MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Príloha č. 1 k Záznamu z PTK

Aktualizovaný návrh opisu predmetu zákazky

Názov zákazky podľa verejného obstarávateľa: Centralizovaný manažment riadenia kybernetickej bezpečnosti verejnej správy

Stručný opis predmetu zákazky:

Zákazka je obstarávaná v rámci projektu „Centralizovaný manažment riadenia kybernetickej bezpečnosti vo verejnej správe[1]", ktorý súvisí najmä s naplnením povinností definovanými v zákone č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon o KyB") a v zákone č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov (ďalej len „zákon o ITVS").

Verejný obstarávateľ predpokladá zadanie danej nadlimitnej zákazky postupom verejnej súťaže, pričom predpokladá, že predmet zákazky bude rozdelený na štyri časti a uchádzač bude môcť predložiť ponuku na každú časť jednotlivo (t.j. na jednu alebo na viacero resp. na všetky časti predmetu zákazky). Verejný obstarávateľ predpokladá, že výsledkom verejného obstarávania bude Zmluva podľa § 269 ods. 2 zákona č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov, ktorá bude uzavretá pre každú časť predmetu zákazky samostatne.

Predpokladaný názov príslušnej časti predmetu zákazky / Predpokladaná lehota na realizáciu danej časti predmetu zákazky:

Časť I: Vládny informačný systém kybernetickej bezpečnosti (VISKB) / 11 mesiacov od účinnosti zmluvy.

Časť II: Vytvorenie metodík, vytvorenie bezpečnostnej a vzorovej dokumentácie pre rôzne druhy OVM, vykonanie analýzy rizík a analýzy dopadov (AR/BIA) v rámci MIRRI a podpora projektov v rámci dopytovej výzvy „Rozvoj governance a úrovne informačnej a kybernetickej bezpečnosti v sektore VS“ / 12 mesiacov od účinnosti zmluvy.

Časť III: Overenie spôsobu implementácie bezpečnostných opatrení prostredníctvom malých pilotných riešení na MIRRI: Implementácia nového 10Gbps Firewallu, implementácia dvojfaktorovej autentifikácie a pilotná implementácia log manažment systému / 10 mesiacov od účinnosti zmluvy.

Časť IV: Overenie spôsobu implementácie bezpečnostných opatrení prostredníctvom malých pilotných riešení na MIRRI: Analýza a pilotná implementácia konceptu bezpečnej správy mobilných zariadení používaných v rámci MIRRI / 10 mesiacov od účinnosti zmluvy.

[1] Detail žiadosti o nenávratný finančný príspevok Centralizovaný manažment riadenia kybernetickej bezpečnosti verejnej správy <https://www.itms2014.sk/schvalena-zonfp?id=656475f1-8bdf-41bc-be30-fec5bf51d694>

1 NÁVRH OPISU ČASTI I. PREDMETU ZÁKAZKY: Vládny informačný systém kybernetickej bezpečnosti (VISKB)

1.1 Špecifikácia úlohy

Cieľom zákazky je podporiť Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky (ďalej ako „MIRRI“) pri výkone správy (governance) v sektore VS, t.j. vytvoriť Vládny informačný systém kybernetickej bezpečnosti (VISKB), ktorý bude MIRRI a jednotlivým OVM slúžiť ako podporný nástroje pre udržiavanie základných evidencii a parametrov v oblasti informačnej a kybernetickej bezpečnosti potrebných pre naplnenie legislatívnych požiadaviek na zvýšenie úrovne informačnej a kybernetickej bezpečnosti a ochrany IKT a sietí používaných v sektore VS.

1.2 Všeobecné vymedzenie predmetu zmluvy

Predmetom zákazky je vývoj a implementácia Vládneho informačného systému kybernetickej bezpečnosti (VISKB).

1.3 Požadované aktivity

V rámci vyššie definovaného predmetu zákazky je požadované dodať najmä nasledovné aktivity:

- Vývoj, testovanie, implementácia a nasadenie Vládneho informačného systému kybernetickej bezpečnosti (VISKB):
  - Centrálny modul VISKB.
  - Centrálny portál VISKB.
  - Samostatný (offline) klientsky modul VISKB.

1.4 Požadované výstupy

Č.	Oblasť A)	Poznámka
	Centrálny modul VISKB	Vývoj, testovanie, implementácie a nasadenie modulu VISKB na uloženie a spracovanie zbieraných údajov z jednotlivých organizácií verejnej správy. Modul pozostáva z relačnej databázy na uloženie štruktúrovaných údajov a webovej aplikácie prístupnej oprávneným používateľom umožňujúcej vyhľadávanie, prezeranie, export a úpravu údajov. Modul zabezpečuje na pravidelnej báze import a aktualizáciu údajov z portálu VISKB. Súčasťou modulu je aj rozhranie na správu portálu VISKB.
	Centrálny portál VISKB	Centrálny portál VISKB slúži na: • nahrávanie údajov zo samostatného klientskeho modulu, • zadávanie a úpravu zbieraných údajov prostredníctvom webového rozhrania pre organizácie, ktoré nemajú nasadený samostatný klientsky modul, • vypĺňanie dotazníkov. Portál pozostáva z relačnej databázy na uloženie šifrovaných údajov, webového rozhrania na nahrávanie a úpravu údajov o organizácii a webového rozhrania pre vypĺňanie dotazníkov. Tieto webové rozhrania budú prístupné z externého prostredia (Internetu) prostredníctvom protokolu HTTPS.

	Samostatný (offline) klientsky modul VISKB – pilot pre MIRRI	Vývoj, testovanie, implementácie a nasadenie modulu VISKB: Samostatný (offline) používateľský nástroj, ktorý umožní evidenciu potrebných údajov v oblasti IB a KYB, najmä evidenciu kontaktných údajov a základných údajov o organizácii, evidenciu aktív, klasifikáciu a kategorizáciu, dáta z AR/BIA, katalóg rizík a pod. a následne umožní riadenie životného cyklu požadovaných údajov a export vybraných údajov do centrálneho modulu VISKB.

1.5 Špecifikácia jednotlivých modulov VISKB

1.5.1 Špecifikácia centrálneho modulu VISKB na spracovanie údajov

Centrálny modul VISKB na spracovanie údajov slúži na uloženie a spracovanie zbieraných údajov z jednotlivých organizácií verejnej správy. Modul pozostáva z relačnej databázy na uloženie štruktúrovaných údajov a webovej aplikácie prístupnej oprávneným používateľom umožňujúcej vyhľadávanie, prezeranie, export a úpravu údajov. Modul zabezpečuje na pravidelnej báze import a aktualizáciu údajov z portálu VISKB. Súčasťou modulu je aj rozhranie na správu portálu VISKB.

1.5.1.1 Spracovávané a zbierané informácie

V rámci modulu sa o jednotlivých organizáciách budú ukladať a spracovávať štruktúrované údaje rôznych typov. V tejto časti špecifikácie sú uvedené základné typy údajov, ktoré musia byť podporované v čase odovzdania diela, no riešenie musí byť navrhnuté, implementované a zdokumentované tak, aby bolo možné v budúcnosti uvedené typy rozšíriť o ďalšie atribúty, ako aj pridať nové typy údajov.

Informácie, ktoré VISKB potrebuje od inštitúcií, a ktoré by teda mali byť medzi evidovanými a exportovanými do centrálneho modulu sú:

- Základné údaje o organizácii:
  - názov organizácie,
  - adresa organizácie,
  - typ organizácie (podľa číselníka typov),
  - poznámka.
- Kontaktné údaje:
  - Meno,
  - e-mail,
  - telefón na pracovisko,
  - mobilný telefón,
  - roly osoby (roly podľa číselníka rolí a možnosť textového popisu iných rolí),
  - dostupnosť kontaktu (8x5, 24x7, ...),
  - poznámka.
- IPv4 adresy:
  - IPv4 adresa alebo rozsah IPv4 adries (adresa siete/dĺžka masky),
  - účel použitia danej adresy (adries),
  - poznámka.
- IPv6 adresy:
  - IPv6 adresa alebo rozsah IPv6 adries (prefix/dĺžka),
  - účel použitia danej adresy (adries),

  - poznámka.
- Doménové mená:
  - doménové meno,
  - priradená IPv4 adresa,
  - priradená IPv6 adresa,
  - účel použitia doménového mena,
  - poznámka.
- Sieťové služby:
  - názov služby,
  - doménové meno služby,
  - IPv4 a IPv6 adresa služby,
  - URL služby (pre služby na báze HTTP(S)),
  - čísla portov a transportné protokoly,
  - siete, z ktorých je služba prístupná (Internet, GOVNET, ... - podľa číselníka),
  - popis služby,
  - ID služby / príslušného informačného systému v MetaIS,
  - klasifikácia služby podľa dôvernosti, integrita a autentickosti, dostupnosti (číselníkové položky),
  - identifikácia, či je služba základnou službou podľa Zákona o kybernetickej bezpečnosti,
  - poznámka.
- Softvér:
  - typ softvéru (operačný systém, aplikačný softvér, firmvér hardvéru, ... - číselníková položka),
  - názov softvéru,
  - verzia softvéru,
  - ID softvéru (podľa číselníka softvéru),
  - počet inštancií softvéru,
  - informácia, či je daný softvér použitý aj na systémoch prístupných z externých sietí,
  - informácia, či je daný softvér použitý aj na systémoch slúžiacich pre poskytovanie základnej služby,
  - poznámka.
- Aktíva
  - rôzne atribúty (typ, hodnota) - minimálne:
    - ID aktíva
    - Názov aktíva
    - Typ aktíva (číselníková položka - PC, server, informačný systém, rôzne sieťové prvky, ...)
    - Popis aktíva
    - IP adresa (aj viacnásobne)
    - MAC adresa (aj viacnásobne)
- Klasifikácia a kategorizácia IS a sietí.
- Parametre a výsledky výkonu (realizácie) AR/BIA (identifikované riziká, hrozby, zraniteľnosti, RTO, RPO, priradenie vlastníkov a pod.) .
- Katalóg rizík (a ich previazania na jednotlivé aktíva), vrátane spôsobov ich riadenia a aktuálneho stavu implementácie prijatých opatrení, termínov, zodpovedných osôb a pod. (komplexný manažment identifikovaných rizík), najmä nasledovné typy údajov:
  - ID rizika,
  - názov rizika,
  - popis rizika,
  - ID aktíva, ktorého sa riziko týka,

    - oblasť riadenia IB, ktorej sa riziko týka (podľa ISO 27002, zákon č. 69/2018 a vyhláška č. 362/2018, zákona o ITVS a aj vyhlášky č. 179/2020 Z. z.),
    - dátum identifikácie rizika,
    - hodnota inherentného rizika (ako výsledok hodnoty dopadu rizika a pravdepodobnosti výskytu hrozby a uplatnenia zraniteľnosti),
    - implementované opatrenia na zníženie/odstránenie rizika,
    - previazanie na politiky pokrývajúce jednotlivé riziká formou uvedenia/výberu názvu konkrétnej politiky (politík) a prípadne odkazu na konkrétnu politiku,
    - hodnota reziduálneho rizika,
    - vlastník rizika,
    - plánované opatrenia na zníženie/elimináciu reziduálneho rizika,
    - termín realizácie plánovaných opatrení,
    - dátum poslednej aktualizácie,
    - atď.
- Evidencia bezpečnostných a iných auditov a bezpečnostných posudzovaní a technických zraniteľností – plán auditov a zoznam realizovaných auditov. Evidované musia byť najmä nasledovné typy údajov:
    - typ auditu (audit kybernetickej bezpečnosti, bezpečnostný audit, audit súladu, technický audit /konfiguračná previerka, testovanie zraniteľností, pentest/, follow-up audit,
    - forma auditu (interný audit / externý audit),
    - plánovaný termín auditu (od - do),
    - termín skutočnej realizácie auditu,
    - odkaz na auditnú správu,
    - atď.
- Evidenciu kybernetických incidentov
- Odpovede na otázky v dotazníkoch:
    - identifikácia dotazníka,
    - identifikácia otázky,
    - kód odpovede,
    - hodnota odpovede.

Okrem údajov týkajúcich sa jednotlivých organizácií sa v rámci modulu budú ukladať a spracovávať údaje globálneho charakteru:

- Dotazníky:
    - názov dotazníka,
    - úvodný popis dotazníka,
    - informácia o role osoby, ktorej je dotazník určený,
    - informácia, či je dotazník otvorený.
- Otázky dotazníkov:
    - identifikácia dotazníka,
    - označenie otázky,
    - typ otázky (podľa číselníka typov otázok),
    - text otázky,
    - pomocné informácie o umiestnení otázky v dotazníku.

1.5.1.2 Číselníky

Systém bude obsahovať potrebné číselníky, najmä:

- typy organizácií,
- roly kontaktných osôb,
- externé siete,

- klasifikačné stupnice pre dôvernosť, integritu a autentickosť, dostupnosť,
- typy softvéru,
- typický softvér a jeho verzie,
- typy otázok v dotazníkoch a definícia prípustných odpovedí.

1.5.1.3 Požiadavky na funkcionalitu

Funkcionalita modulu bude prístupná prostredníctvom webového rozhrania. Okrem toho bude modul zabezpečovať pravidelný import a aktualizáciu údajov z portálu VISKB. Jednotlivé oblasti funkcionality sú bližšie špecifikované v nasledujúcich častiach.

1.5.1.3.1 Identifikácia autentifikácia používateľa

- identifikácia a autentifikácia používateľa pomocou mena a hesla a následné pridelenie rolí,
- zmena a reset hesla,
- príprava na použitie dvojfaktorovej autentifikácie.

1.5.1.3.2 Spracovanie údajov o organizáciách

- vyhľadanie, zobrazenie a úpravu informácií o konkrétnej organizácii,
- vyhľadávanie a zobrazenie údajov minimálne na základe:
  - IPv4/IPv6 adresy (hľadá sa vo všetkých IPv4 a IPv6 adresách a rozsahoch evidovaných v rôznych typoch záznamov) s možnosťou vložiť do vyhľadávania aj zoznam IP adries,
  - doménového mena (hľadá sa vo všetkých doménových menách evidovaných v rôznych typoch záznamov) s možnosťou vložiť do vyhľadávania aj zoznam doménových mien,
  - používaného softvéru,
  - roly osoby,
  - typu organizácie,
  - (čiastočného) názvu organizácie,
- zobrazenie údajov jedného typu s možnosťou filtrovania podľa atribútov typu,
- export údajov jedného typu (z každého zobrazenia) vo formáte csv,
- export evidovaných údajov zvolených typov o organizácii vo formáte xml

1.5.1.3.3 Správa dotazníkov a spracovanie odpovedí

- vytváranie a úprava dotazníkov,
- vytváranie a úprava otázok v dotazníkoch,
- vytváranie a úprava typov otázok a definícia možných odpovedí,
- prideľovanie dotazníkov organizáciám (individuálne, podľa typu organizácie)
- prezeranie odpovedí konkrétnej organizácie,
- export odpovedí (jednej organizácie, viacerých organizácií) vo formáte csv na ďalšie spracovanie,
- vyhľadávanie organizácií podľa odpovede na vybranú otázku z dotazníka,
- export dotazníkov a ich pridelení organizáciám do portálu VISKB,
- notifikácia kontaktných osôb o pridelení dotazníka (emailom na kontaktnú adresu).

1.5.1.3.4 Správa organizácií

- pridanie novej organizácie
  - generovanie dočasných autentifikačných údajov,
- import zoznamu nových organizácií zo súboru vo formáte csv,
- automatický export základných údajov o novej organizácii do portálu VISKB,
- nastavenie, či organizácia používa samostatný klientsky modul alebo portál VISKB na správu svojich údajov.

1.3.5 Správa interných používateľov

- vytváranie a úprava používateľských účtov,
- zmena hesiel,
- prideľovanie rolí používateľom.

1.3.6 Prezeranie auditných záznamov centrálneho modulu VISKB na spracovanie informácií aj centrálneho portálu VISKB

- prezeranie auditných záznamov,
- vyhľadávanie v auditných záznamoch,
- kopírovanie vybraných logov do externého úložiska (syslog).

1.5.1.3.5 Import a aktualizácia údajov z portálu

Údaje o organizáciách a odpovede na otázky v dotazníkoch sa budú do modulu importovať z databázy portálu VISKB. Pri importe budú údaje dešifrované a zmenené údaje sa prenesú do databázy modulu VISKB na spracovanie údajov, pričom sa zachová úplná história zmien. Funkcia importu sa bude spúšťať automaticky v definovaných intervaloch a bude ju možné spustiť aj manuálne prostredníctvom webového rozhrania.
Bude možnosť aj opačného prenosu údajov (z centrálneho modulu na spracovanie údajov do databázy portálu VISKB) pre prípad prechodu z používania samostatného klientskeho modulu na používanie portálu na správu údajov zo strany organizácie.

1.5.1.3.6 Spoločné požiadavky na funkcionalitu

Všetky ukladané údaje budú ukladané so zachovaním plnej histórie zmien. Zobrazovanie, vyhľadávanie a exporty budú možné aj len v aktuálnych údajoch, aj vo všetkých údajoch. Údaje budú ukladané vrátane informácie o období ich platnosti.

1.5.1.3.7 Správa portálu VISKB

- správa používateľských účtov organizácií poskytujúcich údaje cez portál
  - zmena autentifikačných údajov,
  - nastavenie vynútenia zmeny autentifikačných údajov pri najbližšom prihlásení,
  - odstraňovanie účtov,
  - generovanie nových dočasných autentifikačných údajov.

1.5.1.3.8 Správa číselníkov VISKB

- Správa číselníkov (pridávanie nových, oprava, zneplatňovanie položiek)

1.5.1.3.9 Integračné REST API

Je potrebné vytvoriť REST API endpoint pre účely projektu nahlasovania zraniteľností. Po úspešnej autentizácií, API endpoint bude na základe IP adresy/doménového mena vracať odpoveď vo formáte JSON s nasledujúcimi údajmi o organizácii:
Názov organizácie: String
Adresa: String
ID: String
Kontaktné osoby: Array of {
Meno kontaktnej osoby: String-
Email: String
Telefónne číslo: String
Mobil: String
Rola: String
Dostupnosť: String
Poznámka: String
}
V prípade úspešného priradenia kontaktných informácií k IP adrese aplikácia vráti JSON údaje o organizácii ako aj HTTP status kód 201. V prípade, že sa nenašiel žiadny prienik medzi IP adresami a požadovanou IP adresou, tak sa vráti HTTP status s kódom 404.
Ďalší endpoint integračného API bude umožňovať nahratie (upload) dokumentu pre organizáciu (cieľom je nahrávanie správ zo skenovania zraniteľností, ktoré budú sprístupnené organizácii prostredníctvom portálu VISKB). Aj tento endpoint musí byť autentifikovaný. Nahratý súbor sa zašifruje kľúčom organizácie (získaným z databázy portálu VISKB) a uloží sa (ako BLOB do DB portálu VISKB alebo

na diskové úložisko portálu VISKB). Vstupom API bude ID organizácie (získateľné v odpovedi na predchádzajúci endpoint), názov súboru a obsah súboru.

1.5.1.4 Požiadavky na implementáciu

Implementácia modulu musí byť prevádzkovateľná na serveri s OS Debian alebo Ubuntu. Relačná databáza, webový server, ako aj všetky ďalšie softvérové nástroje tretích strán potrebné na prevádzku aplikácie modulu musia byť zahrnuté v štandardnej distribúcii operačného systému ako plne podporované (aby bola zabezpečená efektívna a bezpečná možnosť ich aktualizácie), prípadne môžu byť podporované zdarma treťou stranou, ktorá poskytuje automatizovaný mechanizmus aktualizácií, ktorý zabezpečuje spoľahlivé overenie autentickosti preberaných komponentov a má zavedený vhodný, verejne známy mechanizmus zabraňujúci pridaniu neautorizovaného obsahu do repozitára aktualizácií .

Spracovávané údaje musia byť uložené v relačnej databáze umožňujúcej viacnásobný súčasný prístup a transakčné spracovanie (napr. MariaDB alebo PostgreSQL).

Implementácia modulu musí byť realizovaná v niektorom z jazykov PHP, Python alebo Java (openjdk), webové rozhranie môže využívať Javascript a musí byť v súlade so špecifikáciami HTML5 a CSS a musí byť plne funkčné minimálne v aktuálnych verziách prehliadačov Mozilla Firefox, Google Chrome, a Microsoft Edge.

1.5.1.5 Bezpečnostné požiadavky

Návrh a implementácia modulu musí využívať techniky, ktoré eliminujú alebo minimalizujú pravdepodobnosť, že výsledné dielo bude obsahovať bežné zraniteľnosti webových aplikácií (ako napr. SQL injection, cross-site scripting, session hijacking, a pod.). Vyžadujeme súlad s bezpečnostnými požiadavkami OWASP ASVS pre kategóriu aplikácii 2.

Modul musí mať implementovanú správu používateľov a ich rolí. Vyžaduje sa minimálne podpora nasledujúcich rolí:

- operátor – má oprávnenie na vyhľadávanie a prezeranie záznamov,
- správca údajov – má oprávnenie na pridávanie organizácií, vyhľadávanie, prezeranie a úpravu evidovaných údajov o organizáciách, export údajov, správu číselníkov, správu portálu VISKB,
- správca používateľov – má oprávnenie na správu používateľov a prideľovanie rolí,
- audítor – má oprávnenie na prezeranie záznamov o operáciách vykonaných v module.

Modul musí byť prístupný len z určených interných sietí, webové rozhranie modulu musí používať protokol HTTPS.

Všetky vykonávané operácie (read, write) používateľmi modulu sa musia zaznamenávať v rozsahu dátum a čas operácie, typ operácie, identifikácia používateľa, identifikácia organizácie a typu údajov, ktorých sa operácia týkala (pre operácie týkajúce sa konkrétnej organizácie). V prípade zmeny evidovaných údajov alebo hesla používateľa portálu VISKB systém zároveň bude zaznamenávať v zázname o operácii informáciu o dôvode zmeny zadanú používateľom, ktorý zmenu vykonáva.

Zaznamenávanie bude konfigurovateľné na úrovni zmenových (change) a zobrazovacích (view) operácií.

1.5.2 Špecifikácia centrálneho portálu VISKB

Centrálny portál VISKB slúži na:

- nahrávanie údajov zo samostatného klientskeho modulu,
- zadávanie a úpravu zbieraných údajov prostredníctvom webového rozhrania pre organizácie, ktoré nemajú nasadený samostatný klientsky modul – klientsky web portál,
- vypĺňanie dotazníkov,
- preberanie dokumentov (napr. správ zo skenovania zraniteľností).

Portál pozostáva z relačnej databázy na uloženie šifrovaných údajov, webového rozhrania na nahrávanie a úpravu údajov o organizácii, preberanie dokumentov (napr. správ zo skenovania zraniteľností) a webového rozhrania pre vypĺňanie dotazníkov. Tieto webové rozhrania budú prístupné z externého prostredia (Internetu) prostredníctvom protokolu HTTPS. Vzhľadom na skutočnosť, že portál bude obsahovať potenciálne zneužiteľné údaje o väčšom počte organizácií verejnej správy, a že

portál bude dostupný z Internetu, všetky údaje musia byť ukladané v šifrovanej podobe – pozri aj časť „bezpečnostné požiadavky“.

1.5.2.1 Spracovávané informácie v rámci klientskeho web portálu – rozhrania pre zadávanie údajov

Klientsky modul – web portál bude slúžiť pre organizácie, ktoré nebudú mať implementovaný samostatný klientsky modul (on-site), alebo ktoré preferujú online riešenie, ktoré nemusia spravovať. Pre organizácie bude prístupný prostredníctvom webového rozhrania.

V rámci modulu budú spracovávané informácie o jednotlivých organizáciách v rozsahu uvedenom v špecifikácii centrálneho modulu VISKB na spracovanie informácií a taktiež aj nižšie špecifikované údaje. Rovnako ako centrálny modul VISKB na spracovanie informácií, aj portál VISKB musí byť navrhnutý, implementovaný a zdokumentovaný tak, aby bolo možné v budúcnosti jednotlivé typy údajov rozšíriť o ďalšie atribúty, ako aj pridať nové typy údajov.

Jednotlivé inštitúcie potrebujú evidovať údaje uvedené pri centrálnom module Ide najmä o nasledovné údaje:

- Kontaktné údaje (meno, funkcia, telefónne čísla, e-mail) relevantných osôb pre riešenie bezpečnostných incidentov a plánov obnovy súvisiacich s organizáciou.
- Evidencia informačných aktív (inventár aktív a ich základných parametrov):
    - verejné IP adresy (IPv4 a IPv6) a ich využitie,
    - doménové mená a ich využitie,
    - poskytované služby prístupné z externých sietí (Internet, Govnet),
    - používané operačné systémy,
    - používané aplikačné softvérové vybavenie,
    - informačné systémy (označenie, klasifikácia, prístupnosť z externého prostredia).
- Aktíva
    - rôzne atribúty (typ, hodnota) - minimálne:
        - ID aktíva
        - Názov aktíva
        - Typ aktíva (číselníková položka - PC, server, informačný systém, rôzne sieťové prvky, ...)
        - Popis aktíva
        - IP adresa (aj viacnásobne)
        - MAC adresa (aj viacnásobne)
- Klasifikácia a kategorizácia IS a sietí.
- Parametre a výsledky výkonu (realizácie) AR/BIA (identifikované riziká, hrozby, zraniteľnosti, RTO, RPO, priradenie vlastníkov a pod.) .
- Katalóg rizík (a ich previazania na jednotlivé aktíva), vrátane spôsobov ich riadenia a aktuálneho stavu implementácie prijatých opatrení, termínov, zodpovedných osôb a pod. (komplexný manažment identifikovaných rizík), najmä nasledovné typy údajov:
    - ID rizika,
    - názov rizika,
    - popis rizika,
    - ID aktíva, ktorého sa riziko týka,
    - oblasť riadenia IB, ktorej sa riziko týka (podľa ISO 27002, zákon č. 69/2018 a vyhláška č. 362/2018, zákona o ITVS a aj vyhlášky č. 179/2020 Z. z.),
    - dátum identifikácie rizika,
    - hodnota inherentného rizika (ako výsledok hodnoty dopadu rizika a pravdepodobnosti výskytu hrozby a uplatnenia zraniteľnosti),
    - implementované opatrenia na zníženie/odstránenie rizika,
    - previazanie na politiky pokrývajúce jednotlivé riziká formou uvedenia/výberu názvu konkrétnej politiky (politík) a prípadne odkazu na konkrétnu politiku,
    - hodnota reziduálneho rizika,

  - vlastník rizika,
  - plánované opatrenia na zníženie/elimináciu reziduálneho rizika,
  - termín realizácie plánovaných opatrení,
  - dátum poslednej aktualizácie,
  - atď.
- Evidencia bezpečnostných a iných auditov a bezpečnostných posudzovaní a technických zraniteľností – plán auditov a zoznam realizovaných auditov. Evidované musia byť najmä nasledovné typy údajov:
  - typ auditu (audit kybernetickej bezpečnosti, bezpečnostný audit, audit súladu, technický audit /konfiguračná previerka, testovanie zraniteľností, pentest/, follow-up audit,
  - forma auditu (interný audit / externý audit),
  - plánovaný termín auditu (od - do),
  - termín skutočnej realizácie auditu,
  - odkaz na auditnú správu,
  - atď.
- Evidenciu kybernetických incidentov

Každý z týchto parametrov (riziko, hrozba, aktívum, zraniteľnosť, pravdepodobnosť, plán auditov a prípadne ďalšie entity sú samostatnou tabuľkou so vzťahom na iné entitity). Parametre budú realizované podľa vzoru na riadenie rizík - ISO 27005.

Klientsky modul – web portál bude mať na rozdiel od samostatného klientskeho modulu z časti obmedzenú funkcionalitu z pohľadu množiny spracúvaných údajov (pozri aj časť „spravované informácie samostatného klientskeho modulu“).

1.5.2.2 Požiadavky na funkcionalitu

1.5.2.2.1 Registrácia používateľa

Systém umožní registráciu používateľského účtu pre konkrétnu organizáciu (ktorej základné údaje boli do systému vložené z centrálneho modulu VISKB na spracovanie informácií vrátane dočasných autentifikačných údajov) na základe dočasných autentifikačných údajov. Pri registrácii používateľa za organizáciu bude vygenerovaný náhodný tajný kľúč, ktorý bude v šifrovanej podobe (pozri aj časť „bezpečnostné požiadavky“) uložený v databáze portálu VISKB.

1.5.2.2.2 Identifikácia a autentifikácia používateľov

- identifikácia a autentifikácia používateľov za jednotlivé organizácie pomocou prihlasovacieho mena (e-mailová adresa) a hesla,
- zmena hesla (vrátane vynútenia dostatočne komplexného hesla, vrátane vynútenia zmeny hesla pri najbližšom prihlásení),
- príprava na použitie dvojfaktorovej autentifikácie.

1.5.2.2.3 Nahrávanie a export údajov zo samostatného klientskeho modulu

- import údajov za organizáciu zo súboru generovaného samostatným klientskym modulom prostredníctvom webového rozhrania,
- import údajov za organizáciu zo samostatného klientskeho modulu prostredníctvom API,
- export údajov z portálu v podobe vhodnej na import do samostatného klientskeho modulu,
- nastavenie, či organizácia používa portál VISKB alebo samostatný klientsky modul,
- možnosť stiahnutia aktuálneho verejného kľúča centrálneho modulu VISKB pre potreby jeho nahratia do samostatného klientskeho modulu.

1.5.2.2.4 Zadávanie, prezeranie, úprava údajov za organizáciu

- načítanie a dešifrovanie uložených údajov za organizáciu,
- zobrazenie, úprava, pridávanie, mazanie údajov za organizáciu prostredníctvom webového rozhrania,
- uloženie údajov v šifrovanej podobe.,

- Funkcionalita v tejto časti je prístupná len organizáciám, ktoré nepoužívajú samostatný klientsky modul.

1.5.2.2.5 Vypĺňanie dotazníkov

- vygenerovanie unikátnej URL pre vyplnenie dotazníka:
  - táto URL môže byť poskytnutá osobe, ktorá má vyplniť dotazník, a ktorá nemusí mať štandardný prístup na portál VISKB za organizáciu,
  - po finálnom vyplnení dotazníka sa táto URL zneplatní,
  - pri novom vygenerovaní URL pre vyplnenie dotazníka budú predtým vyplnené odpovede prístupné (teda je možné znovusprístupnenie dotazníka aj po jeho predošlom vyplnení),
- vypĺňanie dotazníka:
  - funkcia je prístupná na základe unikátnej URL bez potreby štandardnej identifikácie a autentifikácie na portál VISKB.

Preberanie dokumentov

- dešifrovanie a stiahnutie dokumentu z portálu
  - Portál zobrazí zoznam nahratých dokumentov a umožní dešifrovanie a stiahnutie dokumentu

1.5.2.3 Požiadavky na implementáciu

Implementácia modulu musí byť prevádzkovateľná na serveri s OS Debian alebo Ubuntu. Relačná databáza, webový server, ako aj všetky ďalšie softvérové nástroje tretích strán potrebné na prevádzku aplikácie modulu musia byť zahrnuté v štandardnej distribúcii operačného systému ako plne podporované (aby bola zabezpečená efektívna a bezpečná možnosť ich aktualizácie), prípadne môžu byť podporované zdarma treťou stranou, ktorá poskytuje automatizovaný mechanizmus aktualizácií, ktorý zabezpečuje spoľahlivé overenie autentickosti preberaných komponentov a má zavedený vhodný, verejne známy mechanizmus zabraňujúci pridaniu neautorizovaného obsahu do repozitára aktualizácií .
Spracovávané údaje musia byť uložené v relačnej databáze umožňujúcej viacnásobný súčasný prístup a transakčné spracovanie (napr. MariaDB alebo PostgreSQL).
Implementácia modulu musí byť realizovaná v niektorom z jazykov PHP, Python alebo Java (openjdk), webové rozhranie môže využívať Javascript a musí byť v súlade so špecifikáciami HTML5 a CSS a musí byť plne funkčné minimálne v aktuálnych verziách prehliadačov Mozilla Firefox, Google Chrome, a Microsoft Edge.

1.5.2.4 Bezpečnostné požiadavky

Návrh a implementácia modulu musí využívať techniky, ktoré eliminujú alebo minimalizujú pravdepodobnosť, že výsledné dielo bude obsahovať bežné zraniteľnosti webových aplikácií (ako napr. SQL injection, cross-site scripting, session hijacking, a pod.).
Všetky vykonávané operácie používateľmi modulu sa musia zaznamenávať v rozsahu dátum a čas operácie, typ operácie, identifikácia používateľa, identifikácia organizácie a typu údajov, ktorých sa operácia týkala. Vyžadujeme súlad s bezpečnostnými požiadavkami OWASP ASVS pre kategóriu aplikácii 2.

Požiadavky na kryptografickú ochranu uložených údajov

Údaje uložené na portáli VISKB musia byť kryptograficky chránené proti narušeniu dôvernosti v prípade úspešného získania neoprávneného prístupu k databáze a/alebo webovému/aplikačnému serveru. Údaje musia byť šifrované tak, aby ich bolo možné dešifrovať so znalosťou jedného z:

- autentifikačné údaje používateľa za organizáciu, ktorej sa údaje týkajú,
- súkromného kľúča centrálneho modulu VISKB na spracovanie informácií určeného na tento účel.

Z tohto dôvodu budú údaje šifrované symetrickým algoritmom AES-256-GCM použitím unikátneho tajného kľúča pre organizáciu, ktorý bol vygenerovaný pri registrácii používateľa. Tento kľúč bude uložený v šifrovanej podobe v dvoch podobách:

- šifrovaný symetrickým algoritmom AES-256-GCM pomocou kľúča odvodeného z autentifikačných údajov používateľa (použitím bezpečnej funkcie na odvodenie kľúčov z hesiel, ako napr. PBKDF2 s vhodnými parametrami, bcrypt, scrypt, a pod.),
- šifrovaný asymetrickým algoritmom (napr. RSA) pomocou verejného kľúča centrálneho modulu VISKB na spracovanie informácií.

Uvedeným spôsobom bude možné dešifrovať kľúč na šifrovanie/dešifrovanie údajov pomocou znalosti autentifikačných údajov oprávneného používateľa, ako aj pomocou súkromného kľúča centrálneho modulu VISKB na spracovanie informácií (táto možnosť sa využije pri importe údajov do uvedeného modulu).

Uvedený spôsob zároveň umožní zmeniť autentifikačné údaje používateľa so znalosťou pôvodných autentifikačných údajov (tajný kľúč pre dáta je možné dešifrovať a opäť zašifrovať pomocou nových autentifikačných údajov), ako aj zmeniť autentifikačné údaje používateľa prostredníctvom funkcionality správy portálu VISKB, ktorá je súčasťou centrálneho modulu VISKB na spracovanie informácií.

Osobitným spôsobom bude riešená ochrana odpovedí na dotazníky. Keďže dotazníky budú vypĺňateľné na základe unikátnej URL bez potreby identifikácie a autentifikácie na portál VISKB, bude pre dotazníky potrebné použiť upravené riešenie. Pri prvom vygenerovaní URL na vyplnenie dotazníka bude vygenerovaný samostatný šifrovací kľúč pre odpovede na tento dotazník, ktorý bude uložený v dvoch kópiách:

- šifrovaný tajným kľúčom pre šifrovanie údajov organizácie,
- šifrovaný unikátnym dočasným tajným kľúčom, ktorý bude náhodne vygenerovaný a bude zahrnutý v URL pre vyplnenie dotazníka.

Pri prístupe k dotazníku pomocou URL bude možné dešifrovať kľúč pre odpovede a pomocou neho šifrovať/dešifrovať odpovede. Po finálnom vyplnení dotazníka sa URL pre vyplnenie zneplatní a príslušná kópia kľúča pre odpovede vymaže. V prípade následného vygenerovania novej URL pre vyplnenie dotazníka bude možné existujúci kľúč pre odpovede dešifrovať a opäť uložiť aj šifrovaný pomocou dočasného tajného kľúča zahrnutého v novej URL.

Symetrické kryptografické kľúče použité v systéme bude systém generovať použitím vhodného generátora náhodných čísel (s výnimkou kľúčov odvádzaných od hesla používateľa podľa špecifikácie vyššie). Asymetrický kľúč centrálneho modulu VISKB bude vygenerovaný mimo systém (vo formáte používanom knižnicou openssl), do centrálneho modulu sa uloží súkromný aj verejný kľúč, do portálu sa uloží verejný kľúč (na tieto operácie nie je vyžadované webové rozhranie), verejný kľúč bude v podobe X.509 certifikátu.

1.5.3 Špecifikácia samostatného klientskeho modulu

Samostatný klientsky modul slúži na spracovanie informácií v prostredí organizácie a umožňuje export vybraných údajov na portál VISKB buď automaticky prostredníctvom API alebo formou exportu do zašifrovaného súboru, ktorý je následne možné importovať na portál VISKB prostredníctvom jeho webového rozhrania. Jeho úlohou bude správa údajov v nižšie uvedenom rozsahu a export vybraných údajov (uvedených v centrálnom module VISKB) v zašifrovanej forme prostredníctvom webového rozhrania portálu do centrálneho modulu,. Modul musí umožniť evidenciu aktív organizácie a ich manažment, vrátane ich klasifikácie a kategorizácie, manažment rizík, poskytovanie reportov a štatistických prehľadov v rozsahu 10 fixných prehľadov, ktoré budú vyšpecifikované vo fáze tvorby DFŠ. Modul by mal mať podobu samostatne spustiteľnej (portable) aplikácie bez potreby inštalácie min. pre OS Windows.

1.5.3.1 Spracovávané informácie

Modul umožňuje evidenciu a úpravu údajov v rozsahu uvedenom v špecifikácii centrálneho modulu VISKB (informácie o jednotlivých organizáciách v rozsahu uvedenom v špecifikácii centrálneho modulu VISKB) a v rozsahu klientskeho modulu – web portál s výnimkou údajov týkajúcich sa dotazníkov.
Okrem toho musí, navyše oproti klientskemu modulu - web portál, vedieť spracovávať aj nasledovné informácie:

- Základné BCM parametre:
  - Zvolená stratégia obnovy jednotlivých IS.
  - Plán zálohovania pre jednotlivé IS.
  - Evidencia BCP a DRP plánov.
- Katalóg identifikovaných incidentov a spôsobov ich riadenia (vrátane Knowledge-base a scenárov riešenia bezpečnostných incidentov).

Rovnako, ako centrálny modul VISKB na spracovanie informácií a klientsky modul-web portál, aj samostatný klientsky modul musí byť navrhnutý, implementovaný a zdokumentovaný tak, aby bolo možné v budúcnosti jednotlivé typy údajov rozšíriť o ďalšie atribúty, ako aj pridať nové typy údajov.

1.5.3.2 Požiadavky na funkcionalitu

Požiadavky na modul sú najmä:

- zobrazenie, úprava, pridávanie, mazanie údajov za organizáciu – komplexná správa vyššie uvedených údajov,
- prenos údajov na portál VISKB prostredníctvom API,
- export údajov do súboru vhodného na import na portál VISKB (napr. šifrovaného XML),
- jednoduchá „customizovateľnosť“ položiek evidencie – pomocou úpravy zdrojového kódu,
- portable aplikácia (bez inštalácie),
- ukladanie údajov do internej databázy (napr. SQLlite), ktorú bude možné jednoducho zmeniť na centrálnu databázu a tak nástroj používať aj ako klient/server aplikáciu.

1.5.3.3 Požiadavky na implementáciu a licenciu

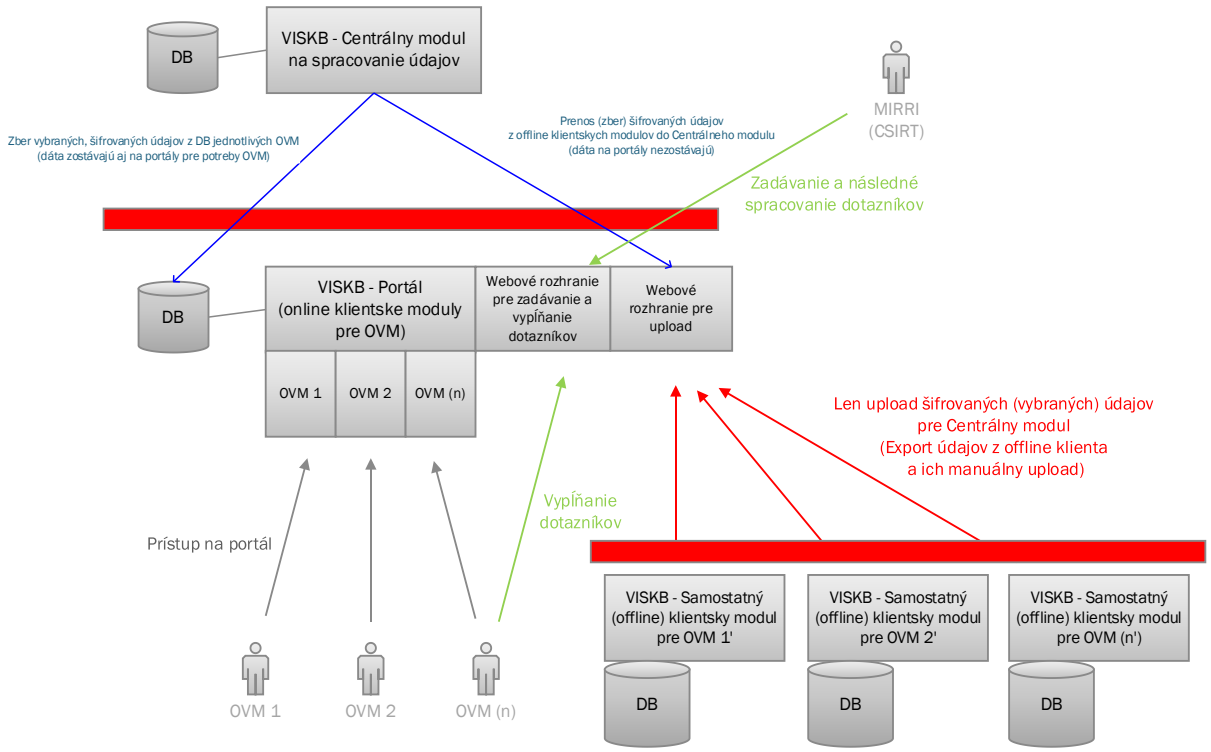
Spustiteľná aplikácia nesmie vyžadovať inštaláciu knižníc a ďalších nástrojov, ktoré si vyžadujú samostatné licencie, ktoré nie sú dostupné bezplatne. Aplikácia musí byť dodaná pod licenciou EUPL a všetky použité komponenty tretích strán musia mať kompatibilnú licenciu.

1.5.3.4 Bezpečnostné požiadavky

Bezpečnostné požiadavky na samostatný klientsky modul sú rovnaké alebo podobné ako na predchádzajúce moduly. Okrem toho je potrebné zabezpečiť najmä:

- správu používateľov a riadenie ich prístupu k aplikácii a samostatne k jednotlivým evidenciám a umožnenie vybraným rolám len read-only prístup,
- šifrovanie exportovaného súboru (údajov) verejným asymetrickým kľúčom centrálneho modulu VISKB,
- voliteľný dvojfaktorový prístup k aplikácii pomocou hardvérových tokenov,
- auditné funkcie a logovanie používateľov a ich aktivít (read, write) a príprava na vyvedenie logov po každej udalosti na centrálny logovací server organizácie (syslog),
- správa šifrovacích kľúčov bude súčasťou aplikácie,
- možnosť používateľsky jednoduchej výmeny certifikátu verejného kľúča centrálneho modulu VISKB v aplikácii (alebo aplikácie) po ich exspirácii.

1.5.4 Vzájomné vzťahy jednotlivých modulov



Synchronizácia údajov medzi modulmi

Synchronizácia údajov prebieha nasledovným spôsobom:

- Pri importe údajov z portálu VISKB alebo z exportu zo samostatného klientskeho modulu do centrálneho modulu VISKB na spracovanie údajov sa údaje zmenené (pridané, upravené, vymazané) po poslednom importe zosynchronizujú tak, že sa príslušné údaje pridajú, upravia alebo vymažú, pričom sa zachová história údajov.
- Pri zmene údajov v centrálnom module VISKB sa zmeny na portál VISKB neprenášajú (týka sa údajov spravovaných organizáciou).
- Pri prenose údajov z centrálneho modulu (pri prechode z používania samostatného klientskeho modulu na používanie portálu VISKB) sa údaje na portáli VISKB nahradia údajmi z centrálneho modulu VISKB.
- Portál VISKB umožňuje export údajov a samostatný klientsky modul umožňuje ich import, pričom v tomto prípade sa údaje v samostatnom klientskom module úplne nahradia importovanými údajmi (táto možnosť slúži na prechod z používania portálu VISKB na používanie samostatného klientskeho modulu).

Z samostatného klientskeho modulu navyše k manuálnemu exportu možný aj automatický export údajov na webové rozhranie pre upload (s cieľom umožniť jednoduchý export na jeden klik).

Za vypĺňanie dát (v online aj offline klientskom module), rovnako aj za ich aktuálnosť a správnosť sú zodpovedné jednotlivé OVM. Do centrálneho modulu sú prenášané len vybrané dáta podľa špecifikácie spracovávaných údajov v rámci centrálneho modulu uvedeného vyššie.

Online klientsky modul všetky šifrované dáta uchováva pre potreby OVM trvalo. Dáta z offline modulu sú na portáli uchovávané len dočasne, t.j. od času ich upload-u do času ich stiahnutia do centrálneho modulu.

1.6 Nefunkčné požiadavky

Z pohľadu návrhu aplikácie sa ráta s nasledovným objemom údajov:

1. rádovo do 10K organizácií a rádovo 100 záznamov na org., t.j. rádovo 1M platných záznamov v rozsahu definovaných atribútov,
2. max. rádovo 10K zmien za mesiac po úvodnom naplnení.

1.7 Forma a spôsob odovzdania predmetu zákazky

Súčasťou dodávky riešenia je aj:

1. dokumentácia návrhu riešenia vrátane dátového modelu, komponentového modelu, špecifikácie rozhraní jednotlivých častí riešenia, popisu jednotlivých súčastí riešenia,
2. komentované zdrojové kódy,
3. odovzdanie automatizovaných unit testov a bezpečnostných testov spustiteľných na open source technológiach (Selenium, Jmeter),
4. podrobný postup na zostavenie diela zo zdrojových kódov a na inštaláciu a konfiguráciu,
5. administrátorská a používateľská dokumentácie,
6. v prípade Samostatného klientskeho modulu aj spustiteľný súbor s aplikáciou a návodom na modifikáciu zdrojového kódu základných atribútových a dizajnových aspektov aplikácie.
7. súčinnosť s vytváraním dokumentov a aktivít vyžadovaných vyhláškou 85/2020 Z.z.

Poznámka: verejný obstarávateľ plánuje aktívne využívať možnosť zmeny programu formou zmien zdrojového kódu od začiatku prevádzky, s čím musí rátať aj budúci prevádzkovateľ SLA. V prípade, ak budú nejasnosti ohľadom chyby (či vznikla činnosťou a zmenami verejného obstarávateľa), budú tieto skutočnosti môcť byť preukázané na pôvodne dodanej verzii.

1.8 Zmenový rozpočet

Súčasťou zákazky je zmenový rozpočet. Zmenový rozpočet bude uchádzačom nacenený vo forme rozsahu človekodní. Zmenový rozpočet nemusí byť čerpaný a bude uvoľnený verejným obstarávateľom na základe objednávky.

Rozsah zmenového rozpočtu je potrebné naceniť v rozsahu 30 MDs.

2 NÁVRH OPISU ČASTI II. PREDMETU ZÁKAZKY: Vytvorenie metodík, vytvorenie bezpečnostnej a vzorovej dokumentácie pre rôzne druhy OVM, vykonanie analýzy rizík a analýzy dopadov (AR/BIA) v rámci MIRRI a podpora projektov v rámci dopytovej výzvy „Rozvoj governance a úrovne informačnej a kybernetickej bezpečnosti v sektore VS“

2.1 Špecifikácia úlohy

Cieľom zákazky je podporiť MIRRI pri výkone správy (governance) v podsektore VS, t.j. vytvoriť metodické usmernenia a šablóny dokumentov, ktoré budú jednotlivým OVM slúžiť ako metodické rámce a ako vzor bezpečnostnej dokumentácie potrebnej pre naplnenie legislatívnych požiadaviek na zvýšenie úrovne informačnej a kybernetickej bezpečnosti a ochrany IKT a sietí používaných v sektore VS.

2.2 Všeobecné vymedzenie predmetu zmluvy

Predmetom zákazky je poskytnutie a dodávka služieb v nasledovných oblastiach:

- Vytvorenie metodík a metodických usmernení v súlade so zákonom o KyB a ďalšími súvisiacimi zákonmi.
- Vytvorenie bezpečnostnej dokumentácie vzorovej dokumentácie pre kategórie ITVS podľa vyhlášky č. 179/2020 Z. z..
- Vykonanie analýzy rizík a analýzy dopadov (AR/BIA) v rámci MIRRI.
- Podpora projektov v rámci dopytovej výzvy „Rozvoj governance a úrovne informačnej a kybernetickej bezpečnosti v sektore VS“.

2.3 Požadované aktivity

V rámci vyššie definovaných oblastí je požadované dodať najmä nasledovné aktivity:

- Vytvorenie metodík a metodických usmernení:
  - Vytvorenie jednotnej metodiky pre výkon AR/BIA, klasifikácie a riadenia rizík, vrátane jednotných parametrov a metrík pre celý sektor VS a návrhu katalógu rizík.
  - Návrh metodického usmernenia k výkladu základných služieb v sektore VS (jednotný prístup a pomenovanie základných služieb pre ISVS, namapovanie na ISVS a jednotlivé agendy a upresňujúce dopadové kritéria).
  - Návrh metodického usmernenia k jednotnému výkonu BCM nad základnými službami v sektore VS.
  - Vytvorenie metodiky pre verejnú správu pre bezpečný vývoj nových aplikácií a systémov v súlade so štandardom SSDLC (Secure System Development Life Cycle) a návrh bezpečnostných požiadaviek pre aplikácie podľa klasifikačných stupňov.
- Vytvorenie vzorovej sady nižšie uvedenej bezpečnostnej dokumentácie (šablón dokumentov s obsahom a popisom jednotlivých kapitol pre fiktívne Ministerstvo mágie a kúziel) pre sektor VS rozdelenej podľa jednotlivých kategórií ITVS (t.j. sadu pre každú kategóriu I. II a III. podľa vyhlášky č. 179/2020 Z. z. a shadowing pre zamestnancov MIRRI pri tvorbe dokumentov:
  - Stratégia kybernetickej bezpečnosti.
  - Bezpečnostná politika.
  - Smernica pre riadenie informačnej bezpečnosti.
  - Klasifikácia informácií a kategorizácia sietí a informačných systémov a riadenie aktív.
  - Smernica výkonu analýzy rizík a analýzy dopadov (AR/BIA).
  - Smernice o bezpečnej prevádzke IS a sietí.
  - Smernica o monitorovaní a riešení kybernetických bezpečnostných incidentov.
  - Politika BCM vrátane stratégie obnovy a návrh pred-vyplnenej šablóny pre BCP a DRP.
  - Bezpečnostný projekt informačného systému v súlade so zákonom č. 95/2019 Z.z. o ITVS.
- Vykonanie analýzy rizík a analýzy dopadov (AR/BIA) v rámci MIRRI:
  - Vykonanie identifikácie a evidencie informačných aktív, IS a sietí MIRRI.
  - Realizácie klasifikácie a kategorizácie nad identifikovanými aktívami.
  - Výkon AR/BIA podľa metodiky z aktivity B).
  - Vytvorenie katalógu identifikovaných rizík a návrhu odporúčaní na ich riadenie (mitigáciu).
  - Podpora pri zavedení predmetných procesov do praxe na MIRRI, napr. aj formou zabezpečenia formálneho rozhodnutia MIRRI ohľadom spôsobov riadenia identifikovaných rizík v súlade s návrhom odporúčaní z predošlého bodu.
- Podpora projektov v rámci dopytovej výzvy „Rozvoj governance a úrovne informačnej a kybernetickej bezpečnosti v sektore VS“.

- QA nad realizáciou a dodávanými výstupmi projektov realizovaných v rámci uvedenej dopytovej výzvy a dohľad nad súladom s navrhnutými metodikami, metodickými usmerneniami a vzorovou dokumentáciou. Táto aktivita bude čerpaná na základe objednávok na základe skutočnej potreby, bez nutnosti vyčerpania celého rámca.

- Projektové riadenie celého CMRKB (ktoré sa skladá z 4 verejných obstarávaní) v súlade s vyhláškou 85/2020 Z.z.

2.4 Požadované výstupy

Č.	Oblasť A)	Poznámka
1	Návrh metodiky pre výkon AR/BIA, klasifikácie a riadenia rizík	Spôsob výkonu identifikácie a evidencie informačných aktív a ich základných parametrov, ich klasifikácie a kategorizácie, spôsob výkonu AR/BIA vrátane jednotných parametrov a metrík pre celý sektor VS a návrhu jednotného katalógu (evidencie) rizík.
2	Návrh metodického usmernenia k výkladu základných služieb v sektore VS	Návrh jednotného prístupu a pomenovania základných služieb pre ISVS a upresňujúce dopadové a klasifikačné kritéria.
3	Návrh metodického usmernenia k jednotnému výkonu BCM nad základnými službami v sektore VS	Návrh jednotných spôsobov vytvárania BCM stratégie, zálohovania, tvorby BCP a DRP plánov a ich testovania v sektore VS.
4	Návrh metodiky pre verejnú správu pre bezpečný vývoj nových aplikácií a systémov v súlade so štandardom SSDLC (Secure System Development Life Cycle)	V súlade s požiadavkami podľa vyhlášky č. 362/2018 Z. z. a vyhlášky 78/2020 Z.z. Bude pokrývať všetky fázy SSDLC z pohľadu bezpečnosti a bezpečnostných požiadaviek: • od fázy zámeru projektu a návrhu požiadaviek (okrem funkčných požiadaviek je potrebné zadefinovať aj bezp. požiadavky) • cez fázy samotného vývoja (zabezpečenie vývojového prostredia a pod.) • testovania (otestovania nie len funkčných ale aj bezp. požiadaviek, vrátane zabezpečenia anonymizácie testovacích dát a pod.) • implementácie, nasadenia a riadenia zmien • až po bezpečné vyradenie IS z prevádzky • checklist bezpečného vývoja webových aplikácií Návrh bezpečnostných požiadaviek pre aplikácie bude obsahovať základnú množinu (base line) týchto požiadaviek rozdelenú podľa klasifikačných stupňov v súlade najmä s: ○ ISO 15408, tzv. Common Criteria, ○ OWASP Application Security Verification Standard 4.0.2, ○ CSIRT.sk usmernením a opatreniami na zaistenie bezpečnosti webových aplikácii.

Č.	**Oblasť B) -** Vzorové, pred-vyplnené šablóny všetkých nižšie uvedených smerníc a dokumentov pre použitie v rámci jednotlivých OVM v sektore VS, rozdelené podľa jednotlivých kategórií ITVS podľa vyhlášky č. 179/2020 Z. z., t.j. sada pre každú kategóriu)	**Poznámka**
1.	Stratégia kybernetickej bezpečnosti	V štruktúre a v súlade s obsahovými požiadavkami podľa prílohy č. 1 vyhlášky č. 362/2018 Z. z.

Č.	**Oblasť B)** - Vzorové, pred-vyplnené šablóny všetkých nižšie uvedených smerníc a dokumentov pre použitie v rámci jednotlivých OVM v sektore VS, rozdelené podľa jednotlivých kategórií ITVS podľa vyhlášky č. 179/2020 Z. z., t.j. sada pre každú kategóriu)	**Poznámka**
2.	Bezpečnostná politika	V obsahovej štruktúre podľa existujúcej prílohy č. 1 vyhlášky č. 362/2018 Z .z
3.	Smernica pre riadenie informačnej bezpečnosti	V súlade s požiadavkami podľa vyhlášky č. 362/2018 Z. z.
4.	Klasifikácia informácií a kategorizácia sietí a informačných systémov a riadenie aktív	V súlade s požiadavkami podľa vyhlášky č. 362/2018 Z. z.
5.	Smernica výkonu analýzy rizík a analýzy dopadov (AR/BIA)	V súlade s požiadavkami podľa vyhlášky č. 362/2018 Z. z.
6.	Smernice o bezpečnej prevádzke IS a sietí	V súlade s požiadavkami podľa vyhlášky č. 362/2018 Z. z. Bude pokrývať najmä oblasti: • bezpečná správa a prevádzka IS a sietí, • riadenie zmien, • riadenie kapacít, • riadenie záplat a aktualizácii, • zálohovanie dát, • posudzovanie technických zraniteľnosti, • riadenie používateľov a prístupových práv, • bezpečnostné požiadavky pre prístupové práva a účty privilegovaných používateľov.
7.	Smernica o monitorovaní a riešení kybernetických bezpečnostných incidentov	V súlade s požiadavkami podľa vyhlášky č. 362/2018 Z. z. Vrátane protokolov hlásení aj na NBÚ
8.	Politika BCM vrátane stratégie obnovy a návrh pred-vyplnenej šablóny pre BCP a DRP	V súlade s požiadavkami podľa vyhlášky č. 362/2018 Z. z. Šablóny pre BCP a DRP budú obsahovať návrh textácie v rámci jednotlivých kapitol dokumentov
9.	Bezpečnostný projekt informačného systému pre kategóriu III.	Bezpečnostný projekt informačného systému podľa 95/2019 Z.z. pre informačné systémy kategórie 3 v zmysle zákona č. 69/2018 Z.z.

Č.	**Oblasť C)**	**Poznámka** Aktuálny stav: • interných zamestnancov cca 850, • 17 sekcii, • 33 IS, 42 web domén a cca 40 plánovaných IS, • cca 220 informačných aktív, • aktuálne 6 budov (pripravuje sa sťahovanie).
	Vykonanie identifikácie a evidencie informačných aktív, IS a sietí MIRRI.	Výstupom bude evidencia identifikovaných informačných aktív MIRRI a ich základných parametrov v súlade s metodikou z bodu B).
	Realizácie klasifikácie a kategorizácie nad identifikovanými aktívami.	Výstupom bude vykonaná klasifikácia a kategorizácia nad aktívami identifikovanými v predošlom bode.
	Výkon AR/BIA podľa metodiky z aktivity B).	Výstupom budú identifikované a ohodnotené riziká a dopady v rámci výkonu AR/BIA podľa jednotnej smernice (metodiky z aktivity B) pre identifikované aktíva z predošlého bodu a pre dátovo-procesné aktíva (biznis agendy) a IKT zdroje MIRRI, ktoré tieto agendy podporujú.
	Vytvorenie katalógu identifikovaných rizík a návrhu odporúčaní na ich riadenie (mitigáciu).	Návrh katalógu identifikovaných rizík z AR/BIA a návrh spôsobu ich udržiavania, aktualizácie a riadenia (mitigácie), ktorý bude obsahovať konkrétne bezpečnostné opatrenia a spôsoby ich riadenia.
	Podpora pri zavedení predmetných procesov do praxe na MIRRI a prenos skúseností a vedomostí na pracovníkov MIRRI.	Knowledge transfer na pracovníkov MIRRI a zabezpečenie podpory pre celý proces riadenia rizík až po formálny zápis alebo protokol ohľadom rozhodnutia akým spôsobom budú riadené jednotlivé identifikované riziká v súlade s predchádzajúcim bodom, t.j. návrhom spôsobu riadenia /mitigácie/ identifikovaných rizík. Naceňovaný rozsah je 40 MD.

Č.	Oblasť D)	Poznámka
	QA nad realizáciou a dodávanými výstupmi projektov realizovaných v rámci dopytovej výzvy „Rozvoj governance a úrovne informačnej a kybernetickej bezpečnosti v sektore VS“	Výstupom budú najmä konzultačné služby a činnosti zamerané na kvalitu dodávaných výstupov a ich súlad s navrhnutými metodikami, metodickými usmerneniami a vzorovou dokumentáciou v rozsahu najviac 800 MD, pričom sa predpokladajú QA aktivity pre minimálne 30 projektov. Čerpanie bude realizované formou objednávok podľa počtu projektov a potrieb MIRRI.

Č.	Oblasť E)	Poznámka
	Projektové riadenie celého CMRKB (ktoré sa skladá z 4 verejných obstarávaní) v súlade s vyhláškou 85/2020 Z.z.	Výstupom budú aktivity a dokumenty vyžadované vyhláškou 85. Naceňovaný rozsah je 200MD. Predpokladá sa aj knowledge transfer.

2.5 Forma a spôsob odovzdania predmetu zákazky

1. definované dokumenty vo verziách pre jednotlivé kategórie ITVS podľa vyhlášky č. 179/2020 Z. z. ako offline dokumenty a zároveň zverejnené na definovanom online portáli,
2. definované dokumenty prispôsobené pre MIRRI,
3. výstupy definované v časti 2.4,
4. transfer know-how na zamestnancov MIRRI formou shadowingu pri realizácii AR/BIA a QA nad dopytovými projektami ako aj pri projektovom riadení.

3 NÁVRH OPISU ČASTI III. PREDMETU ZÁKAZKY: Overenie spôsobu implementácie bezpečnostných opatrení prostredníctvom malých pilotných riešení na MIRRI: Implementácia nového 10Gbps Firewallu, implementácia dvojfaktorovej autentifikácie a pilotná implementácia log manažment systému

3.1 Špecifikácia úlohy

Verejné obstarávanie je súčasťou projektu Centralizovaný manažment riadenia kybernetickej bezpečnosti verejnej správy, ktorého jedným z cieľov je overiť spôsob implementácie bezpečnostných opatrení prostredníctvom malých pilotných riešení na MIRRI. Výsledkom projektu budú na vybranej časti infraštruktúry MIRRI implementované:

- implementácia nového 10Gbps Firewallu prepojeného na log manažment,
- implementácia dvojfaktorovej autentifikácie na VPN prístupe a vybraných aplikáciách,
- prevádzkový monitoring Zabbix celej siete MIRRI,
- pilotná implementácia log manažment systému.

Pre túto úlohu je potrebné zabezpečiť:

- hardvér a licencie na jednotlivé produkty,
- implementáciu do prostredia MIRRI,
- zaškolenie používateľov a administrátorov,
- vyhodnotenie opatrení a odporúčania na implementáciu pre ďalšie rezorty.

3.2 Popis infraštruktúry verejného obstarávateľa

Verejný obstarávateľ má aktuálne cca 1000 zamestnancov, ktorí sa pripájajú z lokality zamestnávateľa alebo z domu do infraštruktúry. Tá aktuálne používa zariadenia Cisco (a chrbticový FW Fortigate) a preto by z tohto pohľadu bolo ideálne, ak budú môcť byť nástroje dvojfaktorová autentifikácia, VPN a endpoint protection integrované s existujúcimi Cisco konzolami. Nutnou požiadavkou však je, aby dodávané produkty mali integrovaný manažment., aby verejný obstarávateľ neskončil s úplne rôznymi konzolami

Požiadavky na zapojenie do existujúcej siete:

- optika 10GB SFP+ moduly na sieťové zariadenia,
- 10 GBit Ethernet na serverové zariadenia, ako SFP moduly.

Firewall by mal v rámci vnútornej siete zabezpečovať nasledovné:

- interný segmentačný FW,
- IPS,
- vynucovanie FW politiky na základe identity užívateľov, nie iba na základe zdrojových sietí/IP adries.

FW by mal pri komunikácii z vnútornej siete von alebo z vonku do vnútornej siete zabezpečovať nasledovné:

- IPS,
- ochranu proti škodlivým botom (kontrola prístupu na C&C servery),
- URL filtering/aplikačnú kontrolu,

- antivírus,
- hĺbkovú SSL inšpekciu,
- sandboxing.

3.3 Špecifikácia predmetu zákazky

Primárnym predmetom zákazky je pilotné nasadenie bezpečnostných riešení a ich overenie v prevádzke spojené s prechodom na chrbticovú sieť založenú na 10Gbit technológii pre cca 1000 používateľov v rôznych lokalitách. MIRRI chce v súvislosti s sťahovaním do novej budovy prejsť na 10Gbit technológiu ako aj lepšie bezpečnostné funkcie. Aktuálne sa používa firewall Fortigate 600D. V tejto súvislosti bude potrebné zakúpiť kombináciu HW, SW a služieb, pričom je primárne na uchádzačovi, aby zvolil čo najefektívnejšiu kombináciu licenčného SW, HW a služieb, ktorá bude vedieť splniť nasledovné požiadavky:

- Dokumentácia, analýza, príprava, manažment a implementácia zmeny chrbticového edge firewallu v high availability konfigurácii (t.j. 2 kusy) s minimálne nasledovnými vlastnosťami:
  - min. 6x 10Gbit SFP+ porty (SFP moduly si obstará MIRRI samostatne),
  - firewall bude umožňovať aj sandboxing (možnosť využiť cloudovú funkciu, nakoľko bude zapnutá na traffic prichádzajúci z internetu),
  - napojenie na RADIUS/SSO a bude podporovať SD-WAN,
  - VPN prístup (1000 konkurentných VPN používateľov),
  - možnosť rozdeliť firewall na min. 2 virtuálne firewally,
  - Firewall by mal byť zložený z komponentov jedného výrobcu, vrátane všetkých poskytovaných funkcionalít typu IPS, AV, AS signatúr, databáz pre URL kategorizáciu, sandbox definícií a pod. Zároveň by mala byť týmto jedným výrobcom zaistená podpora minimálne po dobu plánovanej životnosti FW,
  - FW by mal obsahovať jeden dedikovaný port pre správu pomocou konzoly,
  - FW by mal obsahovať aspoň jeden dedikovaný OOB management port pre plnohodnotnú správu FW,
  - FW by mal byť schopný ukladať údaje na interný HDD disk,
  - FW by mal podporovať agregáciu portov pomocou protokolu 802.3ad (LACP),
  - FW by mal byť rozmerovo kompatibilný s 19 "rozvádzačom,
  - FW by mal podporovať dva nezávislé redundantné zdroje napájania AC 230V, vymeniteľné za behu zariadenia,
  - FW by mal plne podporovať IPv4 aj IPv6,
  - FW by mal podporovať preklady adries typu Static NAT, Dynamic NAT, PAT, NAT64,
  - FW by mal podporovať smerovanie typu Static route, RIP, OSPFv2, OSPFv3, BGP, PIM, IGMP a PBR (Policy Based Routing),
  - PBR by malo byť možné nakonfigurovať na základe všetkých dostupných metrík typu interface, zóna, IP adresa, užívateľ,
  - FW by mal podporovať režim clusteringu, využiteľný pre prípadné dodatočné zvýšenie priepustnosti aj v geograficky oddelených lokalitách,
  - FW by mal podporovať site-to-site VPN pomocou protokolu IPSec,
  - FW by mal podporovať Remote Access VPN pomocou protokolov IPSec a SSL (min. TLS v1.2), vrátane možnosti konfigurácie profilov pre vynútenie prihlásenie do vpn v závislosti od prístupovej siete (napr. mimo pracoviska),
  - počet súčasne pripojených užívateľov nesmie byť licenčne obmedzený,
  - správa sieťových a bezpečnostných funkcií bude možná bez nutnosti používania centrálneho management servera,

  - FW by mal podporovať aplikačnú detekciu a kontrolu ako svoju natívnu funkcionalitu,,
  - FW by mal podporovať vytváranie bezpečnostných pravidiel na základe používateľských identít
  - FW by mal obsahovať integrovaný systém ochrany proti zraniteľnostiam (virtual patching) a sieťovým útokom (IPS). Databáza IPS signatúr by mala byť uložená priamo vo FW.min. 2.5 Gbps priepustnosť rozhrania so zapnutými funkciami:
    - IPS, malware protection, url filtering, application control (L7),
    - SSL inšpekcia v režime pre prichádzajúci/odchádzajúci traffic na WAN rozhranie.

- Súčasťou tejto zmeny budú aj nasledovné aktivity:
  - analýza súčasnej dokumentácie,
  - porovnanie dokumentácie so súčasným stavom,
  - aktualizácia dokumentácie AS IS stavu, alebo vytvorenie novej dokumentácie (súčasná dokumentácia pozostáva iba z nákresu) na úrovni L1, L2 a L3,
  - uloženie informácii do repozitára,
  - vytvorenie štatistiky sieťovej prevádzky,
  - návrh cieľového stavu stavu na úrovni L1, L2 a L3,
  - vytvorenie komunikačnej matice zero trust a návrh zodpovedajúcich FW pravidiel,
  - vytvorenie zmeny na výmenu firewallu,
  - výmena chrbticového firewallu, jeho zapojenie, migrácia a optimalizácia,
  - zapojenie sieťových zariadení do Zabbix-u,
  - vytvorenie aktuálnych prevádzkových záznamov (konfigurácií),
  - zaškolenie IT pracovníkov MIRRI do používania a administrácie,
  - shadowing pre vybraných pracovníkov MIRRI počas trvania projektu.
- Zavedenie dvojfaktorovej autentifikácie vo VS. Zvýšenie úrovne identifikácie a najmä autentifikácie pracovníkov VS („bežných používateľov“), najmä pri vzdialených prístupoch vynucovaných COVID pandémiou, ale aj zvýšenie úrovne bezpečnosti pri správe IKT vo VS z pozície „power“ používateľov a administrátorov systémov („privilegovaných účtov“). Dvojfaktorová autentifikácia bude zavedená:
  - na VPN prístup na FW z bodu 1,
  - na vzdialený prístup k emailom,
  - na prihlásenie do MS ActiveDirectory domény ako súčasť prihlasovania sa do pracovných staníc Windows (integrácia druhého faktoru do štandardného prihlasovacieho formulára), aj v offline režime (keď nie je možné pripojenie na autentifikačný server),
  - po analýze na niektoré (alebo všetky) z aplikácií ITMS, CSRU, IOM, MetaIS a DKS (Fabasoft), samotná zmena aplikácii nie je predmetom dodania.
- Zavedenie bezpečnosti pracovných staníc:
  - ochrana pre škodlivým kódom – anti-malware, anti-ransomware, anti-bot, anti-phuishing,
  - kontrola komunikácie – personal firewall, url filtering,
  - kontrola lokálnych portov – použitie dôveryhodných vymeniteľných médií, úplne zakázanie vymeniteľných médií,
  - šifrovanie údajov – plne šifrované pracovné stanice (pre-boot), šifrovanie logických celkov, šifrovanie vymeniteľných médií,
  - kontrola konfigurácie – sledovanie súladu s definovanými pravidlami – compliance check,

  - podpora riešenia bezpečnostných incidentov - zber logov a auditných záznamov, izolovanie koncového zariadenia, vzdialený prístup, aktívne kroky na odstránenie incidentu (live response pri riešení incidentu).
- Zavedenie prevádzkového monitoringu Zabbix s nasledovnými požadovanými vlastnosťami:
  - implementácia a zavedenie do praxe open source nástroja Zabbix na jednom serveri (server dodá MIRRI) a zapojenie dodávaných zariadení do monitoringu,
  - zapojenie existujúcich sieťových zariadení MIRRI do monitoringu v min. celkovom rozsahu 60 zariadení (primárne switchov a niekoľko ďalších zariadení ako serverov),
  - zaškolenie obsluhy, dokumentácia a optimalizácia inštalácie, prepojenie na dodávaný log manažment (viď nižšie).
- Zavedenie Log manažment systému na vybranej infraštruktúre MIRRI. Súčasťou projektu bude aj:
  - analýza a návrh spôsobu zaznamenávania logov a auditných udalostí, ich centrálneho zberu a zhromažďovania, ukladania, uchovávania, rotácie, poskytovania analýz a reportovania,
  - konsolidácia logov pre efektívne a spoľahlivé fungovanie nadstavbových analytických a iných systémov vyhodnocovania bezpečnostných incidentov (napr. SIEM) za účelom minimalizácie „false positive“ a „false negative“ hlásení a vytvorenie metodických postupov a manuálov pre postupné zavádzanie LMS v ďalších OVM,
  - grafické GUI s vyhľadávaním, centrálnym prehľadom, analytickými prehľadmi,
  - tvorba vlastných dashboardov,
  - parsovanie logov, minimálne pre svet Windows (Active Directory, Exchange), Linuxový svet, SMTP, Cisco zariadenia, Fortinet firewall),
  - retenčná doba logov sa predpokladá min. 6 mesiacov,
  - REST API pre potenciálnu integráciu,
  - agent na zbieranie logov pre operačné systémy Windows, Linux,
  - možnosť obohacovania logov o doplnkové informácie (geoip, threat intelligence, ...),
  - možnosť exportu logov do CSV,
  - možnosť kompresie logov,
  - možnosť automatického zálohovania logov na externé úložisko,
  - možnosť jednoducho škálovať len pridaním ďalšieho nodu,
  - licenčne neobmedzený počet zdrojov, EPS, objemu logov,
  - kontrola prístupu na základe rolí, podpora viacfaktorovej autentifikácie,
  - Implementácia sa predpokladá nad nasledovnými systémami:
    - MetaIS,
    - ITMS,
    - CSRU,
    - IOM,
    - MS Exchange,
    - DKS (Fabasoft),
    - sieťové prvky MIRRI.

3.4 Požadované výstupy

Č.	Požadovaný výstup	Merná jednotka a počet	Príklad dodávky
1.	Hardvér, dokumentácia, analýza, príprava, manažment a implementácia zmeny firewallu v high availability konfigurácii	2 kusy - HA mód, licencia min. na 2 roky	CISCO, FortiGate, Juniper firewally s funkciami sandboxing, VPN, threat protection atď.
2.			
3a.	Pilotný projekt zavedenia dvojfaktorovej autentifikácie na	používateľ – 1000 používateľov na 2 roky	VPN Anyconnect- pripojenie VPN klienta do siete,

	vybranej službe/agende a VPN prístupe. Riešenie musí byť redundantné. Dvojfaktorová autentifikácia bude podporovať integráciu cez najpoužívanejšie protokoly (openID, oAuth, SAML),		Duo Security – 2FA
3b.	Pilotný projekt zavedenia dvojfaktorovej autentifikácie na vybranej službe/agende – HW tokeny	kus – 500 kusov	Yubico Yubikey 5 series Cisco Duo Token
4.	Bezpečnosť pracovných staníc	Endpoint security riešenie	AMP endpoint security – Ochrana koncových staníc, Cisco Umbrella - aplikovanie firemných politík po zapnutí PC mimo office bude vyžadovať prihlásenie sa do VPN ináč nebude možné sa pripojiť na WiFi (hotspot), MS Defender
5.	Monitoring Zabbix	Implementácia Zabbixu a integrácia 60 zariadení do monitoringu	Implementácia Zabbix na HW zdrojoch, ktoré poskytne MIRRI
6.	Analýza a implementácia zavedenia LMS na infraštruktúre MIRRI vrátane hardvéru	logy za sekundu - min. 4000 EPS	Logmanager
7.	Nastavenie a optimalizácia systému	Po nasadení systému je potrebná jeho optimalizácia a vyladenie.	dlhodobé sledovanie a nastavenie všetkých dodávaných komponentov a ich pravidiel tak, aby správne zachytili a vyhodnotili podozrivé aktivity
8.	Customizácia, integrácia a podpora nad rámec tu uvedených požiadaviek	Práce potrebné na prípravu na integráciu aplikácii MIRRI na LMS a 2FA, ktoré budú objednané samostatne. Naceňovaný rozsah je 80 MD.	3rd level support

3.5 Forma a spôsob odovzdania predmetu zmluvy

Ku každému z požadovaných výstupov bude dodané:

- technický návrh - high a low level design nasadenia do infraštruktúry MIRRI,
- nasadený sw/hw,
- školenia administrátorov na inštalované technológie v rozsahu 3 ľudí na každú technológiu,
- školenia používateľov v elektronickej forme použiteľné aj ako praktický návod,
- návod na inštaláciu,
- vyhodnotenie spokojnosti používateľov s prevádzkou,
- vyhodnotenie riešenia z pohľadu prevádzky a poučenia do budúcnosti,
- odporúčania pre iné inštitúcie,
- súčinnosť s vytváraním dokumentov a aktivít vyžadovaných vyhláškou 85/2020 Z.z.

4 NÁVRH OPISU ČASTI IV. PREDMETU ZÁKAZKY: Overenie spôsobu implementácie bezpečnostných opatrení prostredníctvom malých pilotných riešení na MIRRI: Analýza a pilotná implementácia konceptu bezpečnej správy mobilných zariadení používaných v rámci MIRRI

4.1 Špecifikácia úlohy

Verejné obstarávanie je súčasťou projektu Centralizovaný manažment riadenia kybernetickej bezpečnosti verejnej správy, ktorého jedným z cieľov je overiť spôsob implementácie bezpečnostných opatrení prostredníctvom malých pilotných riešení na Ministerstve investícií, regionálneho rozvoja a informatizácie SR (ďalej len „MIRRI“). Výsledkom projektu bude analýza a pilotná implementácia konceptu bezpečnej správy mobilných zariadení používaných v rámci MIRRI (MDM – mobile device management) s posúdením možností využitia aj konceptu BYOD a s posúdením možností nasadzovania tohto riešenia aj na ďalšie OVM v rámci sektoru VS.

Pre túto úlohu je potrebné zabezpečiť:

- licencie na jednotlivé produkty,
- implementáciu produktov do prostredia MIRRI,
- zaškolenie používateľov a administrátorov.

4.2 Špecifikácia predmetu zákazky

Primárnym predmetom zákazky je pilotné nasadenie bezpečnostného riešenia a jeho overenie v prevádzke:

- Analýza a implementácia konceptu bezpečnej správy mobilných zariadení (MDM – mobile device management) používaných vo VS (v rámci tohto pilotného projektu na MIRRI) s možnosťou posúdenia využitia aj konceptu BYOD. Riešenie umožní najmä centralizovanú bezpečnú správu a konfiguráciu mobilných zariadení, oddelenie pracovných a súkromných záležitostí (prostredí), zabezpečenie vzdialených prístupov z mobilných zariadení k IKT zdrojom OVM, zabezpečenie ochrany dát nachádzajúcich sa na mobilných zariadeniach, zabezpečenie prípadného bezpečného zmazania mobilného zariadenia na diaľku a pod..

Predmetom nasadenia MDM sú:

- OS Windows 10 (počítače) v počte 100ks s opciou na celkovo 700ks,
- IOS (mobily),
- Android (mobily).

Z vecného pohľadu budú riešené nasledovné agendy:

- email, kalendár a kontakty,
- prístup k súborom v rámci file systém-u MIRRI (DMS),
- instant messaging a kolaboračné služby.

4.3 Požadované výstupy

Č.	Požadovaný výstup	Merná jednotka a počet	Príklad dodávky

1.	Analýza a pilotná implementácia konceptu bezpečnej správy mobilných zariadení používaných vo VS (MDM – mobile device management) s možnosťou posúdenia využitia aj konceptu BYOD.	licencia - používateľ – 1000 používateľov na dva roky, prípadne perpetuálna licencia na 2000 zariadení	Microsoft Intune
2.	Nastavenie a optimalizácia systému	Po nasadení systému je potrebná jeho optimalizácia a vyladenie.	Dlhodobé sledovanie a nastavenie systému pravidiel tak, aby správne zachytil a vyhodnotil podozrivé aktivity
3.	Zvýšená podpora	Naceňuje sa podpora počas trvania projektu v rozsahu 40MD	3rd level support

4.4 Forma a spôsob odovzdania predmetu zmluvy

Ku každému z požadovaných výstupov bude dodané:

A. technický návrh - high a low level design nasadenia do infraštruktúry MIRRI, preferujeme nasadenie do cloud-u s konektormi do infraštruktúry MIRRI v high availability prevedení pre konektory nachádzajúce sa v infraštruktúre MIRRI,

- nasadený sw/hw,
- školenia administrátorov,
- školenia používateľov,
- návod na inštaláciu,
- vyhodnotenie spokojnosti používateľov s prevádzkou,
- vyhodnotenie riešenia z pohľadu prevádzky a poučenia do budúcnosti pre ostatné OVM,
- súčinnosť s vytváraním dokumentov a aktivít vyžadovaných vyhláškou 85/2020 Z.z.