# projekt\_991\_Projektovy\_zamer\_detailny

**PROJEKTOVÝ ZÁMER**

Identifikovanie požiadaviek **na funkčnú časť riešenia**

**Identifikácia projektu**

|  |  |
| --- | --- |
| **Povinná osoba** | Národná agentúra pre sieťové a elektronické služby |
| **Názov projektu** | Detekcia zraniteľnosti koncových obslužných bodov |
| **Zodpovedná osoba za projekt** | Ing. Michal Seliga – projektový manažér |
| **Realizátor projektu** | Národná agentúra pre sieťové a elektronické služby |
| **Vlastník projektu** | Národná agentúra pre sieťové a elektronické služby |

**Schvaľovanie dokumentu**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Položka** | **Meno a priezvisko** | **Organizácia** | **Pracovná pozícia** | **Dátum** | **Podpis**  (alebo elektronický súhlas) |
| Vypracoval | Michal Seliga | NASES | PM | 26.1.2021 |  |

**Obsah**

1. [POPIS ZMIEN DOKUMENTU. 3](#_Toc63764322)

[1.1.              História zmien. 3](#_Toc63764323)

1. [ÚČEL DOKUMENTU, SKRATKY (KONVENCIE) A DEFINÍCIE. 3](#_Toc63764324)

[2.1.              Použité skratky (príklady). 4](#_Toc63764325)

[2.1.1.                Konvencie – pravidlá názvoslovia, číslovania a verzionovania - požiadaviek (príklady). 4](#_Toc63764326)

[2.1.2.                Použité skratky (príklady). 4](#_Toc63764327)

[2.1.3.                Konvencie pre typy požiadaviek (príklady) 4](#_Toc63764328)

1. [DEFINOVANIE PROJEKTU. 5](#_Toc63764329)

[3.1.              Manažérske zhrnutie. 5](#_Toc63764330)

[3.2.              Motivácia a rozsah projektu. 5](#_Toc63764331)

[3.3.              Zainteresované strany/Stakeholderi 6](#_Toc63764332)

[3.4.              Ciele projektu a merateľné ukazovatele. 6](#_Toc63764333)

[3.5.              Riziká a závislosti 7](#_Toc63764334)

[3.6.              Alternatívy a Multikriteriálna analýza. 7](#_Toc63764335)

[3.6.1.                Stanovenie alternatív pomocou biznisovej vrstvy architektúry. 7](#_Toc63764336)

[3.6.2.                Multikriteriálna analýza. 8](#_Toc63764337)

[3.6.3.                Stanovenie alternatív pomocou aplikačnej vrstvy architektúry. 8](#_Toc63764338)

[3.6.4.                Stanovenie alternatív pomocou technologickej vrstvy architektúry. 8](#_Toc63764339)

1. [POŽADOVANÉ VÝSTUPY (PRODUKT PROJEKTU). 9](#_Toc63764340)

[4.1.              NÁHĽAD ARCHITEKTÚRY. 9](#_Toc63764341)

[4.2.              APLIKAČNÁ VRSTVA - POŽIADAVKY NA DODRŽANIE DÁTOVÝCH ŠTANDARDOV. 10](#_Toc63764342)

[4.2.1.           ROZSAH INFORMAČNÝCH SYSTÉMOV. 10](#_Toc63764343)

[4.2.2.           VYUŽÍVANIE SPOLOČNÝCH A NADREZORNTÝCH MODULOV VEREJNEJ SPRÁVY. 10](#_Toc63764344)

[4.2.3.           PREHĽAD IS NA EXTERNÚ INTEGRÁCIU SPOLOČNÝCH MODULOV UPVS. 11](#_Toc63764345)

[4.2.4.           INTEGRÁCIA NA NADREZORTNÉ CENTRÁLNE BLOKY. 12](#_Toc63764346)

[4.2.5.           INTEGRÁCIA NA MODUL PROCESNEJ INTEGRÁCIE A INTEGRÁCIE ÚDAJOV (IS CSRÚ) 12](#_Toc63764347)

[4.2.6.           POSKYTOVANIE ÚDAJOV. 13](#_Toc63764348)

[4.2.7.           KONZUMOVANIE ÚDAJOV. 13](#_Toc63764349)

[4.3      DÁTOVÁ vrstva - požiadavky na dodržanie dátových štandardov. 14](#_Toc63764350)

[4.3.1            Údaje v správe organizácie. 14](#_Toc63764351)

[4.3.2            DÁTOVÝ ROZSAH PROJEKTU.. 14](#_Toc63764352)

[4.3.3            KVALITA a ČISTENIE ÚDAJOV. 15](#_Toc63764353)

[4.3.3.1         Zhodnotenie objektov evidencie z pohľadu dátovej kvality. 15](#_Toc63764354)

[4.3.3.2         ROLE a PREDBEŽnÉ PERSONÁLNE ZABEZPEČENIE PRI RIADENÍ DÁTOVEJ KVALITY. 16](#_Toc63764355)

[4.4      REFERENČNÉ ÚDAJE. 16](#_Toc63764356)

[4.4.1            Objekty evidencie z pohľadu procesu ich vyhlásenia za referenčné. 16](#_Toc63764357)

[4.4.2            Identifikácia údajov pre konzumovanie alebo poskytovanie údajov – do / z CSRU.. 17](#_Toc63764358)

[4.5      OTVORENÉ ÚDAJE. 17](#_Toc63764359)

[4.6      ANALYTICKÉ ÚDAJE. 18](#_Toc63764360)

[4.7      MOJE ÚDAJE. 18](#_Toc63764361)

[4.8      PREHĽAD JEDNOTlivých kategórii údajov. 19](#_Toc63764362)

[4.9      LEGISLATÍVA. 19](#_Toc63764363)

[4.10             Bezpečnosť údajov (technické a organizačné zabezpečenie – pre prístup k údajom). 19](#_Toc63764364)

[4.10.1          posúdenie vplyvu a dopadu na ochranu osobných údajov (DPIA – data protection impact assesment). 20](#_Toc63764365)

1. [ROZPOČET A PRÍNOSY. 20](#_Toc63764366)
2. [HARMONOGRAM JEDNOTLIVÝCH FÁZ PROJEKTU a METÓDA JEHO RIADENIA. 22](#_Toc63764367)
3. [PROJEKTOVÝ TÍM.. 23](#_Toc63764368)
4. [PRACOVNÉ NÁPLNE. 24](#_Toc63764369)
5. [ODKAZY. 25](#_Toc63764370)
6. [PRÍLOHY. 25](#_Toc63764371)

[Tabuľka 1 Prehľad dotknutých informačných systémov v projekte. 9](#_Toc63764279)

[Tabuľka 2 Prehľad spoločných modulov a aplikačných služieb. 10](#_Toc63764280)

[Tabuľka 3 Prehľad integrácii informačných systémov na spoločné moduly. 10](#_Toc63764281)

[Tabuľka 4 Prehľad integrácii informačných systémov na nadrezortné bloky verejnej správy. 11](#_Toc63764282)

[Tabuľka 5 Prehľad integračných väzieb medzi IS VS a IS CSRÚ.. 12](#_Toc63764283)

[Tabuľka 6 Prehľad informačných systémov určených na poskytovanie do IS CSRÚ.. 12](#_Toc63764284)

[Tabuľka 7 Prehľad informačných systémov určených na konzumovanie z IS CSRÚ.. 12](#_Toc63764285)

[Tabuľka 8 Prehľad objektov evidencie v jednotlivých ISVS v projekte. 14](#_Toc63764286)

[Tabuľka 9 Kategorizácia údajov z pohľadu ich využiteľnosti 15](#_Toc63764287)

[Tabuľka 10 Prehľad rolí a personálneho zabezpečenia pre riadení dátovej kvality. 15](#_Toc63764288)

[Tabuľka 11 Prehľad identifikovaných referenčných údajov. 16](#_Toc63764289)

[Tabuľka 12 Prehľad identifikovaných referenčných údajov. 16](#_Toc63764290)

[Tabuľka 13 Prehľad otvorených údajov. 17](#_Toc63764291)

[Tabuľka 14 Prehľad sprístupnených dátových zdrojov určených na analytické účely. 17](#_Toc63764292)

[Tabuľka 15 Prehľad údajov identifikovaných pre službu „moje údaje“. 17](#_Toc63764293)

[Tabuľka 16 Kategorizácia údajov z pohľadu ich využiteľnosti (účelu) 18](#_Toc63764294)

[Obrázok 1: Prehľad informačných systémov dotknutých v projekte. 11](#_Toc63764295)

[Obrázok 2: Príklad integrácie na IS CSRÚ.. 13](#_Toc63764296)

[Obrázok 3: Príklad doménového modelu. 14](#_Toc63764297)

[Obrázok 4: Príklad zjednodušeného doménového modelu. 14](#_Toc63764298)

# 1.     POPIS ZMIEN DOKUMENTU

## 1.1.         História zmien

|  |  |  |  |
| --- | --- | --- | --- |
| Verzia | Dátum | Zmeny | Meno |
| 0.1 | DD.MM.YYYY | doplň | XY |
| 0.2 | DD.MM.YYYY | doplň | XY |
|  |  |  |  |
|  |  |  |  |

# 2.     ÚČEL DOKUMENTU, SKRATKY (KONVENCIE) A DEFINÍCIE

Doplniť vstupy v **PRÍPRAVNEJ FÁZE:**

* V súlade s [***Vyhláškou č. 85/2020 Z.z***](https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2020/85/)***. o riadení projektov*** - je dokument ***Projektový zámer*** pre prípravnú fázu určený na rozpracovanie informácií k projektu, aby bolo možné rozhodnúť o pokračovaní prípravy projektu, alokovaní rozpočtu, ľudských zdrojov a prechode do iniciačnej fázy.

Doplniť vstupy v**INICIAČNEJ FÁZE:**

* V súlade s ***Vyhláškou č. 85/2020 Z.z. o riadení projektov -*** je dokument ***Projektový zámer*** pre iniciačnú fázu určený na rozpracovanie detailných informácií prípravy projektu.

## 2.1.         Použité skratky (príklady)

### 2.1.1.      Konvencie – pravidlá názvoslovia, číslovania a verzionovania - požiadaviek (príklady)

|  |  |  |
| --- | --- | --- |
| **ID** | **SKRATKA** | **POPIS** |
| 1. | U | Užívateľská požiadavka |
| 2. | P | Procesná požiadavka |
| 3. | R | Požiadavka na reporting |
| 4. | I | Integračná požiadavka |
| 5. | C | Kapacitné požiadavky procesov |
| 6. | S | Požiadavka na bezpečnosť |
| 7. | O | Prevádzková požiadavka (Operations) |
| 8. | D | Požiadavka na dokumentáciu |
| 9. | L | Legislatívna požiadavka |
| 10. | O | Ostatné |
| 11. | ... | ... |

### 2.1.2.      Použité skratky (príklady)

|  |  |  |
| --- | --- | --- |
| **ID** | **SKRATKA** | **POPIS** |
| 1. | MIRRI | Ministerstvo investícií, regionálneho rozvoja a informatizácie |
| 2. | NASES | Národná agentúra pre sieťové a elektronické služby |
| 3. | mID | Aplikácie mobilné ID |
| 4. | ESDV | Aplikácia eSlovenskoDoVrecka |
| 5. | UPVS | Ústredný portál verejnej správy |
| 6. | ESD | Systém pre detekciu hrozieb a prienikov na úrovni endpoint a session |
| 7. | TXM | Systém pre detekciu hrozieb a prienikov na úrovni transakcií |
| 8. | MITM | Man In The middle útok |
| 9. | MITB | Main In the browser útok |
| 10. | RAT | Remote Access Trojan |
| 11. | API | Aplikačné rozhranie |
| 12. | RASP | runtine application self-protection |
| 13. | WAF | Web aplikačný firewall |
| 14. | SIEM | Security information and event management |
| 15. | CSIRT | Computer Security Incident Response Team |
| 16. | SOC | Security operational center |
| 17. | SPA | Single page application |
| 18. | ENISA | Agentúra Európskej únie pre kybernetickú bezpečnosť |
| 19. | DDoS | Distribuované odmietnutie služby |

### 2.1.3.      Konvencie pre typy požiadaviek (príklady)

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

**Užívateľské požiadavky majú nasledovnú konvenciu:**

**U\_nn\_Rxx**

* U – užívateľská požiadavka
* nn – typ používateľa
* R – označenie požiadavky
* xx – číslo požiadavky

**Procesné požiadavky majú nasledovnú konvenciu:**

**P\_ABXY\_Rxx**

* P – procesná požiadavka
* AB – označenie procesu
* XY – číslo podprocesu
* R – označenie požiadavky
* xx – číslo požiadavky

**Reportingové požiadavky majú nasledovnú konvenciu:**

**R\_nn\_Rxx**

* R – reportingová požiadavka
* nn – číslo reportu
* R – označenie požiadavky
* xx – číslo požiadavky

**Kapacitné požiadavky majú nasledovnú konvenciu:**

**C\_aa\_Rxx**

* C – kapacitná požiadavka
* aa – kapacitná oblasť
* R – označenie požiadavky
* xx – číslo požiadavky

**Bezpečnostné požiadavky majú nasledovnú konvenciu:**

**S\_aa\_Rxx**

* S – bezpečnostná požiadavka
* aa – bezpečnostná oblasť
* R – označenie požiadavky
* y – číslo požiadavky

**Prevádzkové požiadavky majú nasledovnú konvenciu:**

**O\_aa\_Rxx**

* O – prevádzková požiadavka
* aa – prevádzková oblasť
* R – označenie požiadavky
* xx – číslo požiadavky

**Ostatné požiadavky majú nasledovnú konvenciu:**

**A\_aa\_Rxx**

* A – ostatná požiadavka
* aa – ostatná oblasť
* R – označenie požiadavky
* xx – číslo požiadavky

**Ostatné typy požiadaviek môžu byť ďalej definované objednávateľom/PM.**

# 3.     DEFINOVANIE PROJEKTU

## 3.1.         Manažérske zhrnutie

NASES vznikla 1. januára 2009 ako príspevková organizácia Úradu vlády SR za účelom plnenia odborných úloh v oblasti informatizácie spoločnosti, vyplývajúcich zo zákona č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon o IS VS“), správy a prevádzkovania elektronických komunikačných sietí a služieb, pre potreby Úradu vlády SR, ktoré Úradu vlády SR vyplývajú z § 24 ods. 3 zákona č. 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy, ako aj §5 ods. 2 zákona č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, a aj pre ostatné orgány štátnej správy, právnické osoby a fyzické osoby, ktoré požadujú informácie, údaje z informačných systémov, databáz a registrov verejnej správy. Jej hlavnou úlohou a predmetom činnosti  je správa, prevádzka a rozvoj vládnej dátovej siete GOVNET a prevádzka a rozvoj služieb Ústredného portálu verejnej správy, ako základných nástrojov informatizácie verejnej správy na Slovensku.

Projekt vychádza zo súčasného stavu kybernetickej bezpečnosti v SR a Operačného programu Integrovaná infraštruktúra - špecifický cieľ 7.9: Zvýšenie kybernetickej bezpečnosti v spoločnosti. Cieľom tejto štúdie uskutočniteľnosti je poskytnúť strategický rámec, plánovaný rozsah, očakávaný časový harmonogram a prípadné odporúčania ďalších aktivít, z ktorých je potrebné pri realizácii implementácie národného projektu vychádzať. V súvislosti s elektronizáciou služieb verejnej správy (e-Government) dochádza k veľmi významnému zvýšeniu závislosti výkonu verejnej správy na informačných systémoch verejnej správy a zvyšujú sa aj potenciálne škody z kybernetických incidentov. Aktuálne SOC NASES spracováva denne cca 46tis eventov a tento počet rastie. Obrázok Príklad zloženie typov eventov

Množstvo chránených služieb prevádzkovaných na vládnej sieti GOVNET (prvok kritickej infraštruktúry) sa postupne rozširuje o nové služby, nové mobilné aplikácie a moderné interaktívne webové aplikácie, ktoré potrebujú špecifický typ ochrany pre hrozbami.

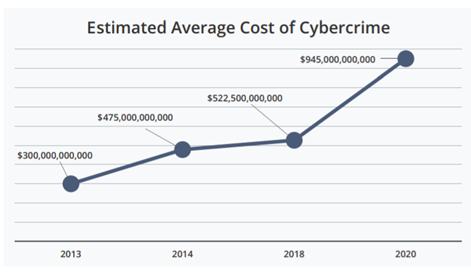
Indikatívna výška finančných prostriedkov na projekt je 6 968 138 eur s DPH. Projekt je výlučne infraštruktúrne orientovaný t.j. nákup HW/licencie.

*Pri vypracovaní projektu sme vychádzali z viacerých renomovaných medzinárodných konzultačno-poradenských spoločností ako sú Forrester, McAfee a Agentúra Európskej únie pre kybernetickú bezpečnosť, ktoré popisujú, že dané riešenie sa používajú v komerčnom sektore. Dané štúdie sú rozpísané nižšie v projekte a prílohe 2 Analýza benefitov.*

V štúdii McAfee The Hidden Costs of Cybercrime By Zhanna Malekos Smith and Eugenia Lostri James A. Lewis, Project Director z roku 2018 je uvedené, že odhadované náklady na riešenie dopadov globálnej počítačovej kriminality dosiahli viac ako 1 bilión dolárov. Finančná strata z počítačovej kriminality bola odhadnutá na približne 945 miliárd dolárov, čo predstavuje viac ako 1% globálneho hrubého domáceho produktu HDP. K tomu sa pridali globálne výdavky na kybernetickú bezpečnosť, ktoré by mali v roku 2020 podľa predpokladaného odhadu prekročiť 145 miliárd dolárov. Vyššie uvedená štúdia taktiež zistila, že počítačová kriminalita stála globálnu ekonomiku 600 miliárd dolárov. V súčasnosti predstavujú tieto výdavky pre globálnu ekonomiku brzda v hodnote 1 bilióna dolárov. Poznatky uvedené v štúdii, ako aj aktuálny vývoj naznačujú nárast v posledných rokoch o viac ako 50%.

Na vypracovaní štúdie sa zúčastnilo 1 500 spoločností, z ktorých iba 4% potvrdili, že nemali v roku 2019 skúsenosť s akýkoľvek druhom kybernetického incidentu. Najvyššie náklady pre organizácie tvorili škody spôsobené malvérom a spywarom , avšak až 92% respondentov uviedlo aj iné škody, nielen finančné. Najväčšia nepeňažná strata bola v zníženej produktivite a v skrátení pracovnej doby. Najdlhšie priemerné prerušenie prevádzky bolo 18 hodín, čo predstavovalo finančnú stratu v priemere viac ako pol miliónov dolárov.

Obrázok: Priemerné náklady na globálnu počítačovú kriminalitu.



Zdroj: <https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf>

Sektory, ktoré boli v období roku 2019 až apríl 2020 najviac zasiahnuté, boli digitálne služby, štátna správa a technologický priemysel. Pritom štátna správa tvorí najatraktívnejší sektor, ktorý čelí útokom ransomwaru, t.j. vydieračský softvér, ktorý blokuje počítačový systém alebo šifruje dáta v ňom zapísané, a následne požaduje od obete výkupné za obnovenie prístupu.[[1]](" \l "_ftn1)

[[1]](" \l "_ftnref1) Zdroj: ENISA - Main incidents in the EU and worldwide From January 2019 to April 2020.[1]

Agentúra Európskej únie pre kybernetickú bezpečnosť (ENISA) je zameraná na dosiahnutie vysokej spoločnej úrovne kybernetickej bezpečnosti. Bola založená v roku 2004 a jej postavenie je posilnené EÚ Zákonom o kybernetickej bezpečnosti. ENISA prispieva k rozvoju v oblasti kybernetickej politiky EÚ, zvyšuje dôveryhodnosť v IKT produkty, služby a procesy so systémami certifikácie kybernetickej bezpečnosti, spolupracuje s členskými štátmi a orgánmi EÚ a pomáha pripraviť sa Európe pre kybernetické výzvy zajtrajška. Viac informácií o ENISA, jej práci a publikáciách možno nájsť na: www.enisa.europa.eu.

Medzi najznámejšie hrozby sa zaraďujú phishing, vhishing, RAT (remote access trojan), session hijacking, account takeover, credentials stealing, MITB, MIM, API scrapping a mnoho ďalších. Z dostupných skúseností je možné konštatovať, že sa v prvom rade jedná o útoky na zariadenie klienta, z ktorého klient až následne pristupuje na služby verejnej inštitúcie.

V rámci štúdie Top 15  hrozieb ENISA označila najčastejšie sa vyskytujúce hrozby. Z nich sme vybrali top 9 hrozieb, ktoré sa priamo dotýkajú projektu:

1) Malware – V analýze trendov hrozieb škodlivého softvéru sa od januára 2019 do apríla 2020 umiestnil na 1. mieste, pričom si zachoval rovnakú pozíciu od roku 2018. Malware je častý typ kybernetických útokov vo forme škodlivého obsahu softvéru.

Zistenia:

* 400 000 detekcií predinštalovaného spywaru a adware na mobilných zariadeniach;
* 67% škodlivého softvéru bolo doručených cez šifrované pripojenia HTTPS;
* 71% organizácií malo skúsenosť s malware aktivitou, ktorá sa rozšírila z jedného zamestnanca na druhého.

2) Webové útoky – Podľa analýzy trendov webových útokov sa od januára 2019 do apríla 2020 umiestnili na 2. mieste a zachovali si tú istú pozíciu ako v roku 2018. Webové útoky sú atraktívnou metódou, pomocou ktorej môžu aktéri hrozieb klamať obete pomocou webových systémov a služieb ako vektorové hrozby.

3) Phishing - Analýza trendov phishingovej hrozby od januára 2019 do apríla 2020 potvrdila jeho stúpajúcu tendenciu, v roku 2018 bol na 4 pozícii. Phishing je podvodný pokus o krádež údajov používateľa, ako je napríklad prihlasovacie údaje, informácie o kreditnej karte. Tento typ útoku sa zvyčajne spustí prostredníctvom e-mailových správ, ktoré sa zdajú byť odoslané od renomovanej firmy so zámerom presvedčiť používateľa, aby si otvoril škodlivú prílohu alebo aby sledoval podvodnú adresu URL.

Zistenia:

* 667% zvýšenie phishingových podvodov iba za 1mesiac počas pandémie COVID-19;
* 42,8% zo všetkých škodlivých príloh boli dokumenty balíka Microsoft Office.

4) Útoky na webové aplikácie – Podľa Analýzy trendov útokov na webové aplikácie si útoky medzi januárom 2019 a aprílom 2020 vymenili pozíciu s pishingom z roku 2018. Pri tomto type útoku sa zneužíva slabosť vstupných funkcií webových aplikácií, ktoré vedú k ďalším škodlivým funkciám, ako napríklad presmerovanie na škodlivý web.

Zistenia:

* 52% zvýšenie počtu útokov na webové aplikácie v roku 2019 v porovnaní s rokom 2018. Podľa výskumníka v oblasti bezpečnosti útoky v porovnaní s rokom 2018 prudko vzrástli.

5) Nevyžiadaná pošta (Spam) - Analýza trendov spamových útokov medzi januárom 2019 a aprílom 2020 ukázala, že má stúpajúcu tendenciu oproti roku 2018 (miesto č.6). Príjem spamu môže vytvoriť príležitosť útočníka ukradnúť osobné informácie alebo nainštalovať malware. Spam sa skladá z hromadného odosielania nevyžiadaných správ.

Zistenia:

* 85% z všetkých e-mailov vymenených v apríli 2019 bol spam, čo je 15-mesačné maximum;
* 83% spoločností nebolo chránených proti odcudzeniu identity;
* 42% hlavných úradníkov pre bezpečnosť informácií sa zaoberalo najmenej jedným spamovým bezpečnostným incidentom.

6) Distribuované odmietnutie služby (DDoS) - Analýza trendov DDoS útokov medzi januárom 2019 a aprílom 2020 ukázala pokles o jedno miesto oproti roku 2018. DDoS nastane, keď používatelia systému alebo služby nemajú prístup k príslušným informáciám, službám alebo iným zdrojom.

Zistenia:

* 241% zvýšenie celkového počtu útokov počas 3. štvrťrok 2019 v porovnaní s rovnakým obdobím roku 2018;
* 84% útokov trvalo menej ako 10 minút.

7) Ukradnutie identity - Analýza trendov medzi januárom 2019 a aprílom 2020 ukazuje stúpajúcu tendenciu, nakoľko táto hrozba stúpla z 13. pozície oproti roku 2018. Krádež identity je nezákonné použitie osobných údajov obete. Zhruba 20 % európskych spotrebiteľov zažilo takzvané „neviditeľné zločiny“, najmä krádež identity, ktoré prispeli k celosvetovému šíreniu finančných podvodov a sprievodných strát. Zhruba každý štvrtý Európan zasiahnutý akýmkoľvek typom finančného podvodu utrpel stratu, pričom celková hodnota krádeže v celej Európe dosiahla za posledné dva roky viac ako 24 miliárd eur. Podvodník, ktorý sa vydáva za túto osobu môže získať finančnú výhodu a ďalšie výhody. V roku 2019 priemerné náklady na krádež poverenia dosiahli hodnotu 413 217 eur a ročné náklady na krádež poverenia dosiahli hodnotu 2,4 mil. eur.

8) Porušenie údajov - Analýza trendov útokov na porušenie ochrany údajov od januára 2019 do apríla 2020 potvrdila rovnakú pozíciu ako v roku 2018. Porušenie údajov je typom kybernetického bezpečnostného incidentu, pri ktorom sú informácie (alebo časť informačného systému) prístupné bez oprávnenej autorizácie, zvyčajne so zlým úmyslom, ktorý vedie k potenciálnej strate alebo zneužitie informácií.

Zistenia:

* 54% zvýšenie celkového počtu porušení do polovice roku 2019 v porovnaní s rokom 2018;
* 71% porušenia ochrany údajov bolo finančne motivovaných;
* 70% porušenia ochrany údajov vyplýva, že sú e-maily;
* 55% \_respondentov na prieskum Eurobarometer prieskum odpovedalo, že majú obavy o svoje údaje, ku ktorým majú prístup útočníci.

9) Vnútorná hrozba - Analýza trendov vnútornej hrozby od januára 2019 do apríla 2020 ostala na rovnakej pozícii ako v roku 2018. Vnútorná hrozba je činnosť, ktorá môže viesť k incidentu, vykonanú niekým alebo skupinou ľudí pridružených alebo pracujúcich pre potenciálnu obeť.

Zistenia:

* 65% dopadu vnútorných hrozieb vplýva na poškodenie dobrého mena organizácie a financií;
* 11,45 milióna  € sú priemerné ročné náklady na kybernetické bezpečnostné incidenty spôsobené členmi v organizácii.

Na problematiku bezpečnosti informačných systémov a aplikácií sa dá pozerať z viacerých strán. V prvom rade je to bezpečnosť z pohľadu siete, t. j. chrániť infraštruktúru pred hrozbami prostredníctvom sieťových prvkov, ktoré vedia chrániť infraštruktúru až po 7 vrstvu OSI modelu, avšak táto ochrana nie je viazaná na aplikačnú logiku. Aplikačná logika sa dá teda považovať za ďalšiu možnosť nazerania na problematiku bezpečnosti. S uvedenými spôsobmi súvisí aj zvýšenie bezpečnosti aplikácie zavedením zásad bezpečného vývoja aplikácii. Prax ukázala, že väčšina útokov na web a mobilné aplikácie sa vykonáva mimo bezpečného prostredia inštitúcie, t.j. na strane klienta a to aj napriek snahe o zabezpečenie danej aplikácie a implementácie rôznych detekčných mechanizmov.

Dôležitosť detekcie zraniteľností aplikácie v bode resp. mieste, kde ju používa klient, umocňuje fakt, že využívaním mobilných aplikácií, a využívaním moderných architektúr (HTML5 a JS frameworkov, natívnych mobilných aplikácií ), dbajúcich na vysokú užívateľskú skúsenosť, rýchly vývoj a sprístupňovanie API rozhraní do internetu,  sa prenáša veľká časť aplikačnej a business logiky z bezpečného prostredia dátového centra inštitúcie do nebezpečného prostredia internetu, zariadenia alebo infraštruktúry klienta, odkiaľ dané služby využíva. V zmysle uvedeného je možné konštatovať, že sa jedná primárne o útoky na zariadenie klienta, z ktorého pristupuje na služby inštitúcie.

Navrhovaný modul detekcie hrozieb a prienikov zahŕňa kľúčové techniky pre ochranu aplikácií postavených na moderných architektúrach. Patrí sem samoochrana aplikácii a detekcia  hrozieb na strane klienta napr. v podobe RASP (runtine application self-protection), detekcie malware (škodlivých aplikácií), detekcie zmien v správaní klienta (behavioral analysis) a zaradenie platformy na automatizáciu pravidelných bezpečnostných udalostí. Treba si uvedomiť, že Detekcia zraniteľnosti koncových obslužných bodov je iba doplnok a nie náhrada za bezpečnostné testovanie, bezpečný vývoj alebo implementáciu prvkov ako sú firewall a WAF. Navrhovaný modul detekcie hrozieb a prienikov rozšíri poskytované služby na vládnej sieti GOVNETE o nasledujúcu funkcionalitu najmä:

- detekciu malware na koncových zariadeniach,

- detekciu bottov,

- telemetriu koncových zariadení,

- behaviorálna biometria,

- analýza risk transakcií,

- detekcia ukradnutia identity,

- detekcia phishingov,

- detekcia screen scraping,

- detekcia ratting v prehliadačoch,

- detekcia prevzatie session

- detekcia onboarding podvody,

- detekcia ukradnutie prihlasovacích údajov,

- detekcia vishing,

- detekcia man in the browser,

- detekcia man in the middle,

- detekcia zneužitie api,

- detekcia simulátorov,

- detekcia prebalíčkovavanie aplikácií,

- detekcia overlay útoky.

**Ako funguje Detekcia zraniteľnosti koncových obslužných bodov**

Techniky a architektúry detekcie zraniteľnosti koncových obslužných bodov chránia aplikáciu z vnútra, bez potreby inštalácie špecializovaného softvéru na strane klientskeho zariadenia (napr. antvirus) prostredníctvom implementácie resp. integrácie do aplikácií, ktoré bežia mimo bezpečného prostredia inštitúcie. Uvedené prostredie sa z princípu musí považovať za prostredie nebezpečné a bez kontroly. Z pohľadu aplikácie je to transparentné a bez dopadu na aplikačnú logiku.

Príklady fungovania detekcie zraniteľnosti koncových obslužných bodov nájdete na: <https://www.ibm.com/security/fraud-protection/trusteer>

Samotná architektúra tohto modulu môže byť postavená na čisto aplikačnej logike, ktorá beží výlučne na strane klienta alebo aj v kombinácii so službami/komponentami bežiacimi na strane servera inštitúcie v bezpečnej infraštruktúre, kde je možné vykonávať hlbšie analýzy pre detekciu sofistikovanejších útokov alebo útokov v prípravnej fáze.

Navrhované riešenie projektu zahŕňa nasledovné techniky pre ochranu aplikácií/služieb:

Prevencia:  
Jedná sa o pasívnu ochranu aplikácií, ktorá pozostáva najmä z code obfucation, white box crytpografia, pinning certifikátov, šifrovania zdrojov, auto expirácie, vlastnej klávesnice, polymorfizmu, odstránenia testovacích dát a nebezpečných aplikačných modulov. Prevencia je mandatórna a mala by byť súčasťou metodiky bezpečného vývoja, pričom neprináša žiadne detekčné mechanizmy.

Základná detekcia:  
Detekcia je zameraná najmä na získanie rôznych atribútov prostredia, v ktorom beží aplikačná logika. Sem patrí napr. detekcia debugerov a emulácií, detekcia rootnutých alebo jailbrake-nutých zariadení, kontrola integrity, fingerprintig zariadenia resp. device binding, detekcia škodlivého kódu na zariadení.

Rozšírená detekcia:  
Sofistikované útoky , resp. rôzne realtime útoky zväčša nie je možné detegovať základnými metódami a je nutná značná systémová a analytická podpora. Do rozšírených metód detekcie patrí detekcia botnetov, metódy na detekciu script injections, api injections, RASP, mutlifactor adaptívna autentifikácia a autorizácia, behaviorálna analýza a detekcia crossesion útočných vektorov.

VÝHODY Detekcie zraniteľnosti koncových obslužných bodov:

* Zisťovanie zraniteľností v reťazci služieb
* Možnosť proaktívneho začatia protiopatrení
* Zvyšovanie spokojnosti koncových používateľov / zákazníkov
* Skrátenie času a úsilia nápravy incidentov približne o 80%
* Eliminácia bezpečnostných incidentov o 75%

Základné princípy integrácie do nových a bežiacich aplikácií (GOVNET isvs\_404,):

1. Udalosti musia byť integrované do SIEM systému NASES využívaných v SOC a následná analýza interným CSIRT tímom;
2. Je to robustný analytický nástroj pre detekciu komplexných útočných vektorov;
3. Možnosť integrácie do WEB-ových (vrátane SPA) a Mobilných aplikácií (Android, iOS);
4. Zabezpečenie multikanálového a multitenantného prístupu;
5. Pre podporu multifaktor autentifikácie resp. risk based autentifikácie sys poskytne rizikové skóre. Aktuálne na Slovensku nie je multifaktor autentifikácie resp. risk based autentifikácie sys.

Navrhované riešenie je bežne dostupné v komerčnom sektore v zahraničí. Príklady sú uvedené v štúdií od medzinárodnej konzultačno-poradenskej spoločnosti Forrester, link: https://tools.totaleconomicimpact.com/go/microsoft/CloudAppSecurity/

Na základe vyššie uvedeného bude **hlavným cieľom projektu** vybudovať riešenie - Modul pre detekciu hrozieb a prienikov na strane klienta a ceste mimo infraštruktúry NASES.

## 3.2.         Motivácia a rozsah projektu

Motiváciou projektu je zníženie dopadov kybernetických útokov, či už finančných, ako aj reputačných, v rámci služieb poskytovaných NASES. Ďalšou motiváciou je naplnenie legislatívy - zákona o kybernetickej bezpečnosti, ktorý definuje národnú jednotku, vládnu jednotku a sektorové jednotky CSIRT, ako aj napĺňanie stratégie kybernetickej bezpečnosti EÚ. V podmienkach digitálneho a kybernetického priestoru SR sú v zmysle Národnej stratégie pre informačnú bezpečnosť v SR a Operačného programu Integrovaná infraštruktúra 2014 – 2020 zavádzané opatrenia, najmä proti úniku informácií a ich neoprávnenému použitiu, narušeniu integrity údajov, porušeniu práv občanov na ochranu osobných údajov a na ochranu pred poškodzovaním a zneužívaním informačných a komunikačných systémov. Projekt v súvislosti s narastajúcou aktivitou v digitálnom priestore postupuje v zmysle opatrení obsiahnutých v Stratégii kybernetickej bezpečnosti EÚ.

**Hlavným prostriedkom na dosiahnutie cieľa projektu** bude rozšírenie poskytovaných služieb na GOVNETE, prostredníctvom nového modulu pre detekciu hrozieb na strane klienta a ceste mimo infraštruktúry NASES. Najzraniteľnejším bodom komunikačnej reťaze je zariadenie klienta, ako aj samotný občan. Využívaním moderných architektúr, kedy sa dbá na vysokú užívateľskú skúsenosť, rýchly vývoj, sprístupňovanie API rozhraní do internetu sa prenáša veľká časť aplikačnej a business logiky z bezpečného prostredia dátového centra inštitúcie do nebezpečného prostredia internetu, zariadenia alebo infraštruktúry klienta, odkiaľ využíva dané služby.

Hlavnou ideou bude implementácia nového modulu pre detekciu hrozieb a prienikov v spojitosti s používaním aplikácií občanmi mimo infraštruktúry Dátového centra, t.j. implementácia riešenia a mechanizmov pre cielenú detekciu už potencionálnych prienikov v čase prípravy (ZERO DAY ATTACK) nezávisle na aplikácii a technológií.

InAppSecurity, resp. detekcia zraniteľností na úrovni session a koncových zariadení beží transparentne od  iných business procesov, môže ovplyvniť každý jeden  business proces/životnú situáciu ktorú rieši občan. Ako bolo spomínané detekcia je transparentná avšak implementáciou preventívneho módu môže dôjsť k intervencii do používateľskej session. Príklad: Ak systém deteguje relevantnú hrozbu v aplikácii resp. na zariadení v už prihlásenej session, počas vykonávania ľubovoľnej  aktivity používateľom systém môže pomocou API vykonať preventívny krok, napr. zablokovať používateľa, zrušiť session.

Z pohľadu samotného modulu pre detekciu hrozieb na koncových zariadeniach a v rámci session sa  jedná o špecifický business proces z kategórie bezpečnostných, ktoré sú zodpovedné za ochranu služby pred hrozbami mimo siete prevádzkovateľa.

## 3.3.         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. | Ministerstvo investícií, regionálneho rozvoja a informatizácie SR | MIRRI | Poskytovateľ služieb centrálnej platformy integrácie údajov | Sieť GOVNET isvs\_404, |
| 2. | Národná agentúra pre sieťové a elektronické služby | NASES | Vlastník procesu | Sieť GOVNET isvs\_404, |
| 3. | Občan/Podnikateľ/OVM |  | Používateľ | Sieť GOVNET isvs\_404, |

## 3.4.         Ciele projektu a merateľné ukazovatele

**V projekte sa predpokladá s nasledujúcim merateľným ukazovateľom:**

***Merateľný programový ukazovateľ OP II, ktorý bude naplnený realizáciou projektu***

**Ciele/Merateľné ukazovatele**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **CIEĽ** | **NÁZOV MERATEĽNÉHO A VÝKONNOSTNÉHO UKAZOVATEĽA (KPI)** | **POPIS UKAZOVATEĽA** | **MERNÁ JEDNOTKA** (v čom sa meria ukazovateľ) | **AS-IS MERATEĽNÉ VÝKONNOSTNÉ HODNTOY** (aktuálne hodnoty) | **TO-BE  MERATEĽNÉ VÝKONNOSTNÉ HODNTOY** (cieľové hodnoty projektu) | **SPÔSOB ICH MERANIA/**  **OVERENIA  PO NASADENÍ** (overenie naplnenie cieľa) | **POZNÁMKA** |
| sem vpíšte identifikáciu /číslo ukazovateľa | sem vpíšte názov cieľa | sem vpíšte názov ukazovateľa (KPI) | sem vpíšte popis ukazovateľa | sem vpíšte - čas, početnosť, financie,... | sem vpíšte aktuálne namerané hodnoty, ktoré chcete realizáciou projektu zlepšiť | sem vpíšte cieľové hodnoty, ktoré chcete dosiahnuť realizáciou cieľa (napr.  \_Zrýchlenie poskytnutia služby (čas), \_Zvýšenie počtu poskytnutých služieb (početnosť), \_Zníženie nákladov na proces (financie), ... atď. | sem vpíšte spôsob (metódu / postup), ako sa po nasadení overí naplnenie cieľa (naplnenie KPI) | sem vpíšte spôsob (metódu / postup), ako sa po nasadení overí naplnenie cieľa (naplnenie KPI) |
| 1 | ŠC 7.9: Zvýšenie kybernetickej bezpečnosti v spoločnosti | P0048-Dodatočný počet informačných systémov verejnej správy s implementovaným nástrojom na rozpoznávanie, monitorovanie a riadenie bezpečnostných incidentov | Ukazovateľ vyjadruje počet systémov podporených z projektu z celkového počtu realizovaných systémov v rámci OP, ktoré majú implementované nástroje na centrálne rozpoznávanie, monitorovanie a riadenie bezpečnostných incidentov, ako ich odhaľovanie, zaznamenávanie detailov a mitigovanie a sú zapojené do centrálneho systému monitorovania bezpečnosti. | počet | 0 | 1 | Kontrola počtu úspešne implementovaných nástrojov u prijímateľa. | Nástroj slúži na mitigovanie bezpečnostných incidentov a centrálne riadenie rizík. |
| 2 | ŠC 7.9: Zvýšenie kybernetickej bezpečnosti v spoločnosti | P0167 - Počet informačných systémov VS zapojených do centrálneho systému monitorovania bezpečnosti v rámci VS | Ukazovateľ vyjadruje počet informačných systémov verejnej správy, ktoré majú implementované nástroje na centrálne rozpoznávanie, monitorovanie a riadenia bezpečnostných incidentov, ako ich odhaľovanie, zaznamenávanie detailov a mitigovanie a ktoré sú zapojené do centrálneho systému monitorovania bezpečnosti. | Počet | 0 | 3 | Kontrola počtu ISVS s úspešne implementovaných nástrojom na centrálne rozpoznávanie, monitorovanie a riadenia bezpečnostných incidentov, ako ich odhaľovanie, zaznamenávanie detailov a mitigovanie. | Nástroj má byť implementovaný nad isvs\_62, Isvs\_10684, isvs\_404 |
| 3 | Zvýšenie kybernetickej bezpečnosti v spoločnosti / Zabezpečenie komplexnej kybernetickej bezpečnosti v spoločnosti | Počet chránených endpointov prostredníctvom detekcie zraniteľnosti koncových obslužných bodov | Ukazovateľ vyjadruje počet endpointov chránených prostredníctvom detekcie zraniteľnosti koncových obslužných bodov. | Počet | 0 | 300 000 | Kontrola počtu úspešne chránených endpointov implementovaným nástrojom u prijímateľa. |  |
| 4 | Zvýšenie kybernetickej bezpečnosti v spoločnosti / Zabezpečenie komplexnej kybernetickej bezpečnosti v spoločnosti | Percentuálna miera automaticky eliminovaných incidentov | Percentuálna miera automaticky eliminovaných incidentov systémom na Detekciu zraniteľnosti koncových obslužných bodov. | % | 0% | 75% | Kontrola percentuálnej miery automaticky eliminovaných incidentov voči počtu manuálne eliminovaných incidentov. |  |
| 5 | Zvýšenie kybernetickej bezpečnosti v spoločnosti / Zabezpečenie komplexnej kybernetickej bezpečnosti v spoločnosti | Percentuálna miera zníženia časovej náročnosti na elimináciu automaticky neeliminovaných incidentov | Ukazovateľ vyjadruje percentuálna miera zníženia časovej náročnosti na elimináciu automaticky neeliminovaných incidentov systémom na Detekciu zraniteľnosti koncových obslužných bodov. | % | 0% | 80% | Kontrola zníženia časovej náročnosti na elimináciu automaticky neeliminovaných incidentov o 80% po treťom roku. | Zníženie časovej náročnosti eliminácie incidentu z 96 hod. na 19,2 hod. po treťom roku od nasadenia projektu. |
| 6 | Zvýšenie kybernetickej bezpečnosti v spoločnosti / Zabezpečenie komplexnej kybernetickej bezpečnosti v spoločnosti | Zníženie času a úsilia potrebného na vykonávanie proaktívneho monitoringu | Ukazovateľ vyjadruje mieru zníženia času a úsilia potrebného na vykonávanie proaktívneho monitorovania a vyhodnocovania bezpečnostných incidentov. | Počet hodín/rok | 46 800 | 9 360 | Kontrola potrebného času na vykonávanie proaktívneho monitorovania a vyhodnocovania bezpečnostných incidentov. |  |
| 7 | Zvýšenie kybernetickej bezpečnosti v spoločnosti / Zabezpečenie komplexnej kybernetickej bezpečnosti v spoločnosti | Zníženie pravdepodobnosti úniku dát | Ukazovateľ vyjadruje mieru zníženia pravdepodobnosti úniku dát v dôsledku nasadenia systému na Detekciu zraniteľnosti koncových obslužných bodov. | % | 1,5% | 0,9% | Expertný odhad miery pravdepodobnosti úniku dát po nasadení systému na Detekciu zraniteľnosti koncových obslužných bodov do prevádzky. |  |

**Špecifikácia potrieb koncového používateľa**

IRELEVANTNÉ- nejedná sa o vývoj aplikácie a projekt nemá frontend

## 3.5.         Riziká a závislosti

|  |  |  |  |
| --- | --- | --- | --- |
| Neschválenie financovania projektu z OP II PO 7 | Stredné riziko | Nízky dosah | Vytvorenie potrebnej dokumentácie v požadovanej kvalite a rozsahu. |
| Nedostatok zamestnancov s potrebnou odbornosťou a skúsenosťami | Pravdepodobné riziko | Vysoký dosah | Celková zmena stratégie odmeňovania, motivovania a udržania si zamestnancov v IT oblasti v rámci verejnej správy. Vzhľadom na možnosti ovplyvniť takúto stratégiu je potrebné využitie zdroje OP EVS. |
| Nedodržanie pravidiel verejného obstarávania | Stredné riziko | Extrémny dosah | Realizácia VO s odbornou starostlivosťou. |
| Výrazná zmena strategických cieľov a princípov pred ukončením projektu | Stredné riziko | Vysoký dosah | Sledovanie výstupov MIRRI, pravidelná komunikácia s gestorom – MIRRI (prostredníctvom Programovej kancelárie VS) v rámci každého projektového míľnika. |
| Implementačný tím nebude mať dostatočnú kapacitu, vedomosti a schopnosti | Slabé riziko | Nízky dosah | Stanoviť prísne požiadavky na kľúčových expertov a ich participáciu počas celého trvania projektu. |
| Služby nebudú poskytované v dostatočnej kvalite (vyskytne sa veľké množstvo chýb, dlhé doby odozvy a pod.) | Stredné riziko | Stredný dosah | Pravidelné vyhodnocovanie pripravenosti riešenia projektu a určiť zodpovedné osoby za jednotlivé výstupy projektu. |
| Náklady na realizáciu projektu sa vymknú kontrole | Slabé riziko | Vysoký dosah | Dôsledne zabezpečiť finančné riadenie a akceptačné konanie. |
| Zmeny obstarávacích cien v čase realizácie projektu | Slabé riziko | Vysoký dosah | Prehodnotiť rozpočet po každej etape. |
| Začatie komunikácie s gestorom predmetnej legislatívy | Pravdepodobné riziko | Stredný dosah | Včasné začatie komunikácie s gestorom predmetnej legislatívy. |

## 3.6.         Alternatívy a Multikriteriálna analýza

Spoločný cieľ pre modul detekcie a hrozieb je minimalizovať stratu a chrániť značku z pohľadu reputačného rizika. Okrem iného z pohľadu úspešnosti detekcie je nutné sa pozerať na problematiku  holisticky, tj.  Aj z pohľadu funkcionality aplikácií, typu aplikácií, určenia a samotných potencionálnych strát.

Ideálny stav je detekcia  hrozieb z vonka v štádiu prípravy (Zero Day Detekcia), t.j .v čase kedy ešte k samotnému útoku neprichádza.

Rovnako kľúčovým parametrom je schopnosť detekcie samotného útoku na koncového používateľa (MIM, MITB, Session... ) pretože v tomto prípade je možné vykonať proaktívne aktivitu a zabrániť škodám v čase prípravy.

### Alternatíva A – „Žiadne riešenie, t.j. nebude sa implementovať modul pre detekciu zraniteľností na koncových zariadeniach"

|  |
| --- |
| **Súhrnný popis** |
| Alternatíva hovorí o tom, že detekcia zraniteľností a prienikov nebude implementovaná, t.j. detekčné procesy budú prebiehať tak ako doteraz. V súčasnosti aktuálny stav v oblasti bezpečnosti detekcie zraniteľnosti koncových obslužných bodov nie je dostatočne zabezpečený. Nemáme informácie, že navrhovaný modul je prevádzkovaný v štátnom sektore v Slovenskej republike |

### Alternatíva B – „Plný scope pre modul detekcia hrozieb a prienikov, t.j. integrácia Detekcia zraniteľnosti koncových obslužných bodov a transakčného monitoringu"

|  |
| --- |
| **Súhrnný popis** |
| Jedná sa o komplexné riešenie zväčša pozostávajúce s viacerých komponentov, pričom Detekcia zraniteľnosti koncových obslužných bodov je *zodpovedná* za session a endpoint a transakčný monitoring za detekciu podozrivých operácií na úrovni business transakcií. |
|  |
| Veľmi komplexný systém, TXM komponent je nutné hlbšie integrovať do aplikačnej architektúry aplikácii s hlbokou analýzou business operácií a ich zraniteľností. V zásade sa jedná, že každá relevantná business operácia by musela byť integrovaná s TXM systémom na úrovni API, pričom kontrolovaná aplikácia musí byť modifikovaná pre nielen z pohľadu interného flow funkcií ale aj z pohľadu používateľského rozhrania. |
| TXM má obmedzené možnosti detekcie  hrozieb resp. útokov v štádiu prípravy a vyžaduje sa hlbšiu integráciu do prostredia aplikácie, čo má za následok dlhú dobu implementácie a skutočné benefity z implementácie daného riešenia prichádzajú  neskôr v čase. Samozrejme podmienkou je implementácia alternatívy C. |

### Alternatíva C – „Modul detekcie zraniteľnosti a podozrivého správania na úrovni koncového zariadenia alebo session"

|  |
| --- |
| **Súhrnný popis** |
| Jedná sa o riešenie, ktoré je zväčša transparentne integrované s už bežiacimi aplikáciami. Samozrejme otvorené pre ďalšie rozširovanie o transakčný monitoring. |
|  |
| Riešenie je jednoducho a rýchlo integrovateľný do prostredia, je otvorený pre hlbšiu *integráciu* s aplikáciami alebo TXM systémom, poskytuje prehľady a analytický nástroj pre SOC a CSIRT.  Je možné implementovať riešenie bez dotknutia aplikačnej logiky. |

### 3.6.1.      Stanovenie alternatív pomocou biznisovej vrstvy architektúry

Na stanovenie alternatív vplývali nasledovné témy:

* Minimalizovať náklady obstaranie modulu detekcie hrozieb;
* Minimalizovať riziká útokov/hrozieb na informačný systém;

Jedná sa o problémy, ktoré sa priamo aj nepriamo týkajú NASES. Napr.: Znižovať riziko eliminácie útokov a tým pádom aj znižovanie nákladov a úspory času na ich odstránenie, efektívne obstaranie modulu detekcie hrozieb a s tým spojené efektívne čerpanie verejných zdrojov s cieľom zachovať maximálnu bezpečnosť prenosu dát.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **KRITÉRIUM** | **ZDÔVODNENIE KRITÉRIA** | **STAKEHOLDER**  **1 MIRRI** | **STAKEHOLDER**  **2 NASES** | **STAKEHOLDER**  **3 Občan/Podnikateľ** |
| BIZNIS VRSTVA | Kritérium A | Zero Day detekcia  (Čím vyššie, tým lepšie) |  | X |  |
| Kritérium B | Rýchlosť implementácie (Čím vyššie, tým lepšie) |  | X |  |
| Kritérium C | Integrácia do prostredia resp. s aplikáciami (Čím ľahšie, tým lepšie) |  | X |  |
| Kritérium D | Detekcia hrozieb v štádiu prípravy na strane klienta (Čím vyššie, tým lepšie) |  | X |  |
| Kritérium E | Detekcia na úrovni business transkacií (Čím vyššie, tým lepšie) | X | X |  |
| Kritérium F | Finančná efektívnosť na obstaranie systému (efektívne využitie verejných zdrojov) | X | X |  |
| Kritérium G | Detekcia hrozieb na strane klienta |  |  | X |

### 3.6.2.      Multikriteriálna analýza

V rámci porovnania alternatív sa uvažovalo s troma základnými alternatívami:

1. Alt. 1 - Existujúce stav;
2. Alt. 2 - „Plný scope pre model detekcie zraniteľnosti, t.j. integrácia modulu detekcie zraniteľnosti koncových obslužných bodov a transakčného monitoringu";
3. Alt. 3. - „Modul detekcia zraniteľnosti a podozrivého správania na úrovni koncového zariadenia alebo session";

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Zoznam kritérií** | **Alternatíva**  **1** | **Spôsob**  **dosiahnutia** | **Alternatíva 2** | **Spôsob**  **dosiahnutia** | **Alternatíva**  **3** | **Spôsob**  **dosiahnutia** |
| Kritérium A | Nie | Keďže zostane AS IS stav riešenia, tak nebudú naplnené ciele PO7 OPII | Áno | Kľúčový parameter, prináša  najrýchlejšie výsledky, preventívny systém. | Áno | Kľúčový parameter, prináša  najrýchlejšie výsledky, preventívny systém. |
| Kritérium B | Nie | Keďže zostane AS IS stav riešenia, tak nebudú naplnené ciele PO7 OPII | Nie | Vzhľadom na vývoj útokov a trendov, je nutné postupovať postupne, t.j. od najrýchlejších implementácií ku veľmi komplexným, tým pádom postupne minimalizovať škody spôsobenými podvodným/nekalým správaním. | Áno | Vzhľadom na vývoj útokov a trendov, je nutné postupovať postupne, t.j. od najrýchlejších implementácií ku veľmi komplexným, tým pádom postupne minimalizovať škody spôsobenými podvodným/nekalým správaním. |
| Kritérium C | Nie | Keďže zostane AS IS stav riešenia, tak nebudú naplnené ciele PO7 OPII | Nie | Súvisí s rýchlosťou implementácia a hovorí, či je nutné, resp. nevyhnutné meniť aplikáciu na strane backendu z dôvodu spustenia systému do produkcie. | Áno | Súvisí s rýchlosťou implementácia a hovorí, či je nutné, resp. nevyhnutné meniť aplikáciu na strane backendu z dôvodu spustenia systému do produkcie. |
| Kritérium D | Nie | Keďže zostane AS IS stav riešenia, tak nebudú naplnené ciele PO7 OPII | Áno | Detekcie hrozieb a zraniteľností spojených s aplikáciou bežiacou u občana (Browser, mobil, PC ... ). | Áno | Detekcie hrozieb a zraniteľností spojených s aplikáciou bežiacou u občana (Browser, mobil, PC ... ). |
| Kritérium E | Nie | Keďže zostane AS IS stav riešenia, tak nebudú naplnené ciele PO7 OPII | Áno | Detekcia hrozieb na úrovni business transakcií. | Áno | Detekcia hrozieb na úrovni business transakcií. |
| Kritérium F | Nie | Keďže zostane AS IS stav riešenia, tak nebudú naplnené ciele PO7 OPII | Nie | Finančná efektívnosť na obstaranie systému (efektívne využitie verejných zdrojov) | Áno | Finančná efektívnosť na obstaranie systému (efektívne využitie verejných zdrojov) |
| Kritérium G | Nie | Keďže zostane AS IS stav riešenia, tak nebudú naplnené ciele PO7 OPII | Áno | Detekcia hrozieb na strane klienta | Áno | Detekcia hrozieb na strane klienta |

Výber alternatív prebieha na úrovni biznis vrstvy prostredníctvom MCA zostavenej na základe kapitoly Motivácia, ktorá obsahuje ciele stakeholderov, ich požiadavky a obmedzenia pre dosiahnutie uvedených cieľov.

Niektoré (nie všetky) kritériá môžu byť označené ako KO kritériá. KO kritériá označujú biznis požiadavky na riešenie, ktoré sú z hľadiska rozsahu identifikovaného problému a motivácie nevyhnutné pre riešenie problému a všetky akceptovateľné alternatívy ich tak musia naplniť. Alternatívy, ktoré nesplnia všetky KO kritériá, môžu byť vylúčené z ďalšieho posudzovania. KO kritériá nesmú byť technologické (preferovať jednu formu technologickej implementácie voči druhej).

### 3.6.3.      Stanovenie alternatív pomocou aplikačnej vrstvy architektúry

IRELEVANTNÉ- z dôvodu, že sa nejedná o agendový systém

### 3.6.4.      Stanovenie alternatív pomocou technologickej vrstvy architektúry

IRELEVANTNÉ- z dôvodu, že sa nejedná o agendový systém

# 4.     POŽADOVANÉ VÝSTUPY  (PRODUKT PROJEKTU)

Z pohľadu výstupov je projekt realizovaný v 1 inkremente, ktorého trvania je predpokladané na 9 mesiacov, pričom bude realizovaný v prostredníctvom nasledujúcich fáz:

* Analýza a dizajn
* Nákup HW a príslušného SW
* Implementácia
* Testovanie
* Nasadenie

Výsledným produktom bude dodané komplexné riešenia modulu pre detekciu hrozieb a prienikov na strane klienta a ceste mimo infraštruktúry NASES, a vlastníkom tohto procesu bude NASES, nakoľko v zmysle zákona o IS VS jej hlavnou úlohou a predmetom činnosti  je správa, prevádzka a rozvoj vládnej dátovej siete GOVNET a prevádzka a rozvoj služieb Ústredného portálu verejnej správy, ako základných nástrojov informatizácie verejnej správy na Slovensku.

Bude sa jednať o formu prenosu informácií, ktorá bráni tretím stranám prístupu k prenášaných údajov, ktoré sa prenášajú z jedného zariadenia do druhého. T.j., že sa jedná o formu prenosu dát, kedy odosielané dáta zo zariadenia odchádzajú zašifrované a rozšifrovať ich môže len prijímateľ. Inými slovami, dáta sú šifrované v zariadení odosielateľa, a potom sa odosielajú do zariadenia príjemcu v nečitateľnom formáte, a následne sú v zariadení príjemcu dekódované. Okrem šifrovania prenášaných dát nám dané riešenie prináša vďaka asymetrickej kryptografii aj ďalšie bezpečnostné prvky, ako je **dôveryhodnosť** **prenášaných dát a ich integrita**. **Dôveryhodnosť** dátznamená, že nám nikto nemôže poslať dáta tak, že by sa vydával za niekoho iného. **Integrita** dát zasa znamená, že počas cesty nedošlo ku zmene obsahu, čo je tiež forma útoku. Niekto dáta po ceste odchytí, upraví a pošle ďalej ich pôvodným smerom.

## 4.1.         NÁHĽAD ARCHITEKTÚRY

**Biznis architektúra:**

|  |
| --- |
| *Implementácia ESD* riešenia dopĺňa službu GOVNET o nové možnosti detekcie zraniteľností a hrozieb  pre služby poskytované Nasesom. Nedochádza k modifikácii business kontextu ani business procesom poskytovaných nadradenými službami, napr. www.slovensko.sk  T.j. ESD riešenie z pohľadu business procesov aplikácie alebo riešenie môže ostať nezmenený alebo sa môže ľahko zmeniť aplikačná logika v závislosti na riziku.  Z pohľadu SOC a CSIRT sa dopĺňa ďalší zdroj udalostí pre analýzu a nápravne aktivity. |
| C:\01489c2df065d29891614781cf2fb62e  Obrázok popisuje generický scenár kedy dochádza k prihláseniu občana do aplikácie od momentu kedy si spustí aplikáciu (WEB, Mobile). Riešenie ESD monitoruje proaktívne atribúty a stav na úrovni koncového zariadenia, vykonáva „fingerprinting“ a behaviorálnu analýzu z pohľadu občana, zariadenia, lokality a session. Táto detekcia prebieha na pozadí a je nezávislá od interakcie občana s aplikáciou. V prípade zvýšenej hrozby je odoslaná správa do SOC, CSIRT. V prípade úzkej integrácie pri zvýšenom riziku je informovaná aplikácia z dôvodu obranných mechanizmov (zrušenie session ,zablokovanie , odhlásenie .. ).  Jedná sa o príklad, ako ESD vstupuje transparentne do všetkých používateľských procesov, napr. prihlásenie, otvorenie schránky, správy, použitie mID....). Jedna sa o monitoring aplikácie, podobne ako to robia bežne antivírusové programy inštalované na PC, tj nezávislé od monitorovanej aplikácie, resp monitorovaná aplikácia nevie o tom, že je monitorovaná.  V zásade sa jedná o štatistické riešenie postavené na pravidlách alebo AI.  Keďže riešenie môže bežať nezávislé od aplikácie, v tzv, silent móde, alebo aj v integrovanom móde je nutné zadefinovať základné rizikové parametre pre výberové konanie riešenia.  False Positive Ratio (FPR) : pomer zle označených udalostí zo všetkých korektných udalostí, resp. sa jedna o nesprávne netegované prípady.  Detection Rate (DR), True positive : je citlivosť, tj. Pomer správne detekovaných oproti všetkým čo mali byť detegovaný.  Ideálny scenár je mať čo najnižšie FPR a najvyššie DR, čo je technicky veľmi obtiažne a závislé od samotnej aplikácie, samotnej integrácie a riešenia modulu pre detekciu hrozieb a prienikov. |

#### Architektúra informačných systémov:

|  |
| --- |
| *Architektúra riešenia pre detekciu hrozieb - je vlastnostné riešenie konkrétneho dodávateľa*, avšak princípy integrácie do *prostredia* NASES ostávajú nemenné.  *Na začiatku* sa predpokladá silent-mode , t.j. integrácia bez užšej aplikačnej integrácie, tj. ESD riešenie bude bežať v transparentnom móde.  Tento transparentný mód je nutný z toho dôvodu, že sa jedná o štatistické riešenie, ktoré si vyžaduje určité ladenie pre dosiahnutie optimálneho FPR a DR. Neoptimálne FPR a DR majú za následok vyššiu administratívnu  záťaž na SOC a CSIRT resp. znižujú používateľskú prítulnosť , resp. zvyšujú nespokojnosť  občanov s používaním aplikácie. Po vyladení riešenia na požadované hodnoty je možné využiť existujúci PUSH/PULL model integrácie s už integrovanými komponentami a automaticky vykonať nápravné akcie, napr. blokácia IP  Z pohľadu implementácie sa jedná o doplnenie technologických komponentov do služby govnet, tak aby sa zvýšil rozsah detekovateľných hrozieb spojených s publikovaním aplikácií prostredníctvom služby Govnet. |

#### Technologická architektúra:

|  |
| --- |
| Riešenia pre detekciu hrozieb a prienikov väčšinou fungujú autonómne. Vyžadujú si dedikovaný HW alebo môžu byť využívané ako cloud PaaS služby. Z dôvodu, že NASES prevádzkuje kritickú infraštruktúru, *bude využívať riešenia inštalované prostredí resp. DC NASES*.  Predpokladom je, že súčasťou dodávky riešenia je dodávka infraštruktúrnych komponentov.  K samotnému riešeniu následne sa bude pristupovať ako k „appliance“ t.j. ako hotovému, predkonfigurovanému riešeniu s jasne popísanými integračnými postupmi.    NASES poskytuje Govnet službu, rovnako prevádzkuje aj SOC, manažuje gov doménu a rovnako je aj prevádzkovateľom UPVS. ESD je postavené na využívaní as-is infraštruktúry Govnet a SOC pričom infraštruktúra sa dopĺňa/vylepšuje o ďalšie komponenty, sú vyznačené červenou.  ADC (application delivery controler), v prostredí Govnet sa využívajú produkty F5. Tieto komponenty musia byť rozšírené z pohľadu výkonu a funkcionality, aby bolo možné integrovať ESD službu.  ESD je služba, implementovaná ako PaaS,SaaS ale onPremise riešenie ako súčasť govnetu, ktorá využíva dáta získané z ADC pre hĺbkovú analýzu a následnú detekciu potencionálneho rizika. Túto hrozbu, udalosť následne posiela na analýzu do SOC.  Služba SOC je natívna súčasť služby Govnet. Množstvo udalosti, ktoré SOC spracováva sa rozšíri o veľkú množinu udalostí z ESD. Z dôvodu skvalitnenia, urýchlenia a zníženie false positive rate eventy budú následne korelované a spracovávané SOAR komponentom, čím sa zabezpečí udržanie personálnych nákladov potrebných pre analýzu rizík/udalostí.  Dodávkou projektu sa tým pádom rozumie:   1. ADC komponenty (HW) pre zvládnutie integrácie, tak aby nedošlo k zníženiu kvality poskytovaných služieb \*.slovensko.sk, resp \*.gov.sk 2. ESD komponent (HW/SW/SaaS) pre analýzu špecifických zraniteľností na úrovni koncových zariadení a session 3. SOAR komponent (SW) ako rozširujúci sw modul aktuálneho SOC podporného systému, ktorý bol implementovaný v rámci projektu NKIVS Zdôvodnenie použitia SOAR licencií tvorí prílohu č.3 projektového zámeru. |
|  |

## 4.2.         APLIKAČNÁ VRSTVA - POŽIADAVKY NA DODRŽANIE DÁTOVÝCH ŠTANDARDOV

**IRELEVANTNÉ**- celá kapitola aj s podkapitolami irelevantná z dôvodu, že bezpečnostné riešenie nepracuje s dátovými objektmi.

## 4.2.1.      ROZSAH INFORMAČNÝCH SYSTÉMOV

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Názov informačného systému VS** | **Kód v META IS** | **Modul ISVS**  Zaškrtnite ak ISVS je modulom | **Stav IS VS** | **Typ IS VS** | **Názov nadradeného ISVS**  V prípade zaškrtnutého checkboxu pre modul ISVS |
|  |  | ☐ | Vyberte jednu z možností. | Vyberte jednu z možností. |  |
|  |  | ☐ | Vyberte jednu z možností. | Vyberte jednu z možností. |  |
|  |  | ☐ | Vyberte jednu z možností. | Vyberte jednu z možností. |  |
|  |  | ☐ | Vyberte jednu z možností. | Vyberte jednu z možností. |  |
|  |  | ☐ | Vyberte jednu z možností. | Vyberte jednu z možností. |  |

Tabuľka 1 Prehľad dotknutých informačných systémov v projekte

Modul ISVS môže mať len jeden materský ISVS. Modul ISVS nesmie mať vzťah na iný modul ISVS. Samostatný ISVS bez modulu, nesmie mať vzťah na žiadny ISVS.

Povinnosť používať spoločné moduly ÚPVS definuje zákon e-Governmente. V prípade, ak IS povinnej osoby využíva funkcionalitu, resp. služby niektorého Spoločného modulu, v MetaIS sa pri danom IS povinnej osoby vytvorí aplikačná služba s názvom "Využitie Spoločných modulov UPVS" a naviaže sa na tú aplikačnú službu/služby ÚPVS na externú integráciu, ktoré využíva. Zdrojom je vždy AS Spoločného modulu.

Používateľská príručka centrálneho metainformačného systému verejnej správy číslo 6546/2020/oSAEG-1 - (<https://metais.vicepremier.gov.sk/help>)

|  |  |  |
| --- | --- | --- |
| **Kód v META IS** | **Názov** | **AS na externú integráciu (využitie Spoločného modulu)** |
| **isvs\_8846** | **Autentifikačný modul IAM** | Autentifikácia používateľa na ÚPVS (BOK) (as\_59698) |
| **isvs\_8847** | **Elektronické schránky** | Vytváranie, odosielanie a prijímanie elektronických správ (as\_59630) |
| **isvs\_8848** | **Modul elektronických formulárov** | Poskytnutie vzorov e\_formulárov (sluzba\_is\_185) |
| **isvs\_9369** | **Modul elektronického doručovania** | Centrálne úradné doručovanie (as\_59701) |
| **svs\_8850** | **Platobný modul** | Realizácia platieb správnych a súdnych poplatkov (as\_59700) |
| **isvs\_9368** | **Modul centrálnej elektronickej podateľne** | Overovanie elektronického podpisu (KEP) (as\_59702) |
| **isvs\_8851** | **Modul dlhodobého uchovávania (nepovinný)** | Uchovávanie elektronických dokumentov (as\_59703) |
| **isvs\_9370** | **Notifikačný modul (nepovinný)** | Zasielanie oznámení prostredníctvom elektronických komunikačných kanálov (sms, email) (as\_59699) |
| **Isvs\_5836** | **Modul procesnej integrácie a integrácie údajov (jeho časť IS CSRÚ)** | Publikovanie informácií na webovom sídle [oversi.gov.sk](http://oversi.gov.sk) (as\_59881), Služba volania technického používateľa CSRÚ (as\_59119), Asistované poskytnutie výpisu o kontrole kvality referencovaných údajov voči referenčným údajom Informačného systému CSRU (as\_49259), Poskytnutie konsolidovaných údajov o subjekte (as\_49250),  Poskytnutie údajov z Informačného systému centrálnej správy referenčných údajov na synchronizáciu (as\_49253), Poskytnutie výpisu o kontrole kvality referencovaných údajov voči referenčným údajom Informačného systému CSRU(as\_49258), Zápis údajov do Informačného systému centrálnej správy referenčných údajov verejnej správy (as\_49251) |

Tabuľka 2 Prehľad spoločných modulov a aplikačných služieb.

## 4.2.3.      PREHĽAD IS NA EXTERNÚ INTEGRÁCIU SPOLOČNÝCH MODULOV UPVS

Prehľad integrácii spoločných modulov v súlade so zákonom č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente) v znení neskorších predpisov (najmä § 10 a nasl.)

|  |  |  |
| --- | --- | --- |
| **Názov informačného systému VS** | **Kód ISVS v META IS** | **Spoločné moduly podľa zákona č. 305/2013  e-Governmente** |
|  |  |  |

Tabuľka 3 Prehľad integrácii informačných systémov na spoločné moduly

## 4.2.4.      INTEGRÁCIA NA NADREZORTNÉ CENTRÁLNE BLOKY

Aplikačné služby môžu mať aj špecifické funkcie. Okrem sprístupňovania aplikačnej funkcie alebo získavanie údajov z iných ISVS, rozlišujeme aj AS slúžiace na evidenciu napojenia konkrétneho IS na nadrezortné centrálne bloky. Vytvorením takéhoto vzťahu medzi AS môjho ISVS a AS nadrezortného centrálneho bloku označujeme, že ISVS využíva funkcionalitu bloku. Zoznam Nadrezortných centrálnych blokov tvorí prílohu (**príloha č.8**) používateľskej **príručky pre META IS**. <https://metais.vicepremier.gov.sk/help>

Do tabuľky uvedenej nižšie je potrebné vypísať prípadne využitie nadrezortných centrálnych systémov prípadne ich jednotlivých modulov.

|  |  |  |
| --- | --- | --- |
| **Názov informačného systému VS** | **Názov nadrezortného ISVS** | **Modul nadrezortného ISVS** |
| **ISVS 1** |  |  |
| **ISVS 2** |  |  |
| **...** |  |  |
| **...** |  |  |
| **...** |  |  |

Tabuľka 4 Prehľad integrácii informačných systémov na nadrezortné bloky verejnej správy

Obrázok 1: Prehľad informačných systémov dotknutých v projekte

## 

## 4.2.5.      INTEGRÁCIA NA MODUL PROCESNEJ INTEGRÁCIE A INTEGRÁCIE ÚDAJOV (IS CSRÚ)

V prípade poskytovania alebo konzumovanie referenčných údajov z IS CSRÚ, je potrebné vytvoriť integračnú väzbu na modul proces integrácie a integrácie údajov podľa  § 10 ods. 11 zákona č 305/2013 Z. z. zákon o e-Governmente a príslušné aplikačné služby . Modul procesnej integrácie a integrácie údajov zabezpečuje prostredie pre elektronickú komunikáciu medzi informačnými systémami v správe rôznych orgánov verejnej moci elektronicky. Tieto integračné väzby a aplikačné služby je potrebné vzťahom AS slúži AS naviazať na služby IS CSRÚ. Detailný popis funkcionalít a služieb IS CSRÚ sa nachádza v dokumente: [Integračný manuál služieb IS CSRÚ](https://datalab.digital/wp-content/uploads/Integracny_manual_sluzieb_IS_CSRU_v1.7.1.docx) (<https://datalab.digital/dokumenty/>)

|  |  |  |
| --- | --- | --- |
| **ID** | **Názov** (integrovaného) **informačného systému VS** | **Integrácie ISVS na IS CSRÚ** |
| **1** |  | ☐ |
| **2** |  | ☐ |
| **3** |  | ☐ |
| **4** |  | ☐ |
| **5** |  | ☐ |
| **x** |  | ☐ |

Tabuľka 5 Prehľad integračných väzieb medzi IS VS a IS CSRÚ

## 4.2.6.      POSKYTOVANIE ÚDAJOV

V MetaIS je potrebné vytvoriť aplikačnú službu s názvom "Poskytnutie údajov z Registra XY", ktorá je poskytovaná na externú a túto AS vzťahom (ISVS realizuje AS) naviazať na príslušný register.

Pre takto vytvorenú službu "Poskytnutie údajov z Registra XY" následne vytvoríme vzťah na aplikačnú službu CSRU as\_59119 "Služba volania technického používateľa CSRÚ" (zdroj služba Poskytnutie údajov z Registra XY, cieľ služba CSRU).

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **Názov informačného systému VS** | **Názov** (poskytovaného) **objektu evidencie** | **Poskytovanie údajov do IS CSRÚ** |
| **1** |  |  | ☐ |
| **2** |  |  | ☐ |
| **3** |  |  | ☐ |
| **4** |  |  | ☐ |
| **5** |  |  | ☐ |
| **x** |  |  | ☐ |

Tabuľka 6 Prehľad informačných systémov určených na poskytovanie do IS CSRÚ

## 4.2.7.      KONZUMOVANIE ÚDAJOV

V MetaIS je potrebné vytvoriť aplikačnú službu s názvom "Konzumácia údajov z CSRÚ", ktorá nie je poskytovaná na externú integráciu a túto AS vzťahom (ISVS realizuje AS) naviazať:

* ak máme CIP – na Centrálnu integračnú platformu (CIP),
* ak nemáme CIP - na môj IS, ktorý potrebuje konzumovať údaje z CSRÚ.

Pre takto vytvorenú službu "Konzumácia údajov z CSRÚ" následne vytvoríme vzťah na aplikačnú službu CSRU sluzba\_is\_49253 "Poskytnutie údajov z Informačného systému centrálnej správy referenčných údajov na synchronizáciu" (zdroj služba CSRU, cieľ služba Konzumácia údajov z CSRU).

[Súčasné dostupné objekty evidencie a údaje v IS CSRÚ](https://datalab.digital/wp-content/uploads/CSRU_poskytovatelia_polozky_v3.xlsx) **(**<https://datalab.digital/referencne-udaje/dostupne-udaje-v-is-csru/)>

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Názov informačného systému VS** | **Názov (konzumovaného) objektu evidencie** | **Kód v META IS zdrojového ISVS** | **Konzumovanie údajov z IS CSRÚ** |
| **1** |  |  |  | ☐ |
| **2** |  |  |  | ☐ |
| **3** |  |  |  | ☐ |
| **4** |  |  |  | ☐ |
| **5** |  |  |  | ☐ |
| **x** |  |  |  | ☐ |

Tabuľka 7 Prehľad informačných systémov určených na konzumovanie z IS CSRÚ

Obrázok 2: Príklad integrácie na IS CSRÚ

# 4.3    DÁTOVÁ vrstva - požiadavky na dodržanie dátových štandardov

**IRELEVANTNÉ**- celá kapitola aj s podkapitolami irelevantná z dôvodu, že bezpečnostné riešenie nepracuje s dátovými objektmi.

# 4.3.1          Údaje v správe organizácie

[Popis dátovej architektúry riešenia na úrovni objektov evidencie a vzťahov medzi nimi](https://docs.google.com/document/d/1yZ4fXDdA_NwQ5hR6hCwfjKg9qDSGNohy/edit#heading=h.2s8eyo1). Je potrebné vychádzať z metodiky Ministerstva vnútra - Metodika identifikácie, vizualizácie a referencovania údajov pri dátovom modelovaní vo verejnej správe. (<https://www.minv.sk/swift_data/source/mvsr_a_eu/fabianova/np_optimalizacia/metodika-modelovania-udajov-vs.pdf> ). Hlavné výstupy: diagram tried a štruktúrovaný popis entít a atribútov vhodný aj pre strojové spracovanie. Diagram tried vo forme úplného logického modelu.

Definovanie procesov organizácie riadenia celého životného cyklu správy údajov kde bude potrebné aj zrozumiteľne zdokumentovať dátové štruktúry, proces tvorby údajov, štatistické metodológie (ak boli použité), dátové zdroje, kontext a ďalšie aspekty manažmentu údajov.

* Proces riadenia pre manažment údajov bude zavedený nad informačnými systémami, ktoré obsahujú objekty evidencie a budú riešené v projekte.
* Po organizačnej stránke je podmienkou zavedenie role dátového kurátora (architekt), v rozsahu ako ju definuje strategická priorita Manažment údajov a strategická priorita Otvorené údaje.
* Znamená to, že v rámci aktivity zavedenie systematického manažmentu údajov dôjde (definovaným výsledkom projektu sú):
* Dátový kurátor (architekt) bude zodpovedný za koncept systematického manažmentu údajov a úpravu organizačnej štruktúry smerom k vytvoreniu rezortnej dátovej kancelárie.
* Zavedenie systematického manažmentu údajov v organizácií vrátane nastavenie príslušných procesov a metodík pre správu celého životného cyklu údajov.

# 4.3.2          DÁTOVÝ ROZSAH PROJEKTU

* Pre budované informačné systémy je potrebné vytvoriť tzv. doménový model, ktorý definuje návrh dátových prvkov súvisiacich s novým projektom v súlade s existujúcim Centrálnym modelom údajov verejnej správy. Dokument je na stiahnutie na <https://datalab.digital/dokumenty/>. Úlohou doménového modelu je vizuálne znázorniť rozsah predmetných údajov daného projektu, pričom je možné abstrahovať od nepodstatných detailov. Je platformovo nezávislý (nie je určený pre konkrétny programovací jazyk) .
* Pre modelovanie doménového modelu je potrebné stiahnuť si Centrálny model údajov verejnej správy v preferovanej distribúcii a v novom modeli použiť existujúce dátové prvky, ak tieto patria do domény projektu. Z technického pohľadu je odporučený jazyk UML alebo ArchiMate.

V prípade že sa používa dátový prvkov z Centrálneho dátového modelu je nutné použiť skrátený formu URI identifikátora daného prvku, napr. pper:PhysicalPerson je skrátený tvar <https://data.gov.sk/def/ontology/physical-person/PhysicalPerson>.. <https://metais.vicepremier.gov.sk/publicspace?pageId=59836112>

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **Register / Objekt evidencie** | **Referencovateľný identifikátor URI dátového prvku (voliteľné)** | **Popis** |
| **1** |  |  |  |
| **2** |  |  |  |
| **3** |  |  |  |
| **4** |  |  |  |
| **5** |  |  |  |
| **x** |  |  |  |

Tabuľka 8 Prehľad objektov evidencie v jednotlivých ISVS v projekte

Obrázok 3: Príklad doménového modelu

Obrázok 4: Príklad zjednodušeného doménového modelu

# 4.3.3          KVALITA a ČISTENIE ÚDAJOV

# 4.3.3.1    Zhodnotenie objektov evidencie z pohľadu dátovej kvality

Zhodnotenie objektov evidencie so zameraním sa na významnosť kvality údajov pre biznis procesy (možné riziká v dôsledku dátovej nekvality). T.j. Ak bude údaj nepresný, bude mať nesprávnu hodnotu, formát, nebude vyplnený, alebo stotožnený voči referenčnému registru, ako významne to ovplyvní príslušnú agendu.

* Zhodnotiť objekty evidencie so zameraním sa na citlivosť kvality údajov, ktorú ovplyvňuje, najmä spôsob vstupu údajov do IS. Ako budú údaje do IS zadané?
* Bude zapracovaná možnosť overenia hodnoty údaja?
* Bude zapracované pri zadávaní údajov obmedzenie hodnôt, napríklad formou číselníka, alebo podmienok?
* Dôjde k migrácii dát z iného IS? Ak áno, je potrebné zhodnotiť
* Na základe toho stanoviť prioritu (poradie dôležitosti) pre meranie dátovej kvality objektov evidencií – t.j. poradie v akom bude správca IS približne realizovať meranie dátovej kvality a čistiť údaje.
* Prvé 2 záznamy sú vyplnené ako príklad. Vymažte, resp. prepíšte ich vlastnými údajmi. Riadky v tabuľke doplňte podľa potreby.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Objekt evidencie** | **Významnosť kvality**  1 (malá) až 5 (veľmi významná) | **Citlivosť kvality**  1 (malá) až 5 (veľmi významná) | **Priorita** – poradie dôležitosti  (začnite číslovať od najdôležitejšieho) |
| **1** | Údaje o štatutárovi | 5 | 3 | 1. |
| **2** | Iné zainteresované osoby | 2 | 3 | 20. |
| **3** |  |  |  |  |
| **4** |  |  |  |  |
| **5** |  |  |  |  |
| **X** |  |  |  |  |

Tabuľka 9 Kategorizácia údajov z pohľadu ich využiteľnosti

# 4.3.3.2    ROLE a PREDBEŽnÉ PERSONÁLNE ZABEZPEČENIE PRI RIADENÍ DÁTOVEJ KVALITY

* definovanie potrebných kapacít pre zabezpečenie riadenia dátovej kvality – napr. dátový kurátor, data steward, dátový špecialista pre dátovú kvalitu, databázový špecialista, projektový manažér.

|  |  |  |
| --- | --- | --- |
| **Rola** | **Činnosti** | **Pozícia zodpovedná za danú činnosť (správca IS / dodávateľ)** |
| **Dátový kurátor** | Evidencia požiadaviek na dátovú kvalitu, monitoring a riadenie procesu | Dátový kurátor správcu IS |
| **Data steward** | Čistenie a stotožňovanie voči referenčným údajom | Pracovník IT podpory |
| **Databázový špecialista** | Analyzuje požiadavky na dáta, modeluje obsah procedúr | Dodávateľ |
| **Dátový špecialista pre dátovú kvalitu** | Spracovanie výstupov merania, interpretácie, zápis biznis pravidiel, hodnotiace správy z merania | Dátový špecialista pre dátovú kvalitu – nová interná pozícia v projekte |
| **\*Iná rola (doplniť)** |  |  |

Tabuľka 10 Prehľad rolí a personálneho zabezpečenia pre riadení dátovej kvality

# 4.4          REFERENČNÉ ÚDAJE

**IRELEVANTNÉ**- celá kapitola aj s podkapitolami irelevantná z dôvodu, že bezpečnostné riešenie nepracuje s dátovými objektmi.

# 4.4.1       Objekty evidencie z pohľadu procesu ich vyhlásenia za referenčné

V predchádzajúcich kapitolách boli identifikované integrácie ISVS na IS CSRÚ. V tejto kapitole je potrebné definovať rozsah a štruktúru na úrovni registrov / objektov evidencie / údajov, ktoré sa navrhujú vyhlásiť za referenčné v naviazanosti na ich z realizovateľné vzájomné zdieľanie medzi subjektami verejnej správy a dodržanie pravidla, že za referenčné údaje/atribúty sú vyhlasované také údaje/atribúty, ktoré sú k subjektu evidencie jedinečné a práve tie, ktoré využívajú subjekty verejnej správy pri realizácii princípu „1 x a dosť“.

* Posúdiť navrhované objekty evidencie k vyhláseniu za referenčné z pohľadu ich dátovej kvality v zmysle podkapitoly venujúce sa kvalite a čisteniu údajov.
* Zabezpečiť dostupnosť poskytovania navrhovaných objektov evidencie za referenčné (t.j. v rámci nich údaje/atribúty) cez Modul procesnej integrácie a integrácie údajov, t.j. integráciou cez jeho dátovú časť - IS CSRÚ (kapitola xxx).
* Proces vyhlasovania a zmeny referenčných údajov (LINK: <https://datalab.digital/referencne-udaje/referencne-udaje-a-zakladne-ciselniky/proces-vyhlasovania-a-zmeny-referencnych-udajov/> )

Metodické usmernenie MIRRI o postupe zaraďovania referenčných údajov do zoznamu referenčných údajov vo väzbe na referenčné registre a vykonávania postupov pri referencovaní: <https://metais.vicepremier.gov.sk/confluence/download/attachments/2621442/Metodicke_usmernenie_UPVII_3639_2019_oDK_1_FINAL.pdf?version=1&modificationDate=1554714761337&api=v2>

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Názov referenčného registra /objektu evidencie:** | **Názov referenčného údaja** | **Identifikácia subjektu, ku ktorému sa viaže referenčný údaj:** | **Zdrojový register a registrátor zdrojového registra:** |
| **1** |  |  |  |  |
| **2** |  |  |  |  |
| **3** |  |  |  |  |
| **4** |  |  |  |  |
| **5** |  |  |  |  |
| **X** |  |  |  |  |

Tabuľka 11 Prehľad identifikovaných referenčných údajov

Zabezpečiť dostupnosť poskytovania navrhovaných objektov evidencie za referenčné (t.j. v rámci nich údaje/atribúty) cez Modul procesnej integrácie a integrácie údajov, t.j. integráciou cez jeho dátovú časť - IS CSRÚ.

# 4.4.2       Identifikácia údajov pre konzumovanie alebo poskytovanie údajov – do / z CSRU

* Identifikovať/kvantifikovať potenciálnych konzumentov týchto objektov evidencie (t.j. navrhovaných k vyhláseniu za referenčné), vrátane ich oprávnenosti/nároku na konzumovanie v zmysle konkrétnych ustanovení osobitných právnych predpisov na strane konzumenta, prípadne aj na strane poskytovateľa. V nadväznosti na uvedené identifikovať osobitné právne predpisy (až na úroveň konkrétneho ustanovenia), ktoré je nutné novelizovať v záujme dosiahnutia “TO-BE stavu” a jeho bezproblémovej aplikovateľnosti. (viď. Tabuľka č. 13).
* Pre úspešné napojenie sa na IS CSRÚ v roli konzumenta údajov je nutné postupovať v zmysle predložených dokumentov:
* „Postup pripojenia OVM do IS CSRÚ v roli poskytovateľa údajov“ (<https://datalab.digital/doumenty>)
* „Postup pripojenia OVM do IS CSRÚ v roli kozumenta údajov“ (<https://datalab.digital/dokuemnty>)
* Zoznam dostupných cez IS CSRÚ <https://datalab.digital/referencne-udaje/>

| **ID** | **Názov referenčného údaja:** | **Konzumovanie / poskytovanie** | **Osobitný právny predpis pre poskytovanie / konzumovanie** |
| --- | --- | --- | --- |
| **1** |  | Vyberte jednu z možností. |  |
| **2** |  | Vyberte jednu z možností. |  |
| **3** |  | Vyberte jednu z možností. |  |
| **4** |  | Vyberte jednu z možností. |  |
| **5** |  | Vyberte jednu z možností. |  |
| **X** |  | Vyberte jednu z možností. |  |

Tabuľka 12 Prehľad identifikovaných referenčných údajov

# 4.5          OTVORENÉ ÚDAJE

**IRELEVANTNÉ**- celá kapitola aj s podkapitolami irelevantná z dôvodu, že bezpečnostné riešenie nepracuje s dátovými objektmi.

* Doplniť názov objektu evidencie identifikovaných pre kategóriu otvorených údajov v kapitole dátový rozsah projektu
* Pravidlá pre úroveň interoperability verejných otvorených údajov (<https://wiki.vicepremier.gov.sk/pages/viewpage.action?pageId=23986518> )
* Požadovaná kvalita:
  + Automatizované publikovanie otvorených údajov v kvalite 3★ (Všetky datasety je potrebné registrovať v centrálnom katalógu otvorených údajov na [data.gov.sk](http://data.gov.sk)). Formát CSV, XML, ODS, JSON
  + Automatizované publikovanie otvorených údajov v kvalite 4★ (Všetky datasety je potrebné registrovať v centrálnom katalógu otvorených údajov na [data.gov.sk](http://data.gov.sk)) Formát údajov RDF, OWL, TriX, JSON
  + Automatizované publikovanie otvorených údajov v kvalite 5★ (Všetky datasety je potrebné registrovať v centrálnom katalógu otvorených údajov na [data.gov.sk](http://data.gov.sk)) Formát udajov RDF, OWL, TriX, JSON

|  |  |  |
| --- | --- | --- |
| **Názov objektu evidencie / datasetu** | **Požadovaná kvalita** 3★ - 5★ | **Periodicita publikovania**  (týždenne, mesačne, polročne, ročne) |
| Príklad: senzorické údaje merania teploty | 3★ | Polročne |
|  | Vyberte jednu z možností. | Vyberte jednu z možností. |
|  | Vyberte jednu z možností. | Vyberte jednu z možností. |
|  | Vyberte jednu z možností. | Vyberte jednu z možností. |
|  | Vyberte jednu z možností. | Vyberte jednu z možností. |
|  | Vyberte jednu z možností. | Vyberte jednu z možností. |

Tabuľka 13 Prehľad otvorených údajov

# 4.6          ANALYTICKÉ ÚDAJE

**IRELEVANTNÉ**- celá kapitola aj s podkapitolami irelevantná z dôvodu, že bezpečnostné riešenie nepracuje s dátovými objektmi.

* Analytické údaje predstavujú obrovskú skupinu dát získavaných vysokou rýchlosťou z vysokého počtu rôznych typov zdrojov. V priestore verejnej správy sa jedná o dátové zdroje, ktoré sú vytvárané a spravované jednotlivými inštitúciami za účelom podpory služieb verejnej správy, služieb vo verejnom záujme alebo verejných služieb. Tieto údaje môžeme okrem uvedenej primárnej funkcie využiť aj na analytické spracovanie, tak aby verejná správa dokázala využívať svoje údaje pre potreby prípravy analýz, na podporu rozhodovania, riadenia a lepší návrh politík. Podmienkou pre plné využitie potenciálu údajov vo verejnej správe je ich poznanie (informácie o dátových zdrojoch, ich obsahu a atribútoch) a zabezpečenie prístupu k analytickým údajom pre analytické jednotky.
* Je organizácia napojená na IS CSRÚ alebo ponúka inú možnosť integrácie s modulom na sprístupňovanie údajov pre analytické jednotky (napr. KAV)
* Sprístupnenie dátových zdrojov organizácie na analytické účely v zmysle zákona (Zákon č. .../2021 Z. z. o údajoch a o zmene a doplnení niektorých údajov):

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **Názov registra / objektu evidencie**  (tabuľka č.8) | **Zoznam atribútov objektu evidencie** | **Popis a špecifiká objektu evidencie** |
| **1** | napr. Dataset vlastníkov automobilov | identifikátor vlastníka; EČV; typ\_vozidla; okres\_evidencie;... | - dataset obsahuje osobné informácie (r.č. vlastníka) |
| **2** |  |  |  |
| **3** |  |  |  |
| **4** |  |  |  |
| **5** |  |  |  |
| **x** |  |  |  |

Tabuľka 14 Prehľad sprístupnených dátových zdrojov určených na analytické účely

# 4.7          MOJE ÚDAJE

**IRELEVANTNÉ**- celá kapitola aj s podkapitolami irelevantná z dôvodu, že bezpečnostné riešenie nepracuje s dátovými objektmi.

Do kategórie mojich údajov spadajú sú údaje, ktoré sa týkajú fyzickej osoby alebo právnickej osoby, zároveň boli zaradené ako dátový prvok medzi moje údaje a sú prístupné elektronicky v strojovo-spracovateľnom formáte automatizovaným spôsobom cez aplikačné programovacie rozhranie, alebo prostredníctvom modulu procesnej integrácie a integrácie údajov pre fyzickú osobu alebo právnickú osobu, ktorej sa týkajú, na základe preukázania jej elektronickej identity osoby.

* Poskytnutie údajov pre službu Moje dáta
* Identifikácia údajov

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **Názov registra / objektu evidencie** | **Atribút objektu evidencie** | **Popis a špecifiká objektu evidencie** |
| **1** |  |  |  |
| **2** |  |  |  |
| **3** |  |  |  |
| **4** |  |  |  |
| **5** |  |  |  |
| **x** |  |  |  |

Tabuľka 15 Prehľad údajov identifikovaných pre službu „moje údaje“

### 

# 4.8          PREHĽAD JEDNOTLIVÝCH kategórii údajov

**IRELEVANTNÉ**- celá kapitola aj s podkapitolami irelevantná z dôvodu, že bezpečnostné riešenie nepracuje s dátovými objektmi.

Výstupom predchádzajúcich kapitol je súhrnná tabuľka pre kategorizáciu množiny údajov z pohľadu ich využiteľnosti.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Register / Objekt evidencie** | **Referenčné údaje** | **Moje údaje** | **Otvorené údaje** | **Analytické údaje** |
| **1** |  | ☐ | ☐ | ☐ | ☐ |
| **2** |  | ☐ | ☐ | ☐ | ☐ |
| **3** |  | ☐ | ☐ | ☐ | ☐ |
| **4** |  | ☐ | ☐ | ☐ | ☐ |
| **5** |  | ☐ | ☐ | ☐ | ☐ |
| **x** |  | ☐ | ☐ | ☐ | ☐ |

Tabuľka 16 Kategorizácia údajov z pohľadu ich využiteľnosti (účelu)

# 4.9          LEGISLATÍVA

Legislatívne požiadavky vo vzťahu k Projektu ustanovuje nasledovný základný európsky a národný legislatívny rámec:

* **smernica Európskeho parlamentu a rady (EÚ) 2016/1148** zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii,
* **vykonávacie nariadenie Komisie (EÚ) 2018/151** z 30. januára 2018, ktorým sa stanovujú pravidlá uplatňovania smernice Európskeho parlamentu a Rady (EÚ) 2016/1148, pokiaľ ide o bližšiu špecifikáciu prvkov, ktoré musia poskytovatelia digitálnych služieb zohľadňovať pri riadení rizík v oblasti bezpečnosti sietí a informačných systémov, a parametrov na posudzovanie toho, či má incident závažný vplyv,
* **nariadenie európskeho parlamentu a rady (EÚ) 2016/679** o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov,
* **nariadenie Európskeho parlamentu a Rady (EÚ) č. 1303/2013** zo 17. decembra 2013, ktorým sa stanovujú spoločné ustanovenia o Európskom fonde regionálneho rozvoja, Európskom sociálnom fonde, Kohéznom fonde, Európskom poľnohospodárskom fonde pre rozvoj vidieka a Európskom námornom a rybárskom fonde a ktorým sa stanovujú všeobecné ustanovenia o Európskom fonde regionálneho rozvoja, Európskom sociálnom fonde, Kohéznom fonde a Európskom námornom a rybárskom fonde, a ktorým sa zrušuje nariadenie Rady (ES) č. 1083/2006,
* **zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti** a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon o kybernetickej bezpečnosti“),
* **zákon 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“),
* **súvisiace vykonávacie predpisy k zákonu o ITVS:**
* 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,
* vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č.78/2020 Z.z. o o štandardoch pre informačné technológie verejnej správy,
* **zákon č. 45/2011 Z.z. o kritickej infraštruktúre** v znení neskorších predpisov,
* **zákon č. 305/2013 Z.z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci** a o zmene a doplnení niektorých zákonov (zákon o e-Governmente),
* **zákon č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,**
* **zákon č. 292/2014 o príspevku poskytovanom z európskych štrukturálnych a investičných fondov** a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

Strategický dokument v oblasti riadenia informačnej a kybernetickej bezpečnosti:

* **Národná stratégia kybernetickej bezpečnosti na roky 2021 až 2025.**

# 4.10        Bezpečnosť údajov (technické a organizačné zabezpečenie – pre prístup k údajom)

Projekt má na zreteli aj riziká pôsobiace na porušenie ochrany citlivých údajov. Porušenie bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene, neoprávnenému poskytnutiu osobných údajov, ktoré sa prenášajú, uchovávajú alebo inak spracúvajú, alebo neoprávnený prístup k nim bude dostatočne podporený technickými a organizačnými opatreniami. NASES vymedzuje rozmer a spôsob bezpečnostných opatrení potrebných na eliminovanie a minimalizovanie hrozieb a rizík pôsobiacich na informačný systém z hľadiska narušenia jeho bezpečnosti, spoľahlivosti a funkčnosti.

Dokumentácia obsahujúca bezpečnostné opatrenia, minimálne v rozsahu:

* Technické opatrenie realizované prostriedkami fyzickej povahy, zabezpečenie objektu pomocou mechanických zábranných prostriedkov;
* Riadenie prístupu poverených osôb, riadenie prístupov a opatrenia na zaručenie platných politík riadenia prístupov;
* Ochrana pred neoprávneným prístupom, šifrová ochrana uložených a prenášaných údajov, pravidlá pre kryptografické opatrenia;
* Autentizácia a autorizácia osôb v informačnom systéme;
* Riadenie zraniteľností, opatrenia na detekciu a odstránenie škodlivého kódu a nápravu následkov škodlivého kódu; ochrana pred nevyžiadanou elektronickou poštou;
* Sieťová bezpečnosť, kontrola obmedzenie alebo zamedzenie prepojenia informačného systému, v ktorom sú spracúvané osobné údaje s verejne prístupnou počítačovou sieťou;
* Zálohovanie, test funkčnosti záložných dátových nosičov;
* Likvidácia osobných údajov a dátových nosičov, technické opatrenia na bezpečné vymazanie osobných údajov z dátových nosičov;
* súlad s bezpečnostnými štandardmi, právnymi predpismi
  + Zákon č. 95/2019 Z.z. o informačných technológiách vo verejnej správe
  + Zákon č. 69/2018 Z.z. o kybernetickej bezpečnosti
  + Zákon č. 45/2011 Z.z. o kritickej infraštruktúre
    - Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 78/2020 Z. z. o štandardoch pre informačné technológie verejnej správy;
    - Vyhláška Úradu na ochranu osobných údajov Slovenskej republiky č. 158/2018 Z. z. o postupe pri posudzovaní vplyvu na ochranu osobných údajov
* Projekt bude spĺňať podmienky ustanovené v Nariadení Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (ďalej aj "Nariadenie GDPR"), a podmienky zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej aj „zákon o ochrane osobných údajov“).
* Pred začatím spracúvania osobných údajov bude potrebné vykonať kroky a úkony smerujúce k správnemu vymedzeniu postavenia organizácie v procese spracúvania, ako aj identifikovať spracovateľské operácie. Pôsobnosť Nariadenia GDPR a zákona o ochrane osobných údajov bude potrebné posudzovať počas celého obdobia implementácie projektu a uvedené predpisy uplatňovať s ohľadom na spracovateľské činnosti, ktoré budú v tejto súvislosti vykonávané. Vymedzenie postavenia NASES v súlade s Nariadením GDPR a zákona o ochrane osobných údajov pri spracúvaní osobných údajov je základným predpokladom k zabezpečeniu zákonnosti spracúvania a ochrany osobných údajov a taktiež k naplneniu povinností, ktoré sa k spracovateľským operáciám viažu. Z pohľadu Nariadenia GDPR bude v tomto projekte NASES prevádzkovateľom a dodávateľ riešenia sprostredkovateľom údajov, pričom bude uzatvorená zmluva o spracúvaní osobných údajov.
* Bude vykonané posúdenie vplyvu na ochranu osobných údajov, ktorého cieľom bude najmä zistiť, či spracovateľské činnosti vyplývajúce z riešenia projektu povedú k vysokému riziku pre práva a slobody dotknutých osôb. Taktiež, v prípade ak vystane otázka určenia oprávneného záujmu, ako jedného z možného právneho základu pre zákonné spracúvanie bez súhlasu dotknutej osoby, bude vykonaný test proporcionality na posúdenie uplatnenia tohto oprávneného záujmu.
* Pri posudzovaní vplyvu na ochranu osobných údajov sa bude postupovať v súlade s vyhláškou Úradu na ochranu osobných údajov Slovenskej republiky č. 158/2018 Z. z. o postupe pri posudzovaní vplyvu na ochranu osobných údajov.

V prípade identifikovania potreby zmeny príslušných právnych predpisov, bude zabezpečená komunikácia s gestorom predmetnej legislatívy.

# 5.     ROZPOČET A PRÍNOSY

Náklady CAPEX projektu predstavuje: nákup licencií „Inappsecurity“ , nákup licencií SOAR, nákup HW – 4 x Server, nákup HW a SW pre F5 systém, inštalačné a infraštruktúrne náklady, „customizáciu“ zakúpeného SW a HW v zmysle katalógu požiadaviek a implementáciu projektu/riešenia (analýza a dizajn, implementácia, testovanie, nasadenie).

Náklady OPEX projektu predstavuje: prolongácia supportu/maintanance zakúpených licencií „Inappsecurity“ a „SOAR“ v 4. roku prevádzky, prolongácia supportu/maintanance SW a HW F5 systému, 7 FTE/ročne na zabezpečenie prevádzky navrhovaného riešenia (modulu Detekcia).

**V*ypočítané prínosy*** v T10 (t.j. na 10 rokov dopredu):

Predmetné prínosy sú detailne popísané v samostatnom dokumente Príloha č.2: Analýza Benefitov NP Detekcia zraniteľnosti koncových obslužných bodov, ktorý tvorí aj prílohu k CBA.

**Rok návratnosti** (doplnenie ukazovateľov: ENPV, FNPV, BCR):

Ekonomická čistá súčasná hodnota (ENPV): 37 624 594 EUR

Finančná čistá súčasná hodnota (FNPV): - 11 238 767 EUR

Pomer prínosov a nákladov (BCR): 5,10

Rok návratu investície (PBP): t3

Sumarizácia nákladov a prínosov:



Zdroje financovania:



# 6.     HARMONOGRAM JEDNOTLIVÝCH FÁZ PROJEKTU a METÓDA JEHO RIADENIA

Realizácia projektu je naplánovaná na 9 mesiacov. Nasledujúci harmonogram zobrazuje realizáciu projektu podľa jeho jednotlivých fáz:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **FÁZA/AKTIVITA** | **ZAČIATOK**  **(odhad termínu)** | **KONIEC**  **(odhad termínu)** | **POZNÁMKA** |
| 1. | Prípravná fáza | 12/2020 | 02/2021 |  |
| 2. | Iniciačná fáza | 03/2021 | 12/2021 |  |
| 3. | Realizačná fáza | 01/2022 | 12/2022 |  |
| 3a | Analýza a Dizajn | 01/2022 | 01/2022 | 1 mesiac |
| 3b | Nákup technických prostriedkov, programových prostriedkov a služieb | 02/2022 | 04/2022 | 3 mesiace |
| 3c | Implementácia a testovanie | 05/2022 | 07/2022 | 3 mesiace |
| 3d | Nasadenie | 08/2022 | 12/2022 | 5 mesiacov |
| **4.** | Dokončovacia fáza | 12/2022 | 02/2023 | 3 mesiace |

Metóda riadenia projektu:

Projekt bude realizovaný waterfall metódou s prihliadnutím na strategické priority podľa NKIVS. Projekt má udaný jasný cieľ a výstupy, ktoré budú priebežne konzultované s vlastníkom projektu.

# 7.     PROJEKTOVÝ TÍM

Riadiaci výbor sa zriaďuje ako najvyšší riadiaci orgán na účely realizácie Projektu „Detekcia zraniteľnosti koncových obslužných bodov“. Riadiaci výbor bude zostavený v nasledujúcom zložení:

|  |  |  |
| --- | --- | --- |
| Predseda RV | Pavel Karel | NASES |
| Podpredseda RV | Martin Sulík | NASES |
| zástupca vlastníkov procesov objednávateľa (biznis vlastník) | Michal Ďurajka | NASES |
| zástupca za MIRRI |  | MIRRI |

Projektový tím pre projekt sa bude skladať s nasledujúcich zúčastnených strán:

1. NASES ako objednávateľ, vlastník a prevádzkovateľ riešenia modulu detekcie hrozieb (interné kapacity)

2. SKIT ako dodávateľ (externé kapacity)

Nasledujúca tabuľka sumarizuje navrhovaných členov projektového tímu MIRRI pre hlavné a podporné aktivity a ich role na projekte:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Meno a Priezvisko** | **Pozícia** | **Oddelenie** | **Rola v projekte** |
| **1.** | Michal Seliga | Projektový manažér za objednávateľa | NASES |  |
| **2.** | Sekcia bezpečnosti | Kľúčový používateľ (end user) | NASES |  |
| **3.** | Sekcia bezpečnosti | Špecialista na bezpečnosť | NASES |  |
| **4.** | Sekcia bezpečnosti | Tester | NASES |  |
| **5.** | Sekcia bezpečnosti | Analytik | NASES |  |
| **6.** | Peter Žovák | IT Architekt | NASES |  |
| **7.** | Sekcia bezpečnosti | Odborník pre IT Senior - Školiteľ IT | NASES |  |
| **8.** | Sekcia bezpečnosti | Manažér kvality | NASES |  |
| **9.** | Miloš Havrilla | Finančný manažér | NASES |  |
| **10.** | SKIT | IT analytik | SKIT |  |
| **11.** | SKIT | Špecialista pre bezpečnosť IT | SKIT |  |
| **12.** | SKIT | Projektový manažér IT projektu | SKIT |  |
| **13.** | SKIT | Špecialista pre infraštruktúrny/HW špecialista | SKIT |  |
| **14.** | SKIT | IT architekt | SKIT |  |
| **15.** | SKIT | IT programátor/vývojár | SKIT |  |
| **16.** | SKIT | IT Tester | SKIT |  |

# 8.     PRACOVNÉ NÁPLNE

Doplniť vstupy v  INICIAČNEJ FÁZE:

* doplniť ***podľa dokumentu z Riadiaceho Výboru*** projektu, prípadne zo splnomocnení alebo menovacích dekrétov - do už vytvoreného dokumentu PROJEKTOVÝ ZÁMER z Prípravnej fázy a aktualizovať a detailne rozpracovať. Tieto vstupy neskôr využijete pri dokumente PID.

VZORY a ŠABLONY zdrojových súborov sú tu: [*https://www.mirri.gov.sk/sekcie/informatizacia/riadenie-kvality-qa/riadenie-kvality-qa/index.html*](https://www.mirri.gov.sk/sekcie/informatizacia/riadenie-kvality-qa/riadenie-kvality-qa/index.html)

Poznámka: Odporúčame – pozrite si VZOR pre ***MENOVACIE DEKRÉTY*** členov projektového tímu – vzor obsahuje názorný popis všetkých projektových rolí, ktoré vyžaduje Vyhláška 85/2020 Z.z.

# 9.     ODKAZY

Doplniť vstupy v  PRÍPRAVNEJ FÁZE:

* doplniť odkazy na už existujúce produkty v maximálnej miere – vyhnúť sa duplikovaným informáciám.

# 10.   PRÍLOHY

Príloha č.1 Zoznam rizík

Príloha č.2 Analýza benefitov

Príloha č.3 Zdôvodnenie použitia SOAR licencií