Opis predmetu zákazky :

Modul 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 funkčných 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.

Užívateľské 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 vyhotovené v slovenskom jazyku vrátane šablón a komentárov,
- softvér musí umožňovať riadiť prístup užívateľov 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 byť 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 31.10.2023.

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

Kontinuita činností musí zadefinovať scenáre rôznych udalostí, ktoré potencionálne 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 potencionálnych 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:

- plán kontinuity na stanovenie požiadaviek a zdrojov,
- plán reakcie na incidenty a plány havarijnej obnovy prevádzky,
- politiku a ciele kontinuity,
- analýzu funkčných dopadov,
- stratégiu riadenia kontinuity vrátane evakuačných postupov,
- 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 31.10.2023.

Modul 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 IPM
- 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.

Modul 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 x 7,
- nepretržitá detekcia kybernetickо-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 – viruálne 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.

Vyžadované SLA parametre sú:

	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**
	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	**Typ zariadenia/názov produktu**	**Počet**	**Proaktívny monitoring**
Firewall	Fortigate 60E	1	8 x 5
virtuálny server pre informačný systém samosprávy	MS Windows 2012 R2	1	8 x 5
virtuálny server pre zálohovanie	MS Windows 2012 R2	1	8 x 5
Domain Controler(Active Directory)	MS Windows 2012 R2	2	8 x 5

Popis	Typ zariadenia/názov produktu	Počet	Proaktívny monitoring
virtuálny server pre zverejňovanie na egov.revuca.sk	MS Windows 2012 R2	1	8 x 5

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

Modul 5. Nasadenie DLP

Nasadenie DLP ako služby je rozdelené do nasledovných krokov:

- Obstaranie SW riešenia a licencií
- Zavedenie DLP do testovaco adaptačnej prevádzky
- Analýza pracovných procesov a dátových tokov a definovanie detekčných pravidiel
- Optimalizácia detekčných pravidiel
- Nasadenie DLP na 60 ks pracovných staníc ako produkčný zdroj informácií pre SOC
- Zaškolenie personálu Prevádzkovateľa

Súčasťou riešenia musí byť aj celkový report zistení s návrhom opatrení.

Všeobecné požiadavky:

- Integrácia s MS Active Directory, Podpora pre MS SQL 2012 alebo novšia,
- Podpora operačných systémov Windows 7, 8.1, 10 a 11.
- Podpora serverových operačných systémov Windows Server 2016, 2019 a 2022. P
- Podpora terminálových prostredí ,
- Centrálna administrátorská konzola, multitenantná administrácia v súlade s organizačným členením subjektov na úrovni OU domény,
- Riadené užívateľské práva do nastavení konzoly, k výsledným logom a administrácie riešenia,
- Skrytý režim na koncovej stanici vrátane procesov a zložiek, a to vrátane lokálnych i doménových administrátorov.

Ochrana proti zastaveniu systému (musí byť aktívna u bežného užívateľa, lokálneho i doménového administrátora, Ochrana proti zastaveniu procesov; V prípade vyšších užívateľských práv dôjde k reštartu zastavených procesov či k použitiu iných spôsobov pre obnovu služby, Ochrana proti odinštalovaniu riešenia bez potrebnej autorizácie, Ochrana proti editácii registrov, systémových komponentov či DLL knižníc, Ochrana proti zmene nastavenia na koncovej stanici, Nutná možnosť ochrany i u operačného systému v režime “safe mode”.

Funkcionality zachované i v offline móde, (ak koncová stanica nie je pripojená k firemnej sieti/ internetu). Možnosť pracovať s historickými dátami. Riešenie musí podporovať možnosť poskytnúť

zálohovanie vlastných komponentov, prevažne všetkých záznamov a nastavení. Automatické generovanie emailových varovaní v prípade incidentov, možnosť zmeniť citlivosť a špecifikáciu incidentu. Automatické generovanie emailových reportov s možnosťou úprav obsahu (množstvo informácií, množina uzlov, frekvencie odosielanie, príjemcovia). Zasielanie logov do SIEM riešenia objednávateľa.

Dátový audit:

- Detailné informácie o aplikáciách, ako čas spustenia a ich aktívnom využití. Aplikácie sú rozdelené do kategórií pre prehľadnú správu. Detailné informácie o weboch, ako ich aktívne využitie, informáciách o URL, použitom protokole, hlavičky webu, a to bez ohľadu na použitý prehliadač. Weby sú rozdelené do kategórií pre prehľadnú správu.
- Detailné informácie o práci so súbormi, ako prehľad užívateľov a aplikácií pracujúcich so súbormi, súborové operácie (otvorenie, premenovanie, kopírovanie, mazanie) a informácie o cestách (systémové, externé, webové, cloudové). Lokálne súborové operácie – kopírovanie, presúvanie, sťahovanie z webu, FTP, mazanie, vytvorenie, otvorenie, a to vrátanie zdrojovej a cieľovej identifikácie: cesta, typ zariadenia, jedinečný identifikátor, Logovanie tlačených úloh a možnosť exportu reportov do XLS, PDF.

Zaznamenávanie komunikácie:

- Podpora POP3, IMAP, MAPI / Exchange protokolov vrátanie SSL šifrovania,Podpora desktopových emailových klientov (Microsoft Outlook, Mozilla Thunderbird,…) – riešenie je schopné zaznamenávať emaily nezávisle od použitej aplikácie, Podpora zaznamenávania súborov odoslaných cez web mailových klientov, Podpora zaznamenávania súborov odoslaných cez IM komunikačné nástroje.

Zaznamenávanie Office 365 cloudu:

- Zaznamenávanie bežných užívateľských akcií prevedených na Office 365 cloudu (OneDrive for Business, SharePoint Online) - základné súborové operácie ako sťahovanie a zdieľanie,
- Zaznamenávanie Office 365 emailové komunikácie (Exchange Online) pre všetkých užívateľov vrátane užívateľov pracujúcich z Outlook Web App, osobných alebo mobilných zariadení.

Všeobecná ochrana: Definícia kategórií citlivých dát dovoľuje obmedzenie pohybu a práce s týmito dátami; určuje, ktoré média môžu byť použité pre prenos, ktoré siete môžu byť použité pre upload, na ktoré emailové adresy môžu byť dáta odoslané, ktoré aplikácie môžu s dátami pracovať. Možnosť aplikácie politík pre konkrétne aplikácie – definícia zdroja a cieľa (prístup na externé zariadenie, sieť, tlač, virtuálnu tlač) a správa užívateľských operácií (použitie schránky, snímanie obrazovky).

- Možnosť správy nepovolených cloudových úložísk.
- Možnosť úplne blokovať užívateľské akcie, informatívna notifikácia užívateľa či samotné logovanie užívateľských akcií, ochrana citlivých dát, možnosť definície citlivých dát pomocou preddefinovaných slovníkov a algoritmov.
- Možnosť definície citlivých dát pomocou vlastných reťazcov či regulárnych výrazov. Možnosť importu vlastných slovníkov.

- Možnosť nastavenia počtu výskytov citlivých údajov. Dynamické reštrikcie nad súbormi a aplikáciami, pokiaľ je detekovaný citlivý obsah.
- Blokácia odoslania dát s citlivým obsahom mimo koncovú stanicu – správa bežných komunikačných kanálov: e-mail, web upload, externé zariadenie, IM komunikačné nástroje, synchronizácia s cloudovými aplikáciami.
- Detekcia dát obsahujúcich citlivý obsah, uložených na koncovej stanici alebo na zdieľanom sieťovom disku. Možnosť integrácie s klasifikáciou tretích strán uložených v metadátach súborov.
- Reštrikcie pre USB zariadenia, pamäťové karty, Bluetooth zariadení, optické disky či FireWire.
- Možnosť vynútenia režimu iba na čítanie u pripojených zariadení.
- Zaznamenávanie všetkých pripojených vzdialení vrátane monitorov, myší a klávesníc. Správa mobilných zariadení – MDM (Android, iOS): Správa, GPS lokalizácia, Vzdialený zámok zariadení. Vzdialené zmazanie zariadení.
- Správa aplikácií.

Osobitné požiadavky na plnenie Modul 5

- Dodávateľ sa zaväzuje do 3 pracovných dní od účinnosti zmluvy predložiť objednávateľovi kontaktné údaje osoby/osôb zodpovednej za riadne plnenie predmetu zmluvy v rozsahu: meno, priezvisko, telefónne číslo a e-mail a zároveň predloží aj telefónne číslo a e-mailovú adresu na hlásenie servisných požiadaviek objednávateľom.
- Dodávateľ do 3 dní od nadobudnutia účinnosti Zmluvy preukáže, že disponuje vlastným systémom na nahlasovanie porúch v režime 24x7 a to minimálne telefonicky, e-mailom s centrálnou adresou monitorovanou počas poskytovania podpory
- Dodávateľ sa zaväzuje garantovať dostupnosť špecialistu na SAFETICA DLP riešenie v pracovnom čase 08:00 – 16:00 hod. s reakčnosťou do 4 hodín.
- Objednávateľ považuje za nevyhnutné na riadne poskytnutie plnenia predmetu zmluvy:
- a) disponovanie minimálne dvomi certifikovanými technikmi na produkt SAFETICA DLP,
- ISO/IEC 27001 (systém manažérstva informačnej bezpečnosti).

Modul 6. 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
- záruka 5 rokov
- kapacita 12TB SATA, 6Gb/s, 256MB cache, 7200 ot.
- čítanie / zápis dát min.: 2300 / 1100 MB/s
- podpora sieťových kariet 10GbE SFP+/RJ-45 a 25GbE SFP28
- redundantný zdroj napájania
- technická a systémová podpora 8/5.

Riešenie musí obsahovať:

pokročilú technológiu vytvárania snímkou 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.
- 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.