**PROJEKTOVÝ ZÁMER**

(Verzia dokumentu v1.82/09\_2021)

Identifikovanie požiadaviek **na funkčnú časť riešenia**

**Identifikácia projektu**

|  |  |
| --- | --- |
| **Povinná osoba** | Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky |
| **Názov projektu** | Posilnenie preventívnych opatrení, zvýšenie rýchlosti detekcie a riešenia incidentov |
| **Zodpovedná osoba za projekt** | Mgr. Filip Tubler |
| **Realizátor projektu**  | Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky |
| **Vlastník projektu** | Ing. Martin Florián, PhD. |

**Schvaľovanie dokumentu**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Položka** | **Meno a priezvisko** | **Organizácia** | **Pracovná pozícia** | **Dátum** | **Podpis**(alebo elektronický súhlas) |
| Vypracoval | Filip Tubler, Lukáš Belušák | MIRRI | Manažér pre investíciu / PM |  |  |

\*Pôvodná verzia dokumentu bola z hľadiska dôvernosti informačných aktív klasifikovaná na stupeň „CHRÁNENÉ“ podľa vyhlášky Národného bezpečnostného úradu z 11. decembra 2018 č. 362/2018, ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení v znení neskorších predpisov a podľa smernice Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky č. 13/2021 zo dňa 22. októbra 2021 o inventarizácii a ochrane informačných aktív Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky.

Z dôvodu zverejnenia dokumentácie v METAIS a vyššie uvedenej klasifikácie dokumentu sú vybrané textové a obrázkové časti redigované.

**Obsah**

[1. POPIS ZMIEN DOKUMENTU 3](#_Toc149337697)

[1.1. História zmien 3](#_Toc149337698)

[2. ÚČEL DOKUMENTU, SKRATKY (KONVENCIE) A DEFINÍCIE 3](#_Toc149337699)

[2.1. Použité skratky 3](#_Toc149337700)

[2.1.1. Konvencie pre typy požiadaviek (príklady) 4](#_Toc149337701)

[3. DEFINOVANIE PROJEKTU 5](#_Toc149337702)

[3.1. Manažérske zhrnutie 5](#_Toc149337703)

[3.2. Motivácia a rozsah projektu 6](#_Toc149337704)

[3.3. Zainteresované strany/Stakeholderi 13](#_Toc149337705)

[3.4. Ciele projektu a merateľné ukazovatele 13](#_Toc149337706)

[3.5. Špecifikácia potrieb koncového používateľa 14](#_Toc149337707)

[3.6. Riziká a závislosti 15](#_Toc149337708)

[3.7. Alternatívy a Multikriteriálna analýza 15](#_Toc149337709)

[3.7.1. Stanovenie alternatív pomocou biznisovej vrstvy architektúry 15](#_Toc149337710)

[3.7.2. Multikriteriálna analýza 17](#_Toc149337711)

[3.7.3. Stanovenie alternatív pomocou aplikačnej vrstvy architektúry 19](#_Toc149337712)

[3.7.4. Stanovenie alternatív pomocou technologickej vrstvy architektúry 19](#_Toc149337713)

[4. POŽADOVANÉ VÝSTUPY (PRODUKT PROJEKTU) 19](#_Toc149337714)

[5. NÁHĽAD ARCHITEKTÚRY 22](#_Toc149337715)

[6. LEGISLATÍVA 27](#_Toc149337716)

[7. ROZPOČET A PRÍNOSY 28](#_Toc149337717)

[8. HARMONOGRAM JEDNOTLIVÝCH FÁZ PROJEKTU a METÓDA JEHO RIADENIA 32](#_Toc149337718)

[9. PROJEKTOVÝ TÍM 33](#_Toc149337719)

[10. PRACOVNÉ NÁPLNE 36](#_Toc149337720)

[11. ODKAZY 38](#_Toc149337721)

[12. PRÍLOHY 38](#_Toc149337722)

# POPIS ZMIEN DOKUMENTU

# História zmien

|  |  |  |  |
| --- | --- | --- | --- |
| Verzia | Dátum | Zmeny | Meno |
| v0.1 | 30.09.2022 | Vytvorenie dokumentu | Ľ. Chnápko |
| v0.2 | 30.12.2022 | Zapracovanie zmeny konceptu budovania nového riešenia SOC na MIRRI SR (nové riešenie) | E. Saller |
| v0.3 | 28.02.2023 | Integrácia EWS riešenia a rozširovanie existujúceho spoločného pracoviska SOC (NASES a VJ CSIRT) | F. Tubler, L. Belušák |
| v0.4 | 30.06.2023 | Aktualizácia náhľad architektúry, projektový tím, zainteresované strany, riziká a závislosti | F. Tubler, L. Belušák |
| v1 | 23.10.2023 | Aktualizácia harmonogramu, rozpočtu, prínosov a ďalšie úpravy. | F. Tubler, L. Belušák |

# ÚČEL DOKUMENTU, SKRATKY (KONVENCIE) A DEFINÍCIE

Dokument **Projektový zámer** je dokument vypracovaný v súlades **vyhláškou č. 85/2020 Z. z. o riadení projektov** a je určený na rozpracovanie detailných informácií prípravy projektu, aby bolo možné rozhodnúť o pokračovaní prípravy projektu, alokovaní rozpočtu, ľudských zdrojov a prechode do realizačnej fázy.

# Použité skratky

|  |  |  |
| --- | --- | --- |
| **ID** | **SKRATKA** | **POPIS** |
| 1 | Achilles | Vládny systém na vyhľadávanie zraniteľností |
| 2 | BCM | Riadenie kontinuity podnikania |
| 3 | BCR | Pomer prínosov a nákladov z pohľadu návratnosti |
| 4 | CBA | Analýza nákladov a prínosov |
| 5 | CSIRT.SK  | Computer Security Incident Response Team Slovakia |
| 7 | EIRR | Ekonomická vnútorná výnosová miera  |
| 8 | ENISA | Európskej agentúry pre kybernetickú bezpečnosť |
| 9 | ENPV | Ekonomická čistá súčasná hodnota  |
| 10 | EWS | Early Warning System (Systém Včasného Varovania) |
| 11 | FNPV | Finančná čistá súčasná hodnota |
| 12 | FO | Fyzická osoba |
| 13 | FTE | Ekvivalent plného pracovného úväzku |
| 14 | GAP analýza | Rozdielová analýza |
| 15 | HDP | Hrubý domáci produkt |
| 16 | HW | Hardvér |
| 17 | IDS  | Systém na detekciu prienikov |
| 18 | IPS | Systém na prevenciu prienikov |
| 19 | IS | Informačný systém |
| 20 | IS VS | Informačný systém verejnej správy |
| 21 | IT | Informačná technológia |
| 22 | ITVS | Informačná technológia verejnej správy |
| 23 | JISKB | Jednotný informačný systém kybernetickej bezpečnosti |
| 24 | KB  | Kybernetická bezpečnosť |
| 25 | KIB | Kybernetická informačná bezpečnosť |
| 26 | MCA | Multikriteriálna analýza |
| 27 | MIRRI | Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky |
| 28 | MISP | Malware Information Sharing Platform |
| 29 | NASES | Národná agentúra pre sieťové a elektronické služby |
| 30 | NBÚ | Národný bezpečnostný úrad |
| 31 | NIS 2 | Európska smernica o opatreniach na zaistenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii |
| 32 | NKIVS | Národná koncepcia informatizácie verejnej správy |
| 33 | OSINT | Open Source Intelligence |
| 34 | OVM  | Orgán verejnej moci |
| 35 | PID | Projektový iniciálny dokument  |
| 36 | PM | Projektový manažér |
| 37 | PO | Právnická osoba |
| 38 | POO | Plán obnovy a odolnosti |
| 39 | PPO | Posilnenie preventívnych opatrení |
| 40 | PZS | Prevádzkovateľov základných služieb  |
| 41 | RV | Riadiaci výbor |
| 42 | SIEM | Systém pre management bezpečnostních informací a událostí |
| 44 | SOAR | Security orchestration, automation and response |
| 45 | SOC  | Security Operations Center (Bezpečnostné Dohľadové Centrum) |
| 46 | SW | Softvér |
| 47 | VISKB | Vládny informačný systém kybernetickej bezpečnosti |
| 48 | VJ CSIRT | Vládna jednotka CSIRT (niekedy označovaná aj skratkou CSIRT.SK) |
| 49 | VO | Verejné obstarávanie |
| 53 | TTP | Techniky, taktiky a procedúry  |
| 54 | IoC | Indikátor kompromitácie (Indicators of Compromise) |

# Konvencie pre typy požiadaviek (príklady)

Hlavné kategórie požiadaviek v zmysle katalógu požiadaviek sú rozdelené na funkčné, nefunkčné a technické. Podskupiny v hlavných kategóriách je možné rozšíriť v závislosti od potrieb projektu, napríklad:

Funkčné požiadavky používajú konvenciu:

*RF\_xxx*

* *RF – funkčná požiadavka*
* *xxx – číslo požiadavky*

Nefunkčné požiadavky používajú konvenciu:

*RNF\_xxx*

* *RNF – nefunkčná požiadavka*
* *xxx – číslo požiadavky*

Ostatné typy požiadaviek môžu byť ďalej definované objednávateľom/PM.

# DEFINOVANIE PROJEKTU

# Manažérske zhrnutie

Predložený dokument je vypracovaný v súlade s vyhláškou č. 85/2020 Z. z. o riadení projektov a vychádza z **Investície č. 6:** *Posilnenie preventívnych opatrení, zvýšenie rýchlosti detekcie a riešenia incidentov (Informačné technológie vo verejnej správe – ITVS)* Komponentu 17 Digitálne Slovensko Plánu obnovy a odolnosti Slovenskej republiky. Hlavným cieľom tejto investície je zlepšiť technické a technologické vybavenie v systémoch kritickej infraštruktúry verejnej správy a zároveň zvýšiť úroveň centralizovaného zberu a vyhodnocovanie informácií s následným vylepšením komunikácie na relevantné subjekty s cieľom znižovania škôd spôsobených kybernetickými bezpečnostnými incidentmi a rýchlosti vyriešenia incidentov (prípadne pokiaľ možno úplne predchádzať škodám na IT verejnej správy).

Cieľom tohto dokumentu je popísať realizáciu špecifických a relevantných IT častí spomenutej investície, ktorá bude realizovaná v rokoch 2023 – 2026. Investícia č. 6 je súčasťou celkového koncepčného riešenia oblasti kybernetickej a informačnej bezpečnosti, ktorého súčasťou sú aj nasledujúce reformy:

* Komponent 17 Reforma č. 5: Skvalitnenie vzdelávania a zabezpečenie spôsobilosti v oblasti KIB;
* Komponent 17 Reforma č. 6: Štandardizácia technických a procesných riešení kybernetickej a informačnej bezpečnosti (ITVS).

Jednotlivé časti investície sa budú realizovať kombináciou viacerých foriem prístupov, avšak pre IT projekt sú relevantné nasledujúce časti:

1. Vybudovanie Systému včasného varovania (EWS – Early Warning System), ktorý bude zabezpečovať zber, koreláciu a vyhodnocovanie informácií naprieč zapojenými OVM a ďalšími zapojenými sektorovými SOCs obohacované o ďalšie zdroje dát.
2. Doplnenie nových služieb a funkčné rozšírenie už existujúceho spoločného bezpečnostného pracoviska (SOC) NASES a MIRRI SR, resp. VJ CSIRT, tzv. Vládneho SOC.
3. Implementácia nástrojov na zvýšenie úrovne kybernetickej bezpečnosti na vybraných OVM a spustenie bezpečnostného monitoringu prostredníctvom Vládneho SOC.
4. Implementácia výstupov z existujúceho systému na vyhľadávanie zraniteľností Achilles, rozšírenie integrácií o ďalšie OVM a ich informačné systémy, zabezpečenie rýchlejšej identifikácie zraniteľných miest, korelácia výsledkov s ďalšími dátami.

Projektom sú zároveň adresované problémy súčasného stavu, ktoré vyplývajú z geopolitického vývoja, vývoja v oblasti kybernetických hrozieb, zrealizovaných auditov kybernetickej bezpečnosti a GAP analýzy vykonanej na vybraných subjektoch verejnej správy:

* Nedostatočné zabezpečenie IS v prostredí VS voči aktuálnym bezpečnostným hrozbám, najmä vzhľadom na ich rastúcu početnosť a komplexnosť;
* Chýbajúce služby proaktívnej bezpečnosti v prostredí VS, vrátane bezpečnostného monitoringu;
* Chýbajúce skúsenosti a spôsobilosti pre udržiavanie kybernetickej bezpečnosti na OVM;
* Nedostatočné personálne kapacity špecialistov na kybernetickú bezpečnosť vo verejnej správe a na pracovnom trhu;
* Nedostatočné zdieľanie dát a výmena informácii medzi subjektami verejnej správy v prípade bezpečnostných hrozieb.

a príležitostí:

* Potreba znižovať dopady kybernetických útokov na sektor verejnej správy a zvýšenia ochrany dát a služieb pre občanov SR;
* Potreba centralizovaného riadenia kybernetickej bezpečnosti v prostredí verejnej správy so zapojením širšej skupiny OVM;
* Dobudovanie pracoviska SOC a zvýšenie kvality monitoringu podľa zadefinovaných štandardov, povinných zdrojov logov a MITRE ATT&CK Frameworku;
* Potreba rozšírenia reaktívnych služieb (prioritne incident handling a incident response) o proaktívne služby monitoringu kybernetickej bezpečnosti, ofenzívnej bezpečnosti a ďalších;
* Potreba rýchlejšej reakcie na minimalizovanie dopadu kybernetických hrozieb;
* Potreba zvýšenia efektívnosti spracovania bezpečnostných údajov vo verejnej správe;
* Potreba obnovy a doplnenia najnovších HW a SW technológií v súlade s technologickým vývojom v oblasti kybernetickej bezpečnosti;
* Vytvorenie platformy na zdieľanie informácií medzi SOC vo verejnej správe;
* Centralizované poskytovanie jednotlivých služieb EWS prinesie konsolidáciu a znižovanie nákladov na obstarávanie a prevádzku bezpečnostných technológií;
* Centralizované a škálovateľné riešenie prinesie možnosť efektívneho rozširovania aj pre ďalšie subjekty, ktoré sa v budúcnosti môžu pripojiť do bezpečnostného monitoringu SOC a systému EWS.

Hlavným cieľom projektu, v súvislosti s vyššie popísanou oblasťou, je **zvýšenie úrovne a rozšírenie zabezpečenia informačných systémov v prostredí verejnej správy pred hrozbami kybernetických útokov**. Zámerom projektu je nastaviť nové štandardy pre úroveň zabezpečenia nie len informačných systémov v prostredí verejnej správy, ale subjektov verejnej správy ako celku so zodpovedajúcou „viditeľnosťou“ do IT prostredia subjektov. To bude zabezpečené pokrytím monitorovania koncových bodov, sieťovej komunikácie, manažmentu zraniteľností a poskytnutím ďalších služieb. Rozšírenie zabezpečenia spočíva v zavedení služieb bezpečnostného monitoringu a ďalších proaktívnych a reaktívnych služieb pre sedem subjektov verejnej správy, ktoré doteraz uvedené služby nemali zabezpečené vôbec alebo iba v obmedzenej miere. Zámerom je zároveň nastaviť základný framework procesov, governance a technológií, ktoré umožnia postupné pripájanie ďalších subjektov verejnej správy do bezpečnostného monitoringu a systému včasného varovania. Po implementácii tohto projektu predpokladáme vytvorenie a spustenie služby SOC as a service, ktorá bude môcť byť ponúkaná aj ďalším OVM na základe nastaveného a v tomto projekte vytvoreného „zlatého štandardu“.

Najvýznamnejšie prínosy projektu, ktoré boli identifikované, sú:

* Zníženie ekonomických škôd a preventívne zabránenie škôd spôsobených kybernetickými útokmi;
* Zvýšenie odolnosti a dostupnosti služieb, ktoré poskytujú OVM;
* Efektívne riadenie IT zdrojov a
* Úsporu nákladov vďaka centralizovaným službám.

Medzi ďalšie prínosy možno zaradiť nasledujúce:

* Celkové zvýšenie úrovne zabezpečenia informačných systémov v prostredí verejnej správy, dostupnosť a dôveryhodnosť elektronických služieb štátu a ochrana dát obyvateľov SR;
* Včasné odhaľovanie potenciálnych hrozieb, detekcia a rýchlejšia reakcia na vzniknuté kybernetické bezpečnostné incidenty;
* Zdieľanie informácií o hrozbách, útokoch a konkrétnych riešeniach medzi OVM;
* Zníženie rizík a ich dopadov vyplývajúcich z realizovaných kybernetických útokov (napr.: nedostupnosť služieb štátu pre občanov a podnikateľov, ohrozenie reputácie organizácie a dôvery v poskytované služby);
* Maximalizácia automatizácie detekcie a reakcie na incidenty;
* Koncentrácia odborných kapacít špecialistov na kybernetickú bezpečnosť na jednom pracovisku;
* Ponuka komplexného riešenia formou efektívne dodávanej služby pre subjekty, kde nedostatočná kapacita ľudských zdrojov, financií a kvality zabezpečenia IT prostredia prináša vysoké riziko dopadu kybernetických útokov;
* Zvyšovanie kompetencie v oblasti kybernetickej bezpečnosti na strane štátu.

Cieľom projektu je naďalej rozvíjať bezpečnostný monitoring v prostredí verejnej správy, zabezpečovať informačné systémy v správe MIRRI, NASES a pripájať OVM do bezpečnostného dohľadového centra prevádzkovaného NASES a VJ CSIRT. Tieto služby budú určené pre tie OVM, ktoré sú prevádzkovateľom základnej služby, sú zaradené do podsektoru ISVS, nedisponujú dostatočnými zdrojmi na budovanie vlastných kapacít, a u ktorých by budovanie vlastného dohľadového centra nebolo efektívne. S každým OVM, ktoré bude zapojené do bezpečnostného monitoringu, je/bude podpísané memorandum o spolupráci s dohodou o mlčanlivosti, vykonaná vstupná analýza a pred nasadením bezpečnostných nástrojov podpísaná zmluva o bezpečnostnom monitoringu.

Projekt predpokladá centrálny nákup bezpečnostných nástrojov, ktoré bude mať podľa funkčného modelu v správe NASES alebo VJ CSIRT vrátane podpory prevádzkových kapacít jednotlivých tímov a rolí pre zabezpečenie novovytvorených a rozšírených služieb pre OVM. Prostredníctvom projektu nie sú financované nákupy vlastných bezpečnostných nástrojov ani kapacity na OVM.

Časť projektových aktivít bude realizovaná prostredníctvom agentúry NASES, s ktorou bude na dobu trvania projektu uzatvorená tzv. sprostredkovateľská zmluva („Zmluva o vykonávaní časti úloh vykonávateľa sprostredkovateľom“). Úlohou NASES bude v spolupráci s MIRRI najmä navrhnúť detailnú architektúru riešenia, nákup technológií pre centrálnu časť riešenia a lokality, integrovať jednotlivé nástroje do technológií dohľadového centra (SIEM, SOAR), prevádzkovať ich, ladiť nástroje, nastavovať pravidlá detekcie a vyhodnocovať bezpečnostné udalosti, ktoré môžu predstavovať potenciálne kybernetické bezpečnostné incidenty. HW a SW, ktorý je predmetom zmluvy, bude mať z dôvodu zjednodušenia prevádzky v správe jednotne NASES. Po skončení projektu bude činnosť krytá prostredníctvom existujúceho kontraktu medzi MIRRI a NASES.

Rámcový harmonogram projektu:

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **FÁZA/AKTIVITA** | **ZAČIATOK****(odhad termínu)** | **KONIEC****(odhad termínu)** |
| **1.** | Prípravná fáza | 06/2022 | 10/2023 |
| **2.** | Iniciačná fáza | 10/2023 | 11/2023 |
| **3.** | Realizačná fáza | 11/2023 | 05/2026 |
| **4.** | Dokončovacia fáza | 05/2026 | 06/2026 |

Celkový rozpočet projektu: 15 564 963 EUR

Celkové náklady spolu (do T10): 27 843 515 EUR

Podrobný rozpočet projektu sa nachádza v kapitole 7. Rozpočet a prínosy.

Opis základných procesov sa nachádza v prílohe CBA\_Procesné mapy.

# Motivácia a rozsah projektu

Kybernetické hrozby v Európskej únii ovplyvňujú životne dôležité sektory nevyhnutné pre chod spoločnosti. Medzi sektory najviac ovplyvnené hrozbami podľa Európskej agentúry pre kybernetickú bezpečnosť[[1]](#footnote-1) (ENISA) patrili v období jún 2021 až jún 2022:

1) verejná správa a štátne inštitúcie (24 % zaznamenaných hrozieb),

2) poskytovatelia digitálnych služieb (13 % zaznamenaných hrozieb),

3) široká verejnosť (12,4 % zaznamenaných hrozieb),

4) služby (11,8 % zaznamenaných hrozieb),

5) finančníctvo/bankovníctvo (8,6 % zaznamenaných hrozieb) a

6) zdravotníctvo (7,2 % zaznamenaných hrozieb).

Podľa správy o kybernetických hrozbách za rok 2022 vypracovanej Európskou agentúrou pre kybernetickú bezpečnosť (ENISA)[[2]](#footnote-2) medzi hlavnými skupinami hrozieb patria nasledovné:

1) Ransomvér: útočníci zamedzia prístup k dátam spoločnosti a požadujú výkupné za znovu umožnenie prístupu;

2) Malvér: škodlivý softvér, ktorý napáda operačný systém užívateľa;

3) Hrozby sociálneho inžinierstva: využitie ľudskej chyby na získanie prístupu k informáciám alebo službám;

4) Hrozby spojené s prístupom k údajom;

5) Hrozby obmedzujúce prístup k údajom;

6) Hrozby spojené s dostupnosťou internetu;

7) Dezinformácie: šírenie zavádzajúcich informácií;

8) Útoky na dodávateľský reťazec.

Na základe údajov o počte závažných kybernetických bezpečnostných incidentov, ktoré VJ CSIRT riešila, sa ich počet v uplynulých rokoch významne zvýšil. Významný zlom nastal po roku 2018. Za uplynulý rok 2022 sa počet závažných incidentov v riešení VJ CSIRT zvýšil na 1 012 s medziročným nárastom o 19 %, k čomu významne prispeli vyššia miera detekcie a nahlasovania incidentov, vypuknutie vojenského konfliktu medzi Ruskom a Ukrajinou a významný nárast aktivity štátom podporovaných skupín. Vplyvom pokračovania konfliktu a pretrvávajúcej podpory Ukrajiny možno očakávať podobný vývoj aj v nasledujúcom období. Medzi najčastejšie tipy závažných incidentov v roku 2022 patrili: získavanie informácií – phishing, social engineering... (55 %), malvér (18 %) a botnet (7 %).

\*Predpoklad na základe dát za Q1/2023

*Obrázok 1: Počet závažných incidentov riešených CSIRT.SK*

Verejná správa ako jeden zo sektorov **vykazuje dlhodobo veľmi zlé výsledky súladu s auditnými požiadavkami**. Pritom je to jeden z najväčších sektorov z pohľadu počtu prevádzkovateľov základných služieb (ďalej aj „PZS”), ktorých je aktuálne 1 410. Horšie výsledky vykazuje už len odvetvie tepelnej energetiky. Podrobný prehľad stavu súladu, resp. nesúladu s auditnými požiadavkami z pohľadu jednotlivých sektorov zobrazuje obrázok nižšie.

*Obrázok 2: Stav súladu podľa vykonaných auditov KB v jednotlivých odvetviach za rok 2022 (Zdroj: Doručené správy auditu KB za rok 2022, NBÚ)*

Jedným z dôvodov dosahovania nízkeho súladu s auditnými požiadavkami vo verenej správe môže byť práve motivácia subjektov. Podľa Správy o stave kybernetickej bezpečnosti v Slovenskej republike za rok 2022 najviac PZS označilo práve legislatívne požiadavky ako faktor, ktorý má najvyšší vplyv na zvyšovanie úrovne kybernetickej bezpečnosti v organizácii, čo určite nemožno považovať za správnu motiváciu. Z toho vyplýva, že:

* 61 % prevádzkovateľov neimplementuje bezpečnostné opatrenia nad rámec zákonných povinností;
* 66 % nevykonáva pravidelné posúdenie efektívnosti prijatých bezpečnostných opatrení;
* v oblasti plánov kontinuity činnosti organizácie (tzv. BCM – Bussiness continuity management) 62 % prevádzkovateľov nemá vypracované plány kontinuity činnosti a len štvrtina prevádzkovateľov, ktorí majú vypracované BCM, overuje jeho využiteľnosť pravidelne, aspoň raz za rok.

Medzi najčastejšie auditné zistenia v sektore Verejná správa patrí aj zistenie, že **organizácia nevypracovala postupy a nemá dostatočné schopnosti na detekciu, zvládanie a poučenie sa z prípadných incidentov**.

Motivácia a rozsah projektu vyplývajú aj z výsledkov GAP analýzy na spolupracujúcich OVM. Zrealizovaný tzv. screening na spolupracujúcich subjektoch verejnej správy potvrdil predpoklady a závery vyplývajúce z viacerých zdrojov (audity, kontroly, osobné stretnutia), ktoré naznačujú nedostatočnú úroveň kybernetickej bezpečnosti vo verejnej správe.  Príčiny aktuálneho stavu vyplývajú z kombinácie interných a externých faktorov. Medzi hlavné možno zaradiť:

* Nekoncepčný prístup k problematike kybernetickej bezpečnosti v sektore verejnej správy aj medzi samotnými subjektami VS;
* Nízka, resp. nesprávna, motivácia štatutárov a zodpovedných zamestnancov na zvyšovaní úrovne kybernetickej bezpečnosti zameraná prioritne na absolvovanie auditov KB, povrchný prístup alebo prijímané formálne bezpečnostné opatrenia;
* Nevyhovujúce, nevhodne aplikované alebo neexistujúce bezpečnostné nástroje, technológie alebo opatrenia, ktoré nereflektujú aktuálne požiadavky na kybernetickú bezpečnosť;
* Zložitosť nasadania a prevádzky systémov vyžadujúcich (pre efektívnu prevádzku) pravidelný bezpečnostný dohľad nad detegovanými udalosťami;
* Dlhodobý nedostatok finančných zdrojov alokovaných pre oblasť kybernetickej bezpečnosti;
* Nízka dostupnosť špecialistov na kybernetickú bezpečnosť na pracovnom trhu spojená s nedostatočnou konkurencieschopnosťou sektora VS v porovnaní s komerčným sektorom;
* Nedostatočné povedomie u zamestnancov a vedúcich pracovníkov o kybernetických hrozbách a možných dopadoch kybernetických bezpečnostných incidentov.

Na základe komparácie zisteného a cieľového (alebo možno povedať aj želaného) stavu u subjektov VS boli identifikované významné rozdiely. Jednotlivé rozdiely možno agregovať do väčších celkov – oblastí. Konkrétne sa jedná o technológie, služby, procesy a personálne kapacity, ktoré síce vystupujú ako samostatné oblasti, ale kľúčovým prvkom pre rozvoj kybernetickej bezpečnosti je ich vzájomná prepojenosť. Čo znamená, že v prípade negatívnych výsledkov viacerých oblastí sa ich negatíva znásobujú. Z pohľadu identifikovaných rozdielov, ktoré sú relevantné z pohľadu aktivít Investície č. 6, možno konštatovať nasledujúce zistenia:

|  |  |
| --- | --- |
| Nesúlad | Chýbajúca detekcia, riešenie a evidencia KBI |
| Riešenie | Detekcia KBI podľa Mitre ATT&CK framework s využitím ďalších bezpečnostných nástrojov, obohacovanie informácií o zdroje Threat Intelligence a zdieľanie údajov v rámci Systému včasného varovania – EWS. Proces riešenia a evidencie KBI plne auditovateľný prostredníctvom SIEM a SOAR. |

|  |  |
| --- | --- |
| Nesúlad | Absencia bezpečnostného monitorovania a analýzy udalostí v informačných systémoch, sieťach a na koncových bodoch. |
| Riešenie | Poskytnutie služby bezpečnostného monitoringu (SIEM) a automatizácie incident managementu a reakcie (SOAR) v režime 24/7 a k tomu prislúchajúcich služieb. |

|  |  |
| --- | --- |
| Nesúlad | Nenasadené bezpečnostné nástroje zabezpečujúce dostatočnú viditeľnosť v interných sieťach. |
| Riešenie | Inštalácia bezpečnostných nástrojov a ich integrácia do SOC (založené na koncepte tzv. SOC triády) pre potreby vyhodnocovania hrozieb a identifikácie potenciálnych KBI. |

|  |  |
| --- | --- |
| Nesúlad | Absencia hodnotenia zraniteľností a bezpečnostných aktualizácií (vulnerability manažmentu)  |
| Riešenie | Kontinuálny a pravidelný manažment zraniteľností organizácie prostredníctvom identifikácie, hodnotenia a manažmentu zraniteľností. |

|  |  |
| --- | --- |
| Nesúlad | Neexistujúce alebo výrazne poddimenzované personálne kapacity špecialistov na oblasť kybernetickej bezpečnosti.  |
| Riešenie | Zabezpečený tím SOC špecialistov pre incident handling, incident respose, use case management, platform support, malvér analýzu, penetračné testovanie, threat intelligence a threat hunting, ktorí budú interným tímom SVS poskytovať aj konzultačné a poradenské služby. |

Predložený projektový zámer vychádza aj zo širších aktivít a iniciatív Európskej únie po roku 2020. Kľúčové odvetvia, ako je doprava, energetika, zdravotníctvo alebo financie, sú pri vykonávaní svojich hlavných funkcií čoraz závislejšie od digitálnych technológií. Hoci digitalizácia prináša obrovské príležitosti a poskytuje riešenia mnohých výziev, ktorým Slovensko a Európa čelia, vystavuje zároveň hospodárstvo a spoločnosť kybernetickým hrozbám. Kybernetická bezpečnosť je zároveň jednou z priorít EÚ v jej reakcii na krízu spôsobenú koronavírusom, keďže počas obmedzenia pohybu došlo k zvýšeným kybernetickým útokom, čo bolo zaznamenané aj v prostredí verejnej správy na Slovensku. Aj v reakcii na koronakrízu, Európska komisia v roku 2020 predstavila novú **stratégiu kybernetickej bezpečnosti EÚ**. Stratégia rieši tri oblasti činnosti: 1) odolnosť, technologickú suverenitu a vedúce postavenie; 2) budovanie operačnej kapacity na prevenciu, odrádzanie a reakciu; 3) spoluprácu zameranú na rozvoj globálneho a otvoreného kybernetického priestoru.

Kybernetická bezpečnosť je takisto kľúčovou oblasťou **priamo riadeného programu Digitálna Európa**[[3]](#footnote-3) o čom svedčí samostatný pracovný program pre kybernetickú bezpečnosť na roky 2023 – 2024.[[4]](#footnote-4) Medzi priority na nasledujúce obdobie boli zaradené:

* podpora spoločných aktivít s cieľom **vytvoriť pokročilý ekosystém detekcie hrozieb a analýzy kybernetických incidentov** budovaním kapacít bezpečnostných dohľadových centier – SOCs;
* zlepšenie prevencie, odhaľovania, analýzy a schopnosti reagovať na kybernetické hrozby a incidenty poskytovaním dodatočných prostriedkov na podporu pripravenosti (ex-ante) a reakcie (ex-post) na rozsiahle kybernetické bezpečnostné incidenty prostredníctvom **Cybersecurity Emergency Mechanism**;
* podpora budovania kapacít v oblasti kybernetickej bezpečnosti na národnej, prípadne regionálnej a miestnej úrovni prostredníctvom národných koordinačných centier, ktorých cieľom bude podpora cezhraničnej spolupráce a príprava spoločných akcií, ako sa vymedzuje v Európskom priemyselnom, technologickom a výskumnom kompetenčnom centre a nariadení o sieti v oblasti kybernetickej bezpečnosti.

V januári 2023 nadobudla platnosť európska smernica o opatreniach na zaistenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii (**skrátene Smernica NIS 2**), ktorej cieľom je zabezpečiť, aby členské krajiny EÚ vedeli rýchlejšie, dôkladnejšie a najmä spoločne reagovať na krízové situácie. Vďaka jasne stanoveným a všeobecne platným pravidlám sa zlepší fungovanie jednotného trhu a zjednotia sa pravidlá týkajúce sa oblasti riadenia kybernetického rizika a oznamovania incidentov. Európska komisia 18. apríla 2023 predstavila návrh zákona o kybernetickej solidarite.[[5]](#footnote-5) Cieľom návrhu, ktorý prichádza ako súčasť širšieho balíka kybernetickej bezpečnosti, je podporiť cezhraničnú a verejno-súkromnú koordináciu v oblasti predvídania a riešenia kybernetických útokov. Najnovšie návrhy zahŕňajú tzv. Európsky kybernetický štít (Cyber Shield), ktorý sa má skladať z bezpečnostných dohľadových centier (SOC) v celej EÚ spojených do niekoľkých platforiem SOC pre viacero krajín. Cyber Shield bude mať za úlohu zlepšiť a zrýchliť detekciu, analýzu a reakciu na kybernetické hrozby. Tieto SOC budú využívať pokročilú technológiu, ako je umelá inteligencia (AI) a dátovú analýzu, aby zisťovali a zdieľali varovania o takýchto hrozbách s autoritami ďalších krajín.

Ako potvrdzujú aj vyššie uvedené štatistiky, aktuálnym trendom v oblasti informačnej a kybernetickej bezpečnosti je nárast bezpečnostných hrozieb v kybernetickom priestore. Kybernetické útoky a počítačová kriminalita sú, čo do počtu a sofistikovanosti, na vzostupe nie len na Slovensku, ale aj v celej Európe. Tento trend má v budúcnosti pokračovať, keďže sa očakáva, že do roku 2025 bude na celom svete na internet vecí napojených 41 miliárd zariadení.[[6]](#footnote-6) Kybernetické útoky sa stávajú sofistikovanejšie, čo v praxi znamená, že samotné útoky sú prevedené rýchlejšie a precíznejšie. Súčasne je možné vidieť posun od väčšieho množstva tzv. plošných útokov k útokom zameraným voči konkrétnym inštitúciám. Z tohto pohľadu je aktuálnym trendom prechod z primárne reaktívnych opatrení (riešenie bezpečnostného incidentu) k proaktívnym činnostiam, ktoré znižujú pravdepodobnosť výskytu bezpečnostného incidentu alebo jeho následkov.[[7]](#footnote-7)[[8]](#footnote-8) Medzi základné proaktívne opatrenia v rámci organizácie môžeme zaradiť aj vyhľadávanie bezpečnostných zraniteľností, zvyšovanie bezpečnostného povedomia zamestnancov organizácie, ako aj zlepšenie prehľadu o situačnom povedomí organizácie.

Situačné povedomie o kybernetickej bezpečnosti by sme mohli definovať v troch úrovniach ako:[[9]](#footnote-9)

1. vnímanie prvkov v kybernetickom prostredí v čase a priestore (úroveň vnímania),
2. pochopenie ich významu (úroveň pochopenia situácie) a
3. projektovanie ich stavu v blízkej budúcnosti (úroveň projekcie situácie).

Situačné povedomie je explicitne spomenuté na viacerých miestach návrhu smernice NIS 2. Konkrétne v čl. 11 ods. 3 písm. d), je jednou z úloh jednotiek CSIRT zhromažďovanie a analýza forenzných údajov a poskytovanie dynamickej analýzy rizík a incidentov a informácie o situácii v kybernetickej bezpečnosti. V čl. 15 ods. 3 písm. n) sa uvádzajú úlohy siete jednotiek CSIRT, ktorá plní aj spoluprácu a výmenu informácií s regionálnymi a EÚ centrami bezpečnostných operácií (SOC) s cieľom zlepšiť spoločné situačné povedomie o incidentoch a hrozbách v celej EÚ.

Medzi dôležité časti kybernetického bezpečnostného povedomia zaraďujeme vnímanie povedomia a jeho následné pochopenie. Prvá časť predstavuje to, ako jednotlivé OVM zberajú údaje, z akých zdrojov a v akom rozsahu.[[10]](#footnote-10) To predstavuje v prenesenom slova zmysle „uši a oči” OVM. Tie v tomto smere nasadzujú rôzne technológie, ktoré im pomáhajú pri takomto vnímaní. Štandardne pôjde o nasadenie rôznych senzorov, zberu sieťového toku a zaznamenávanie údajov o sieťovej prevádzke. V tomto smere je nevyhnutné neustále aktualizovať a dopĺňať rôzne typy senzorov a možnosti zberu bezpečnostných údajov. V rámci projektu sa predpokladá **posilnenie viacerých OVM** práve o túto **schopnosť vnímania situačného povedomia**.

Súčasťou projektu nie je len zvyšovanie schopnosti vnímania situačného povedomia o jednotlivých OVM, ale aj nutnosť jeho komplexného vyhodnocovania vo verejnej správe. Z tohto dôvodu projekt predpokladá **budovanie vládneho SOCu** ako dôležitej časti pri chápaní aktuálnej bezpečnostnej situácie. Jednotlivé OVM budú do centrálneho vládneho SOC zasielať bezpečnostné údaje relevantné pre vyhodnotenie už spomínaného komplexného situačného povedomia vo verejnej správe. To umožní lepšie chápať aktuálny vývoj bezpečnostných hrozieb a ich vplyvu na jednotlivé OVM, ako aj na bezpečnosť verejnej správy v SR.

Ako sme už vyššie uviedli, v rámci bezpečnostného monitoringu bude dochádzať k zberu a uchovávaniu bezpečnostných údajov. Tie môžeme rozdeliť do 2 skupín.[[11]](#footnote-11) Prvú skupinu predstavujú operačné údaje, teda údaje z rôznych typov senzorov (firewallov, systémov detekcie a prevencie útokov, antimalvérových riešení a pod.), ale aj bezpečnostné údaje získané z testovania a analýzy bezpečnostných zraniteľností. Tieto údaje predstavujú hlavný zdroj pre pochopenie situačného povedomia. V rámci vládnej jednotky CSIRT je v prevádzke systém na automatizované testovanie bezpečnostných zraniteľností - **systém Achilles**. Výstupy z tohto systému sú rovnako dôležitým zdrojom informácií, ktoré dotvárajú komplexnejší pohľad na zraniteľnosti jednotlivých OVM ako aj na veľkú časť sektora verejnej správy. V rámci projektu dôjde k posilneniu a rozšíreniu schopností tohto systému a doplneniu komplexného vulnerability management kombináciou výstupov z externých a interných skenov zraniteľností.

K lepšiemu pochopeniu situačného povedomia je nutné vziať do úvahy aj druhú skupinu údajov, a to strategických údajov. Pôjde najmä o kombináciu informácií poskytovaných samotnými subjektami (napr. výsledky analýz rizík, aktíva atď.) a údaje vyplývajúce z činnosti SOC a EWS ako napr. reporty z riešenia incidentov, digitálnej forenznej analýzy, alebo údaje získavané z otvorených zdrojov (OSINT) alebo spravodajských informácií.[[12]](#footnote-12) V rámci navrhovaného projektu sa majú na centrálnej úrovni posilniť schopnosti v oblasti práce s threat intelligence zdrojmi, čoumožňuje predvídať a identifikovať potenciálne hrozby skôr, než nastane útok. TI poskytuje informácie o nových typoch malware, exploitoch, taktikách útočníkov a iných hrozbách, čo umožňuje prijať preventívne opatrenia potrebné k ich zabráneniu. Zabezpečenie tejto schopnosti na centrálnej úrovni je vysoko efektívne, keďže služby na úrovni OVM by bolo nielen nákladné, ale chýbal by aj konkrétny nadhľad nad celým sektorom verejnej správy.

Čo je dôležitejšie pre samotné situačné povedomie, je vyhodnocovanie získaných bezpečnostných údajov[[13]](#footnote-13). Pochopenie reálnej bezpečnostnej situácie prostredníctvom získaných údajov je nevyhnutné pre rozhodnutie organizácie (OVM), aké bezpečnostné opatrenia aplikuje, resp. ako vyhodnotí aktuálnu situáciu. Z tohto dôvodu je nutné zozbierané údaje analyzovať a vhodne vyhodnocovať. Výsledkom tejto časti má byť informovanie o komplexnom situačnom povedomí vo verejnej správe ako aj analýza situačného povedomia pre každý OVM zvlášť. K tomuto účelu predpokladá projekt s budovávaním analytických pozícií.

Kritickou časťou kybernetickej bezpečnosti každého subjektu je **rýchla** **reakcia na bezpečnostné incidenty**. Plánované riešenie prinesie vopred plánovaný a koordinovaný postup, ktorý subjektu zaručí efektívnu a rýchlu reakciu na kybernetické incidenty a bezpečnostné udalosti. Rýchla reakcia predchádza vážnym dôsledkom bezpečnostného incidentu pre subjekt a obmedzuje výšku škôd spôsobených incidentom.

Poslednou časťou je schopnosť **predpovedať vývoj budúceho stavu situačného povedomia**. To umožňuje organizáciám sa pripraviť na vývoj situácie vrátane bezpečnostných hrozieb a prijať adekvátne bezpečnostné opatrenia. Z tohto dôvodu je súčasťou projektu budovanie **systému včasného varovania** (Early Warning System - EWS). Nevyhnutným predpokladom pre tento systém je existencia vnímania a analýzy situačného povedomia na určitej úrovni u viacerých OVM so zriadeným bezpečnostným dohľadovým centrom. Analýzou a koreláciou väčšieho množstva a zdrojov dát je možné rýchlejšie identifikovať problémy (napr. bezpečnostné zraniteľnosti), vývoj bezpečnostných hrozieb týkajúci sa napr. sektora verejnej správy a takto adresne odporúčať vykonanie preventívnych opatrení. Týmto sa zvyšuje schopnosť jednotlivých OVM zabezpečovať kybernetickú bezpečnosť svojich informačných systémov a týmto aj bezpečnosť a dostupnosť svojich služieb občanom.

Motiváciu projektu vytvárajú a ovplyvňujú rôzne aspekty, ktoré možno agregovať do niekoľkých celkov. Prioritne boli identifikované tzv. drivers alebo hnacie prvky, stanovené ciele a princípy, na ktorých majú byť výstupy projektu postavené. V neposlednom rade boli identifikovaní stakeholderi, resp. zainteresované strany kam spadajú fyzické aj právnické osoby. Sumarizáciu motivácie projektu prezentuje nasledujúci obrázok.



Obrázok 3 Motivačná architektúra

**Zainteresované osoby:**

* **Fyzické osoby**
	+ Občan.
* **Právnické osoby**
	+ Podnikateľ;
	+ MIRRI;
	+ CSIRT.SK;
	+ NASES;
	+ OVM a ich podsektory;
	+ NBÚ, SIS, VOS.

Detailný popis zainteresovaných osôb je definovaný v podkapitole 3.3.

**Na základe vykonanej analýzy boli identifikované nasledovné problémy súčasného stavu, ktoré sa týkajú tejto oblasti:**

* Nedostatočne zabezpečenie IS v prostredí VS voči aktuálnym bezpečnostným hrozbám, najmä vzhľadom na ich rastúcu početnosť a komplexnosť;
* Chýbajúce služby proaktívnej bezpečnosti v prostredí VS, vrátane bezpečnostného monitoringu;
* Nedostatočné personálne kapacity špecialistov na kybernetickú bezpečnosť vo verejnej správe a na pracovnom trhu;
* Nedostatočné zdieľanie dát a výmena informácii medzi subjektami verejnej správy v prípade bezpečnostných hrozieb.

**Z identifikovaných problémov súčasného stavu vyplývajú nasledujúce príležitosti:**

* Potreba znižovať dopady kybernetických útokov na sektor verejnej správy a zvýšenia ochrany dát občanov SR;
* Potreba centralizovaného riadenia kybernetickej bezpečnosti v prostredí verejnej správy so zapojením širšej skupiny OVM;
* Potreba rozšírenia reaktívnych služieb (prioritne incident handling a incident response) o proaktívne služby monitoringu kybernetickej bezpečnosti, ofenzívnej bezpečnosti a ďalších;
* Potreba zvýšenia efektívnosti spracovania bezpečnostných údajov vo verejnej správe;
* Potreba obnovy a doplnenia potrebných HW a SW technológií.

Hlavným cieľom projektu je **zvýšenie úrovne a rozšírenie zabezpečenia informačných systémov v prostredí verejnej správy pred hrozbami kybernetických útokov**. Očakávaným priamym dopadom naplnenia stanoveného cieľa sa predpokladá:

1. zníženie ekonomických a reputačných škôd na strane štátu spôsobených kybernetickými útokmi a
2. zvýšenie odolnosti a dostupnosti služieb poskytovaných OVM

V súvislosti s hlavným cieľom je identifikovaných **viacero parciálnych cieľov** projektu:

* Prechod od reaktívnych k proaktívnym službám v oblasti kybernetickej bezpečnosti;
* Koordinácia a zdieľanie dát medzi sektormia podsektormi v rámci Systému včasného varovania;
* Budovanie centrálnej služby, ktorú bude možné efektívne škálovať a rozširovať pre ďalšie subjekty verejnej správy, ktoré v budúcnosti prejavia záujem o služby včasného varovania;
* Vytvorenie nadrezortnej platformy pre budovanie know-how vo verejnej správe;
* Efektívnejšie využívania ľudských a finančných zdrojov koncentráciou odborných kapacít a technológie;
* Adresné zasielanie včasných varovaní na predchádzanie KBI;
* Podpora subjektov verejnej správy pri zavádzaní bezpečnostného monitoringu.

**Aplikované princípy** (v zmysle NKIVS):

* Optimálna úroveň bezpečnosti;
* Včasné riešenie bezpečnosti;
* Maximalizácia zdieľania a spoločného využívania údajov;
* Údaje sú starostlivo chránené;
* Údaje sú konzistentné a zrozumiteľné;
* Správca pre každý údaj;
* Kvalita a spoľahlivosť;
* Prednostné využívanie digitálnych služieb a dát pre rozhodovanie.

Projekt pozostáva z troch modulov. Schéma prezentujúca zloženie projektu je znázornená na obrázku nižšie. Centrálna časť riešenia systému včasného varovania (Modul 1) umožní skrátiť čas detekcie a reakcie na kybernetické bezpečnostné incidenty a umožní zbierať, vyhodnocovať a poskytovať informácie o aktuálnych kybernetických bezpečnostných hrozbách. Tieto informácie budú zbierané prostredníctvom bezpečnostných nástrojov nasadených v internej infraštruktúre pripojeného subjektu verejnej správy (Modul 3) a zabezpečeným spojením budú dáta posielať do spoločného pracoviska SOC prevádzkovaného Národnou agentúrou pre sieťové a elektronické služby (NASES) a vládnou jednotkou CSIRT. Ďalšie informácie o kybernetických bezpečnostných incidentoch budú zbierané z ostatných SOC-ov budovaných v prostredí verejnej správy, pôjde najmä o tzv. sektorové dohľadové centrá, ktoré budú pripojené do systému včasného varovania. Budovanie tzv. sektorových SOC bude podporené na základe Výzvy na predkladanie žiadostí o poskytnutie prostriedkov mechanizmu na Podporu budovania bezpečnostných dohľadových centier v prostredí verejnej správy.

*Obrázok 4: Štruktúra projektu*

Motivácia subjektov verejnej správy využívať služby bezpečnostného monitoringu je prirodzene rôzna. Medzi spoločné menovatele patrí nedostatok vlastných zdrojov na zabezpečenie tejto služby internými kapacitami, nedostatok finančných zdrojov na outsourcing komplexných služieb monitoringu od dodávateľa a dosiahnutie súladu s platnou legislatívou. Tá aktuálne vyžaduje bezpečnostný monitoring u všetkých prevádzkovateľov základných služieb (ďalej len „PZS“) podľa zákona o kybernetickej bezpečnosti a aj u správcov informačných technológií verejnej správy podľa zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon o ITVS“). Všeobecne platí, že úroveň a rozsah bezpečnostných opatrení sú u PZS rôzne. Závisia napríklad od kategorizácie sietí a informačných systémov (napr. pre informačné systémy spadajúce do kategórie III sa vyžaduje najväčší rozsah bezpečnostných opatrení). Zároveň platí, že zabezpečenie funkčného bezpečnostného monitoringu je v zodpovednosti každého PZS osobitne a to až po úroveň interných sietí, serverov, služieb, informačných systémov a ich používateľov. V projekte sa celkovo počíta s participáciou siedmich subjektov verejnej správy. Služby bezpečnostného monitoringu a ďalšie služby bezpečnostného dohľadového centra (NASES a VJ CSIRT) budú jednotlivým OVM poskytované na základe zmluvných vzťahov. Zmluvy budú uzatvorené pred samotnou inštaláciou HW, SW a použitím licencii na OVM.

# Zainteresované strany/Stakeholderi

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **AKTÉR/STAKEHOLDER** | **SUBJEKT**(názov/skratka) | **ROLA**(vlastník procesu/vlastník dát/zákazník/užívateľ …. člen tímu atď.) | **Informačný systém**(názov ISVS a MetaIS kód) |
| 1. | Občan/Podnikateľ | FO/PO | Používateľ služieb štátu. Úžitok zo zvýšenej bezpečnosti a dostupnosti verejných elektronických služieb vrátane vyššej ochrany osobných údajov. | N/A |
| 2. | Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky | MIRRI | Subjekt zodpovedný za realizáciu Investície č. 6 a jednotlivých riešení. | Vládny informačný systém kybernetickej bezpečnosti (isvs\_11573)Vládny SOC(IS nie sú evidované v MetaIS) |
| 3. | Computer Security Incident Response Team Slovakia | CSIRT.SK | Prevádzkovateľ novo-vzniknutého EWS; prevádzkovateľ systému Achilles; prevádzkovateľ príslušných služieb Vládneho SOC. | Zvýšenie spôsobilosti VJ CSIRT (projekt\_2056)Vládny SOC(IS nie sú evidované v MetaIS) |
| 4. | Národná agentúra pre sieťové a elektronické služby | NASES | Prevádzkovateľ príslušných služieb a infraštruktúry Vládneho SOC-u a EWS | Vládny SOC(IS nie sú evidované v MetaIS) |
| 5. | Orgány verejnej moci a ich podsektory | OVM a ich podsektory | Integrácia monitorovacích nástrojov a logov do „Vládneho SOC“Participácia pri budovaní EWS a zdieľanie dát medzi SOC vo verejnej správe. | Vládny informačný systém kybernetickej bezpečnosti (isvs\_11573) |
| 6. | Národný bezpečnostný úrad | NBÚ | Gestor v rámci KB v SR.Zdieľanie dát prostredníctvom budúceho EWS riešenia s touto organizáciou, hlásenie KBI | N/A |
| 7. | Slovenská informačná služba, Vojenské obranné spravodajstvo | SIS, VOS | Zdieľanie dát prostredníctvom budúceho EWS riešenia s týmito organizáciami. | N/A |

# Ciele projektu a merateľné ukazovatele

**Ciele/Merateľné ukazovatele**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **ID** | **CIEĽ** | **MERATEĽNÝ UKAZOVATEĽ (KPI)** | **MERNÁ JEDNOTKA**(v čom sa meria ukazovateľ) | **AS ISMERATEĽNÉ VÝKONNOSTNÉ HODNTOY**(aktuálne hodnoty) | **TO BE MERATEĽNÉ VÝKONNOSTNÉ HODNTOY**(cieľové hodnoty projektu) | **SPÔSOB ICH MERANIA/OVERENIA PO NASADENÍ**(overenie naplnenie cieľa) |
| ID\_1 | Zvyšovanie úrovne zabezpečenia informačných systémov verejnej správy. | Zvýšenie počtu IT systémov v prostredí verejnej správy zapojených do systému včasného varovania  | Počet | 70 | 500 | Zoznam pripojených IT systémov v prostredí VS |
| ID\_2 | Zvyšovanie úrovne zabezpečenia informačných systémov verejnej správy. | Počet OVM pripojených do bezpečnostného dohľadového centra SOC | Počet | 6 | 13 | Zoznam OVM. |
| ID\_3 | Zvyšovanie úrovne zabezpečenia informačných systémov verejnej správy. | Počet bezpečnostných dohľadových centier zapojených do systému včasného varovania | Počet | 0 | 4 | Zoznam SOC |
| ID\_4 | Zvyšovanie úrovne zabezpečenia informačných systémov verejnej správy. | Počet detekčných scenárov, ktoré pokrývajú techniky a taktiky (TTPs podľa MITRE ATT&CK Framework) | Počet  | 130 | 500 | Report |

Na účely tohto projektu sa IT systémom v prostredí verejnej správy rozumie každý technický prostriedok, na ktorom je nasadený nástroj na monitorovanie a riadenie bezpečnosti (agent), a nasledujúce technické prostriedky v zabezpečenom alebo garantovanom prostredí, ktorých bezpečnostné logy sú monitorované a vyhodnocované:

a. prvok zabezpečujúci sieťovú komunikáciu (smerovač, core prepínač),

b. prvok zabezpečujúci ochranu komunikujúcich zariadení pomocou vynucovania stanovených pravidiel (FW, WAF, NGFW, IPS, IDS, DoS, DDoS ochrana a pod.),

c. prvok zabezpečujúci vzdialené bezpečné pripojenie do siete z prostredia internetu (VPN server, SD-WAN a pod.),

d. prvok zabezpečujúci autorizáciu zariadení alebo používateľov pre použitie služieb ponúkaných v internej sieti (Active Directory, Kerberos a pod.).

Vyššie uvedené sa primerane vzťahuje aj na prostredie cloudu.

Medzi IT systémy v prostredí verejnej správy nepatria bezdrôtové prístupové body a koncové užívateľské zariadenia (počítače, tablety, telefóny, tlačiarne).

# Špecifikácia potrieb koncového používateľa

Realizáciou projektu sa rieši zvýšenie úrovne zabezpečenia informačných systémov v prostredí verejnej správy, pričom primárnym zámerom projektu je:

* implementácia a nasadenie nového riešenia včasného varovania, ktoré bude získavať a zdieľať bezpečnostné údaje v prostredí tzv. sektorových SOC-ov (podporené z výzvy č. 17I06-04-V01 vyhlásenej v rámci Plánu obnovy a odolnosti)
* rozšírenie a doplnenie služieb a funkcionalít už existujúcich riešení v správe CSIRT.SK a NASES (Achilles, vládny SOC)
* doplnenie HW a SW na existujúcom riešení spoločného pracoviska SOC.

Projektom sa neimplementujú žiadne koncové služby pre obyvateľov a podnikateľov. Z tohto dôvodu nie je potrebné definovať potreby koncového používateľa samostatným používateľským prieskumom. Vyššie uvedené rozširovanie a doplnenie služieb bezpečnostného monitoringu bude poskytované iným inštitúciám verejnej správy. Zo zvýšeného zabezpečenia formou zavedenia a zlepšenia proaktívnych a reaktívnych služieb pracoviska SOC a CSIRT.SK budú priamo benefitovať subjekty verejnej správy využívajúce tieto služby a nepriamo aj občania/podnikatelia, pre ktorých budú elektronické služby štátu bezpečnejšie a zároveň bude zabezpečená ich vysoká dostupnosť.

# Riziká a závislosti

Riziká a závislostí sú spracované v Prílohe č. 1 – **Zoznam RIZÍK a ZÁVISLOSTI.**

# Alternatívy a Multikriteriálna analýza

# Stanovenie alternatív pomocou biznisovej vrstvy architektúry

Jednotlivé subjekty verejnej správy sami zodpovedajú za zabezpečenie primeranej úrovne informačnej a kybernetickej bezpečnosti podľa platnej legislatívy a sú povinné na tieto účely prijímať bezpečnostné opatrenia v rámci interných preventívnych činností. Taktiež zabezpečenie funkčného bezpečnostného monitoringu je v zodpovednosti každého prevádzkovateľa osobitne a to až na úrovni interných sietí, serverov, služieb, informačných systémov a ich používateľov. Primárnym cieľom zlepšovania úrovne kybernetickej bezpečnosti je priblížiť sa stavu, v ktorom sú siete a informačné systémy schopné odolávať kybernetickým hrozbám na primeranom stupni spoľahlivosti. Každá inštitúcia je zodpovedná za definovanie vlastnej úrovne informačnej a kybernetickej bezpečnosti a aj snahou o jej dosiahnutie. Zavedenie kvalitných bezpečnostných procesov a technológií si však vyžaduje významné finančné, personálne a časové nároky.

Subjekty verejnej správy majú v prípade zabezpečenia služieb bezpečnostného monitoringu IT hneď niekoľko možností:

* Z pohľadu menších subjektov je najdostupnejšia možnosť využívať externé služby bezpečnostného monitoringu od komerčných poskytovateľov, ktoré sú však finančne nákladné, ale zároveň riešia prekážku obmedzených personálnych kapacít a ich nedostatočných znalostí v danej problematike, resp. nedostupnosti odborných kapacít na pracovnom trhu všeobecne. Z prieskumu zmlúv zverejnených na Centrálnom registri zmlúv (https://www.crz.gov.sk/) sa priemerná cena za základný bezpečnostný monitoring pohybuje na úrovni od 1 000 EUR mesačne. Napriek výhodnej dostupnosti týchto služieb, konkrétne ponúkané produkty neposkytujú ucelenú ochranu IT infraštruktúry a pokrývajú iba vybrané segmenty kybernetickej bezpečnosti, napr. do monitoringu vstupuje len obmedzený rozsah logov, pokryté sú len niektoré vektory úrokov, režim monitoringu je 8/5 a podobne.
* V prípade subjektov verejnej správy so zložitou sieťovou infraštruktúrou, ktoré zároveň disponujú veľkým množstvom citlivých údajov a širokou škálou kriticky dôležitých informačných systémov v rôznorodom prostredí, je alternatívou aj vlastná prevádzka bezpečnostného dohľadového centra. Tá poskytuje subjektom prioritne vysokú mieru flexibility pri implementácii zmien, personalizáciu riešení a služieb podľa interných požiadaviek a úplnú kontrolu nad dátami. Naráža však na dve elementárne prekážky: 1) vysoké vstupné náklady na zriadenie bezpečnostného dohľadového centra a jeho následnú prevádzku; 2) nedostatok špecialistov na pracovnom trhu potrebných na pokrytie prevádzky všetkých pozícií a služieb v rôznych režimoch (24/7, 10/5, 8/5).
* Ďalším riešením je koncentrácia personálnych a finančných zdrojov štátu pre poskytovanie služieb ostatným subjektom verejnej správy. V súlade s týmto konceptom bude MIRRI SR spolu s NASES postupne budovať a rozvíjať centrálne riešenie bezpečnostného dohľadového centra pre verejnú správu, do ktorého budú v prípade záujmu zapájať ďalšie subjekty verejnej správy .

Nižšie sa nachádzajú alternatívy, ktoré reflektujú hlavné ciele a motiváciu pre realizáciu projektu v zmysle jednotlivých aspektov uvedených v rámci motivačnej architektúry.

**Alternatívy riešenia:**

|  |  |
| --- | --- |
| **Riešenie 1** |  |
| Biznis alternatíva 1 | Zachovanie pôvodného stavu |
| Popis | Alternatíva spočíva v tom, že by nedošlo k žiadnym zmenám v oblasti zberu, spracovania a vyhodnocovania bezpečnostných údajov a v oblasti preventívnych opatrení, rýchlosti detekcie a riešenia incidentov. V súčasnom stave to znamená nedostatočnú „viditeľnosť“ do prostredia jednotlivých OVM s dlhou reakčnou dobou, bez dostatočného množstva dát, vzájomného zdieľania informácii a poskytovania proaktívnych služieb. |
| "Must have" kritériá pre aplikačnú vrstvu | N/A |
| "Nice to have" kritériápre aplikačnú vrstvu | N/A |
| Alternatíva pretechnologickú vrstvu | N/A |

|  |  |
| --- | --- |
| **Riešenie 2** |  |
| Biznis alternatíva 2 | Postupné zavádzanie proaktívnych a reaktívnych služieb formou bezpečnostných nástrojov a monitoringu na jednotlivých OVM internými kapacitami decentralizovane. |
| Popis | Alternatíva spočíva v tom, že by nedošlo k zásadným zmenám v oblasti zberu, spracovania a vyhodnocovania bezpečnostných údajov a v oblasti preventívnych opatrení, rýchlosti detekcie a riešenia incidentov. Avšak jednotlivé riešenia, nástroje a technológie by boli budované postupne a agendy v oblasti KB a jednotlivé oblasti by boli zefektívňované postupnými krokmi, viacerými projektmi v gescii jednotlivých OVM/organizácií spolu s budovaním interných tímov špecialistov SOC. |
| "Must have" kritériá pre aplikačnú vrstvu | Postupné nasadzovanie jednotlivých bezpečnostných riešení, nástrojov a technológií pre zber, spracovanie a vyhodnocovanie bezpečnostných údajov, realizáciu preventívnych opatrení, detekciu a riešenie incidentov v rámci jednotlivých OVM. |
| "Nice to have" kritériápre aplikačnú vrstvu | N/A |
| Alternatíva pretechnologickú vrstvu | Vlastná infraštruktúra |

|  |  |
| --- | --- |
| **Riešenie 3** |  |
| Biznis alternatíva 3 | Využitie externých služieb bezpečnostného monitoringu a existujúcich služieb VJ CSIRT. |
| Popis | Alternatíva spočíva v tom, že bezpečnostný monitoring a s tým súvisiace služby v oblasti zberu, spracovania a vyhodnocovania bezpečnostných údajov a v oblasti preventívnych opatrení, rýchlosti detekcie a riešenia incidentov si budú jednotlivé OVM zabezpečovať na základe verejnej súťaže a zmluvných vzťahov s tretími stranami formou „SOC as service“ |
| "Must have" kritériá pre aplikačnú vrstvu | Tretia strana dodáva jednotlivé nástroje pre bezpečnostný monitoring, ktoré zabezpečujú zdroje dát a integráciu dát z existujúcich systémov OVM do  |
| "Nice to have" kritériápre aplikačnú vrstvu | N/A – neboli identifikované žiadne iné funkcionality |
| Alternatíva pretechnologickú vrstvu | Infraštruktúra dodávateľa služieb alebo kombinácia |

|  |  |
| --- | --- |
| **Riešenie 4** |  |
| Biznis alternatíva 4 | Zber, spracovanie a vyhodnocovanie bezpečnostných údajov, realizácia preventívnych opatrení, detekcia a riešenie incidentov budú pre subjekty verejnej správy poskytované centralizovane od NASES a VJ CSIRT.  |
| Popis | Alternatíva spočíva v tom, že dôjde k zmenám v oblasti zberu, spracovania a vyhodnocovania bezpečnostných údajov a v oblasti preventívnych opatrení, rýchlosti detekcie a riešenia incidentov. Jednotlivé proaktívne a reaktívne služby v oblasti KB budú podporené budovaním centralizovaného riešenia formou rozvoja Vládneho SOC. Na OVM budú nasadzované technológie, ktoré umožnia zber údajov. Spracovanie údajov, ich analýza a vyhodnocovanie vrátane riešenia incidentov budú realizované centralizovane. |
| "Must have" kritériá pre aplikačnú vrstvu | Bude vybudovaný nový systém EWS, ktorý poskytne nasledovné funkcionality:* Tvorba a udržovanie Mapy hrozieb s referenciou na MITRE ATT&CK Framework
* Distribúcia indikátorov možnej kompromitácie (Indicators of Compromise – IoC)
* Ohlasovanie bezpečnostného incidentu
* Poskytovanie threat intelligence (TI) feedov
* Monitoring digitálnej stopy pre jednotlivé OVM
* Impersonifikovanie VIP zamestnancov jednotlivých OVM
* Monitoring relevantných uniknutých dát
* Pravidelné reporty na základe zdrojov z threat intelligence platformy
* Služba upozornenia na zraniteľnosti
* Zber, analýza a dodávanie Techník, taktík a procedúr (TTP)
* Komunikácia bezpečnostného povedomia na OVM
* Vyhodnocovanie podaných a automaticky generovaných hlásení
* Informovanie o bezpečnostných incidentoch

Riešenie bude integrované na relevantné systémy a databázy.Vládny SOC bude rozšírený o nasledovné funkcionality, kompetencie a tímy:* Monitoring kybernetickej bezpečnosti
	+ Monitoring sieťovej komunikácie
	+ Monitoring procesov na koncových zariadeniach
	+ Zber a korelácia logov
	+ Automatizácia vyšetrovacích a reakčných procesov
	+ Monitoring L1
	+ Analýza L2 a L3
	+ Pravidelný reporting
	+ Threat intelligence a Threat hunting
* Ofenzívna bezpečnosť
	+ Vulnerability manažment
	+ Red Teaming a Purple Teaming
	+ Penetračné testovanie

V rámci riešenia Achilles budú dobudované integrácie, aby boli výsledky externých scanov zraniteľností systému Achilles integrované s výsledkami interných scanov pri SOC, čím sa zabezpečí vyššia relevancia identifikovaných zraniteľností a automatizácia procesov.Na vybraných OVM budú na základe detailného návrhu riešenia (DNR) nasadené rôzne bezpečnostné riešenia umožňujúce zber, analýzu, vyhodnocovanie a reakciu na kybernetické bezpečnostné udalosti:* Bezpečnostný nástroj 1
* Bezpečnostný nástroj 2
* Bezpečnostný nástroj 3
* Bezpečnostný nástroj 4
* Zber logov z ďalších zdrojov prostredníctvom kolektorov
 |
| "Nice to have" kritériápre aplikačnú vrstvu | Ďalšie zdroje logov:Mobile device management (MDM)WAF - Web Application FirewallCloud platforms (Azure, AWS, Google, atď.) |
| Alternatíva pretechnologickú vrstvu | Vlastná centrálna infraštruktúra a infraštruktúra na lokalite |

# Multikriteriálna analýza

Výber alternatív prebieha na úrovni biznis vrstvy prostredníctvom MCA zostavenej na základe kapitoly Motivácia, ktorá definuje hlavné problémy súčasného stavu, príležitosti a obsahuje ciele zainteresovaných osôb.

**Kritériá:**

* Zabezpečenie budovania technického a technologického vybavenia OVM za účelom zberu informácií z koncových zariadení, sieťovej komunikácie a prevádzkovaných IS;
* Zefektívnenie, zrýchlenie a automatizácia spracovania bezpečnostných udalostí z OVM z OVM;
* Zavedenie efektívneho manažmentu informácií týkajúcich sa prevádzky IS z pohľadu kybernetickej bezpečnosti;
* Zvýšenie zabezpečenia IS v prostredí VS;
* Efektívne využívanie spracovaných dát s cieľom včasného varovania, rýchlej reakcie a minimalizácie škôd.

Kritériá MCA

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **KRITÉRIUM** | **Občan** | **Podnikateľ** | **MIRRI** | **CSRIT.SK** | **NASES** | **OMV a ich podsektory** | **NBÚ, SIS, VOS** |
| Zabezpečenie budovania technického a technologického vybavenia OVM za účelom zberu informácií z koncových zariadení, sieťovej komunikácie a prevádzkovaných IS |  |  | *x* |  | *x* | *x* | *x* |
| Zefektívnenie, zrýchlenie a automatizácia spracovania bezpečnostných udalostí z OVM  |  |  | *x* | *x* | *x* | *x* | *x* |
| Zavedenie efektívneho manažmentu informácií týkajúcich sa prevádzky IS z pohľadu kybernetickej bezpečnosti |  |  | *x* | *x* | *x* | *x* |  |
| Zvýšenie zabezpečenia IS v prostredí VS | *x* | *x* | *x* | *x* | *x* | *x* | *x* |
| Efektívne využívanie spracovaných dát s cieľom včasného varovania, rýchlej reakcie a minimalizácie škôd |  |  | *x* | *x* | *x* | *x* | *x* |

Vyhodnotenie MCA

|  |  |  |
| --- | --- | --- |
| **Zoznam kritérií** | **Alternatíva** **1** | **Spôsob** **dosiahnutia** |
| Zabezpečenie budovania technického a technologického vybavenia OVM za účelom zberu informácií z koncových zariadení, sieťovej komunikácie a prevádzkovaných IS | nie | N/A |
| Zefektívnenie, zrýchlenie a automatizácia spracovania bezpečnostných udalostí z OVM | nie | N/A |
| Zavedenie efektívneho manažmentu informácií týkajúcich sa prevádzky IS z pohľadu kybernetickej bezpečnosti | nie | N/A |
| Zvýšenie zabezpečenia IS v prostredí VS | nie | N/A |
| Efektívne využívanie spracovaných dát s cieľom včasného varovania, rýchlej reakcie a minimalizácie škôd | nie | N/A |

|  |  |  |
| --- | --- | --- |
| **Zoznam kritérií** | **Alternatíva** **2** | **Spôsob** **dosiahnutia** |
| Zabezpečenie budovania technického a technologického vybavenia OVM za účelom zberu informácií z koncových zariadení, sieťovej komunikácie a prevádzkovaných IS | čiastočne | Budovanie technického a technologického vybavenia OVM za účelom bezpečnostného monitoringu bude realizované postupne jednotlivými OVM v rôznej kvalite |
| Zefektívnenie, zrýchlenie a automatizácia spracovania bezpečnostných udalostí z OVM  | nie | N/A |
| Zavedenie efektívneho manažmentu informácií týkajúcich sa prevádzky IS z pohľadu kybernetickej bezpečnosti | čiastočne  | Jednotlivé OVM si budú samostatne spravovať dohľad nad informáciami, ktoré sa týkajú prevádzky IS z pohľadu kybernetickej bezpečnosti |
| Zvýšenie zabezpečenia IS v prostredí VS | čiastočne | Postupným budovaním niektorých riešení na úrovni OVM dôjde k čiastočnému zvýšeniu zabezpečenia IS v prostredí VS. |
| Efektívne využívanie spracovaných dát s cieľom včasného varovania, rýchlej reakcie a minimalizácie škôd | nie | N/A |

|  |  |  |
| --- | --- | --- |
| **Zoznam kritérií** | **Alternatíva** **3** | **Spôsob** **dosiahnutia** |
| Zabezpečenie budovania technického a technologického vybavenia OVM za účelom zberu informácií z koncových zariadení, sieťovej komunikácie a prevádzkovaných IS | áno | Budovanie technického a technologického vybavenia OVM za účelom bezpečnostného monitoringu bude zabezpečovať tretia strana formou SOC as service. |
| Zefektívnenie, zrýchlenie a automatizácia spracovania bezpečnostných udalostí z OVM  | áno | Dôjde k zefektívneniu, zrýchleniu a automatizácii spracovania údajov zo zabezpečených systémov avšak úroveň poskytovaných služieb bude závisieť od finančných možností jednotlivých OVM a úrovne poskytovaných služieb tretími stranami, pretože riešenie vyvoláva vysoké finančné náklady. |
| Zavedenie efektívneho manažmentu informácií týkajúcich sa prevádzky IS z pohľadu kybernetickej bezpečnosti | čiastočne | Manažment informácií týkajúcich sa prevádzky IS z pohľadu kybernetickej bezpečnosti bude realizovaný len z pohľadu jednotlivých OVM decentralizovane (ak si službu u dodávateľa obstarajú) |
| Zvýšenie zabezpečenia IS v prostredí VS | áno | Zabezpečovanie bezpečnostného monitoringu treťou stranou formou SOC as service na úrovni OVM dôjde k zvýšeniu zabezpečenia IS v prostredí VS. |
| Efektívne využívanie spracovaných dát s cieľom včasného varovania, rýchlej reakcie a minimalizácie škôd | nie | N/A |

|  |  |  |
| --- | --- | --- |
| **Zoznam kritérií** | **Alternatíva** **4** | **Spôsob** **dosiahnutia** |
| Zabezpečenie budovania technického a technologického vybavenia OVM za účelom zberu informácií z koncových zariadení, sieťovej komunikácie a prevádzkovaných IS | áno | Budovanie technického a technologického vybavenia OVM za účelom bezpečnostného monitoringu bude realizované na základe jednotnej metodiky a prístupu tak, aby jednotlivé OVM boli v čo najväčšej miere odbremenené od súvisiacej administratívy. |
| Zefektívnenie, zrýchlenie a automatizácia spracovania bezpečnostných udalostí z OVM | áno | Realizáciou zmien a riešení dôjde k zefektívneniu, zrýchleniu a automatizácií spracovania údajov z OVM, pričom bude zabezpečená rovnaká úroveň poskytovaných služieb. Na jednotlivých OVM budú nasadené jednotné nástroje pre bezpečnostný monitoring. |
| Zavedenie efektívneho manažmentu informácií týkajúcich sa prevádzky IS z pohľadu kybernetickej bezpečnosti | áno | Manažment informácií týkajúcich sa prevádzky IS z pohľadu kybernetickej bezpečnosti bude realizovaný efektívne a centralizovane. |
| Zvýšenie zabezpečenia IS v prostredí VS | áno | Budovaním riešení dôjde k celkovému zvýšeniu zabezpečenia IS v prostredí VS. |
| Efektívne využívanie spracovaných dát s cieľom včasného varovania, rýchlej reakcie a minimalizácie škôd | áno | Budú implementované riešenia, ktoré zabezpečia využívanie dodatočných spravodajských zdrojov a spracovaných dát na včasné varovanie s cieľom včasného varovania, rýchlej reakcie na detegované incidenty a minimalizácie škôd. |

# Stanovenie alternatív pomocou aplikačnej vrstvy architektúry

Alternatívy na úrovni aplikačnej vrstvy architektúry reflektujú alternatívy vypracované na základe „nadradenej“ architektonickej biznis vrstvy, pričom vďaka uplatneniu nasledujúcich princípov aplikačná vrstva architektúry dopĺňa informácie k alternatívam stanoveným pomocou biznis architektúry. Z pohľadu aplikačnej architektúry sa javí ako alternatíva aj využitie opensource bezpečnostných riešení, ktorých hlavnou výhodou sú nižšie náklady na TCO projektu a udržateľnosť riešenia. V prípade budovania centrálneho riešenia bezpečnostného monitoringu, ktorý bude zabezpečovať služby aj pre kriticky dôležité inštitúcie a informačné systémy verejnej správy na Slovensku však nie je použitie výlučne opensource riešení vhodné. Medzi základnými nedostatkami boli identifikované: nižšia miera spoľahlivosti nástrojov, nižšia miera automatizácie, vyššie náklady spojené s vývojom a prispôsobením nástrojov pre existujúce aplikačné a technologické prostredie, vyššia časová a personálna náročnosť na udržiavanie, replikovanie riešenia na ďalšie subjekty a absentujúce alebo oneskorené aktualizácie a vývoj. Projekt počíta aj s využitím kombinácie opensource riešenia a proprietárneho softvéru. Kombinovaný prístup bude použitý v prípade služieb threat intelligence a ich integrácie pomocou MISP (Malware Information Sharing Platform & Threat Sharing), ktorá je považovaná za najpoužívanejšiu open-source threat information sharing platformu. MISP slúži na registráciu rizík, zdieľanie informácií, nástrojov, taktík a postupov cielených útokov a potenciálnych zraniteľností. Na aplikačnej vrstve budú projektom riešené len aplikačné moduly/funkcionality, ktoré sú nevyhnutné pre dosiahnutie cieľov vybranej alternatívy č. 4.

# Stanovenie alternatív pomocou technologickej vrstvy architektúry

Z hľadiska infraštruktúry potrebnej na zabezpečenie prevádzky jednotlivých bezpečnostných nástrojov, sú definované alternatívy technologickej architektúry ako:

* Využitie existujúcej technologickej základne dátového centra NASES, ktorý už aktuálne prevádzkuje infraštruktúru spoločného bezpečnostného dohľadového centra NASES a VJ CSIRT a jej prípadné rozšírenie
* Hybridná technologická alternatíva – rozšírenie infraštruktúry NASES a integrácia vybraných komerčných cloudových služieb
* Vládny cloud
* Plná realizácia v komerčnom cloude

Uvažované varianty sú porovnávané vzhľadom na informácie o súčasných technologických a ľudských kapacitách na strane NASES a VJ CSIRT, ktoré by umožňovali prevádzku infraštruktúry na zabezpečenie prevádzky bezpečnostných nástrojov v rámci bezpečnostného dohľadového centra, monitorovacích nástrojov a systému včasného varovania. Konkrétne parametre, ako aj sizing jednotlivých uvažovaných prostredí bude stanovený v rámci detailného návrhu riešenia. Následne bude prioritne preverená možnosť zabezpečenia potrebnej infraštruktúry v rámci existujúceho prostredia NASES (rozšírenie existujúcej technologickej architektúry - on-premise riešenie, alebo presun celého prostredia do Private Cloud Appliance . V prípade nemožnosti zabezpečenia potrebnej on-premise infraštruktúry v rámci kapacít NASES, bude preferované nasadenie v hybridnom prostredí. To predstavuje kombináciu on-premise riešenia a cloudových služieb, ktoré sú, resp. môžu byť súčasťou technologického architektúry jednotlivých bezpečnostných nástrojov. Vzhľadom na charakter projektu, prevádzku a monitoring kritickej infraštruktúry a základných služieb, je z pohľadu nákladovosti a bezpečnosti a ochrany osobných údajov najmenej vyhovujúcou alternatívou plná realizácia v komerčnom cloude.

Alternatívy na úrovni technologickej architektúry reflektujú alternatívy vypracované na základe „nadradenej“ architektonickej aplikačnej vrstvy, pričom sa prioritne uvažuje o využití kapacít dátového centra NASES, ktoré už aktuálne prevádzkuje infraštruktúru spoločného bezpečnostného dohľadového centra NASES a VJ CSIRT, na ktorej projekt stavia. V inom prípade by boli vyvolané ďalšie dodatočné investičné alebo prevádzkové náklady, pričom by ostali nevyužité existujúce technologické predpoklady NASES.

# POŽADOVANÉ VÝSTUPY (PRODUKT PROJEKTU)

Realizáciou projektu budú dodané nasledujúce špecializované a manažérske produkty pre jednotlivo realizované aktivity. Každá z aktivít, resp. častí projektu, bude mať svoje špecifiká a bude realizovať len relevantné časti špecializovaných produktov v zmysle Vyhlášky č. 85/2020 Z. z.

|  |
| --- |
| **Realizačná fáza projektu** |
| **Manažérsky produkt** |
| Projektový iniciálny dokument (PID) (R-01) |
| **Hlavné aktivity**  | **Špecializovaný produkt** |
| Analýza a dizajn  | Detailný technický návrh riešenia (R1-1) |
| Plán testov (R1-2) |
| Nákup technických prostriedkov, programových prostriedkov a služieb | Obstaranie technických prostriedkov (R2-1) |
| Obstaranie programových prostriedkov a služieb (R2-2) |
| Implementácia a Testovanie | Vývoj, migrácia údajov a integrácia (R3-1) |
| Testovanie (R3-2) |
| Školenia personálu (R3-3) |
| Dokumentácia (R3-4) |
| Nasadenie a Postimplementačná podpora | Nasadenie do produkcie (vyhodnotenie) (R4-1) |
| Preskúšanie a akceptácia spustenia do produkcie (vyhodnotenie) (R4-2) |
| **Dokončovacia fáza projektu** |
| **Manažérsky produkt** |
| D-01 Správa o dokončení projektu |
| D-01 Správa o získaných poznatkoch |
| D-01 Plán kontroly po odovzdaní projektu |
| D-01 Odporúčanie nadväzných krokov |
| **Služby projektového riadenia** |
| **Manažérsky produkt** |
| M-01 Plán etapy |
| M-02 Manažérske správy, reporty, zoznamy a požiadavky |
| M-03 Akceptačný protokol |
| M-04 Audit kvality projektu na mieste |

Pre časti projektu, v ktorých bude realizovaná aj aktivita realizačnej fázy „Nákup technických prostriedkov, programových prostriedkov a služieb“ je potrebné zvážiť v rámci špecifikácie predmetu zákazky aj ďalšie relevantné činnosti:

* Realizácia obhliadky;
* Príprava projektu inštalácie;
* Inštalácia zariadení;
* Revízia;
* Certifikácia;
* Uvedenie do prevádzky.

Po zhodnotení jednotlivých alternatív a ich vyhodnotenia pomocou stanovených kritérií výstupom projektu bude súbor viacerých

vzájomne prepojených „krabicových“ riešení v podobe bezpečnostných nástrojov a hardvéru ako uceleného informačného systému, ktorého cieľom je riešiť získavanie a zdieľanie informácií za účelom vykonávania včasného varovania, identifikácie kybernetických bezpečnostných incidentov v prostredí verejnej správy a rýchla reakcia pri ich riešení.

Primárnym výstupom je vybudovanie systému včasného varovania (EWS) – modul 1, ktorý predstavuje centralizovaný zber, analýzu, vyhodnocovanie bezpečnostných udalostí, reakciu na kybernetické bezpečnostné incidenty, identifikáciu možných bezpečnostných zraniteľnosti z informačných systémov v prostredí verejnej správy a ďalších spravodajských zdrojov a zdieľanie informácií medzi orgánmi verejnej správy prevádzkujúcimi služby bezpečnostných dohľadových centier. EWS bude poskytovať nasledujúce funkcionality:

* Tvorba a udržovanie Mapy hrozieb s referenciou na MITRE ATT&CK Framework
* Distribúcia indikátorov možnej kompromitácie (Indicators of Compromise – IoC)
* Ohlasovanie bezpečnostného incidentu
* Poskytovanie Threat intelligence (TI) feedov
* Monitoring digitálnej stopy pre jednotlivé OVM
* Impersonifikovanie VIP zamestnancov jednotlivých OVM
* Monitoring relevantných uniknutých dát
* Pravidelné reporty na základe zdrojov z Threat Intelligence platformy
* Služba upozornenia na zraniteľnosti
* Zber, analýza a dodávanie Techník, taktík a procedúr (TTP)
* Komunikácia bezpečnostného povedomia na OVM
* Vyhodnocovanie podaných a automaticky generovaných hlásení
* Informovanie o bezpečnostných incidentoch

Druhým výstupom projektu bude rozšírenie služieb, technológie, funkcionalít a tímu aktuálneho bezpečnostného dohľadového centra, ktorý spoločne prevádzkuje NASES a VJ CSIRT v režime 24/7 – modul 2. Vládny SOC bude rozšírený o nasledovné funkcionality, kompetencie a tímy:

* Monitoring kybernetickej bezpečnosti
	+ Monitoring sieťovej komunikácie
	+ Monitoring procesov na koncových zariadeniach
	+ Zber a korelácia logov
	+ Automatizácia vyšetrovacích a reakčných procesov
	+ Monitoring L1
	+ Analýza L2 a L3
	+ Pravidelný reporting
	+ Threat intelligence a Threat hunting
* Ofenzívna bezpečnosť
	+ Vulnerability manažment
	+ Red Teaming a Purple Teaming
	+ Penetračné testovanie

Na OVM, ktoré budú využívať služby bezpečnostného monitoringu poskytovaného Vládnym SOC, budú nasadené nástroje zabezpečujúce zber, pokročilú analýzu a vyhodnocovanie logov z koncových staníc a sieťovej prevádzky – modul 3. Nástroje budú okrem detekcie umožňovať aj vykonávanie reakcie na detegované udalosti s využitím automatizácie procesov.

Nové služby EWS a rozšírenie služieb Vládneho SOC budú poskytované tímami špecialistov, pričom ich úlohou bude onboarding OVM do monitoringu, analýza bezpečnostného prostredia, monitorovanie a vyhodnocovanie kybernetických bezpečnostných udalostí, incidentov a zraniteľností, ktoré budú identifikované uvedenými nástrojmi. Personálne kapacity budú agregované podľa vykonávaných úloh, činností a kompetencií do nasledujúcich tímov: onboarding tím; analytici L1, L2; use case manažment tím; pentesting tím; threat intelligence tím; tím reakcie na incidenty; manažment zraniteľností a platform support tím.

Služby budú poskytované v úzkej súčinnosti s administrátormi IT prostredia jednotlivých OVM, resp. s tretími stranami, ktoré im zabezpečujú prevádzku a bezpečnosť IT. Bez úzkej kooperácie medzi špecialistami SOC a interným IT na monitorovaných OVM nebude možné realizovať opatrenia na presnú identifikáciu a minimalizovanie hrozieb a incidentov. Služby EWS a bezpečnostného dohľadového centra budú vykonávané prostredníctvom dvoch možných prístupov. V centrálnej lokalite budú umiestnené pracovné stanice, ktoré budú používané pre účely prístupu členov jednotlivých tímov fyzicky. Druhou možnosťou bude využitie VDI infraštruktúry pripojením cez VPN. Požadovaná bezpečnostná architektúra je uvedená v nasledujúcej kapitole.

N/A

*Obrázok 5: High level governance model podľa použitých technológií*

# NÁHĽAD ARCHITEKTÚRY

Biznis architektúra budúceho stavu reflektuje zámer projektu, ktorým je posilnenie preventívnych opatrení, zvýšenie rýchlosti detekcie a riešenia incidentov. Z pohľadu prístupových miest a kanálov realizáciou projektu dôjde k zmenám a doplneniu funkcionalít používateľského rozhrania pre SOC. Zároveň vznikne novo-vybudované používateľské rozhranie pre EWS a Service Desk, ktorý dnes slúži prioritne na nahlasovanie prevádzkových incidentov pre organizácie využívajúce služby vládnej siete Govnet.



*Obrázok 6: Biznis architektúra budúceho stavu*

Zásadné zmeny v rámci navrhovaného riešenia sa dotknú nasledovných biznis funkcií:

* **Získavanie špecifických bezpečnostných údajov** – získavanie bezpečnostných údajov bude v budúcom stave rozšírené o nové zdroje dát, ktoré budú poskytovať vyššiu mieru tzv. viditeľnosti do prostredia monitorovaných OVM a s tým spojený väčší rozsah bezpečnostných údajov, ktoré budú môcť byť detailne analyzované a vyhodnocované.
* **Manažment zberu a spracovanie bezpečnostných údajov** – bezpečnostné údaje budú zbierané na základe definovaných kritérií a spracované do požadovaného formátu na základe sofistikovaných metód s cieľom zavádzania čo najvyššej miery automatizácie v oblasti včasnej identifikácie potencionálnych hrozieb, resp. útokov.
* **Vyhodnocovanie a analýza údajov** – centralizované vyhodnocovanie a analýza údajov získaných z viacerých zdrojov s cieľom identifikácie potencionálnych zraniteľnosti, resp. hrozieb. Vyhodnocovanie a analýza budú vykonávané najmodernejšími technológiami využívajúce prvky strojového učenia a umelej inteligencie za účelom, korelácie rôznych dát, presnejšej detekcie s minimalizáciou tzv. false positive ratio, teda podielu falošne pozitívnych výsledkov, ktoré majú negatívne dopady na efektívnosť práce analytikov a ďalších špecialistov na SOC a monitorovaných OVM.
* **Monitorovanie a evidencia kybernetických bezpečnostných incidentov** – monitorovanie, evidencia a zdokumentovanie bezpečnostných incidentov, ktoré vznikli v minulosti s cieľom predchádzania podobných incidentov v budúcnosti v súlade s klasifikáciou TTPs využívanou frameworkom MITRE.
* **Vyhodnocovanie údajov získaných z externých skenov zraniteľnosti** – sofistikované vyhodnocovanie získaných údajov na základe pokročilých metód vyhodnocovania dát a tvorba pokročilých dátových a analytických vizualizácií. Integrácia výstupov z externých skenov monitorovaných OVM realizovaných prostredníctvom systému Achilles do platformy SOAR.
* **Manažment rizík a zraniteľností** – manažment rizík a zraniteľností bude realizovaný kombináciou výsledkov interných a externých skenov v súlade s vyhodnocovaním na základe CVE (Common Vulnerabilities and Exposures) s MITRE ATT&CK Framework cez SOAR, kde budú zraniteľnosti evidované a kontinuálne sledovaný stav riešenia identifikovaných rizík a zraniteľností na OVM.
* **Publikovanie informácií a vytváranie bezpečnostného povedomia** - údaje budú zdieľané a publikované viacerými spôsobmi. Jednu kategóriu predstavujú zdieľané údaje z OVM a tvorba dashboardov, ktoré budú zapojené do systému včasného varovania. Druhou kategóriou je publikovanie verejne dostupných informácií na webstránke VJ CSIRT a/alebo do centrálneho portálu KB na základe definovaného formátu a štruktúry, ktorý bude vytvorený v rámci Reformy č. 4: Štandardizácia technických a procesných riešení kybernetickej a informačnej bezpečnosti (ITVS).
* **Reakcia na hrozby a incidenty** – rozšírenie funkcií v budúcom stave umožni pomocou najmodernejších technológií vykonávať rýchle reakcie na detegované hrozby a incidenty. Riešenie umožní vykonávať automatizované aj manuálne vykonávanie reakcie SOC špecialistom (alebo aj interným bezpečnostným tímom) v reálnom čase za účelom minimalizovať dopady a následky kybernetických incidentov. Okrem reakcie nástroje umožnia aj spätné vyšetrovanie a popísanie priebehu incidentu.

Realizáciou projektu vzniknú tieto nové biznis funkcie:

* **Manažment technológií zabezpečujúcich zber bezpečnostných údajov** – implementáciou nového riešenia umožní centrálny manažment technológií (bezpečnostných nástrojov) používaných na zabezpečenie monitoringu na jednotlivých OVM, ktoré bude spravovať SOC čo prispeje k zabezpečeniu rovnakých štandardov a postupov pri správe nástrojov.
* **Včasné varovanie pred kybernetickými bezpečnostnými incidentami** – rozšírené zdroje údajov a ich automatizované spracovanie a vyhodnocovanie umožní generovať včasné varovania pre OVM zapojené do EWS na základe detailnej dátovej analýzy získaných dát z koncových zariadení, siete, manažmentu zraniteľností a ďalších spravodajských údajov.
* **Threat intelligence a Threat hunting** – v budúcom riešení vznikne platforma integrujúca viacero zdrojov spravodajských údajov. Riešenie je navrhnuté tak aby zhromažďovalo, agregovalo a organizovalo informácie o hrozbách z viacerých zdrojov a formátov. Platforma Threat intelligence umožní prostredníctvom EWS jednoducho zdieľať údaje o hrozbách s ostatnými OVM a bezpečnostnými dohľadovými centrami. Nové funkcionality budú zabezpečovať monitorovanie uniknutých dát OVM zapojených do EWS, vytváranie prehľadov hrozieb, distribúciu indikátory kompromitácie (IoC) do monitorovacích systémov, vytvárať hypotézy a realizovať threat hunting, teda proces proaktívneho a opakovaného prehľadávania sietí s cieľom odhaliť a izolovať pokročilé hrozby, ktoré sa vyhýbajú existujúcim bezpečnostným riešeniam.
* **Získavanie, spracovanie a vyhodnocovanie údajov z interných skenov zraniteľností** – navrhovaným riešením vznikne nová biznis funkcia v podobe možnosti získavania, spracovania a vyhodnocovania dát z interných skenov zraniteľností monitorovaných OVM. Tým sa doplnia údaje systému Achilles, ktorý už v súčasnosti skenuje a analyzuje zraniteľnosti na úrovni verejných IP adries. V prípade veľkého množstva identifikovaných kritických položiek je kľúčovou funkciou pre faktické odstránenie zraniteľností prioritizácia, ktorá zohľadňuje aj ďalšie dôležité parametre než len CVSS. Predovšetkým poskytuje aktuálne informácie z Threat Intelligence, informácie o možnosti exploitácie a definuje jej náročnosť alebo spresňuje typ zraniteľného systému.
* **Red teaming a Purple teaming** – nové bezpečnostné nástroje v budúcom riešení vytvoria predpoklad pre vykonávania Red teamimg-u, ktorý využíva taktiky, techniky a procedúry (TTP) na simuláciu reálnych kybernetických hrozieb na základe bezpečnostného profilu OVM. Cieľom Red teamu je okrem overenia úrovne kybernetickej bezpečnosti organizácie pomôcť obrannému tímu organizácie detegovať kybernetický útok a reagovať naň. Zámerom je simulovať realistický útok na organizáciu, ktorý je založený na relevantných hrozbách a TTP pre organizáciu. Pri tejto simulácií je cieľom taktiež preveriť bezpečnostné opatrenia, technológie, procesy, bezpečnostný tím organizácie a identifikovať možné nedostatky. Red teaming sa obyčajne vykonáva bez znalosti bezpečnostného tímu organizácie s výnimkou vybraných zamestnancov.

Predstaveným projektom a navrhnutým riešením sa zároveň zásadne rozširujú poskytované služby v oblasti kybernetickej bezpečnosti. Projektom sa priamo vytvoria podmienky pre poskytovanie nových proaktívnych služieb a zvýšenie kvality a dostupnosti tzv. reaktívnych služieb, teda služieb zameraných na riešenie konkrétnych hrozieb, incidentov a identifikovaných zraniteľností. Zoznam služieb systému včasného varovania (EWS) a bezpečnostného dohľadového centra rozdelené na proaktívnu a reaktívnu časť sú zosumarizované v nasledujúcich obrázkoch.

N/A

*Obrázok 7: Prehľad služieb bezpečnostného dohľadového centra (SOC) – budúci stav*

N/A

*Obrázok 8: Prehľad služieb systému včasného varovania (EWS) – budúci stav*

V budúcom stave vďaka realizácii tejto investície dôjde v aplikačnej architektúry k viacerým zmenám. Vznikne nový komponent EWS a zároveň dôjde k úpravám, resp. doplneniu funkcionalít už existujúcich komponentov a rozšírenie integrácií s cieľom centralizovaného zberu a vyhodnocovaniu údajov z relevantných zdrojov.

Hlavným komponentom navrhovaného budúceho riešenia bude novo-vytvorený **EWS**, ktorý bude na zabezpečenie kybernetickej bezpečnosti využívať pri monitoringu prevádzky pravidelne aktualizovanú databanku informácií o rizikách zloženú kombinovane z rôznych zdrojov a z vlastného výskumu alebo zdrojov VJ CSIRT takým spôsobom, aby poskytoval čo možno najširšie, vždy aktuálne informácie o hrozbách a skracoval priemerný čas identifikácie kybernetických bezpečnostných incidentov.

Cieľom budúceho riešenia je dobudovať také komponenty **Vládneho SOC**, ktoré sa budú zameriavať predovšetkým na nástroje a technológie, ktoré pomáhajú bezpečnostným expertom monitorovať, analyzovať, reagovať na bezpečnostné incidenty a posielať relevantné údaje do systému včasného varovania. Vládny SOC bude integrovaný s EWS. V rámci projektu budú nasadené a na Vládny SOC napojené **Monitorovacie nástroje na OVM**.

V rámci projektu budú doplnené integrácie na výsledky manažmentu externých zraniteľností **systémom Achilles**, ktorý bude poskytovať relevantné zistené bezpečnostné údaje pre EWS.

V budúcom riešení sa plánujú integrácie aj na ďalšie riešenia, resp. nástroje. Prvou skupinou sú systémy/nástroje, ktoré sú a/alebo budú v správe VJ CSIRT alebo NASES. Konkrétne sa jedná o nasledujúce integrácie:

* SIEM;
* SOAR;
* Monitorovacie nástroje na OVM;
* MISP;
* Zdroje threat intelligence;
* Service Desk
* Nástroje pre manažment zraniteľností spolu so systémom Achilles;
* VISKB (Vládny informačný systém kybernetickej bezpečnosti);
* Sektorový SOC verejnej správy podporený z výzvy na budovanie a rozvoj bezpečnostných dohľadových centier z Investície č. 6 Komponentu 17 Plánu obnovy a odolnosti.

Druhou skupinou sú externé systémy, resp. systémy, ktoré nie sú pod správou VJ CSIRT a NASES. V budúcom riešení budú vytvorené také technické predpoklady, aby boli systémy v budúcnosti integrované s EWS. Tieto integrácie nebudú realizované v rámci projektu:

* JISKB (Jednotný informačný systém kybernetickej bezpečnosti);

# LEGISLATÍVA

Z pohľadu predmetu projektu a nových poskytovaných služieb je dotknutá nasledovná legislatíva v rámci SR:

* Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov;
* Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 179/2020 Z. z. ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy v znení neskorších predpisov;
* Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov;
* Vyhláška Národného bezpečnostného úradu č. 362/2018 Z. z. ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení v znení neskorších predpisov;
* Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 85/2020 Z. z. o riadení projektov v znení neskorších predpisov.

V rámci definovaného projektu nie sú potrebné legislatívne úpravy.

Projekt má takisto pozitívne dopady aj na stav súladu spolupracujúcich OVM s vyhláškou NBÚ č. 362/2018 Z. z. Vďaka implementácii bezpečnostných nástrojov a bezpečnostnému monitoringu možno predpokladať zvýšenie úrovne celkovej bezpečnosti na OVM, čo sa prejaví na výsledkoch auditov kybernetickej bezpečnosti. Služby Vládneho SOC sa dotknú niekoľkých oblastí bezpečnosti znázornených v zjednodušenom schematickom prehľade nižšie. Počas prevádzky Vládneho SOC sa predpokladá súčinnosť zo strany OVM pri riadení komplementárnych bezpečnostných opatrení, ktoré majú zásadný (priamy) vplyv na kvalitu poskytovaných služieb. Plnenie vybraných bezpečnostných opatrení bude súčasťou procesov a postupov, ktoré budú predmetom zmluvného vzťahu medzi MIRRI a OVM.

*Obrázok 9: Očakávané pokrytie bezpečnostných opatrení podľa vyhlášky č. 362/2018 Z. z. – budúci stav*

# ROZPOČET A PRÍNOSY

**ROZPOČET**

Rozpočet projektu je tvorený z pohľadu troch častí (modulov) projektu v nasledovne:

Vytvorenie Systému včasného varovania (EWS – Early Warning System) – modul 1

* Riešenie bude implementované kombináciou externých dodávateľov jednotlivých technológií, internými kapacitami MIRRI / VJ CSIRT a interným tímom NASES zodpovedným sa prevádzku bezpečnostného dohľadového centra;
* Rozpočet na externú dodávku je v zmysle relevantnej metodiky (BC/CBA) definovaný na základe stanovenia funkčných a nefunkčných požiadaviek na riešenie – viď záložka „KATALOG\_POZIADAVKY“ a stanovených parametrov (TCF, ECF a UAW). Vzhľadom na vysokú mieru špecifickosti navrhnutého riešenia, použitie sofistikovaných high-tech bezpečnostných technológií a vysokú mieru integrácií bola v rámci tvorby BC/CBA aplikovaná vyššia hodnota produktivity faktora. Jednotlivé role relevantné z pohľadu externého vývoja, vrátane počtu MD a MD rate, sú definované v záložke „AKTIVITY\_POZICIE“, pričom sadzby MD vychádzajú z revidovanej analýzy MIRRI SR (2023) Sadzby prác externých IT odborníkov nakupovaných štátom podľa jednotlivých profesií. Zadefinované pozície projektu reflektujú potrebu implementácie špecifických bezpečnostných technológií, ktoré sú v podobnom rozsahu vo verejnom sektore na Slovensku používané v minimálnej miere.
* Interné kapacity, vrátane počtu, zapojenia a ceny práce, sú definované v záložke „POZICIE\_INTERNE“.

Implementácia nástrojov na zvýšenie kybernetickej bezpečnosti na vybraných OVM a spustenie bezpečnostného monitoringu prostredníctvom tzv. Vládneho SOC-u

* Časť Implementácia nástrojov bezpečnostného monitoringu a reakcie na kybernetické bezpečnostné incidenty (modul 3) na vybraných OVM bude realizovaná kombináciou externých dodávateľov a interných zamestnancov/dohodárov na strane MIRRI a NASES. V prípade inštalácie bezpečnostných nástrojov v infraštruktúre OVM budú využité aj kapacity interných tímov IT a bezpečnosti na samotných OVM:
	+ Externou dodávkou je nacenené dodanie (vrátane dovezenia, inštalácie, zapojenia, integračných prác, ladenie riešenia, zaškolenia atď.) HW a SW licencií definovaných v záložke „Rozpočet - HW a licencie“;
	+ Interné kapacity, vrátane počtu, zapojenia a ceny práce, sú definované v záložke „POZICIE\_INTERNE“.
* Časť Vládny SOC (modul 2) bude realizovaný rovnako kombináciou externých dodávateľov, ktorí budú dodávať a implementovať nástroje bezpečnostného monitoringu na OVM a internými zamestnancami/dohodármi na strane MIRRI a NASES:
	+ Externou dodávkou je nacenené dodanie (vrátane dovezenia, inštalácie, zapojenia, integračných prác, ladenie riešenia, zaškolenia atď.) HW a SW licencií definovaných v záložke „Rozpočet - HW a licencie“;
	+ Interné kapacity, vrátane počtu, zapojenia a ceny práce, sú definované v záložke „POZICIE\_INTERNE“.

Projektové riadenie bude realizované internými kapacitami. V prípade všetkých dodaných technológii bude súčasťou aj zaškolenie administrátorov a používateľov na strane monitorovaných OVM a na EWS/SOC.

Časť realizácie projektu bude zabezpečovať NASES na základe sprostredkovateľskej zmluvy z Investície 6. Ostatné aktivity, resp. úlohy, vyplývajú NASES zo zriaďovacej zmluvy a činnosti, ktoré už aktuálne pre MIRRI SR vykonáva. V prípade projektu to predstavuje nevyhnutné rozšírenie HW a SW pre ďalšie zabezpečenie prevádzky spoločného pracoviska bezpečnostného dohľadového centra a systému včasného varovania na centrálnej úrovni.

**PRÍNOSY**

V rámci ekonomickej analýzy je kladený dôraz predovšetkým na definovanie prínosov navrhovaného projektu a to ako kvalitatívnych, tak aj kvantitatívnych (finančné a ekonomické).

**Kvantitatívne prínosy**

* Zníženie ekonomických škôd a preventívne zabránenie škôd spôsobených kybernetickými útokmi;
* Úspory vyplývajúce z centralizácie riešenia pri poskytovaní služieb proaktívneho a reaktívneho charakteru.

Výpočet prínosov z pohľadu zabránenia ekonomických škôd v CBA uvažuje s konzervatívnym odhadom vo viacerých oblastiach:

* Škody vyčíslené ako % k HDP sú stanovené konzervatívne na úrovni 0,5% k HDP. Podľa dostupných vedeckých štúdii zo zahraničia sa v súčasnosti výška škôd spôsobená kybernetickými útokmi pohybuje až na úrovni 1% k HDP (pre rozvinuté krajiny) s predpokladom ďalšieho rastu v najbližších rokoch[[14]](#footnote-14).
* HDP Slovenska je vyčíslený a zostáva uvedený pre rok 2022. Je možné očakávať rast HDP v priebehu 10 rokov.
* Kybernetické útoky sú do počtu a sofistikovanosti celosvetovo na vzostupe, čo potvrdzujú aj štatistiky prezentované v časti MOTIVÁCIA A ROZSAH PROJEKTU. Celkový počet incidentov pre účely výpočtov zostáva zachovaný.

Pre výpočet prínosov sú uvažované niektoré čiastočné prínosy v roku T2 (2024) a v celkovom rozsahu od roku T3 (2025). Výpočet je postavený na znížení ekonomických škôd spôsobených kybernetickými útokmi vyčíslených ako definované % z HDP pre Slovensko. Celková vyčíslená škoda bola prepočítaná pre verejnú správu cez pomer výšky štátneho rozpočtu k HDP. Zároveň bola vypočítaná priemerná cena na jeden incident z celkového počtu incidentov vo verejnej správe. Projekt vytvorí predpoklady pre zníženie ekonomických škôd spôsobených kybernetickými útokmi v organizáciách zapojených do EWS, čo vyplýva z rýchlejšej detekcie, automatizácie reaktívnych činností a lepšieho zdokumentovania celého incidentu, čo významne prispieva v procese následného vyšetrovania. V prípade reaktívnych služieb sa zároveň očakáva vyššia miera zachytených incidentov z celkového počtu incidentov a s tým spojená aj vyššia potreba ich riešenia a šetrenia.

V prípade prínosov vyplývajúcich z centralizácie riešenie sa vychádza z viacerých predpokladov. Koncept centralizácie aktivít a služieb EWS a SOC spočíva v koncentrácii a zdieľaní:

* technológií (HW, SW, licencie) z pohľadu obstarávania a následnej prevádzky;
* tímu špecialistov na kybernetickú bezpečnosť, ktorých je na trhu nedostatok;
* budovanie know-how v sektore verejnej správy.

Úspory realizovaného projektu vyplývajú z rozsahu pri centrálnom nákupe a správe licencií na bezpečnostné nástroje prostredníctvom, ktorých bude monitorovaná IT infraštruktúra OVM a možnosti zdieľania informácii, ako kľúčového komponentu v oblasti proaktívnej kybernetickej bezpečnosti. Parametre k výpočtu úspor sú prezentované v CBA.

**Ďalšie prínosy**

Okrem prínosov, ktoré je možné definovať z kvantitatívneho pohľadu, je nevyhnutné hovoriť celkovo aj o prínosoch pripravovaného projektu a implementovaných riešení, ktoré nie je možné exaktne kvantifikovať. Napriek tomu majú nižšie uvedené prínosy zásadný vplyv na zvyšovanie kybernetickej bezpečnosti Slovenska a to najmä zo strednodobého a dlhodobého hľadiska:

* **Celkové zvýšenie úrovne zabezpečenia verejnej správy pred kybernetickými hrozbami** – zavedením aktívnych (preventívnych) opatrení sa po počiatočnom náraste počtu incidentov (spôsobené tým, že aktuálne OVM často ani nemajú vedomosť, že ich IT infraštruktúra bola kompromitovaná) očakáva zníženie frekvencie výskytu bezpečnostných incidentov, zníženie ich závažnosti a následne aj nižšie náklady na ich riešenie a odstránenie. To bude mať za následok zvýšenie odolnosti štátu voči kybernetickým útokom a zvýšenie dôveryhodnosti občanov v elektronické služby štátu.
* **Včasné odhaľovanie, včasná komunikácia a včasná reakcia na bezpečnostné hrozby** - dobudovanie ako aj implementácia nových nástrojov umožňujúcich zber, monitoring a vyhodnocovanie informácií na centrálnej úrovni umožní realizovať včasné odhaľovanie, včasnú komunikáciu a rýchlu reakciu na bezpečnostné hrozby.
* **Zdieľanie informácií o hrozbách, útokoch a konkrétnych riešeniach medzi OVM** - legislatívne zmeny prijaté v novej smernici NIS2 vyžadujú od členských štátov väčšie zapojenie do zdieľania bezpečnostných údajov. Projekt má v pláne vybudovať kapacity, ktoré majú potenciál pomôcť Slovenskej republike pri tejto výzve. Lepšie zdieľanie informácií o hrozbách, útokoch a konkrétnych riešeniach zvýši schopnosť a efektivitu detekcie rôznych typov kybernetických útokov, zvýši aj schopnosť reakcie na bezpečnostné incidenty, keďže OVM zasiahnuté kybernetickým útokom môžu využiť informácie a skúsenosti z iných OVM, kde už takýmto útokom prešli.
* **Zvyšovanie kompetencie v oblasti kybernetickej bezpečnosti na strane štátu** – v rámci projektu sa posilní budovanie analytických kapacít spoločného pracoviska NASES a Vládnej jednotky CSIRT, čím sa vytvárajú predpoklady pre udržateľnosť výsledkov projektu a následne budovanie ďalších odborných kapacít v prostredí štátu. Participácia zamestnancov OVM zodpovedných za bezpečnosť bude mať v konečnom dôsledku pozitívny dopad aj na zvýšenie schopností, znalostí a skúseností širšej skupiny zamestnancov verejnej správy.

**Parametre použité pre vyčíslenie prínosov**

Jednotlivé údaje sú z vybraných štatistických údajov, ak nie je uvedené inak – bližšie informácie k nižšie uvedeným parametrom a vysvetlenia sú uvedené v BC/CBA na záložke Faktory.

Zníženie škôd:

* Hrubý domáci produkt na Slovensku za rok 2022 dosiahol v bežných cenách: 109 651 900 000 EUR;
* Priemerné ročné ekonomické škody kybernetických útokov v EÚ sú odhadované na 0,5% z HDP (priemerná hodnota stanovená podľa odborných štúdií zo zahraničia <https://www.csis.org/analysis/economic-impact-cybercrime>; <https://www.rand.org/pubs/research_reports/RR2299.html>), pričom pri vysoko príjmových krajinách dosahujú až 1% z HDP;
* Štátny rozpočet SR za rok 2022: 26 945 417 000 EUR;
* Pomer štátneho rozpočtu k HDP (pomer štátneho rozpočtu k HDP rámcovo vyjadruje počet informačných systémov štátnej správy k počtu informačných systémov celkovo a teda aj nižší "attack surface"): 24,57%;
* Priemerné ročné ekonomické škody kybernetických útokov vo verejnej správe (hodnota prepočítaná pomerom štátneho rozpočtu k HDP reflektuje minimálnu variantu škôd na úrovni 0,5%): 134 727 085 EUR;
* Celkový ročný počet riešených incidentov VJ CSIRT za rok 2022 v súbore 1 417 poskytovateľov základnej služby (PZS) v sektore verejná správa: 1 012;
* Celkový počet incidentov 2022 (prepočítaný celkový počet incidentov vo verejnej správe vzhľadom na odhad zachytených incidentov prostredníctvom štatistiky. Celkový počet incidentov vo verejnej správe je vyšší ako uvádza štatistika): 5 060;
* Odhad detekcie incidentov v súčasnom stave (nasadený len antivírusový softvér): 20,00%, čiže 1012;
* Odhad detekcie incidentov v budúcom stave: 80,00%, čiže 4048;
* Priemerná spôsobená škoda incidentu v zmysle škody, ktorú incident spôsobil vo verejnej správe: 26 626 EUR (Variant 1 počítaná cez HDP) alebo priemerný dopad incidentu vypočítaný na základe interných dát o závažných incidentoch a metodike VJ CSIRT, ktorá identifikuje riešené závažné kybernetické incidenty podľa závažnosti (nízka, stredná vysoká a kritická): 21 123 EUR (Variant 2);
* Pre samotný výpočet bola použitá priemerná hodnota Variant 1 a Variant 2, spolu odhadovaná škoda 23 874 EUR/kybernetický bezpečnostný incident.
* Pre sektor verejnej správy je počet PZS podľa Správy o KB 1417. Z toho 894 tvoria obce a mestské časti, ktoré z pohľadu veľkosti IS a dopadov na služby občanom nie sú relevantné pre predložený projekt. Čistý počet relevantných PZS pre bezpečnostný dohľad SOC vo verejnej správe predstavuje 523.
* Plánované novo-pripojené PZS do bezpečnostného monitoringu v rámci projektu predstavujú 1,3 % z relevantných PZS pre EWS. V prípade útoku na organizáciu existuje reálne riziko možného rozšírenia, tzv. preliatia útoku na spolupracujúce PZS. Expertný odhad vychádzajúci z doterajších incidentov riešených CSIRT.SK stanovil minimálnu pravdepodobnosť na úrovni 20%. Celkový podiel chránených/dohľadovaných PZS, ktoré sú priamo a nepriamo vystavené KBI sa v tom prípade zvýši na 1,6 % (resp. 8,4 PZS).
* Na základe počtu detegovaných incidentov v budúcom stave a ich prepočtu na počet chránených PZS (projektom) bol pre rok 2022 (t0) vypočítaný počet potenciálne detegovaných incidentov na úrovni 65 ročne, čo predstavuje ročné odhadované škody 1,5 mil. EUR.
* Prínosy pre uvedený faktor boli počítané pre obdobie t3 až t10 so započítaným medziročným nárastom počtu znemožnených KBI o 5 % a výške škôd o 5 %. Podrobný výpočet, zdôvodnenie použitia jednotlivých premenných a zdroje údajov sú sumárne spracované v BC/CBA na záložke Faktory.

Zdieľanie Threat intelligence platformy:

* Vzájomným zdieľaním dát medzi subjektami zapojenými do systému včasného varovania sa významne znižujú finančné náklady na získavanie širokého spektra služieb a dát, ktoré vyplývajú z podstaty Therat intelligence platforiem.
* Pre OVM monitorované Vládnym SOC bude zdieľanie Threat intelligence zdrojov poskytované ako „custom“ služba pre jednotlivé OVM, pričom nepriamo môžu z poskytovanej služby benefitovať aj ďalšie podriadené a/alebo príspevkové organizácie monitorovaných OVM, ktoré môžu využívať napr. najaktuálnejšie prehľady hrozieb, zraniteľností a podobne. Uvedená časť nie je započítavaná do kvantifikácie prínosov.
* Prostredníctvom MISP bude TIP v plnom rozsahu poskytovaná pre potreby ďalších SOC vo verejnej správe, ktorých projekty na budovanie a rozvoj bezpečnostných dohľadových centier budú podporené výzvou vyhlásenou v rámci Investície 6 Komponentu 17 Plánu obnovy a odolnosti. Finančné prostriedky alokované na výzvu predpokladajú financovanie minimálne troch projektov. Výpočet prínosov teda vychádza z predpokladu obstarania a prevádzky Threat intelligence platformy pre 4 SOC (vrátane Vládneho SOC). Obstarávacia cena platformy (ročné predplatné licencie) na úrovni 400 000 EUR bola stanovaná na základe odhadu podľa priemernej hodnoty troch cenových ponúk v CBA. Prínosy z centrálneho obstarania a poskytovania TIP boli kvantifikované na úrovni 400 000 EUR ročne. Do kvantifikácie prínosov neboli započítané prínosy v podobe zníženia škôd formou prijímania preventívnych opatrení, ku ktorým významne prispeje samotná Threat intelligence platforma.

Centrálne obstaranie a správa bezpečnostných nástrojov:

Jedným z benefitov projektu je jednotný a centralizovaný nákup a správa bezpečnostných nástrojov nevyhnutných na zabezpečenie služieb bezpečnostného monitorovania OVM. Centralizovaný prístup je preferovaný z dvoch hlavných dôvodov:

1. Plošné nasadenie, správa a používanie jednotných technológií, čo zásadne zjednodušuje operatívu bezpečnostným analytikom na SOC a zvyšuje ich efektivitu práce (napr. jedna centrálna konzola vs. práca vo viacerých konzolách len pre jeden bezpečnostný nástroj). Zjednotením technológií sa zároveň zásadne znižujú nároky a náklady na integračné práce a proces onboardingu sa v rámci možností čo najviac zjednodušuje, resp. unifikuje;
2. Zníženie nákladov na obstarávanie, správu a podporu bezpečnostných nástrojov nasadených na monitorovaných OVM:
	* Predpokladaná ročná cena obstarávaných nástrojov centrálne predstavuje 2 000 000 EUR ročne. Cena bola stanovená podľa priemerných hodnôt indikatívnych cenových ponúk pre stanovenie rozpočtu projektu a BC/CBA.
	* Expertný odhad zníženia nákladov na obstaranie, prevádzku a správu licencií, SW a HW potrebného na vykonávanie bezpečnostného monitoringu na OVM vyplývajúci z centralizácie riešenia. Odhad počíta s minimálnym variantom na prevádzkovú úsporu nákladov na úrovni 15 % ročne. Uvedený odhad vychádza zo štúdie ÚHP (2020) Informatizácia 2.0 - revízia výdavkov Externá príloha č. 1. Z tejto časti sa očakáva ekonomický prínos projektu vo výške približne 300 000 EUR ročne.
3. Substitúcia licencie antivírusu pokročilejším bezpečnostným nástrojom, čím OVM odpadnú náklady na ich obstaranie a prevádzku:
	* Priemerná ročná cena za antivírus licenciu pre 1 koncové zariadenie vypočítaná na základe prieskumu uzatvorených zmlúv vo verejnej správe je 12 EUR
	* Celková ročná úspora pre OVM v prípade nahradenia 6000 antivírus licencií pokročilejšou technológiou, ktorá v sebe zahŕňa aj funkcionalitu antivírusu predstavuje 71 400 EUR ročne (nezapočítané personálne náklady spojené s procesom obstarávania na všetkých OVM samostatne).

Centrálny manažment služieb SOC a EWS:

* Kvantifikácia úspor v podobe personálnych nákladov v porovnaní s prevádzkou bezpečnostného monitoringu vlastnými internými tímami špecialistov na jednotlivých OVM.
* Výpočty vychádzajú z priemernej ceny práce od 3 000 EUR/osoba/mesiac. V prípade v BC/CBA (záložka Faktory) uvedených predpokladov by ročná cena práce špecialistov kybernetickej bezpečnosti SOC pre 7 OVM predstavovala 885 650 EUR ročne. Každým ďalším zapojeným OVM do Vládneho SOC a systému včasného varovania budú prínosy v podobe šetrenia personálnych nákladov lineárne rásť. V prípade realizácie projektu budú využité existujúce interné kapacity špecialistov NASES a VJ CSIRT, ktorí už v súčasnosti prevádzkujú spoločné pracovisko SOC v režime 24/7 aj so službami incident response a incident handling.
* Službou centrálneho úložiska bezpečnostných udalostí, OVM v budúcom riešení nebudú musieť samostatne obstarávať systémy na ukladanie a správu logov – LMS alebo log management system (povinnosť podľa vyhlášky č. 362/2018). Služba bude poskytovaná rozšírením aktuálnych SW a HW kapacít (prioritne rozšírenie úložiska za účelom retencie logov min. 6 mesiacov a viac), čo si vyžiada predpokladaný jednorazový náklad 300 000€ (expertný odhad stanovený podľa vypočítaného počtu EPS, ktoré budú generovať zapojené OVM). Priemerná cena LMS pre jednu inštitúciu s viac ako 500 zamestnancami sa podľa prieskumu zmlúv v CRZ pohybuje od 150 000 EUR. V prípade 7 OVM to predstavuje približne 1,1 mil. EUR, čím môže úspora dosiahnuť 800 000 EUR bez zohľadnenia ďalších úspor vďaka efektívnemu zdieľaniu prevádzkových nákladov, udržiavanie tzv. HA architektúry, nákladov na zálohovanie a testovanie záloh.

**Sumárny prehľad identifikovaných úspor:**

|  |  |  |  |
| --- | --- | --- | --- |
| 1 | Zníženie ekonomických škôd a dopadov spôsobených kybernetickými bezpečnostnými incidentmi | spolu za t3 až t10 | 19 748 994 € |
| 2 | Zdieľanie Threat intelligence platformy ako služby pre ďalšie sektorové SOC vo verejnej správe | ročne od t3 | 400 000 € |
| 3 | Úspora vyplývajúca z centrálneho nákupu a správy licencií | ročne od t3 (v t2 očakávaná polovičná úspora) | 300 000 € |
| 4 | Substitúcia licencie antivírusu pokročilejším riešením. | ročne | 71 398 € |
| 5 | Vzdialený výkon reaktívnych služieb | ročne | 6 650 € |
| 6 | Služba manažmentu zraniteľností (Vulnerability Alerting Service) | ročne | 126 000 € |
| 7 | Služba tvorby a udržiavania detekčných scenárov | ročne | 168 000 € |
| 8 | Forenzná analýza | ročne | 54 000 € |
| 9 | Služba Threat Intelligence | ročne | 63 000 € |
| 10 | Služba 24/7 bezpečnostného monitoringu | ročne | 468 000 € |
| 11 | Služba centrálneho úložiska bezpečnostných udalostí | jednorazovo + po piatich rokoch, na ktoré sa vzťahuje podpora od výrobcov HW | 803 928 € |

Celkový prehľad úspor vrátane spôsobu výpočtu a zdrojov údajov sa nachádzajú v BC/CBA (záložka Faktory).

**Sumarizácia nákladov a prínosov**

|  |  |  |
| --- | --- | --- |
| **Hlavné aktivity** | Vývoj aplikácií | 4 747 007 € |
|
|
| Nákup HW a SW | 10 717 565 € |
|
|
| **Prevádzka** | Aplikácie | 3 551 434 € |
|
|
| HW a SW | 8 727 118 € |
|
|
| **Podporné aktivity** | Projektový manažment | 100 390 € |
|
| Publicita | 0 € |
|
| Ostatné výdavky | 0 € |
| **Výstupné náklady** | 0 € |
|
| **SPOLU** | **27 843 515 €** |

|  |  |  |
| --- | --- | --- |
| **Prínosy** |  |  **35 234 635 €**  |
| **Finančné prínosy** |  |  - €  |
|  | Administratívne poplatky |  *- €*  |
|  | Ostatné daňové a nedaňové príjmy |  *- €*  |
| **Ekonomické prínosy** |  |  35 234 635 €  |
|  | Občania (€) |  *- €*  |
|  | Úradníci (€)  |  *- €*  |
|  | Úradníci (FTE) |  *N/A*  |
|  | Kvalitatívne prínosy | 35 234 635 €  |

\*Všetky ceny sú uvedené s DPH.

Rok návratu investície projektu: t7

Pomer prínosov a nákladov (BCR): 1,13

Ekonomická vnútorná výnosová miera (EIRR): 19 %

Finančná čistá súčasná hodnota (FNPV): -24 598 192 EUR s DPH

Ekonomická čistá súčasná hodnota (ENPV): 7 023 503 EUR s DPH

Detailné informácie k TCO sú uvedené v samostatnej prílohe BC/CBA.

# HARMONOGRAM JEDNOTLIVÝCH FÁZ PROJEKTU a METÓDA JEHO RIADENIA

Celkový harmonogram jednotlivých fáz projektu v zmysle Vyhlášky č. 85/2020 Z. z.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **FÁZA/AKTIVITA** | **ZAČIATOK****(odhad termínu)** | **KONIEC****(odhad termínu)** | **POZNÁMKA** |
| **1.** | Prípravná fáza | 06/2022 | 10/2023 |  |
| **2.** | Iniciačná fáza | 10/2023 | 11/2023 |  |
| **3.** | Realizačná fáza | 11/2023 | 05/2026 |  |
| **3a** | Analýza a Dizajn | 11/2023 | 04/2024 | Pre všetky časti projektu  |
| **3b** | Nákup technických prostriedkov, programových prostriedkov a služieb | 11/2023 | 10/2024 | Pre všetky časti projektu |
| **3c** | Implementácia a testovanie  | 03/2024 | 12/2025 | Pre všetky časti projektu |
| **3d** | Nasadenie a Postimplementačná podpora | 10/2025 | 05/2026 | Pre všetky časti projektu |
| **4.** | Dokončovacia fáza | 05/2026 | 06/2026 |  |

Projekt bude implementovaný v zmysle vyhlášky č. 85/2020 Z. z. o projektovom riadení bez rozdelení na viaceré inkrementy. Rozdelenie na inkrementy v projekte nie je možné vzhľadom na požiadavky inkrementu definovaných vyhláškou, podľa ktorých nie je možné realizovať viaceré inkrementy súbežne. Vzhľadom na charakter a rozsah projektu budú jednotlivé moduly, ktoré spolu vytvárajú jeden inkrement realizované paralelne v zmysle prístupu k implementácii jednotlivých častí projektu.

Realizačná fáza projektu bude rozdelená na 4 etapy:

* Analýza a dizajn
* Nákup HW, SW a služieb
* Implementácia a testovanie
* Nasadenie a post-implementačná podpora

V rámci high-level harmonogramu (obrázok nižšie) sú pre lepšiu prehľadnosť samostatne naplánované fáza nasadenia a fáza testovania. V prípade všetkých modulov budú paralelne prebiehať analýza a dizajn spolu s nákupom HW, SW a služieb. Počas prípravy projektovej dokumentácie a BC/CBA už boli špecifikované požiadavky na jednotlivé bezpečnostné nástroje a ďalšie technológie, čo umožní spustiť proces obstarávania v krátkom časovom horizonte po schválení projektu. Obdobne bude riešená aj etapa implementácia a testovanie. Realizačná fáza je naplánovaná na 31 mesiacov.

Indikatívny harmonogram realizačnej fázy jednotlivých častí projektu (harmonogram bude detailizovaný v rámci Projektového iniciálneho dokumentu ku každej časti projektu):

# PROJEKTOVÝ TÍM

Zostavuje sa Riadiaci výbor (RV) v minimálnom zložení:

* Predseda;
* podpredseda;
* vlastník alebo vlastníci procesov MIRRI SR (biznis vlastník) alebo nimi poverený zástupca alebo zástupcovia;
* vlastník alebo vlastníci procesov NASES (biznis vlastník) alebo nimi poverený zástupca alebo zástupcovia;
* zástupca alebo zástupcovia kľúčových používateľov MIRRI SR (end user);
* zástupca alebo zástupcovia kľúčových používateľov NASES (end user);
* riaditeľ odboru riadenia kybernetickej a informačnej bezpečnosti MIRRI SR;
* zástupca odboru riadenia programov a implementácie zmien MIRRI SR;
* zástupca odboru implementácie plánu obnovy a odolnosti MIRRI SR;
* Zástupcovia kľúčových dodávateľov (bude doplnený až po ukončení VO/voliteľný člen).

Určuje sa Projektový manažér verejného obstarávateľa (PM) a zostavuje sa projektový tím v nasledujúcom zložení:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Meno a Priezvisko** | **Pozícia** | **Oddelenie** | **Rola v projekte** |
| **1.** | Bude definovaný najneskôr v čase predloženia prvej žiadosti o platbu | Bude definovaný najneskôr v čase predloženia prvej žiadosti o platbu | SKB | IT Architekt |
| **2.** | Bude definovaný najneskôr v čase predloženia prvej žiadosti o platbu | Bude definovaný najneskôr v čase predloženia prvej žiadosti o platbu | SKB, NASES | Kľúčový používateľ |
| **3.** | Bude definovaný najneskôr v čase predloženia prvej žiadosti o platbu | Bude definovaný najneskôr v čase predloženia prvej žiadosti o platbu | SKB | IT Analytik |
| **4.** | Bude definovaný najneskôr v čase predloženia prvej žiadosti o platbu | Bude definovaný najneskôr v čase predloženia prvej žiadosti o platbu | SKB, NASES | Vlastník procesov |
| **5.** | Bude definovaný najneskôr v čase predloženia prvej žiadosti o platbu | Bude definovaný najneskôr v čase predloženia prvej žiadosti o platbu | VJ CSIRT | Projektový manažér |
| **6.** | Bude definovaný najneskôr v čase predloženia prvej žiadosti o platbu | Bude definovaný najneskôr v čase predloženia prvej žiadosti o platbu | VJ CSIRT | Manažér kvality |
| **7.** | Bude definovaný najneskôr v čase predloženia prvej žiadosti o platbu | Bude definovaný najneskôr v čase predloženia prvej žiadosti o platbu | SKB | Manažér kybernetickej bezpečnosti |
| **8.** | Bude definovaný najneskôr v čase predloženia prvej žiadosti o platbu | Bude definovaný najneskôr v čase predloženia prvej žiadosti o platbu | SKB | Projektový manažér |
| **9.** | Bude definovaný najneskôr v čase predloženia prvej žiadosti o platbu | Bude definovaný najneskôr v čase predloženia prvej žiadosti o platbu | SKB | SOC špecialista |
| **10.** | Bude definovaný najneskôr v čase predloženia prvej žiadosti o platbu | Bude definovaný najneskôr v čase predloženia prvej žiadosti o platbu | NASES | Bezpečnostný analytik L1/L2 - NASES |
| **11.** | Bude definovaný najneskôr v čase predloženia prvej žiadosti o platbu | Bude definovaný najneskôr v čase predloženia prvej žiadosti o platbu | SKB | Špecialista na manažment zraniteľností |
| **12.** | Bude definovaný najneskôr v čase predloženia prvej žiadosti o platbu | Bude definovaný najneskôr v čase predloženia prvej žiadosti o platbu | SKB | Špecialista pre riešenie kybernetických incidentov |
| **13.** | Bude definovaný najneskôr v čase predloženia prvej žiadosti o platbu | Bude definovaný najneskôr v čase predloženia prvej žiadosti o platbu | NASES | Integračný špecialista bezpečnostných nástrojov - NASES |
| **14.** | Bude definovaný najneskôr v čase predloženia prvej žiadosti o platbu | Bude definovaný najneskôr v čase predloženia prvej žiadosti o platbu | NASES | Platform support - NASES |
| **15.** | Bude definovaný najneskôr v čase predloženia prvej žiadosti o platbu | Bude definovaný najneskôr v čase predloženia prvej žiadosti o platbu | NASES | Špecialista pre onboarding - NASES |



# PRACOVNÉ NÁPLNE

Podrobné pracovné náplne, povinnosti projektového tímu a ich zodpovednosti budú predmetom menovacích dekrétov.

**Projektový manažér**

* Zodpovedá za riadenie projektu počas celého životného cyklu projektu. Riadi projektové (ľudské a finančné) zdroje, zabezpečuje tvorbu obsahu, neustále odôvodňovanie projektu (aktualizuje BC/CBA) a predkladá vstupy na rokovanie Riadiaceho výboru. Zodpovedá za riadenie všetkých (ľudských a finančných) zdrojov, členov projektovému tím objednávateľa a za efektívnu komunikáciu s dodávateľom alebo stanovených zástupcom dodávateľa.
* Zodpovedá za riadenie prideleného projektu - stanovenie cieľov, spracovanie harmonogramu prác, koordináciu členov projektového tímu, sledovanie dodržiavania harmonogramu prác a rozpočtu, hodnotenie a prezentáciu výsledkov a za riadenie s tým súvisiacich rizík. Projektový manažér vedie špecifikáciu a implementáciu projektov v súlade s firemnými štandardami, zásadami a princípmi projektového riadenia.
* Zodpovedá za plnenie projektových/programových cieľov v rámci stanovených kvalitatívnych, časových a rozpočtovým plánov a za riadenie s tým súvisiacich rizík. V prípade externých kontraktov sa vedúci projektu/projektový manažér obvykle podieľa na ich plánovaní a vyjednávaní a je hlavnou kontaktnou osobou pre zákazníka.

**Kľúčový používateľ**

* Zodpovedný za reprezentáciu záujmov budúcich používateľov projektových produktov alebo projektových výstupov a za overenie kvality produktu.
* Zodpovedný za návrh a špecifikáciu funkčných a technických požiadaviek, potreby, obsahu, kvalitatívnych a kvantitatívnych prínosov projektu, požiadaviek koncových používateľov na prínos systému a požiadaviek na bezpečnosť.
* Kľúčový používateľ (end user) navrhuje a definuje akceptačné kritériá, je zodpovedný za akceptačné testovanie a návrh na akceptáciu projektových produktov alebo projektových výstupov a návrh na spustenie do produkčnej prevádzky. Predkladá požiadavky na zmenu funkcionalít produktov a je súčasťou projektových tímov

**IT analytik**

* Zodpovedá za zber a analyzovanie funkčných požiadaviek, analyzovanie a spracovanie dokumentácie z pohľadu procesov, metodiky, technických možností a inej dokumentácie. Podieľa sa na návrhu riešenia vrátane návrhu zmien procesov v oblasti biznis analýzy a analýzy softvérových riešení. Zodpovedá za výkon analýzy IS, koordináciu a dohľad nad činnosťou SW analytikov.
* Analyzuje požiadavky na informačný systém/softvérový systém, formálnym spôsobom zaznamenáva činnosti/procesy, vytvára analytický model systému, okrem analýzy realizuje aj návrh systému, ten vyjadruje návrhovým modelom.
* Analytik informačných technológií pripravuje špecifikáciu cieľového systému od procesnej až po technickú rovinu. Mapuje a analyzuje existujúce podnikateľské a procesné prostredie, analyzuje biznis požiadavky na informačný systém, špecifikuje požiadavky na informačnú podporu procesov, navrhuje koncept riešenia a pripravuje podklady pre architektov a vývojárov riešenia, participuje na realizácii zmien, dohliada na realizáciu požiadaviek v cieľovom riešení, spolupracuje pri ich preberaní (akceptácie) používateľom.
* Pri návrhu IT systémov využíva odbornú špecializáciu IT architektov a projektantov. Študuje a analyzuje dokumentáciu, požiadavky klientov, legislatívne a technické podmienky a možnosti zvyšovania efektívnosti a výkonnosti riadiacich a informačných procesov. Navrhuje a prerokúva koncepcie riešenia informačných systémov a analyzuje ich efekty a dopady. Zabezpečuje spracovanie analyticko-projektovej špecifikácie s návrhom dátových a objektových štruktúr a ich väzieb, užívateľského rozhrania a ostatných podkladov pre projektovanie nových riešení.
* Spolupracuje na projektovaní a implementácii návrhov. Môže tiež poskytovať poradenstvo v oblasti svojej špecializácie. Zodpovedá za návrhovú (design) časť IT - pôsobí ako medzičlánok medzi používateľmi informačných systémov (biznis pohľad) a ich realizátormi (technologický pohľad).

**IT architekt**

* Zodpovedá za návrh architektúry riešenia IS a implementáciu technológií predovšetkým z pohľadu udržateľnosti, kvality a nákladov, za riešenie architektonických cieľov projektu dizajnu IS a súlad s architektonickými princípmi.
* Vykonáva, prípadne riadi vysoko odborné tvorivé činnosti v oblasti návrhu IT. Študuje a stanovuje smery technického rozvoja informačných technológií, navrhuje riešenia na optimalizáciu a zvýšenie efektívnosti prostriedkov výpočtovej techniky. Navrhuje základnú architektúru informačných systémov, ich komponentov a vzájomných väzieb. Zabezpečuje projektovanie dizajnu, architektúry IT štruktúry, špecifikácie jej prvkov a parametrov, vhodnej softvérovej a hardvérovej infraštruktúry podľa základnej špecifikácie riešenia.
* Zodpovedá za spracovanie a správu projektovej dokumentácie a za kontrolu súladu implementácie s dokumentáciou. Môže tiež poskytovať konzultácie, poradenstvo a vzdelávanie v oblasti svojej špecializácie. IT architekt, projektant analyzuje, vytvára a konzultuje so zákazníkom riešenia na úrovni komplexných IT systémov a IT architektúr, najmä na úrovni aplikačného vybavenia, infraštruktúrnych systémov, sietí a pod. Zaručuje, že návrh architektúry a/alebo riešenia zodpovedá zmluvne dohodnutým požiadavkám zákazníka v zmysle rozsahu, kvality a ceny celej služby/riešenia.

**Manažér kvality**

* Zodpovedá za priebežné vyžadovanie, hodnotenie a kontrolu kvality (vecnej aj formálnej) počas celého projektu. Je zodpovedný za úvodné nastavenie pravidiel riadenia kvality a za následné dodržiavanie a kontrolu kvality jednotlivých projektových výstupov. Sleduje a hodnotí kvalitatívne ukazovatele projektových výstupov a o zisteniach informuje projektového manažéra objednávateľa formou pravidelných alebo nepravidelných správ/záznamov.
* Plánuje, koordinuje, riadi a kontroluje systém manažérstva kvality, monitoruje a meria procesy a identifikuje príležitosti na trvalé zlepšovanie systému manažérstva kvality v organizácii v súlade s platnými normami. Zabezpečuje tvorbu cieľov a koncepcie kvality, vrátane kontroly ich plnenia a vykonáva interné a externé audity kvality v súlade s plánom.
* Počas celej doby realizácie projektu zabezpečuje zhodu kvality projektových výstupov s požiadavkami. Realizuje postupy riadenia kvality tak, aby výsledkom boli projektové výstupy spĺňajúce požiadavky objednávateľa. Kontroluje, či sa riadenie a proces zabezpečenia kvality vykonáva správnym spôsobom, v správnom čase a správnymi osobami.

**Vlastník procesov**

* Zodpovedá za proces - jeho výstupy i celkový priebeh poskytnutia služby alebo produktu konečnému užívateľovi. Kľúčová rola na strane zákazníka (verejného obstarávateľa), ktorá schvaľuje biznis požiadavky a zodpovedá za výsledné riešenie, prínos požadovanú hodnotu a naplnenie merateľných ukazovateľov. Úlohou tejto roly je definovať na užívateľa orientované položky (user-stories), ktoré budú zaradzované a prioritizované v produktovom zásobníku. Zodpovedá za priebežné posudzovanie vecných výstupov dodávateľa v rámci analýzy, návrhu riešenia vrátane DNR z pohľadu analýzy a návrhu riešenia aplikácii IS.
* Zodpovedný za schválenie funkčných a technických požiadaviek, potreby, obsahu, kvalitatívnych a kvantitatívnych prínosov projektu. Definuje očakávania na kvalitu projektu, kvalitu projektových produktov, prínosy pre koncových používateľov a požiadavky na bezpečnosť. Definuje merateľné výkonnostné ukazovatele projektov a prvkov. Vlastník procesov schvaľuje akceptačné kritériá, rozsah a kvalitu dodávaných projektových výstupov pri dosiahnutí platobných míľnikov, odsúhlasuje spustenie výstupov projektu do produkčnej prevádzky a dostupnosť ľudských zdrojov alokovaných na realizáciu projektu.

**Manažér kybernetickej a informačnej bezpečnosti**

* Zodpovedá za dodržanie princípov a štandardov v oblasti informačnej a kybernetickej bezpečnosti a za kontrolu a audit implementovaných bezpečnostných opatrení (technológií, procesov atď.).
* Koordinuje a riadi činnosť v oblasti bezpečnosti prevádzky IT, spolupracuje na projektoch, na rozvoji nástrojov a postupov k optimalizácii bezpečnostných systémov a opatrení. Stanovuje základné požiadavky, podmienky a štandardy pre oblasť bezpečnosti programov, systémov, databázy či sieti. Spracováva a kontroluje príslušné interné predpisy a dohliada nad plnením týchto štandardov a predpisov. Kontroluje a riadi činnosť nad bezpečnostnými testami, bezpečnostnými incidentmi v prevádzke IT. Poskytuje inštrukcie a poradenstvo používateľom počítačov a informačných systémov pre oblasť bezpečnosti.

**SOC špecialista**

* Zodpovedá za vývoj a doručenie detekčných scenárov podľa definovanej Threat mapy (na základe MITRE ATT&CK Framework). Testuje a nasadzuje detekčné scenáre do produkčného prostredia SIEM. Spolupracuje s Onboarding tímom a definuje, ktoré logy/eventy sú potrebné pre dostatočné pokrytie definovaných hrozieb v Threat mape. Spolupracuje s analytikmi na zlepšovaní kvality používaných detekčných scenárov – whitelisting, false positive reduction, zmena tresholdov, atď.
* Spravuje dostupné zdroje údajov spravodajských informácií o hrozbách, overuje ich relevantnosť a zabezpečuje správu Threat intelligence platformy a platformy MISP. Vyhľadáva a identifikuje skryté hrozby pomocou najnovších informácií o hrozbách.

**Špecialista na manažment zraniteľností**

* Spravuje interné a externé skeny zraniteľností a má za úlohu analyzovať aktuálny stav manažmentu zraniteľností v rámci jednotlivých OVM.
* Pripravuje hodnotenie pravdepodobnosti zneužitia zraniteľnosti. Integruje výsledky skenov do SIEMu a poskytuje výsledky pre Threat Intelligence tím. Na základe výsledkov skenov odporúča pre OVM nápravné opatrenia na odstraňovanie zraniteľností. Overuje odstraňovanie zraniteľností.

**Špecialista pre riešenie kybernetických incidentov**

* Zabezpečuje vyšetrovanie incidentov a v spolupráci s analytikmi vytvára a rozvíja procesy a postupy SOC. Riadi riešenie kritických incidentov a je zodpovedný za nepretržité aktívne vyhľadávanie hrozieb.
* Riadi proces reakcie na identifikovaný incident, ktorý zahŕňa identifikáciu útoku, pochopenie jeho závažnosti a stanovenie priorít, vyšetrenie a zmiernenie útoku, obnovenie operácií a prijatie opatrení, aby sa incident neopakoval.

**Bezpečnostný analytik L1/L2**

* Analytik L1 kontroluje výstrahy/udalosti a prideľuje im relevantnosť a naliehavosť (triáž zaznamenaných udalostí a incidentov). Spravuje tickety pre výstrahy, ktoré signalizujú incident a vyžadujú kontrolu úrovne L2 a reakciu na incident.
* Analytik L2 vyhodnocuje eskalované tickety generované analytikmi úrovne L1. Využíva informácie o vznikajúcich hrozbách na identifikáciu postihnutých systémov a rozsahu útoku. Vykonáva reakciu na detegované udalosti. Kontroluje a zhromažďuje údaje o aktívach v týchto systémoch na účely ďalšieho vyšetrovania a riadi činnosti pre nápravu funkčností.

**Integračný špecialista bezpečnostných nástrojov**

* Zabezpečuje návrh a integráciu medzi jednotlivými bezpečnostnými nástrojmi na lokalitách a v centrálnej časti riešenia. Implementácia techník detekcie a reakcie na hrozby a správa bezpečnostných informácií a udalostí (SIEM) spolu s automatizáciou procesov v SOAR.
* Spolupráca pri zadefinovaní požiadaviek a výbere optimálneho hardvéru a definovanie logických štruktúr pre súčasné a budúce produkty. Kooperácia pri tvorbe dokumentácie a dohľad nad úpravami súvisiacimi s architektúrou na základe požiadaviek na bezpečnosť a integráciu dát.

**Platform support**

* Zodpovedá za chod, údržbu a aktualizáciu nástrojov a systémov. Pripravuje dokumentáciu, ktorú môžu potrebovať iní členovia tímu. Vytvára riešenia a nástroje, ktoré pomáhajú organizáciám riešiť prerušenie prevádzky.

**Špecialista pre onboarding**

* Zabezpečuje integráciu zdrojov logov z jednotlivých OVM čerpajúcich služby Vládneho SOC. Nastavenie integrácie, normalizácie a parsovania logov (syntaktická analýza textu) z jednotlivých OVM podľa definovaného zoznamu „povinných logov“.
* Zodpovedá za doručenie logov do SIEMu a korektné nastavenie zdrojov logovania.

# ODKAZY

Usmernenia/metodiky relevantné pre realizáciu investície:

* Systém implementácie plánu obnovy a odolnosti (SIPOO);
* Usmernenia a relevantné informácie k plánu obnovy uvedené na stránke plánu obnovy (<https://www.planobnovy.sk/realizacia/dokumenty/>).

# PRÍLOHY

**Príloha 1: Zoznam rizík a závislostí**

**Príloha 2: BC\_CBA**

1. Najaktuálnejšie údaje v čase spracovania dokumentácie. Dostupné na: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022 [↑](#footnote-ref-1)
2. Dostupné na: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022 [↑](#footnote-ref-2)
3. Podrobnejšie na: https://digital-strategy.ec.europa.eu/sk/activities/cybersecurity-digital-programme [↑](#footnote-ref-3)
4. Celé znenie programu dostupné na: https://digital-strategy.ec.europa.eu/en/activities/work-programmes-digital [↑](#footnote-ref-4)
5. Dostupné na: https://digital-strategy.ec.europa.eu/sk/policies/cyber-solidarity [↑](#footnote-ref-5)
6. Dostupné na: https://www.consilium.europa.eu/sk/policies/cybersecurity/#challenges [↑](#footnote-ref-6)
7. Sun, Nan, et al. "Data-driven cybersecurity incident prediction: A survey." *IEEE communications surveys & tutorials* 21.2 (2018): 1744-1772. [↑](#footnote-ref-7)
8. Cho, Jin-Hee, et al. "Toward proactive, adaptive defense: A survey on moving target defense." *IEEE Communications Surveys & Tutorials* 22.1 (2020): 709-745. [↑](#footnote-ref-8)
9. Endsley, Mica R. "Design and evaluation for situation awareness enhancement." *Proceedings of the Human Factors Society annual meeting*. Vol. 32. No. 2. Sage CA: Los Angeles, CA: Sage Publications, 1988. [↑](#footnote-ref-9)
10. Evesti, Antti, Teemu Kanstrén, and Tapio Frantti. "Cybersecurity situational awareness taxonomy." *2017 international conference on cyber situational awareness, data analytics and assessment (Cyber SA)*. IEEE, 2017. [↑](#footnote-ref-10)
11. Husák, Martin, Tomáš Jirsík, and Shanchieh Jay Yang. "SoK: contemporary issues and challenges to enable cyber situational awareness for network security." *Proceedings of the 15th International Conference on Availability, Reliability and Security*. 2020. [↑](#footnote-ref-11)
12. Zhang, Hongbin, et al. "Network security situation awareness framework based on threat intelligence." *CMC: Comput. Mater. Continua* 56.3 (2018): 381-399. [↑](#footnote-ref-12)
13. Franke, Ulrik, and Joel Brynielsson. "Cyber situational awareness–a systematic review of the literature." *Computers & security* 46 (2014): 18-31. [↑](#footnote-ref-13)
14. Štúdie skúmajúce odhad škôd, ktoré boli spôsobené kybernetickými útokmi:

Lewis, J. (2018). Economic Impact of Cybercrime — No Slowing Down. The Center for Strategic and International Studies (CSIS) <https://www.csis.org/analysis/economic-impact-cybercrime>

Dreyer, P., Jones, T., Klima, K., Oberholtzer, J., Strong, A., Welburn, J. W., & Winkelman, Z. (2018). Estimating the global cost of cyber risk. Research Reports RR-2299-WFHF, Rand Corporation. <https://www.rand.org/pubs/research_reports/RR2299.html>

Gavėnaitė-Sirvydienė, J., & Miečinskienė, A. (2021). Forecasting costs of cyber attacks using estimation the Global Cost of Cyber Risk Calculator V 1.2. Contemporary Issues in Business, Management and Economics Engineering, 278-286. [↑](#footnote-ref-14)