánu kontinuity s ohľadom na riadenie incidentov v prípade katastrofy alebo iného rušivého incidentu a ako sa obnovia činnosti v stanovených termínoch,
- strategickým imperatívom procesu riadenia kontinuitu s ohľadom na predchádzanie ďalším stratám.

Súčasťou kontinuity činností musí byť vypracovanie analýzy funkčných dopadov a kvalifikácia potenciálnych dopadov a straty v prípade prerušenia alebo narušenia prevádzky u všetkých procesov organizácie. Požiadavkou analýzy funkčného dopadu musí byť určenie:

- cieľovej doby obnovy jednotlivých procesov, siete a informačných systémov a aplikácií, a to najmä určením doby obnovy prevádzky, po uplynutí ktorej je po kybernetickom bezpečnostnom incidente obnovená najnižšia úroveň poskytovania základných služieb,
- cieľového bodu obnovy jednotlivých procesov, siete a informačných systémov základnej služby, a to najmä určením najnižšej úrovne poskytovania služieb, ktorá je dostatočná na používanie, prevádzku a správu siete a informačného systému a zachovanie kontinuity základnej služby.

Kontinuitou musia byť zavedené postupy zálohovania na obnovy siete a informačného systému po jeho narušení alebo zlyhaní v dôsledku kybernetického bezpečnostného incidentu obsahujúce najmenej:

a) frekvenciu a rozsah zdokumentovania a schvaľovania obnovy záloh,
b) určenie osoby zodpovednej za zálohovanie,
c) časový interval, identifikáciu rozsahu údajov, zadefinovanie dátového média zálohovania a zabezpečenie vedenia dokumentácie o zálohovaní,
d) umiestnenie záloh v zabezpečenom prostredí s riadeným prístupom,
e) zabezpečenie šifrovania záloh obsahujúcich aktíva klasifikačného stupňa chránené a prísne chránené,
f) vykonávanie pravidelného preverenia záloh na základe vypracovaného plánu, testovanie obnovy záloh a precvičovanie zavedených krízových plánov najmenej raz ročne.

Kontinuita činností musí obsahovať minimálne:

1. Plán kontinuity na stanovenie požiadaviek a zdrojov,
2. Plán reakcie na incidenty a plány havarijnej obnovy prevádzky,
3. Politiku a ciele kontinuity,
4. Analýzu funkčných dopadov,
5. Stratégiu riadenia kontinuity vrátane evakuačných postupov,
6. Plán údržby a kontroly BCMS.

Požiadavky na výkon činností manažéra pre riadenie kontinuity činností:

a. riadenie incidentov v prípade katastrofy alebo rušivého incidentu,
b. realizácia a výkon interných auditov a analýz dopadov,
c. precvičovanie zavedených krízových plánov,
d. aktualizácia plánov reakcie na incidenty a plánov obnovy po katastrofe,
e. návrh opatrení riadenia kontinuity,
f. monitorovanie zariadení podstatných pre prípadný vznik incidentu.

Verejný obstarávateľ požaduje oceniť, vytvoriť a zaviesť kontinuitu činností v plnom rozsahu stanovenom zákonom č.: 69/2019 Z. z. o kybernetickej bezpečnosti a vyhláškou č.: 362/2018 Z. z., ako aj implementovať procesy kontinuity v podmienkach verejného obstarávateľa, vyškoliť zamestnancov verejného obstarávateľa a zabezpečiť výkon špecialistu (manažéra pre riadenie kontinuity) až do termínu ukončenia realizácie projektu.

Položka 3 - Zavedenie a správa nástroja na riadenie kapacít v zmysle zákona č. 69/2018 Z. z. a vyhlášky 362/2018 Z. z. (§11) prostredníctvom systému na monitorovanie zariadení, technológií a služieb s dosahom na zabezpečenie kybernetickej bezpečnosti

Musí byť pokryté monitorovanie dostupných technologických kapacít dôležitých sieťových zariadení a služieb podľa nakonfigurovaných pravidiel. Monitorovací nástroj musí informovať o vzniknutých technických problémoch a nedostatku kapacít správcu príslušnej služby alebo servera. Musí byť schopný monitorovať rôzne druhy zariadení ako sú fyzické a virtuálne servery, sieťové prvky, dátové úložiská a iné zariadenia, ktoré dokážu poskytnúť údaje o svojej prevádzke. Monitoring musí byť v reálnom čase s možnosťou údaje okamžite vizualizovať prostredníctvom grafov, máp a rôznych náhľadov. Musí byť schopný porovnávať dáta v rôznych časových obdobiach, analyzovať históriu.

Funkčné požiadavky:

- Monitorovanie kľúčových informačných systémov a ich jednotlivých komponentov
- Nastavenie prahových hodnôt alertov a notifikácií
- Eskalácia notifikácií
- Tvorba reportov
- Tvorba vlastných sledovacích schém.
-

Do monitoringu bude zahrnutých 10 zariadení a služieb, komponentov infraštruktúry z množiny:

- Sieťových a výkonových zariadení
- VMware služieb
- Databázových a zálohovacích zariadení
- Webových služieb
- Kritického hardvéru.

Zber údajov musí podporovať:

- Agentov SNMP a IPMI
- Bezagentový a špeciálny monitoring
- Monitoring virtuálnych zariadení
- Webové aplikácie a Java scenáre
- Monitoring databáz
- Kalkulované a agregované položky
- Interné sledovanie výkonu.

Musí byť podporovaná vizualizácia vo webovom rozhraní a informovanosť v rozsahu:

- Grafov a máp so zloženými pohľadmi
- Globálnych Dashboardov
- Prístupu k získaným hodnotám a zoznamu udalostí

- Zasielania oznámení
- Potvrdenia a eskalácie prijatých informácií
- Schopnosti prijať opatrenia.

Systém musí byť schopný automatizácie, napr. cez Network alebo Low-level discovery. Musí byť schopný správy aj cez smartfón, schopný nasadenia vlastných skriptov s prístupom k funkciám cez API. Musia sa dať definovať pravidlá hodnotenia údajov poskytujúce logické definície stavu zariadení.

Položka 4 - Zriadenie SOC ako služby v prevádzke 24/7

Dodávka služieb súvisiacich s dohľadovým centrom bezpečnostných incidentov – SOC (Security Operations Center). Služba musí zahŕňať:

- zber a monitorovanie udalostí v sieťach a kritických prvkoch informačných systémov v režime 24/7,
- nepretržitá detekcia kyberneticko-bezpečnostných incidentov,
- zber relevantných informácií pri zistených kybernetických incidentoch,
- návrh riešenia kybernetických bezpečnostných incidentov a zníženia následkov zistených kybernetických bezpečnostných incidentov,
- vyhodnocovanie riešenia kybernetických bezpečnostných incidentov a návrh systémových opatrení s cieľom minimalizovať výskyt obdobných kybernetických bezpečnostných incidentov,
- podrobná evidencia bezpečnostných incidentov, ich riešení a príslušnej komunikácie prostredníctvom na to určeného nástroja (ticketing/service desk),
- pravidelný reporting (1 x mesačne).

Sondu pre zber dát požadujeme – virtuálne zariadenie. Súčasťou dodávky zariadenia je jej inštalácia a implementácia v rozsahu:

- inštalácia funkcionality zbierania záznamov z prevádzky informačných systémov,
- zabezpečenie a sprevádzkovanie sieťovej konektivity,
- konfigurácia systémov SOC s ohľadom na špecifickosť prostredia.

Minimálne požiadavky na systém SIEM:

- Dodané riešenie musí byť dostatočne stabilné, bezpečné a musí poskytovať nasledovné základné prevádzkové vlastnosti:
    - intuitívne používateľské rozhranie,
    - možnosť parametrizácie (možnosti používateľského nastavenia a /prispôsobenia),
    - umožňovať centralizovanú správu,
    - umožňovať širokú podporu monitorovaných systémov (hardware / software),
- Systém SIEM musí ďalej podporovať rozhrania a protokoly pre získavanie informácií minimálne v nasledujúcom rozsahu:
    - CEF
    - Syslog TCP/UDP
    - FTP
    - SCP
    - SNMP

    - ODBC / JDBC
    - CP-LEA
    - SDEE
    - Priame získavanie z databáz Oracle, MS SQL a prípadné iné
    - Integrácia na API
    - Vstupy priamo zo súboru
    - Čítanie Windows event collection WinRM/RPC
    - Log file
- Riešenie musí umožniť rozšírenie na vyšší počet EPS v budúcnosti
- Riešenie musí umožňovať poslať notifikáciu o každej zmene prístupových práv do SIEM.
- Riešenie musí umožňovať, aby všetky informácie v rámci SIEM systému boli logované (na úroveň používateľského identifikátora). SIEM musí disponovať vlastným logovacím modulom, ktorý bude logovať vlastné operácie formou auditných logov.
- Riešenie musí umožňovať prezerať vlastné log. záznamy.
- Riešenie musí umožňovať uchovávať auditné logy na úroveň používateľského identifikátora.
- Riešenie musí umožňovať prezerať uchované auditné logy. o Riešenie musí umožňovať generovanie viacerých úrovní reportov.
- Riešenie musí umožňovať personalizovať reporty zobrazované v používateľskom rozhraní.
- Riešenie musí umožňovať personalizovať exportované reporty. o Riešenie musí poskytovať preddefinované reporty s možnosťou ich parametrizácie, ako aj s možnosťou vytvárať reporty na základe aktuálnych požiadaviek. o Riešenie musí umožňovať exportovať ľubovoľný report do niektorých z formátov: CSV, XLSX, XML.
- Riešenie musí umožňovať tlač ľubovoľného reportu.
- Riešenie musí byť flexibilné a musí generovať rôzne typy reportov na požiadanie alebo v periodických intervaloch.
- Riešenie musí poskytnúť rozhranie pre reporting, pomocou ktorého je možné vytvárať nové zostavy pomocou grafického editora bez nutnosti zostavovať databázové querry.
- Riešenie používa štandardne výrobcom SIEM odporúčané korelačné algoritmy.
- Riešenie musí umožňovať individuálne vytvárať a nastavovať korelačné algoritmy.
- Riešenie musí umožňovať personalizovať dashboardy zobrazované v používateľskom rozhraní.
- Riešenie musí umožňovať vnorenie do logov priamo z grafiky zobrazovaného reportu alebo udalosti (tzv. „drill down“).
- Riešenie musí umožňovať vyšetrovanie vektora zachyteného útoku, t.j zdroja útoku, použitého nástroja, použitej cesty, spôsobu vedenia útoku a cieľ útoku.
- Riešenie musí umožňovať export logov a auditných logov.
- Riešenie by malo umožňovať aby exportované logy a auditné logy boli v takom formáte, ktorý je možné elektronicky podpísať.
- Riešenie musí umožňovať logovať všetky úkony vykonané v monitorovaných systémoch rolami ako napr. administrátormi, vývojármi a analytikmi.
- Riešenie musí umožňovať integráciu s threat intelligence feeds podľa štandardov STIX/TAXII.

- Riešenie musí umožňovať rýchle a intuitívne vytváranie reportov, dashboardov a korelačných scenárov.
- Riešenie musí umožňovať normalizáciu prijatých logov. o Riešenie musí umožňovať sledovať (monitorovať) zmeny nastavenia úrovne logovania na úrovni monitorovaných systémov, ak tieto takúto možnosť poskytujú.
- Riešenie musí umožňovať aby prenášané dáta boli zabezpečené proti možnej manipulácii počas prenosu zo zdroja ak to zdrojové zariadenie podporuje
- V riešení musí byť integrovaný nástroj pre behaviorálnu analýzu používateľov - administrátorov.
- Riešenie musí umožňovať rýchle vyhľadanie v auditných záznamoch, tieto musia byť indexované.
- Riešenie musí umožňovať riadenie prístupov na základe najmenších privilégií.
- Riešenie musí umožniť rozšírenie o možnosť analyzovať a vyhodnocovať incidenty aj na základe strojového učenia.
- Riešenie SIEM musí umožniť spojiť dva a viac incidentov s rovnakým indexom (napr. používateľ, IP adresa, vlastný atribút) do jedného celku a poskytnúť tak komplexný pohľad na incident.
- Riešenie musí umožniť integráciu prostredníctvom otvoreného API rozhrania využiteľného na integráciu s riešením tretích strán.
- Riešenie musí umožniť rozšírenie funkcionality pomocou aplikačného frameworku s verejne dostupným obsahom od výrobcu riešenia a výrobcov tretích strán.
- Riešenie musí umožňovať vykonávať analýzu dlhodobých trendov, ktoré vychádzajú z predchádzajúcich udalostí.

Vyžadované SLA parametre sú:

Kategórie incidentov	**Garantovaný čas odozvy SOC**
Incident kategórie HIGH - vysoko nebezpečné incidenty, ktoré môžu spôsobiť vážne škody resp. môžu mať negatívny dopad na kritické aktíva.	maximálne 2 hodiny
Incident kategórie MEDIUM - incidenty strednej závažnosti, t.j. ktoré akútne neohrozujú kritické časti prostredia.	maximálne 4 hodiny
Incident kategórie LOW - incidenty nízkej závažnosti bez priameho negatívneho vplyvu na kontinuitu služby.	maximálne 8 hodín

Zoznam kategórií bezpečnostných incidentov

Kategória	**Subkategória**	**SLA priority**
Sociálne inžinierstvo	Nevyžiadaná pošta	LOW
	Obťažovanie	LOW
	Vyhrážanie	LOW
	Potláčanie práv a slobôd	LOW
Škodlivý kód	Vírus, červ, Trójsky kôň	MEDIUM
Získavanie	Skenovanie siete	MEDIUM
	Odpočúvanie	MEDIUM
	Sociálne inžinierstvo	MEDIUM
Pokus o prienik	Využitie známej zraniteľnosti	MEDIUM

	Opakované pokusy o prihlásenie	MEDIUM
	Útok s neznámymi znakmi	MEDIUM
Podozrenie na úspešný prienik do systému	Skompromitovanie privilegovaného účtu	HIGH
	Skompromitovanie obmedzeného účtu	HIGH
	Skompromitovanie aplikácie	HIGH
	Botnet	HIGH
Nedostupnosť	DoS, DDoS	MEDIUM
	Sabotáž	MEDIUM
Ohrozenie bezpečnosti Informácii	Neoprávnený prístup k informáciám	MEDIUM
	Neoprávnená zmena Informácii	MEDIUM
Podvod	Neoprávnené využívanie	MEDIUM
	Porušenie autorských práv	MEDIUM
	Prevzatie identity	MEDIUM
	Phishing	MEDIUM
Iné		LOW

Monitorované zariadenia

Popis	**Počet**	**Proaktívny monitoring**
Firewall	1	8 x 5
Server pre zálohovanie	1	8 x 5
Domain Controler (Active Directory)	2	8 x 5
Korwin - Spracovávanie, evidencia a riadenie informácií hospodársko-správnych agend a výkonu kompetencií miest a obcí v zmysle platnej legislatívy.	1	8 x 5
Memphis - Správa registratúry	1	8 x 5
Mail server	1	8 x 5
Webová stránka - www.trstena.sk	1	8 x 5

Súčasťou služby a jej ceny sú všetky implementačné, softvérové, hardvérové a licenčné prostriedky potrebné pre jej chod.

Položka 5 - Nasadenie zálohovania

Nasadenie zálohovania na osobitnom zálohovacom serveri:

- Obstaranie SW a HW riešenia a licencií
- Implementácia zálohovacieho systému
- Analýza zálohovacích boxov a pravidiel
- Nasadenie obnovy záloh
- Zaškolenie personálu Prevádzkovateľa

Minimálne parametre zálohovacieho systému:

- RackStation 2,2GHz, 4GBRAM, 8xSATA, 2xUSB3.0
- kapacita 40TB SATA, 6Gb/s, 256MB cache, 7200 ot., min. 4 disky
- čítanie / zápis dát min.: 2300 / 1100 MB/s
- podpora sieťových kariet 10GbE SFP+/RJ-45 a 25GbE SFP28
- 2 x switch 24x1G port, 4xGE SFP, L2+L3
- 2 x switch 24x1G port, 4xGE SFP, L2+L3, 12 x POE (min. 802.3at (PoE+), minimálny celkový PoE budget ~150–200 W)
- štandardné L2 funkcionality, t. j. 802.1Q VLAN, Spanning Tree (STP/RSTP, prípadne MSTP), LACP (Link Aggregation), port mirroring, storm control, IGMP snooping
- L3 funkcionality: postačuje základné statické smerovanie, vrátane definície statických trás a možnosti ACL (Access Control Lists),
- redundantný zdroj napájania,
- Minimálne 3 VLAN s možnosťou mať ich všetky aktívne,
- Minimálna switching capacity na úrovni zodpovedajúcej plnoduplexnej prevádzke na všetkých portoch (napr. 56 Gbps a viac, pri 24×1G + 4×SFP). Forwarding rate úmerne k tomu (napr. > 40 Mpps),
- s podporou SNMP v2c,
- záruka 5 rokov,
- technická a systémová podpora 8/5.

Riešenie musí obsahovať:

- pokročilú technológiu vytvárania snímkov zaisťujúcu plánovateľnú a temer okamžitú ochranu dát zdieľaných zložiek a jednotiek LUN,
- obnovu dát na úrovni súborov a zložiek s obnovením konkrétnych súborov alebo zložiek,
- flexibilný systém kvóty pre zálohy,
- automatické opravy súborov napr. pomocou zrkadlených metadát a konfiguráciou RAID,
- vloženú komprimáciu dát pred zápisom na disk,
- možnosť integrácie s ľubovoľnou virtualizačnou platformou,
- zálohovanie bez licencií určených k ochrane počítačov a serverov so systémom Windows,
- virtuálnych počítačov, ďalších súborových serverov a cloudových aplikácií,
- konsolidáciu úloh zálohovania pre fyzické i virtuálne prostredie s možnosťou rýchleho obnovenia súborov, celých fyzických počítačov a virtuálnych počítačov,
- webové (GUI) a CLI rozhranie, prípadne REST API pre správu,

- zálohovanie v prostredí Google Workspace, Gmail, kontaktov, kalendárov a služby Drive zálohovanie dát sady Microsoft 365, OneDrive for Business, SharePoint Online, e-mailov, kontaktov a kalendárov.

Položka 6 - Vypracovanie analýzy dopadov

Analýza dopadov musí:

- identifikovať rôzne kategórie procesov na základe ich kritickosti a posúdiť ich vzájomné závislosti,
- určiť potenciálne dôsledky (škody/straty) pri rôznych dobách trvania kritických situácií,
- stanoviť maximálne akceptovateľné doby prerušenia (MTO),
- stanoviť minimálne ciele kontinuity podnikania (MBCO),
- určiť cieľové časy obnovy (RTO) a cieľové body obnovy (RPO),
- identifikovať potenciálne dopady vyplývajúce z možného prerušenia činností a stanoviť výšku:
    - funkčných dopadov,
    - finančných dopadov,
    - dopadov spôsobených stratou údajov a dokumentov.
- identifikovať zdroje a prostriedky na obnovu procesov so zásadným vplyvom na kontinuitu činností organizácie na základe hodnoty RTO procesu v min. tomto typovom rozsahu zdrojov:
    - ľudia,
    - aplikácie / databázy,
    - údaje uložené v elektronickej podobe (nezahrnuté v aplikáciách a databázach),
    - údaje uložené na papierovom médiu,
    - IT a komunikačné zariadenia,
    - komunikačné kanály,
    - ostatné vybavenie,
    - vybavenie a infraštruktúra,
    - pracovný kapitál.

Záverečná správa, ako výstup z analýzy dopadov musí obsahovať:

- prehľad vykonávaných činností, ktorý bude obsahovať názov činnosti, jej vymedzenie, vlastníka, MTO a MBCO,
- zoznam procesov, ktorý bude (ak to je možné) obsahovať názov procesu, druh procesu, vlastníka procesu, RTO a RPO procesu (údaje, na základe ktorých bolo stanovené príslušné RTO a RPO budú taktiež súčasťou správy),
- špecifikácie nevyhnutných zdrojov a prostriedkov pre zabezpečenie kontinuity činností.

Pri analýze dopadov je potrebné identifikovať:

- kritické obdobie,
- množstvo práce vykonanej v kritickom období,
- minimálne prijateľné množstvo práce vykonávanej bezprostredne po krízovej situácii,
- či môže definovaný typ krízovej situácie spôsobiť prerušenie procesu.

Pričom kritickým obdobím až krízovou situáciou môže byť:

- nedostupnosť informačných technológií a/alebo dát,
- nedostupnosť prevádzkových priestorov,
- nedostupnosť kritickej časti ľudských zdrojov – zamestnancov,

- zlyhanie kľúčového externého dodávateľa služieb.

Položka 7 Dodanie a nasadenie servera
Minimálne parametre servera:

- RackStation
- Procesor 2x Intel Xeon Silver 4309Y 2.8G, 8C/16T, 10.4GT/s, 12M Cache
- pamäť 2x 64GB RDIMM, 3200MT/s,
- pevný disk 2x M.2 Sticks 480GB
- pevný disk 6 x 1.2TB Hard Drive ISE SAS 12Gbps 10
- iDRAC9 Enterprise 15G (alebo ekvivalent),
- záruka min. 5 rokov
- redundantný zdroj napájania
- technická a systémová podpora 8/5.
- 2 x switch 48 x 1G port, 4 xGE SFP, L2+L3
- 2 x switch 48 x 1G port, 4 xGE SFP, L2+L3 24xPOE

Licencie:

Počet ks	Licencia
1	Windows Server® 2022,Standard,16CORE
50	Windows Server® 2022 - device cal
4	SQL server 2022 standart 2core

Montáž, inštalácia servera, nastavenie Domény, konfigurácia Active Directory, migrácia dát a migrácia databáz.

Položka 8 - WiFi prístupový bod a switche
Počet ks 8 WI FI prístupových bodov
Minimálne parametre:

- Štandard WiFi: Súlad s IEEE 802.11a/b/g/n/ac/ax (min. WiFi 6).
- Maximálna prenosová rýchlosť: Až 2400 Mb/s.
- Pásmo: Dual-Band (podpora pre 2.4 GHz a 5 GHz frekvencie), umožňujúce efektívne spravovanie siete a minimalizáciu rušenia.
- Bezpečnostné protokoly: Podpora min. WPA-PSK a WPA-Enterprise, zabezpečujúca pokročilú ochranu a autentifikáciu v sieťových prostrediach.
- Napájanie: PoE (Power over Ethernet) kompatibilita, umožňujúca jednoduchú a flexibilnú inštaláciu bez potreby samostatných elektrických zdrojov.
- Technológia: MU-MIMO (Multi-User, Multiple Input, Multiple Output), zvyšujúca efektivitu prenosu dát v prostrediach s viacerými používateľmi.
- 2 x switch 8 x 1G port, 2 x GE SFP, L2+L3, 8 x POE,
- štandardné L2 funkcionality, t. j. 802.1Q VLAN, Spanning Tree (STP/RSTP, prípadne MSTP), LACP (Link Aggregation), port mirroring, storm control, IGMP snooping
- L3 funkcionality: postačuje základné statické smerovanie, vrátane definície statických trás a možnosti ACL (Access Control Lists),
- Centrála správa – manažovateľná (roaming, monitoring, jednotlivé politiky, aktualizácie).

Položka 9 - Dodanie a implementácia next-gen firewall technológie
NGFW musí obsahovať:

- Next-Generation Firewall (NGFW) v redundantnej konfigurácii, t. j. dve fyzické zariadenia, ktoré budú fungovať v režime vysokej dostupnosti (High Availability – HA).
- štandardné funkcie brány firewall, ako je kontrola stavu
- IPS ochranu (Integrovaná prevencia vniknutia) založenú na štatistickej analýze, heuristickej analýze, analýze protokolu, pasívneho DNS monitoringu a vlastnej signatúry na na rozpoznanie tajných hrozieb a ich rýchle zastavenie
- zariadenie musí vedieť identifikovať aplikáciu z obsahu dátového toku a nie len podľa použitého portu (Aplication Visibility Control -AVC)
- musí vedieť detegovať a blokovať škodlivý kód ako sú počítačové vírusy, spywary, botnety, počítačové červy a trojské kone (Advanced Malware protection - AMP)
- musí vedieť vykonať SSL/TLS dekrypciu šifrovanej prevádzky pre potreby jej analýzy
- musí podporovať sandboxovú analýzu neznámych hrozieb.
- podpora pre OSPF, BGP, policy routes
- musí umožniť vytváranie virtuálnych firewallov
- musí umožniť definíciu bezpečnostných zón a ich používanie pri tvorbe bezpečnostných politík.
- Podpora DHCP v režime Server alebo Relay. Pri funkcii DHCP servera musí umožňovať aj statické prideľovanie IP adries zariadeniam
- musí vedieť vytvárať IPSec VPN tunely s podporou IKEv1 a IKEv2
- musí umožniť tvorbu bezpečnostných politík na základe aplikácie alebo aplikačnej skupiny politík
- musí umožniť tvorbu bezpečnostných politík na základe užívateľskej identity a príslušnosti užívateľa v užívateľskej skupine.
- správa zariadenia pomocou webového grafického používateľského rozhrania (GUI) a cez príkazový riadok
- musí obsahovať reporting o zachytených hrozbách, podľa používateľov, spojení, zdrojov a pod
- musí obsahovať sadu preddefinovaných reportov a taktiež možnosť vytvárať vlastné reporty
- musí vedieť zaslať udalosti o stave zariadenia a o stave bezpečnostných politík pomocou protokolov Syslog, SNMP a SNTP
- musí obsahovať minimálne 1 x USB Management port.
- musí mať rozhrania na firewalle využiteľné pre spracovanie komunikácie minimálne 6 x GE RJ45 port
- musí podporovať Link Aggregation IEEE 802.3ad.
- musí mať podporu dvoch WAN rozhraní v konfigurácii failover.
- musí podporovať integrácia používateľov s Active Directory.
- musí mať podporu TLS minimálne verzie 1.3.
- musí obsahovať Antivírus
- musí obsahovať Web filter
- musí obsahovať Antispam
- musí obsahovať SD-WAN router
- musí obsahovať UTM firewall
- musí obsahovať možnosť zapojenia firewallu v režime vysokej dostupnosti.

Výkonnostné parametre minimálne:

- Priepustnosť FW pri zapnutí IPS minimálna priepustnosť ~~1,4~~ 1 Gbps
- Priepustnosť FW pri zapnutí IPS, Application Control, Antivirus, Web Filtering a zapnutým logovaním minimálne ~~900~~ 800 Mbps.
- Počet súčasných TCP spojení firewallu minimálne ~~1,5~~ 1 milion.
- Počet nových TCP spojení za sekundu (setup-rate) minimálne ~~45000~~ 40000.
- URL filt. & AMP): 900 Mbps
- Priepustnosť SSL dešifrovania/SSL inšpekcie minimálne ~~715~~ 700 Mbps (HTTPS prevádzka, merané v kombinácii s IPS kontrolou).
- minimálny počet súčasných VPN spojení: ~~200~~ 50 pre GW to GW IPsec VPN Tunnels, ~~2500~~ 2000 pre Client to GW IPsec VPN Tunnels
- počet firewall policies minimálne ~~5000~~ 2000.
- Podpora redundantných rozhraní.
- podpora minimálne ~~10~~ 5 virtuálnych firewall domén/kontextov
- min. 6x 1GE LAN porty 10/100/100BASE-T
- min. 2x 1GE WAN porty (combo RJ45/SFP)
- form faktor: rack mount, 1RU
- napájanie 230 V AC
- Vnútorná pamäť ~~128~~ 64 GB SSD.
- ~~Možnosť správy v prípade 2 stupňového overenia až pre 500 tokenov (ako SW, tak HW token forme).~~
- Podpora centrálnej správy až pre 16 smerovačov a minimálne 48 prístupových bodov.

Implementácia NGFW:

- analýza súčasného stavu
- návrh implementačného konceptu a dizajnu riešenia
- inštalácia nového HW v priestoroch objednávateľa
- základná konfigurácia FW (IP adresa, názov, zóny, manažment ....)
- vytváranie nových pravidiel podľa pripraveného konceptu
- konfigurácia VPN tunelov
- migrácia objektov, smerovania, NAT
- migrácia komunikačných pravidiel
- integrácia so všetkými prvkami sieťovej infraštruktúry
- testovanie riešenia v testovacom prostredí
- migrácia do produkčného prostredia
- vyriešenie komunikačných problémov (prepojenie na externé subjekty, portály a pod.
- Z inštalácie a kompletnej konfigurácie zariadenia
- Aktualizácia, vypracovanie a dodanie príslušnej systémovej a používateľskej dokumentácie k vykonaným zmenám
- Zaškolenie IT personálu
- Podpora – 5 rokov
- Licencie s platnosťou minimálne 5 rokov

Položka 10 - Notebook a príslušenstvo

Minimálne parametre:

- **Základné informácie:** Operačný systém: Windows 11 Pro 64-bit, zabezpečujúci pokročilé správcovské funkcie a bezpečnostné nástroje.

- **Procesor:** Procesor, poskytujúci vysoký výkon pre multitasking a náročné aplikácie. Počet jadier: Minimálne 14 , umožňujúce efektívnu prácu s viacerými aplikáciami súčasne. Pamäť cache: 24 MB, zvyšujúca rýchlosť prístupu k často používaným dátam. Frekvencia: 3,80 – 5,00 GHz, poskytujúca dynamické zrýchlenie v závislosti od záťaže.
- **Pamäť:** RAM: 32 GB (2x16GB), DDR5-3200 MHz, zabezpečujúca vysokú rýchlosť a kapacitu pre náročné úlohy.
- **HDD:** 1000 GB M.2 PCIe SSD, zabezpečujúci rýchly štart systému a aplikácií, ako aj dostatočnú kapacitu pre údaje a programy.
- **Displej:** Veľkosť: 15,6 palca (39,62 cm). Pomer strán: 16:9, štandardný pomer pre väčšinu aplikácií a multimédií. Povrch: Matný, minimalizujúci odrazy a zlepšujúci čitateľnosť na priamom svetle. Technológia: IPS, poskytujúci široké pozorovacie uhly a živé farby. Typ: LCD s LED podsvietením, zaručujúci dobrú viditeľnosť a energetickú efektívnosť.
- **Grafika:** Minimálne 8 GB, GDDR6, nezdieľaná grafická pamäť, poskytujúca vysoký grafický výkon pre graficky náročné aplikácie a hry.
- **Porty a pripojenie:** USB 3.1: 2x USB 3.1 Typ-C: 2x HDMI: 1x Analógový audio I/O: 1x Bezdrôtové pripojenie: WiFi s podporou MU-MIMO a Bluetooth.
- **Multimédia a vstupné zariadenia:** Webová kamera: HD Klávesnica: Lokalizácia SK, s numerickou časťou, podsvietená, vodeodolná.
- **Bezpečnostné funkcie:** Bezpečnostný zámok: Áno, poskytujúci fyzickú ochranu pred krádežou.
- **Príslušenstvo:** Taška
- **Kancelársky softvér**: Office

Pri realizácii je potrebné postupovať v zmysle nasledujúcej legislatívy:

- Zákon č. 69/2018 Z.z. o Kybernetickej bezpečnosti
- Zákon č. 45/2011 Z.z. o Kritickej infraštruktúre
- Zákon č. 351/2011 Z.z. o elektronických komunikáciách (ochrana súkromia a osobných údajov, ochrana sietí a zariadení)
- Zákon č. 272/2016 Z.z. o dôveryhodných službách (elektronický podpis) a o dôveryhodných službách pre elektronické transakcie na vnútornom trhum (EiDAS)
- Trestný zákon č. 300/2005 Z.z. (trestné činy páchané pomocou elektronických prostriedkov a v elektronickom prostredí)
- Vyhláška č. 179/2020 Z.z. k spôsobom kategorizácie a obsahu bezpečnostných opatrení ITVS
- Metodika pre Systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti (CSIRT)
- Smernica č. 7/2019 o riešení Bezpečnostných incidentov Vládnou jednotkou CSIRT
- Vyhláška NBU č. 166/2018 Z.z., o podrobnostiach o technickom, technologickom a personálnom vybavení jednotky pre riešenie kybernetických bezpečnostných incidentov
- Vyhláška NBU č. 164/2018 Z.z., ktorou sa určujú identifikačné kritériá prevádzkovanej služby (kritériá základnej služby)
- Vyhláška NBU č. 362/2018 Z.z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení

- Vyhláška NBU č. 436/2019 Z.z., o audite kybernetickej bezpečnosti a znalostnom štandarde audítora

Návrh na plnenie kritérií/cenová ponuka je samostatnou prílohou k špecifikácii.