PROJEKTOVÝ ZÁMER

(Verzia dokumentu v1.82/09_2021)

Identifikovanie požiadaviek **na funkčnú časť riešenia**

Identifikácia projektu

Povinná osoba	Národné centrum zdravotníckych informácií
Názov projektu	Budovanie kapacít a zvýšenia spôsobilosti pracoviska bezpečnostných operácii SOC NCZI
Zodpovedná osoba za projekt	Mgr. Silvia Strešková
Realizátor projektu	Národné centrum zdravotníckych informácií
Vlastník projektu	Mgr. Peter Lukáč, PhD., riaditeľ NCZI

Schvaľovanie dokumentu

Položka	Meno a priezvisko	Organizácia	Pracovná pozícia	Dátum	Podpis (alebo elektronický súhlas)
Vypracoval	Mgr. Silvia Strešková	Národné centrum zdravotníckych informácií	Projektový manažér	15.10.2023	

OBSAH

1. POPIS ZMIEN DOKUMENTU

1.1. HISTÓRIA ZMIEN

Verzia	Dátum	Zmeny	Meno
0.7	30.09.2023	Final pre podanie na hodnotenie	Strešková
0.8	10.11.2023	Doplnenie prínosov	Strešková

2. ÚČEL DOKUMENTU, SKRATKY (KONVENCIE) A DEFINÍCIE

V súlade s **Vyhláškou ÚPVII č. 85/2020 Z.z. 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.

V súlade s vyhláškou ÚPVII 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

2.1.2. POUŽITÉ SKRATKY

ID	SKRATKA	POPIS
1.	API	Application programming interface
2.	BPMN	Business Process Model and Notation
3.	CSRÚ	Centrálna správa referenčných údajov
4.	DevOps	Je skrátený názov pre developer, security alebo aj automatizovaný devops ako súbor procesov medzi vývojom a prevádzkou, skratka z developer operations. Vysvetlenie detail viď https://en.wikipedia.org/wiki/DevOps
5.	DMS	Document management system
6.	EDR	Endpoint Detection and Response
7.	ezdravie	Programové označenie Národného zdravotníckeho informačného systému
8..	EÚ	Európska únia
9.	HW	Hardware
10.	HLD	High level dizajn – vysokoúrovňový dizajn napr architektúru, bezpečnosť
11.	IaaS	Infrastructure as a service
12.	IAM	Identity and Access Management
13.	IKT	Informačno-komunikačné technológie
14.	IS	Informačný systém
15.	IS VS	Informačný systém verejnej správy
16.	ISZI	Informačný systém zdravotníckych indikátorov
17.	JRÚZ	Jednotná referenčná údajová základňa rezortu zdravotníctva.
18.	KPI	Key performance indicator – Kľúčové indikátory, prostredníctvom ktorých sa meria naplnenie cieľov projektu.
19.	LLD	Low level dizajn – nízkoúrovňový dizajn napr. pre architektúru, bezpečnosť. Obsahuje detailné dizajny až na úrovní nastavení parametrov
20.	MDM	Mobile devicemanagement
21.	MIRRI	Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky
22.	MV SR	Ministerstvo vnútra SR
23.	MZ SR	Ministerstvo zdravotníctva Slovenskej republiky
24.	NCZI	Národné centrum zdravotníckych informácií
25.	NKIVS	Národná koncepcia informatizácie verejnej správy
26.	NZIS	Národný zdravotnícky informačný systém

27.	OOÚ	Ochrana osobných údajov
28.	PO	Plán obnovy a odolnosti
29.	OVM	Orgán verejnej moci
30.	PaaS	Platform as a service
31.	PILOT	PILOT - Prevádzka riešenia na vybraných aktéroch na produkčnom prostredí.
32.	PoC	PoC - Implementovaný prototyp riešenia nasadený do produkčnej prevádzky a overený E2E testami minimálne s využitím mockov
33.	PR	Projektové riadenie
34.	PrZS	Prijímateľ zdravotnej starostlivosti
35.	PZS	Poskytovateľ zdravotnej starostlivosti
36.	ROLLOUT	ROLLOUT - Postupné pripájanie ostatných aktérov na produkčnom prostredí.
37.	RFO	Register fyzických osôb
38.	RPO	Register právnických osôb
39.	RÚVZ	Regionálne úrady verejného zdravotníctva
40.	SDL metodika	Security development lifecycle – interná metodika pre postup implementácie vydaný NCZI.
41.	SFTP	SSH File Transfer Protocol
42.	SLA	Service level agreement
43.	SOAP	Simple Object Access Protocol
44.	SOAR	Security orchestration, automation and response
45.	SR	Slovenská republika
46.	ŠÚ SR	Štatistický úrad Slovenskej republiky
47.	ŠÚKL	Štátny ústav pre kontrolu liečiv
48.	ÚDZS	Úrad pre dohľad nad zdravotnou starostlivosťou
49.	VÚC	Vyšší územný celok alebo iný povoľovací orgán
50.	PR	Projektové riadenie
51.	VÚC	Vyšší územný celok alebo iný povoľovací orgán

3. DEFINOVANIE PROJEKTU

3.1. MANAŽÉRSKE ZHRNUTIE

Jedným zo strategickým cieľov koncepcie kybernetickej bezpečnosti schválenej vládou Slovenskej republiky je otvorený, bezpečný a chránený národný kybernetický priestor, ktorý zabezpečí vybudovanie dôvery v spoľahlivosť a bezpečnosť štátu a to najmä kritickej infraštruktúry a komunikačnej infraštruktúry, ako aj istoty, že táto bude plniť svoje funkcie a slúžiť národným záujmom aj v prípade kybernetického útoku. Súčasné kybernetické útoky nie sú už len fiktívnou hrozbou. Prostredníctvom nich sú ohrozované nielen súkromné spoločnosti, ale aj kritická infraštruktúra štátu. Nedostatky v zabezpečení ochrany informácií zvyšujú riziko straty dôvery v štát a znižujú reputáciu krajiny. Je preto nevyhnutné prijať dôsledné opatrenia na zabezpečenie bezpečnosti krajiny v tejto oblasti a ochranu nielen dôležitých informačných systémov, ale aj informácií, ktoré sú vo veľkej miere, v rámci implementácie efektívnej verejnej správy, teda aj v sektore „Zdravotníctvo" poskytované, ukladané a vymieňané v kybernetickom priestore. Zavedením správnych opatrení je možné minimalizovať riziká, ktoré kybernetický priestor prináša, a to hlavne:

- odcudzenie, zneužitie alebo strata dôvernosti a/alebo dostupnosti osobných a inak citlivých údajov,
- poškodenie dobrého mena,
- znefunkčnenie vybraných služieb, a ďalšie.

Z dôvodu prudkého nárastu kybernetických hrozieb je nevyhnutné dobudovanie kapacít a zvýšenia spôsobilosti pracoviska bezpečnostných operácii SOC NCZI v oblasti kybernetickej bezpečnosti takým spôsobom, aby bola zaistená integrita, dôvernosť a dostupnosť zdravotníckych informácií všetkých občanov SR. Národné centrum zdravotníckych informácií (ďalej ako „NCZI"), v súlade s ustanoveniami § 4 zákona č.69/2018 Z. z. o kybernetickej bezpečnosti, ako organizácia, ktorá je správcom nadrezortného informačného systému vo svojej pôsobnosti zabezpečuje kybernetickú bezpečnosť informačných systémov. V súlade s ustanoveniami § 20 zákona č.69/2018 Z. z. o kybernetickej bezpečnosti je Národné centrum zdravotníckych informácií (ďalej ako „NCZI") povinné plniť predmetné opatrenia. V prostredí MZ SR, Úradu verejného zdravotníctva SR (ďalej len "UVZ SR") a NCZI zákonné povinnosti zabezpečuje NCZI - štátna príspevková organizácia, ktorej zriaďovateľom je MZ SR. Postavenie a úlohy NCZI upravuje zákon č.153/2013 Z.z. Zákon o národnom zdravotníckom informačnom systéme a o zmene a doplnení niektorých zákonov, pričom podrobnejšie kompetencie a pôsobnosť NCZI ustanovuje § 12 zákona č.153/2013 Z.z. Na základe vyššie uvedených kompetencií NCZI prevádzkuje elektronické služby zdravotníctva a prevádzkuje národný zdravotnícky informačný systém. Pracovisko bezpečnostného dohľadového centra (ďalej len „SOC") prevádzkované NCZI zabezpečuje pokrytie významných

aspektov kybernetickej bezpečnosti, ktoré majú vplyv na MZ SR, UVZ SR a NCZI. Týmito aspektami sú najmä monitorovanie a analýza interného kybernetického prostredia MZ SR, UVZ SR a NCZI, výmena informácií o kybernetických hrozbách, ako aj riešenie mimoriadnych situácií. Cieľom projektu je zaistenie kybernetickej ochrany v podmienkach rezortu zdravotníctva v súlade s ustanoveniami zákona č.69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len „zákon o kybernetickej bezpečnosti"). Takto dobudovaná systémová infraštruktúra pracoviska SOC bude spĺňať požiadavky na moderné vysoko dostupné systémy s využitím pokročilých metód odhaľovania kybernetických ohrození, zároveň bude poskytovať podporu pre zákonom stanovené služby v oblasti prevencie kybernetických bezpečnostných incidentov, ako aj pre reaktívne služby definované zákonom o kybernetickej bezpečnosti. Zákon definuje preventívne služby ako služby, ktoré sa zameriavajú na prevenciu kybernetických bezpečnostných incidentov a to najmä:

- vytváraním bezpečnostného povedomia,
- spoluprácou s ostatnými jednotkami CSIRT,
- monitorovaním a evidenciou kybernetických bezpečnostných incidentov,
- pripojením na jednotný informačný systém kybernetickej bezpečnosti,
- poskytovaním informácií a údajov do jednotného informačného systému kybernetickej bezpečnosti,
- prijímaním a zasielaním včasného varovania pred kybernetickými bezpečnostnými incidentmi prostredníctvom jednotného informačného systému kybernetickej bezpečnosti.

V zmysle ustanovení zákona sa reaktívne služby zameriavajú na riešenie kybernetických bezpečnostných incidentov a sú nimi najmä:

- výstrahy a varovania,
- detekcia kybernetických bezpečnostných incidentov,
- analýza kybernetických bezpečnostných incidentov,
- odozva, ohraničenie, riešenie a náprava následkov kybernetických bezpečnostných incidentov,
- asistencia pri riešení kybernetického bezpečnostného incidentu na mieste, pričom pod pojmom asistencia rozumie realizácia takých úkonov a činností počas riešenia kybernetických bezpečnostných hrozieb a incidentov, ktoré nevyžadujú priame zásahy do prostredia, kde boli hrozby alebo incidenty odhalené. Asistencia spočíva v konzultáciách na strane NCZI a dodávateľa tejto služby.
- reakcia na kybernetický bezpečnostný incident,
- podpora reakcií na kybernetické bezpečnostné incidenty,
- koordinácia reakcií na kybernetické bezpečnostné incidenty,
- návrh opatrení na zabránenie ďalšiemu pokračovaniu, šíreniu a opakovanému výskytu kybernetických bezpečnostných incidentov.

Predmetom projektu tak je:

Projekt budovania kapacít a zvýšenia spôsobilosti pracoviska bezpečnostných operácii SOC NCZI je zameraný na dobudovanie infraštruktúry, posilnenie kybernetickej bezpečnosti NZIS **a vybraných IS subjektov v zriaďovateľskej pôsobnosti MZ SR,** zlepšenie procesov, komunikácie, zberu dát, analýzy, predchádzanie incidentom, zrýchlenie riešenia kybernetických bezpečnostných incidentov, zvýšenie personálnej a znalostnej spôsobilosti pracoviska SOC a zabezpečenie primeraných pracovných podmienok pracoviska SOC.

Z pohľadu rozsahu implementovaných IS a konečných užívateľov výhod je stav v zmysle jednotlivých subjektov nasledovný:

ÚVZ:

- Integrovaný systém verejného zdravotníctva (ďalej len IS ÚVZ) predstavuje digitalizovanú formu všetkých procesov ÚVZ a jeho regionálnych pobočiek v celkovom počte 36. V systéme je integrovaných 20 modulov (informačných systémov).
- IS Moje eZDravie ako systém pre riadenie pandemickej situácie z pohľadu testovania a očkovania je rovnako využívaný všetkými občanmi.

Koncovými užívateľmi výhod sú vzhľadom na internú a verejnú časť zmieňovných IS všetci občania Slovenskej republiky.

MZ SR:

- Interná infraštrukúra MZ SR.

Koncových užívateľov výhod predstavujú šetci zamestnanci MZ SR.

NCZI:
Súbor nosných a podporných systémov elektronizácie zdravotníckych informačných systémov v správe národného centra slúžiacich na zber, spracúvanie a poskytovanie informácií v zdravotníctve určených na správu údajovej základne; súčasťou národného zdravotníckeho informačného systému je aj Národný portál zdravia.:

- IS Ezdravie produkčné a predprodukčné prostredie.
- IS JRÚZ
- ISZI,
- Infraštruktúra NCZI
- EAlerts.

Koncovými užívateľmi výhod sú vzhľadom na internú a verejnú časť zmieňovných IS všetci občania Slovenskej republiky.

NCZI, ÚVZ a MZ SR predstavujú pilotné subjekty celkového zamýšľaného rozsahu 40 subjektov definovaných MZ SR kám spadajú nemocnice, Štátny ústav pre kontrolu liečiv Bratislava, Operačné stredisko záchrannej zdravotnej služby SR v Bratislave, Slovenská zdravotnícka univerzita v Bratislave a ďalšie.

Iniciatíva projektu vychádza z viacerých základných predpokladov, ktoré sú zároveň vzájomne previazané:

- Nárast rizika kybernetických útokov zameraných na subjekty poskytovateľov zdravotnej starostlivosti a kľúčové IS štátu po vypuknutí vojenského konfliktu na Ukrajine.
- Potreba posilnenia personálnych kapacít špecialistov interného tímu pre potreby vykonávania analýz a stabilizácia kľúčových členov a podporného tímu administrátorov jednotlivých technológii.
- Potreba zvýšenia visibility v monitorovaných IS a dobudovanie forenzného laboratória, laboratória dátových analýz, laboratórium malvér vyplývajúca.
- Ambícia získania kompetencie pre zriadenie a prevádzkovanie jednotky CSIRT pre rezort zdravotníctva.
- Potreba kontinuálneho vzdelávania a zvyšovania znalostného štandardu pracoviska SOC NCZI.
- Naplnenie zákonných a regulatórnych požiadaviek.

Cieľmi projektu sú zvýšenie spôsobilostí po technickej, procesnej a personálnej stránke, stabilizácia jadra tímu a naplnenie predpokladov cieľa vytvorenia a prevádzkovania rezortnej jednotky CSIRT.
Ciele budú naplnené nasledovnými aktivitami:

- Zefektívnenie procesov reakcie na bezpečnostné hrozby a zníženie potreby manuálnej intervencie pri riešení incidentov implementáciou nástroja SOAR.
- Zvýšenie visibility a kvality zdrojov logov implementáciou: EDR/XDR, DLP, Skener zraniteľnosti, SOAR, EDR, Forenzný lab, Malver lab, Vybavenie pracoviska SOC, Mobile device MGMT, WAF.

Implementácia vyššie uvedených technológie prispeje k rozšíreniu poskytovaných služieb SOC NCZI pre monitorované IS o proaktívne služby s rozšírením zberu a kvality bezpečnostne relevantných informácií ich evidencie triedenia, zrýchlenie identifikácie, analýzy a riešenie hrozieb, čím sa znižuje doba, počas ktorej je organizácia vystavená riziku. Integrácie implementovaných bezpečnostných nástrojov umožní centralizované riadenie a monitorovanie bezpečnostných operácií. Tieto platformy budú prispôsobené konkrétnym potrebám a prostrediam organizácie tak, aby zabezpečili optimálnu ochranu pred kybernetickými hrozbami.

Rozšírenie poskytovaných služieb bude zároveň podporené školeniami, vzdelávaním a motivačným navýšením finančného ohodnotenia, odmeňovacím systémom vlastných personálnych kapacít pre udržanie a stabilizáciu personálu a finančným krytím pre nábor nových špecialistov pod dobu trvania projektu.

Ciele projektu korešpondujú s dlhodobou stratégiou rozvoja SOC NCZI, ktorá súvisí s postupným rozširovaním proaktívnych služieb a rozsahu monitorovaných IS subjektov rezortu zdravotníctva formou budovania bezpečnostného dohľadového centra s ambíciou rozvoja na rezortné pracovisko CSIRT. Rovnaké ciele sú súčasťou stratégiu NCZI a MZ SR. Naplnením cieľov projektu zabezpečíme plynule zvládnutie vyššej vyťaženosti tímu SOC NCZI pri prípadných útokoch a navýšení počtu monitorovaných subjektov.

Výsledky projektu prinesú:

- Hĺbkový prehľad („visibility") o bezpečnosti IT prostredí, ktoré budú do Centrálneho bezpečnostného, logovacieho a vyhodnocovacieho nástroja pripojené, ktorý je nevyhnutný na včasné reakcie na kybernetické bezpečnostné ohrozenia.
- Automatizované výstrahy o incidentoch pri porušení bezpečnostných politík.
- Kontinuálny zber a možnosť analýzy sieťových tokov až do aplikačnej vrstvy OSI/ISO modelu.
- Možnosť forenznej analýzy sieťových tokov.
- Detekciu anomálií na úrovni tokov a rozpoznávanie známych hrozieb na základe DPI za pomoci detekčných signatúr.
- Identifikáciu porušenia interných bezpečnostných politík pomocou analýzy správania sa porovnaním s definovanou komunikačnou maticou, ako aj technikami na detekciu neštandardného správania sa v monitorovaných sieťach.

Projekt priamo prispieva k naplneniu cieľa definovaného v Národnej koncepcii informatizácie verejnej správy SR 2021 a to k cieľu 4.1 pre prioritnú os 4: Zvýšenie schopnosti včasnej identifikácie kybernetických incidentov vo verejnej správe. Hlavné výstupy

projektu priamo prispievajú k zvýšeniu schopnosti včasnej identifikácie kybernetických incidentov vo verejnej správe. V neposlednom rade je prioritná os zameraná na zvyšovania počtu incidentov, ktoré vládna jednotka CSIRT alebo SOC v spolupráci s verejnou správou odhalia a dokážu minimalizovať škody, prípadne úplne predísť škodám na IT verejnej správy čo týmto projektom bude zabezpečenné nakoľko sa rozšíri úroveň logsource-ov ale aj analytiky, identifikácie incidentov a predikcie.

MU NKIVS: Počet ISVS so zriadenými internými organizačnými útvarmi zabezpečujúcimi náležitý monitoring a dohľad nad ich kybernetickou bezpečnosťou (SOC).

Zároveň aktivity sú v súlade s cieľmi Plánu obnovy a odolnosti v oblasti kybernetickej bezpečnosti - Investície č. 6., projekt Budovania kapacít a zvýšenia spôsobilosti pracoviska bezpečnostných operácii SOC NCZI prispieva k posilneniu preventívnych opatrení, zvýšenie rýchlosti detekcie a riešenia incidentov s cieľom prispieť k vytvoreniu systému včasnej reakcie v oblasti kybernetickej bezpečnosti verejnej správy. Projekt sleduje v súlade s cieľmi Plánu obnovy konkrétne tieto ciele:
- začlenia sa nové technické a technologické riešenia systému včasnej reakcie do infraštruktúry riadenia incidentov kybernetickej bezpečnosti;
- implementuje rámec pravidelných hĺbkových bezpečnostných auditov, hodnotenia zraniteľnosti, ako aj penetračného testovania v celkovej architektúre kybernetickej bezpečnosti;
- zvýši sa úroveň technologického bezpečnostného vybavenia zariadení kritickej infraštruktúry;
- vypracuje sa katalóg hrozieb a metodika riadenia kybernetickej bezpečnosti;
- vypracuje sa centralizovaný prístup k implementácii bezpečnostných záplat.
V rámci prevencie sa posilní všeobecná úroveň kvality fyzickej a procesnej bezpečnosti kritickej infraštruktúry verejnej správy. To sa dosiahne zlepšením bezpečnosti procesu, rekonštrukciou a dobudovaním zabezpečených priestorov pre informačné systémy kritickej infraštruktúry.

3.2. MOTIVÁCIA A ROZSAH PROJEKTU

NCZI ako správca a prevádzkovateľ národného zdravotníckeho informačného systému a správca národných zdravotných registrov podľa zákona č. 153/2013 Z. z. o národnom zdravotníckom informačnom systéme a o zmene a doplnení niektorých zákonov je povinný okrem iného zaistiť aj primeranú ochranu spracúvaných zdravotníckych informácií voči kybernetickým hrozbám aj v súlade s povinnosťami vyplývajúcimi z ustanovení zákona č.69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov. Pri rozhodovaní o potrebe SOC v prostredí NCZI je potrebné zohľadniť fakt morálnej a fyzickej opotrebovanosti existujúcich bezpečnostných technológií. Nevyhnutnosť dobudovania pracoviska SOC odôvodňuje aj skutočnosť pretrvávajúcich a systematických kybernetických útokov na systémy prevádzkované NCZI, UVZ SR a MZ SR.
Súčasné bezpečnostné mechanizmy v oblasti monitoringu a hodnotenia zraniteľnosti implementované v národnom zdravotníckom informačnom systéme tvoria základ, ktorý si vyžaduje ďalší rozvoj pre zaistenie primeranej ochrany spracúvaných zdravotníckych informácií voči kybernetickým hrozbám a zároveň zabezpečenie súladu s povinnosťami vyplývajúcimi z ustanovení zákona č.69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov.

Okrem legislatívnych požiadaviek je nevyhnutné brať do úvahy aj aktuálny stav nechcenej negatívnej publicity a poškodzovania reputácie a dobrého mena NCZI, jeho zriaďovateľa MZ SR, ale aj UVZ SR ktorá je z časti spôsobená neschopnosťou včasnej detekcie možného kybernetického útoku z dôvodu chýbajúcich analytických nástrojov a nedostatku kvalitných zdrojov bezpečnostne relevantných záznamov.

Zvýšenie spôsobilosti Security Operation Center (SOC) je kľúčové pre zabezpečenie informačnej bezpečnosti a ochranu pred kybernetickými hrozbami pre NCZI ako centrálneho bodu zberu a spracovania zdravotníckych dát, ktorý predstavuje srdce celého procesu elektronizácie zdravotníctva. Realizáciou projektu dôjde k zvýšeniu spôsobilosti v nasledujúcich oblastiach:

- Rýchlejšia detekcia a reakcia na hrozby: Zlepšenie schopnosti identifikácie a reakcie na kybernetické hrozby v reálnom čase. To zahŕňa lepšiu analýzu logov, monitorovanie udalostí a upozornení, a automatizáciu procesov pre rýchlejšiu identifikáciu a potlačenie hrozieb.
- Rozšírená analýza hrozieb: Vytvorenie a zdokonalenie analytických schopnosti pre hĺbkovú analýzu kybernetických hrozieb implementáciou nástrojov na analýzu malvéru, rozpoznávanie správania útočníkov a predikcia budúcich hrozieb.
- Lepšie využitie technológií: Integrácia a efektívne využívanie nových technológii a nástrojov, ako sú umelá inteligencia, strojové učenie a automatizácia. To umožní rýchlejšie a presnejšie identifikovať hrozby a zároveň zníženie manuálnych úkonov.
- Zlepšenie spolupráce a komunikácia: Posilnenie spoluprácu medzi tímami v rámci organizácie, vrátane oddelení IT, prevádzky a vedenia, aby sa lepšie zdieľali informácie o hrozbách a koordinovali sa reakcie na incidenty.
- Odbornosť a školenia: Posilnenie spôsobilosti tímu SOC prostredníctvom odborných školení a certifikácií. Udržiavanie členov tímu oboznámených s najnovšími hrozbami a postupmi, a dobudovanie interného tímu náborom odborníkov na kybernetickú bezpečnosť.

- Kontinuálne zlepšovanie procesov: Pravidelné preskúmavanie a zlepšovanie pracovných postupov a procesov SOC na základe skúseností získaných počas detekcie a riešenia incidentov, implementáciou nástrojov a zvyšovaním znalostného štandardu členov tímu.
- Kontinuálna analýza úspešnosti: Monitorovanie úspešnosti SOC v detekcii, reakcii a prevencii kybernetických hrozieb pomocou merateľných ukazovateľov výkonu. Tieto údaje sa potom môžu použiť na ďalšie zlepšenie schopností pracoviska SOC.
- Pripravenosť na nové technológie a trendy: Pripravenosť na nové technológie, trendy a taktiky kybernetických útokov a prispôsobovať sa im v čo najkratšom čase.
- Zabezpečenie finančných a personálnych zdrojov: Zabezpečenie dostatočného financovania, personálnych a technických zdrojov pre efektívne fungovanie SOC.
- Sledovanie právnych a regulačných požiadaviek: Zabezpečiť, aby činnosti SOC boli v súlade s platnými právnymi a regulačnými požiadavkami týkajúcimi sa ochrany údajov a kybernetickej bezpečnosti.

Tieto aktivity pomôžu pracovisku SOC k vytvoreniu efektívneho a odolného systému na identifikáciu, monitorovanie a riešenie kybernetických hrozieb s cieľom ochrany organizácie pred potenciálnymi útokmi a položia základ budúceho rezortného pracoviska CSIRT.

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.	Národné centrum zdravotníckych informácií SR	NCZI	Vlastník procesu/ vlastník dát/ prevádzkovateľ / Užívateľ IS	Jednotná referenčná údajová základňa (JRÚZ) isvs_7756 Informačný Systém Zdravotníckych Indikátorov (ISZI) isvs_7755 Národný zdravotnícky informačný systém (NZIS) isvs_400 Národný register zdravotníckych pracovníkov isvs_8795 Národný register prijímateľov zdravotnej starostlivosti isvs_10734 Národný register organizácií s osobitnými úlohami v zdravotníctve isvs_8797 Národný register poskytovateľov zdravotnej starostlivosti isvs_8796 Dohľadové centrum spôsobilostí isvs_11591
2.	Ministerstvo investícií, regionálneho rozvoja a informatizácie SR	MIRRI	Gestor eGovernmentu	NZIS isvs_400
3.	Poskytovatelia zdravotnej starostlivosti	PZS	Užívateľ	NZIS isvs_400
4.	Prijímatelia zdravotnej starostlivosti	PrZS	Užívateľ	NZIS isvs_400
5.	Zdravotnícki pracovníci	ZPr	Užívateľ	NZIS isvs_400
6.	Zdravotné poisťovne	ZP	Vlastník dát/ Užívateľ IS	NZIS isvs_400
7.	Ministerstvo Zdravotníctva SR	MZ SR	Vlastník dát/ prevádzkovateľ / Užívateľ IS	NZIS isvs_400, ISVS Register zdravotníctva – isvs_11408, Register

				humánnej farmácie isvs_9427
8.	Regionálny úrad verejného zdravotníctva	RÚVZ	Vlastník dát/ prevádzkovateľ / Užívateľ IS	Register povolení, ako súčasť ISVS „Register zdravotníctva – isvs_11408"
9.	Občan		Zákazník Užívateľ	N/A
10.	Podnikateľ		Zákazník Užívateľ	N/A

3.4. CIELE PROJEKTU A MERATEĽNÉ UKAZOVATELE

Hlavným cieľom je zabezpečenie kybernetickej bezpečnosti národného zdravotníckeho informačného systému, vrátane včasnej a efektívnej reakcie na kybernetické útoky. Zároveň by sa malo dosiahnuť kvalitnejšie a transparentnejšie riadenie celého životného cyklu identifikovaných kybernetických incidentov a zjednotenie postupov a technologickej úrovne kybernetickej odolnosti informačných systémov v oblasti zdravotníctva. Všeobecnými cieľmi preto sú:

- Kvalitnejšie a rýchlejšie riadenie, monitorovanie a reagovanie na kybernetické hrozby.
- Zvýšenie efektívnosti ochrany informačných systémov v oblasti zdravotníctva.
- Zvýšenie odolnosti informačných systémov poskytovateľov zdravotnej starostlivosti voči kybernetickým útokom.
- Automatizovaný reporting o vzniku kybernetického bezpečnostného incident.

Ciele/Merateľné ukazovatele

P.Č.	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
1.	Zvyšovanie úrovne zabezpečenia informačných systémov v prostredí verejnej správy prostredníctvom budovania a rozvoja bezpečnostných dohľadových centier, ktoré budú súčasťou systému včasného varovania	Počet zabezpečených IT systémov v prostredí VS prostredníctvom centrálneho systému monitorovania bezpečnosti, ktorý je súčasťou riadenia kybernetických bezpečnostných incidentov a systému včasného varovania	Ukazovateľ vyjadruje počet informačných systémov v prostredí verejnej správy, ktoré majú implementované nástroje na centrálne rozpoznávanie, monitorovanie a riadenia kybernetických bezpečnostných incidentov, ako ich odhaľovanie, zaznamenávanie detailov a mitigovanie, a ktoré sú zapojené do centrálneho	Počet	0	450	Nástroj na monitorovanie	a. Počet prvkov zabezpečujúcich sieťovú komunikáciu - 90 b. Počet prvkov zabezpečujúcich ochranu komunikujúcich zariadení pomocou vynucovania stanovených pravidiel - 85 c. Počet prvkov zabezpečujúcich vzdialené bezpečné pripojenie do siete z prostredia internetu - 9 d. Počet prvkov zabezpečujúcich autorizáciu zariadení alebo

			systému monitorovania bezpečnosti					používateľov pre použitie služieb ponúkaných v internej sieti – 82 e. - virtualizačná vrstva (napr. VMware) - (výkonové) servery (napr. Windows, Linux) - 545
2.	Zvyšovanie úrovne zabezpečenia informačných systémov v prostredí verejnej správy prostredníctvom budovania a rozvoja bezpečnostných dohľadových centier, ktoré budú súčasťou systému včasného varovania	Používatelia nových a modernizovaných verejných digitálnych služieb, produktov a procesov	Počet používateľov digitálnych verejných služieb, produktov a procesov, ktoré boli novo vyvinuté alebo významne modernizované vďaka podpore pochádzajúcej z opatrení v rámci mechanizmu.	Počet	8	14	Uzatvorená pracovná zmluva	Počet zamestnancov as-is a to-be stav

3.5. ŠPECIFIKÁCIA POTRIEB KONCOVÉHO POUŽÍVATEĽA

Predmetom projektu nie je vývoj alebo rozvoj ISVS/elektronických služieb, ktoré majú grafické alebo iné používateľské rozhranie a sú určené pre občanov /podnikateľov, ďalej koncových používateľov. NCZI je povinný ako správca nadrezortného informačného systému zabezpečiť kybernetickú a informačnú bezpečnosť. Pre koncového používateľa je nevyhnutné zabezpečiť bezpečné a dostupné riešenie eslužieb, ktorych správcom je NCZI. Projekt zabezpečuje implementáciu technickej/bezpečnostnej infraštruktúry bez dopadu na biznisovú a aplikačnú časť systémov, preto žiadne nové potreby koncového používateľa nedefinuje.

3.6. RIZIKÁ A ZÁVISLOSTI

ID	NÁZOV RIZIKA a ZÁVISLOSTI	POPIS / NÁSLEDOK
1	Nebude možné naplniť všetky kvalitatívne požiadavky projektu.	Nebudú plne dosiahnuté očakávané benefity projektu.
2	Jednotlivé komponenty projektu nebudú vykazovať známky 100% kompatibility.	Vzhľadom na vytvorenie ekosystému je dôležité, aby jednotlivé prvky boli schopné komunikovať vzájomne a mali rovnaké východiskové požiadavky na obojsmernú programovú komunikáciu.
3	Nedostupnosť komponentov novej infraštruktúry	Nedostupnosť komponentov novej infraštruktúry, prípadne ich veľmi dlhé dodacie lehoty môžu mať negatívny vplyv na termín ukončenia projektu.
4	Projekt nebude realizovaný a nasadený podľa plánu.	V prípade omeškania dodávok projektu resp. v prípade omeškania nasadenia výstupov projektu, nebude možné efektívne a včas reagovať na bezpečnostné incidenty.

5	Nepridelené finančné prostriedky	Predčasné ukončenie projektu, predĺženie doby realizácie projektu.
6	Komplikácie s verejným obstarávaním	V prípade neskorého vypísania VO, prípadne komplikácií v procese VO by bol ohrozený začiatok implementačnej fázy.
7	Neúplné požiadavky	Neúplné požiadavky môžu spôsobiť predĺženie trvania projektu, navýšenie nákladov, z dôvodu potreby dodatočného obstarávania komponentov.
8	Vysoké náklady na prevádzku	Náklady na prevádzku budú vyššie ako plánované. Prekročenie plánovaných nákladov na prevádzku. Potreba dodatočných finančných zdrojov.
9	Ohrozenie prevádzky a dostupnosti systému	Ohrozenie prevádzky a dostupnosti systému z dôvodu možných kybernetických útokov.
10	Necertifikované technické prostredie	Od certifikácie technického prostredia budú závisieť mnohé nadväzné termíny v rámci realizácie ako aj celkovo vôbec možnosť projekt dokončiť.
11	Nedostatočné vyhodnotenie kvality	Neodhalenie slabých miest v jednotlivých fázach implementácie projektu.
12	Nesúčinnosť a nespoľahlivosť dodávateľa	Predčasné ukončenie projektu, alebo predĺženie doby realizácie projektu.
13	Nedostatok ľudských zdrojov	Predĺženie doby realizácie projektu. Výstupy projektu budú dodané v nedostatočnej kvalite.

Riziká a závislosti sú detailnejšie popísané v prílohe Zoznam rizík a závislostí (excel).

3.7. ALTERNATÍVY A MULTIKRITERIÁLNA ANALÝZA

3.7.1. STANOVENIE ALTERNATÍV POMOCOU BIZNISOVEJ VRSTVY ARCHITEKTÚRY

V rámcii biznisovej vrstvy architektúry sme porovnávali 3 variantné alternatívy riešenia súčasného stavu. Na základe identifikovaného rozsahu problému v projektovom zámere boli stanovené tri rôzne riešenia. Ako najefektívnejšia bola vybraná Alternatíva č. 2, taká, kt. pokrýva procesy a požiadavky všetkých stakeholderov a celú životnú situáciu rieši komplexne.

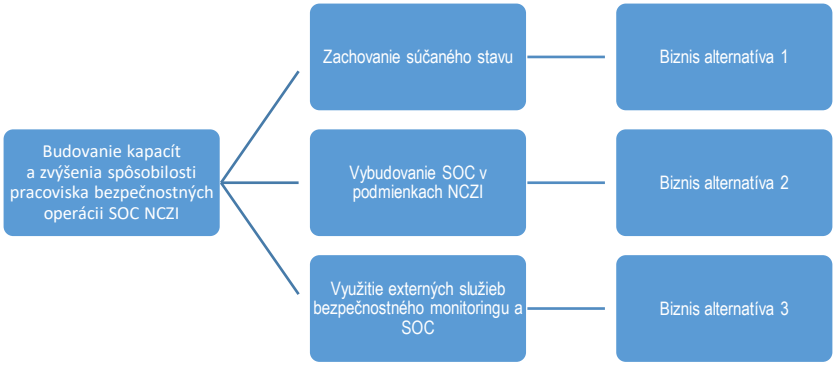
Alternatíva 1 - PONECHANIE SÚČASNÉHO STAVU
Prvou alternatívou je ponechanie existujúceho stavu ochrany informačných systémov a ochranu zdravotníckych informácií v prostredí národného zdravotníckeho informačného systému riešiť na základe existujúcej Zmluvy s CSIRT č.03378/2020/SK-CERT-002. Zachovanie pôvodného stavu nezabezpečí povinnosť ochrany informácií a informačných aktív a je v plnom rozpore s povinnosťami vyplývajúcimi zo zákona č.69/2018 Z.z. Rovnako dôjde k obmedzeniu spôsobilosti existujúceho pracoviska z dôvodu chýbajúcich finančných prostriedkov na ďalší rozvoj, dôsledkom čoho dôjde aj k podstatnému zníženie potenciálu zabezpečovania služieb SOC pre rezort zdravotníctva a mareniu efektivity minulých investícii.

Alternatíva 2 – VYBUDOVANIE SOC V PODMIENKACH NCZI
Táto alternatíva predstavuje komplexné a systémové riešenie voči kybernetickým útokom resp. voči politicky motivovaným kampaniam. Zabezpečí zavedenie systémových opatrení a zároveň vytvorí predpoklady na zefektívnenie poskytovaných služieb v oblasti zdravotnej starostlivosti. Realizáciou tohoto opatrenia sa zabezpečí systémové riešenie reakcie na kybernetické útoky a naplnia sa zákonom stanovené úlohy v oblasti kybernetickej bezpečnosti. Realizáciou tejto alternatívy dôjde k naplneniu predpokladov pre poskytovanie dostatočného rozsahu služieb pracoviska SOC pre NZIS ako aj pre organizácie spadajúce pod rezort zdravotníctva.

Hlavné prínosy tejto alternatívy predstavuje:
- technické vybavenie, ktorým sa zabezpečí zvýšenie viditeľnosti a kvality zbieraných a vyhodnocovaných informácií z informačných systémov, zvýšenie miery automatizácie a rozsahu procesov životného cyklu kybernetických incidentov a s tým spojené zníženie chybovosti ľudského faktoru.
- personálne zabezpečenie posilnením interného tímu, čím sa zvýši spôsobilosť a ušetria sa finančné prostriedky v porovnaní s využitím služieb tretích strán.

- procesná spôsobilosť zabezpečená vytvorením detailných postupov práce a dokumentácie, čím sa zabezpečí automatizácia a zníži chybovosť ľudského faktoru.

Alternatíva 3 – VYUŽITIE EXTERNÝCH SLUŽIEB BEZPEČNOSTNÉHO MONITORINGU A SOC
Detekcia bezpečnostných udalosti, zraniteľnosti a incidentov pre zabezpečenie ochrany zdravotníckych informácií v súvislosti s požiadavkami legislatívy prostredníctvom SOC služieb zabezpečených tretími stranami. Realizáciou tejto alternatívy dôjde k zvýšeniu finančného zaťaženia NCZI a štátneho rozpočtu pre potreby pokrytia nákladov spojených so zabezpečením služieb SOC. Využívanie služieb SOC poskytovaných treťou stranou zvyšuje dopady na GDPR postupovaním potenciálne citlivých dát a pravdepodobnosťou ich úniku. Taktiež dôjde k predraženiu prevádzky a zvýšenej potrebne kontrolných činnosti a z toho vyplývajúce finančné zaťaženie.



Obrázok 1 – Business alternatívy

3.7.2. MULTIKRITERIÁLNA ANALÝZA

Výber alternatív prebieha prostredníctvom MCA zostavenej na základe kapitoly Motivácia a rozsah projektu, 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)

Tabuľka č.6 – Kritéria pre MCA

	KRITÉRIUM	ZDÔVODNENIE KRIÉRIA	OBČAN/ PODNIKATEĽ	ÚRADNÍK	NCZI	MZSR	Ústavné a špecializované zdravotnícke zariadenia
STANOVENÉ ALTERNATÍVY	Kritérium A (KO) Kvalitnejšie a rýchlejšie riadenie kybernetickej bezpečnosti, Monitorovanie kritických informačných systémov.	Nový systém by mal výrazne skvalitniť poskytovanie služieb kybernetickej ochrany pre IS v zriaďovateľskej pôsobnosti MZ SR		X	X	X	X
	Kritérium B (KO) Zníženie	Automatizácia výkonu		X	X	X	X

	administratívnej náročnosti a zvýšenie efektívnosti detekcie bezpečnostných incidentov.	kybernetickej ochrany a hĺbková detekcia.					
	Kritérium C (KO) Integrácia všetkých používaných systémov.	Zjednotenie kybernetickej ochrany v rámci rezortu zdravotníctva.	X	X	X	X	X
	Kritérium D (KO) Jednotnosť procesov a používaných Aplikácií.	Jednotnosť procesov a postupov je základným cieľom poskytovania zdravotnej starostlivosti a iba tak sa dá zabezpečiť jej efektívne riadenie bezpečnosti.	X	X	X	X	X
	Kritérium E (KO) . Zber štruktúrovaných údajov o stave kybernetickej bezpečnosti IS-	Kvalitné a efektívne riadenie kybernetickej bezpečnosti sa dá zabezpečiť iba pomocou existencie štruktúrovaných informácií na základe ktorých sa dajú prijímať rýchle a kvalifikované rozhodnutia.	X		X	X	X
	Kritérium F Bezpečné prepojenie so systémami NZIS na elektronický prenos zdravotníckych informácií.	Systematické zvýšenie úrovne zabezpečenia prenosu citlivých Údajov.	X	X	X	X	X

Tabuľka č.7 – Vyhodnotenie MCA

ZOZNAM KRITÉRIÍ	ALTER-NATÍVA 1	SPÔSOB DOSIAHNUTIA	ALTER-NATÍVA 2	SPÔSOB DOSIAHNUTIA	ALTER-NATÍVA 3	SPÔSOB DOSIAHNUTIA
Kritérium A	nie	alternatíva 1 je zachovanie statusu quo bez realizácie projektu	áno	Implementáciou alternatívy 2 sa zabezpečí kvalitnejšie a rýchlejšie riadenie kybernetickej bezpečnosti, Monitorovanie kritických	áno	Implementáciou alternatívy 3 sa zabezpečí kvalitnejšie a rýchlejšie riadenie kybernetickej bezpečnosti, Monitorovanie kritických informačných systémov.

				informačných systémov.		
Kritérium B	nie	alternatíva 1 je zachovanie statusu quo bez realizácie projektu	áno	Implementácia alternatívy 2 sa zabezpečí zníženie administratívnej náročnosti a zvýšenie efektívnosti detekcie bezpečnostných incidentov.	áno	Implementácia alternatívy 3 sa zabezpečí zníženie administratívnej náročnosti a zvýšenie efektívnosti detekcie bezpečnostných incidentov.
Kritérium C	nie	alternatíva 1 je zachovanie statusu quo bez realizácie projektu	áno	Implementácia alternatívy 2 zabezpečí zjednotenie kybernetickej ochrany v rámci rezortu zdravotníctva.	nie	Implementácia alternatívy 3 nezabezpečí zjednotenie kybernetickej ochrany v rámci rezortu zdravotníctva.
Kritérium D	nie	alternatíva 1 je zachovanie statusu quo bez realizácie projektu	áno	Implementácia alternatívy 2 prispeje k jednotnosti procesov a používaných Aplikácií.	nie	Implementácia alternatívy 3 neprispeje k jednotnosti procesov a používaných Aplikácií.
Kritérium E	nie	alternatíva 1 je zachovanie statusu quo bez realizácie projektu	áno	Implementácia alternatívy 2 zabezpečí zber štruktúrovaných údajov o stave kybernetickej bezpečnosti IS.	áno	Implementácia alternatívy 3 zabezpečí zber štruktúrovaných údajov o stave kybernetickej bezpečnosti IS.
Kritérium F	nie	alternatíva 1 je zachovanie statusu quo bez realizácie projektu	áno	Implementácia alternatívy 2 sa zabezpečí bezpečné prepojenie so systémom NZIS na elektronický prenos zdravotníckych informácií.	áno	Implementácia alternatívy 3 sa zabezpečí bezpečné prepojenie so systémom NZIS na elektronický prenos zdravotníckych informácií.

Na základe vyhodnotenia MCA analýzy vychádza Alternatíva 2 ako jediná, ktorá spĺňa všetky požiadavky.

3.7.3. STANOVENIE ALTERNATÍV POMOCOU APLIKAČNEJ VRSTVY ARCHITEKTÚRY

Alternatívy na úrovni aplikačnej 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. Ako najvýhodnejšiu z danej analýzy považujeme Alternatívu 2. Výber Aplikačnej architektúry reflektuje výber nadradenej biznis architektúry.

3.7.4. STANOVENIE ALTERNATÍV POMOCOU TECHNOLOGICKEJ VRSTVY ARCHITEKTÚRY

Výber alternatívy na úrovni technologickej a bezpečnostnej vrstvy architektúry kopíruje výber alternatívy č. 2 na základe MCA. Riešenie bude prevádzkované na HW infraštruktúre NCZI a s dodávateľom bude podpísaná zmluva o podpore prevádzky SLA. Náklady na údržbu a prevádzku projektu sú uvedené v CBA analýze ako percentuálny pomer z obstarávacej ceny diela.

4. POŽADOVANÉ VÝSTUPY (PRODUKT PROJEKTU)

Výstupom projektu je funkčný, stabilný, efektívny, bezpečný systém, ktorý sa dosiahne doplnením SW a HW infraštruktúry. Výstupom bude aj dodanie používateľskej príručky, inštalačnej príručky a pokynov na inštaláciu (úvodnú/opakovanú), prevádzkový opis a pokyny pre servis, údržbu a diagnostiku, pokyny na obnovu pri výpadku alebo havárii (Havarijný plán) a bezpečnostný projekt. Na dodržanie štandardov sa použije M-04 Audit kvality zameraný na výstupy z iniciačnej, realizačnej a dokončovacej fázy projektu.

Realizácia projektu bude v zmysle vyhlášky ÚPVII č. 85/2020 Z. z. pozostávať z uvedených etáp:

- Analýza a dizajn,
- Nákup technických prostriedkov, programových prostriedkov a služieb
- Implementácia a testovanie,
- Nasadenie.

NCZI SR bude pri implementácii postupovať v zmysle vyhlášky ÚPVII č. 85/2020 Z. z. a požadované výstupy budú dodávane primerane vzhľadom na charakter projektu:

Etapa	Požadované výstupy
Analýza a dizajn	**Úvodná správa (Projektový iniciálny dokument, ďalej ako „PID") pre všetky funkčné oblasti** - Zoznam požiadaviek - Akceptačné kritériá - Rámcová špecifikácia riešenia (Popis produktu, Dekompozícia produktu, Vývojový diagram produktu) - Biznis architektúra - Aplikačná architektúra - Technologická architektúra – časť systémová architektúra - Bezpečnostná architektúra - Stratégia testovania - Plán testovania - Testovacie scenáre a prípady **Detailná funkčná špecifikácia riešenia** - vypracovanie registratúrneho poriadku - detailný popis funkcionality a biznis požiadaviek, - Blokové a dátové modely finálneho produktu **Detailná technická špecifikácia, pre všetky systémy samostatne** - technická architektúra – časť fyzická architektúra - špecifikácia správy používateľov a používateľských profilov (vrátane rolí a práv) - špecifikácia podpory identifikácie používateľov a autentifikácie vykonávaných činností - špecifikácia technologických riešení a predpokladov na dosiahnutie výkonnostných požiadaviek - Plán testovania - Testovacie scenáre a prípady - Plán Implementácie
Implementácia a testovanie	**Implementácia:** **Implementačný plán pre všetky funkčné oblasti samostatne:** - Implementácia systémov pre všetky funkčné oblasti samostatne - Implementácia integrácií systémov pre všetky funkčné oblasti samostatne - Úvodná konfigurácia systému podľa reálnych biznis procesov pre testovacie účely - Vybudovanie testovacieho prostredia, jeho nasadenie a oživenie diela pre všetky systémy a pre všetky funkčné oblasti samostatne - Implementácia procesov **Testovanie:** **Zrealizovanie testovania minimálne v nasledovnom rozsahu:** - Funkčné testy - Bezpečnostné testy - v rozsahu dokumentu „Metodika pre systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti" (dostupná na https://www.csirt.gov.sk/doc/MetodikaZabezpeceniaIKT_v2.0.pdf) - Záťažové testy - Systémové integračné testy - Testy použiteľnosti

	- Používateľské akceptačné testovanie
Nasadenie	**Nasadenie do produkcie:** - Príprava produkčného prostredia - Administratívna príprava produkčného prostredia (procesy, dokumentácia) - Inštalácia riešenia do produkčného prostredia - Sprístupnenie riešenia v produkčnom prostredí vybraným používateľom

5. NÁHĽAD ARCHITEKTÚRY

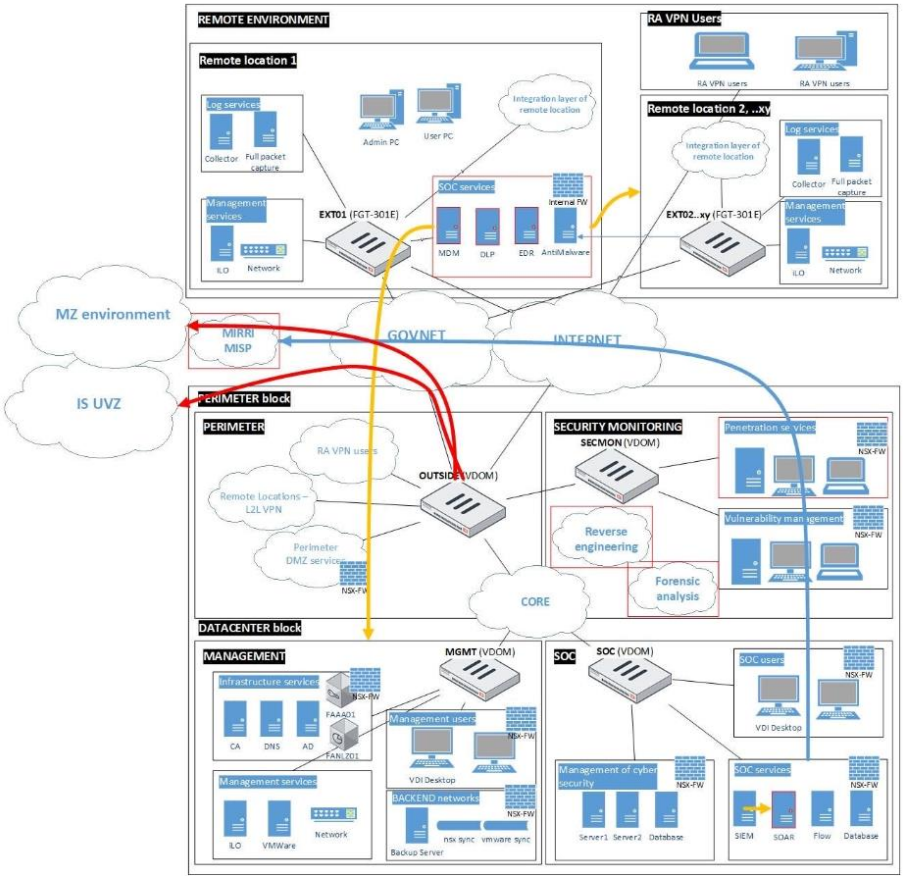
Za účelom zvýšenia úrovne zavedených postupov a opatrení týkajúcich sa kybernetickej a informačnej bezpečnosti (KIB) v NCZI je potrebné konsolidovať existujúcu bezpečnostnú architektúru a dobudovať security operation center implementáciou nových a inováciou existujúcich bezpečnostných nástrojov a procesov, a to najmä v nasledovných oblastiach:

- kybernetická ochrana a bezpečnostný monitoring a identifikácia bezpečnostných incidentov,
- riadenie bezpečnostných incidentov,
- ochrana proti externým hrozbám,
- ochrana dát, dátových prenosov a komunikácie,
- zvyšovanie bezpečnostného povedomia,
- implementácia bezpečnostných opatrení na zabezpečenie súladu so zákonom,

Služby a funkcie uvedené v tejto kapitole poskytujú z dôvodu, že sa jedná o projekt kybernetickej bezpečnosti len základné informácie a základný architektonický rámec riešenia, ktoré by malo byť implementované projektom. Budúce riešenie zabezpečenia informačnej a kybernetickej bezpečnosti sa bude skladať najmä z nasledovných funkcií:

- **Kybernetická ochrana a detekcia škodlivých aktivít a bezpečnostných incidentov:** Bezpečnostný monitoring IS, platforiem, aplikácií a používateľských činností a aktivít. Monitoring sietí, monitoring činností a aktivít privilegovaných používateľov. Analýza založená na big-data a machine learning algoritmoch.
- **Riadenie bezpečnostných incidentov:** Identifikácia a hlásenie bezpečnostných incidentov, registrácia, kategorizácia a klasifikácia bezpečnostných incidentov. Akceptácia bezpečnostných incidentov a určenie riešiteľov. Analýza a vyšetrovanie bezpečnostných incidentov a zber dôkazov. Riešenie bezpečnostných incidentov a obnova prevádzky, uzatvorenie bezpečnostných incidentov, vyhodnotenie bezpečnostných incidentov, zavedenie do KB DB, spätná väzba a poučenie sa z bezpečnostného incidentu.
- **Zvýšenie ochrany pred útokmi z externého prostredia:** Ochrana pred malware a ransomware, manažment bezpečnosti sietí, manažment bezpečnostných konfigurácií (implementácia systému pre jednotnú správu a deployment bezpečnostných politík a bezpečnostných konfigurácií).
- **Ochrana dát, dátových prenosov a komunikácie:** Bezpečnosť virtualizovaných prostredí, ochrana dát na úrovni databáz a dátových úložísk, ochrana dát na úrovni koncových zariadení. Riadenie prístupov (implementácia nástrojov IAM – riešenie IAM bude implementované z DOP-OPII-16/2023, jeho prevádzka ani údržba nebude hradená z tohoto projektu). Proces bezpečnej výmeny informácií prostredníctvom EWS s vládnou jednotkou CSIRT, integráciou na JISKB, riadenie SW záplat (Patch management), manažment zraniteľností.
- **Zvýšenie ochrany pred útokmi z externého prostredia:** Ochrana pred malware a ransomware. Manažment bezpečnosti sietí, manažment bezpečnostných konfigurácií.

Bloková schéma architektúry riešenia:



Jednotlivé funkcie budú zabezpečovať nasledujúce komponenty architektúry riešenia:

FORENZNÝ LAB
Modul Forezný lab je zložený z HW a SW nástroja na Forenznú analýzu. Modul bude zabezpečovať digitálnu forenznú analýzu a správu elektronických dôkazov. Modul je určený pre zber, analýzy a správy dát a vizualizáciu ich vzájomných vzťahov. Taktiež implementuje nástroj na extrakciu a analýzu dát z mobilných zariadení a digitálnych médií, dešifrovanie týchto dát a generovanie reportov.

PENTEST LAB
Modul pre penetračné testovanie zabezpečí implementovanie testovania bezpečnosti webových aplikácií (Web Application Security Testing Tool), ktorý sa používa na identifikáciu a odstraňovanie bezpečnostných zraniteľností vo webových aplikáciách. Modul bude zabezpečovať automatizáciu penetračného testovania počas životného cyklu vývoja softvérových riešenie (SDLC).
Cieľom implemntácie pentest labu je automatizované skenovanie webových aplikácií s cieľom odhaliť rôzne druhy bezpečnostných zraniteľností.

Súčasťou pentest labu bude nástroj na simuláciu protivníka a operácii červeného tímu, ako spôsob hodnotenia bezpečnosti, ktoré replikujú taktiku a techniky pokročilého protivníka v sieti tzv. "red teaming" alebo "adversary simulation," pri ktorých bezpečnostné tímy, alebo iné organizácie testujú svoju vlastnú bezpečnosť pomocou nástrojov a taktík, ktoré by mohli použiť skutoční útočníci.Zatiaľ čo penetračné testy sa zameriavajú na neopravené zraniteľnosti a nesprávne konfigurácie, tieto posúdenia sú prínosom pre bezpečnostné operácie a reakciu na incidenty.

MALVÉR LAB
Malvér lab implementuje sadu nástrojov:
Nástroj automatizovaného reverzného inžinierstva na analýzu softvérových aplikácií, zdrojového kódu a iných digitálnych entít za účelom pochopenia ich fungovania, identifikácie zraniteľností a iných bezpečnostných rizík.
Nástroj reverzného inžinierstva na analýzy binárneho kódu pre prácu s binárnym kódom a disassemblovaním programov.
Nástroj, ktorý umožňuje analýzu škodlivého softvéru a jeho správanie v izolovanom a bezpečnom prostredí.
Nástroj na detekciu, monitorovanie a zbieranie informácií o kybernetických útočníkoch a hrozbách v informačných systémoch formou vytvárania falošného cieľa pre útočníkov.

SOAR – MONITROING

Systém pre orchestráciu a automatizáciu bezpečnostných procesov (SOAR) bol vyvinutý s cieľom zefektívniť a urýchliť manuálne a časovo náročné úlohy v oblasti kybernetickej bezpečnosti. Jeho účelom je automatizovať opakujúce sa pracovné postupy v pracovisku Security Operations Center (SOC), orchestrovať rôzne bezpečnostné nástroje a zabezpečiť pokročilú, rýchlu, efektívnu a automatizovanú reakciu na bezpečnostné incidenty. SOAR systém umožňuje šetriť čas, finančné prostriedky a ľudské zdroje, zároveň posilňuje kybernetickú obranu organizácie. Obsahuje verejne dostupnú knižnicu s preddefinovanými pracovnými postupmi (workflows) a umožňuje organizáciám definovať vlastné pracovné postupy. Ďalšou výhodou je jednoduchá integrácia so SIEM (Security Information and Event Management) riešeniami, manažmentom zraniteľnosti a ticketovacími nástrojmi, čo zabezpečuje prehľadný reporting o spustených pracovných postupoch a celkový prehľad o kybernetických hrozbách a bezpečnostných incidentoch.

SIEŤOVÝ FW (LOGSOURCE)
Zabezpečenie sieťového perimetra siete NCZI, z ktorej pristupujú správcovia k informačným systémom NZIS.

INTEGRÁCIA NA THREAT INTELIGENCE PLATFORMU A JISKB
NCZI plánuje dobudovať riešenie opensource servera MISP ako platformy na zhromažďovanie, ukladanie, distribúciu a zdieľanie indikátorov kybernetickej bezpečnosti a hrozieb týkajúcich sa analýzy incidentov kybernetickej bezpečnosti a analýzy malvéru.

EDR
Cieľom implemntácie pokročilého riešenia Endpoint Detection and Response (EDR) je zabezpečiť bezpečnosť a ochranu všetkých koncových zariadení a serverov, v správe NCZI. Prioritou implemntácie modulu EDR je detekcia, monitorovanie a rýchla reakcia na kybernetické hrozby. Implemntáciou modulu EDR sa zabezpečí schopnosť identifikovať a zabrániť rôznym typom hrozieb, vrátane malvéru, ransomvéru a iných škodlivých aktivít, pričom toto riešenie podporuje tkz. „samoučiaci režim", ochranu pred neznámymi hrozbami a anti-ransomware ochranu. Riešenie umožní monitorovať všetky koncové zariadenia v reálnom čase, ponúknuť centralizovanú správu, vytvárať správy pre bezpečnostných administrátorov a definovať politiky pre jednotlivé skupiny administrátorov. EDR riešenie umožní rýchlu reakciu na incidenty, vrátane izolácie postihnutých zariadení, odstránenia hrozieb a obnovy systémov, a podporí threathunting s funkciou vizualizácie a minimálnou 30-dňovou retenciou dát.

MDM
Modul pre správu a monitorovanie mobilných zariadení, ako sú mobilné telefóny a tablety, používané zamestnancami v pracovnom prostredí. Nástroj zabezpečí bezpečnosť firemných dát uložených na mobilných zariadeniach a zabráni neoprávnenému prístupu alebo úniku citlivých informácií. Implemntáciou nástroja sa vytvorí centralizovaný systém pre správu všetkých mobilných zariadení a aplikácií, vrátane možnosti vzdialenej konfigurácie a ich aktualizácie. Podpora BYOD (Bring Your Own Device) - umožní zamestnancom používať vlastné zariadenia v pracovnom prostredí, s dôrazom na oddelenie pracovných a osobných dát. Podpora COPE (corporate-owned, personally enabled) - umožní zamestnancom používať mobilné zariadenie vo vlastníctve zamestnávateľa pre pracovné aj osobné účely. Modul MDM Zabezpečí dodržiavanie nastavených pravidiel a politík spoločnosti a generovať správy o stave zariadení a aplikácií. Riešenie umožní registrovať a konfigurovať zariadenia, spravovať aplikácie a ich distribúciu, riadiť prístup a oprávnenia užívateľov, monitorovať a zaznamenávať aktivity, vzdialene spravovať a uzamknúť zariadenie v prípade jeho straty alebo krádeže.

DLP
Modul pre identifikáciu, monitorovanie a ochranu citlivých dát a informácií pred ich stratou. Riešenie poskytne automatizovanú identifikáciu, klasifikáciu a monitorovanie citlivých údajov, zároveň bude zaznamenávať užívateľské akcie vykonávané v rámci Office 365 cloudu, vrátane základných súborových operácií, ako je sťahovanie a zdieľanie. Modul DLP bude monitorovať a vyhodnocovať emailovú komunikáciu pre všetkých užívateľov vrátane tých, ktorí používajú Outlook Web App, osobné alebo mobilné zariadenia. Riešenie umožní úplné zablokovanie užívateľských akcií, informatívne upozornenia užívateľa a umožní logovanie užívateľských akcií, a to aj s ochranou citlivých dát. Nástroj DLP umožňuje definovať citlivé dáta pomocou preddefinovaných slovníkov a algoritmov, ako aj vlastných reťazcov a regulárnych výrazov. Riešenie umožní blokovať odosielanie dát s citlivým obsahom mimo koncových staníc a spravovať bežné komunikačné kanály, ako sú e-mail, web upload, externé zariadenia, IM komunikačné nástroje a synchronizácia s cloudovými aplikáciami. Riešenie by malo byť schopné detegovať dáta obsahujúce citlivý obsah, uložené na koncových staniciach alebo na zdieľaných sieťových diskoch, a integrovať sa s klasifikáciou tretích strán uložených v metadátach súborov. Okrem toho by malo byť schopné riadiť použitie USB zariadení, pamäťových kariet, Bluetooth zariadení a optických diskov, a umožniť nastavenie iba na čítanie pre pripojené zariadenia, pričom zaznamenáva všetky pripojené zariadenia.

Potreba jednotlivých komponentov cieľovej architektúry vychádza z analýzy súčasného stavu bezpečnostnej a technickej architektúry prostredia NCZI, analýzy rizík (ide o utajované a citlivé informácie, výsledky analýzy rizík sú neverejné a prístupné len pracovníkom s príslušnou bezpečnostnou previerkou) a potreby naplnenia legislatívnych požiadaviek. Jednotlivé komponenty architektúry bližšie popisujeme v dokumente Prístup k projektu, kde uvádzame technickú špecifikáciu a požiadavky na jednotlivé komponenty, spoločne s motiváciou, odôvodnením a účelom týchto komponentov.

6. LEGISLATÍVA

Projekt nepredpokladá potrebu legislatívnych zmien pre naplnenie cieľov a dodanie výstupov projektu. V tejto kapitole sú vymenované legislatívne normy, ktoré sa týkajú informačných systémov verejnej správy a agendy Národného centra zdravotníckych informácií. Zoznam neobsahuje usmernenia a technické predpisy. Zoznam legislatívnych noriem v tomto dokumente iba orientačný.

Zákon Národnej rady Slovenskej republiky č. 145/1995 Z. z. o správnych poplatkoch v znení neskorších predpisov,
Zákon č. 71/1967 Zb. o správnom konaní (správny poriadok) v znení neskorších predpisov.

Zákony a vyhlášky týkajúce sa eGovernmentu:

Zákon č. 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách) v znení neskorších predpisov
Zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
Zákon č. 9/2010 Z. z. o sťažnostiach v znení neskorších predpisov
Zákon č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
Zákon č. 357/2015 Z. z. o finančnej kontrole a audite a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
Zákon č. 10/1996 Z. z. o kontrole v štátnej správe v znení neskorších predpisov
Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe
Vyhláška ÚPVII č. 78/2020 Z. z. o štandardoch pre informačné technológie verejnej správy
Zákon č. 540/2001 Z. z. o štátnej štatistike
Zákon č. 211/2000 Z. z. o slobodnom prístupe k informáciám (zákon o slobode informácií)
Zákon č. 177/2018 Z. z. o niektorých opatreniach na znižovanie administratívnej záťaže využívaním informačných systémov verejnej správy a o zmene a doplnení niektorých zákonov (zákon proti byrokracii)
Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti
Vyhláška ÚPVII č. 85/2020 Z. z. o riadení projektov
Zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy,
Výnos č. 55/2014 Z. z. o štandardoch pre informačné systémy verejnej správy,
Výnos č. 478/2010 Z. z. o základnom číselníku úsekov verejnej správy a agend verejnej správy,
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),
Vyhláška ÚV SR č. 8/2014 Z. z., ktorou sa vykonávajú niektoré ustanovenia zákona o e-Governmente,
Vyhláška č. 25/2014 Z. z. o integrovaných obslužných miestach a podmienkach ich zriaďovania, označovania, prevádzky a o sadzobníku úhrad,
Výnos MF SR č. MF/009269/2014-173 o jednotnom formáte elektronických správ vytváraných a odosielaných prostredníctvom prístupových miest,
Vyhláška MF SR č. 275/2014 Z. z. o zaručenej konverzii.
Zákon č. 215/2002 Z. z. o elektronickom podpise,
Vyhláška NBÚ č. 131/2009 Z. z. o certifikátoch a kvalifikovaných certifikátoch,
Vyhláška NBÚ č. 132/2009 Z. z. o podmienkach na poskytovanie akreditovaných certifikačných služieb a o požiadavkách na audit, rozsah auditu a kvalifikáciu audítorov,
Vyhláška NBÚ č. 133/2009 Z. z. o obsahu a rozsahu prevádzkovej dokumentácie vedenej certifikačnou autoritou a o bezpečnostných pravidlách a pravidlách na výkon certifikačných činností,
Vyhláška NBÚ č. 134/2009 Z. z., ktorou sa ustanovujú podrobnosti o požiadavkách na bezpečné zariadenia na vyhotovovanie časovej pečiatky a požiadavky na produkty pre elektronický podpis,
Vyhláška NBÚ č. 135/2009 Z. z. o vyhotovení a overovaní elektronického podpisu a časovej pečiatky,
Vyhláška NBÚ č. 136/2009 Z. z. o spôsobe a postupe používanie elektronického podpisu v obchodnom styku a administratívnom styku,
Zákon č. 351/2011 Z. z. o elektronických komunikáciách,
Zákon č. 22/2004 Z. z. o elektronickom obchode,
Zákon č. 220/2007 Z. z. o digitálnom vysielaní,
Zákon č. 45/2011 Z. z. o kritickej infraštruktúre,
Výnos MV SR č. 525/2011 Z. z. o štandardoch pre elektronické informačné systémy na správu registratúry,
Zákon č. 253/1998 Z. z. o hlásení pobytu občanov SR a registri obyvateľov,
Zákon č. 3/2010 Z. z. o národnej infraštruktúre pre priestorové informácie,
Zákon č. 272/2015 Z. z. o registri právnických osôb, podnikateľov a orgánov verejnej moci a o zmene a doplnení niektorých zákonov,
Zákon č. 455/1991 Zb. o živnostenskom podnikaní (Živnostenský zákon),
Vyhláška č. 84/2016 Z. z. Vyhláška Ministerstva zdravotníctva, ktorou sa ustanovujú určujúce znaky jednotlivých druhov zdravotníckych zariadení,
Nariadenie vlády Slovenskej republiky č. 296/2010 Z. z. o odbornej spôsobilosti na výkon zdravotníckeho povolania, spôsobe ďalšieho vzdelávania zdravotníckych pracovníkov, sústave špecializačných odborov a sústave certifikovaných pracovných činností,
Nariadenie vlády Slovenskej republiky č. 513/2011 Z. z. o používaní profesijných titulov a ich skratiek viažucich sa na odbornú spôsobilosť na výkon zdravotníckeho povolania,
Zákon č. 125/2015 Z. z. o registri adries a o zmene a doplnení niektorých zákonov,

Nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu
Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 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)
Zákon č. 153/2013 Z. z. o národnom zdravotníckom informačnom systéme a o zmene a doplnení niektorých zákonov
Zákon č. 581/2004 Z. z. o zdravotných poisťovniach, dohľade nad zdravotnou starostlivosťou
Zákon č. 355/2007 Z. z. o ochrane, podpore a rozvoji verejného zdravia a o zmene a doplnení niektorých zákonov
Zákon č. 578/2004 Z. z. o poskytovateľoch zdravotnej starostlivosti, zdravotníckych pracovníkoch, stavovských organizáciách v zdravotníctve
Zákon č. 362/2011 Z. z. o liekoch a zdravotníckych pomôckach
Zákon č. 576/2004 Z. z. o zdravotnej starostlivosti, službách súvisiacich s poskytovaním zdravotnej starostlivosti
Zákon č. 538/2005 Z. z. o prírodných liečivých vodách, prírodných liečebných kúpeľoch, kúpeľných miestach a prírodných minerálnych vodách a o zmene a doplnení niektorých zákonov
Zákon č. 577/2004 Z. z. o rozsahu zdravotnej starostlivosti uhrádzanej na základe verejného zdravotného poistenia a o úhradách za služby súvisiace s poskytovaním zdravotnej starostlivosti
Zákon č. 579/2004 Z. z. o záchrannej zdravotnej službe
Zákon č. 580/2004 Z. z. o zdravotnom poistení a o zmene a doplnení zákona č. 95/2002 Z. z. o poisťovníctve
Vyhláška č. 191/2022 Z. z. Vyhláška Ministerstva zdravotníctva Slovenskej republiky, ktorou sa ustanovujú podrobnosti o postupe, metódach, okruhu spravodajských jednotiek a lehotách hlásenia údajov do Národného registra zdravotníckych pracovníkov a jeho charakteristiky
Vyhláška č. 74/2014 Z. z. Vyhláška Ministerstva zdravotníctva Slovenskej republiky, ktorou sa ustanovuje zoznam hlásení do národných zdravotných registrov, ich charakteristiky, podrobnosti o obsahu národných zdravotných registrov, postupe, metódach, okruhu spravodajských jednotiek a lehotách hlásení do národných zdravotných registrov
Vyhláška 141/2016 Z. z. Vyhláška Ministerstva zdravotníctva Slovenskej republiky, ktorou sa mení a dopĺňa vyhláška Ministerstva zdravotníctva Slovenskej republiky č. 74/2014 Z. z.
Vyhláška č. 10/2014 Z. z. Vyhláška Ministerstva zdravotníctva Slovenskej republiky, ktorou sa ustanovuje zoznam štatistických výkazov v zdravotníctve, podrobnosti o postupe, metódach, okruhu spravodajských jednotiek a lehotách hlásení v rámci štatistického zisťovania v zdravotníctve a ich charakteristiky
Vyhláška č. 44/2014 Z. z. Vyhláška Ministerstva zdravotníctva Slovenskej republiky, ktorou sa ustanovujú podrobnosti o postupe, metódach, okruhu spravodajských jednotiek a lehotách hlásení pri zisťovaní udalostí charakterizujúcich zdravotný stav populácie a ich charakteristiky
Vyhláška č. 107/2015 Z. z. Vyhláška Ministerstva zdravotníctva Slovenskej republiky, ktorou sa ustanovujú štandardy zdravotníckej informatiky a lehoty poskytovania údajov
Metodika Jednotný dizajn manuál elektronických služieb verejnej správy (dostupným na https://www.mirri.gov.sk/sekcie/oddelenie-behavioralnych-inovacii/jednotny-dizajn-manual-elektornickych-sluzieb-verejnej-spravy/index.html)
Metodické pokyny, usmernenia a príručky zverejnené na https://metais.vicepremier.gov.sk/help.
Pri tvorbe, vývoji a implementácii diela dodržiavať bezpečnostné požiadavky špecifikované v Metodike pre systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti (dostupná na https://www.csirt.gov.sk/wp-content/uploads/2021/08/MetodikaZabezpeceniaIKT_v2.1.pdf?csrt=3181741314547744407),
Pri tvorbe, vývoji a implementácii Diela, ktoré je realizované v rámci projektu financovaného z Operačného programu Integrovaná infraštruktúra, Zákonom o eGovernmente a Metodickým usmernením (č. 3639/2019/oDK-1) o postupe zaraďovania referenčných údajov do zoznamu referenčných údajov vo väzbe na referenčné registre a vykonávania postupov pri referencovaní (dostupným na https://metais.vicepremier.gov.sk/help a Postup-pripojenia-OVM-v-roli-konzumenta-udajov-1.pdf (datalab.digital)) a Používateľskej príručky na registráciu URI v MetaIS (dostupná na Pouzivatelska_prirucka_na_registraciu_URI_v_MetaIS_v3-5.pdf (datalab.digital))
Vyhláška Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky č. 545/2021 Z. z., ktorou sa mení a dopĺňa vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 85/2020 Z. z. o riadení projektov v znení neskorších predpisov
Vyhláška Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky č. 546/2021 Z. z., ktorou sa mení a dopĺňa vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 78/2020 Z. z. o štandardoch pre informačné technológie verejnej správy v znení neskorších predpisov
Vyhláška Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky č. 547/2021 Z. z. o elektronizácii agendy verejnej správy
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
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

7. ROZPOČET A PRÍNOSY

NÁKLADY

Sumarizácia nákladov:

Typ aktivity	Oblasť výdavku	Suma	OPEX / CAPEX	Int / ext	Zdroj finacovania - %						
					Suma %	Vlastné OPEX	Vlastné CAPEX	ESIF OPEX	ESIF CAPEX	POO OPEX	POO CAPEX
Hlavné aktivity	Vývoj aplikácií	2 982 972 €	OPEX	Externé							
			CAPEX	Externé	100%						100%
			OPEX	Interné	100%					100%	
	Nákup HW a SW	3 402 051 €	OPEX	Externé							
			CAPEX	Externé	100%						100%
			OPEX	Interné							
Prevádzka	Aplikácie	0 €	OPEX	Externé							
			CAPEX	Externé							
			OPEX	Interné							
	HW a SW	1 524 243 €	OPEX	Externé	100%	100%					
			CAPEX	Externé	100%		100%				
			OPEX	Interné							
Podporné aktivity	Projekový manažment	229 068 €	OPEX	Externé							
			OPEX	Interné	100%					100%	
	Publicita	0 €	OPEX	Externé							
			OPEX	Interné							
	Ostatné výdavky		Ostatné zmiešané výdavky								
Výstupné náklady		0 €		Externé							
				Interné							
SPOLU		8 138 334 €		-							

Sumarizácia nákladov a prínosov riešenia za obdobie 10 rokov:

TO BE - AS IS (€, SUM)			Spolu	SOC služby	Forenzný lab	Malvér lab	Pentest lab	SOAR - monitroing	Vybavenie pracoviska SOC/ HW	sieťový FW (logsource)	EDR	MDM	DLP	Školenia
Náklady s DPH			**8 138 334 €**	**3 089 989 €**	**1 672 763 €**	**310 631 €**	**84 707 €**	**709 642 €**	**1 169 285 €**	**190 139 €**	**304 962 €**	**187 386 €**	**204 070 €**	**214 760 €**
	Všeobecný materiál		- €	- €	- €	- €	- €	- €	- €	- €	- €	- €	- €	- €
	IT - CAPEX		5 218 028 €	1 314 048 €	1 276 927 €	242 246 €	66 720 €	558 948 €	862 383 €	140 902 €	240 203 €	147 594 €	160 735 €	207 322 €
		Aplikácie	*1 314 048 €*	*1 314 048 €*	- €	- €	- €	- €	- €	- €	- €	- €	- €	- €
		SW	*2 070 458 €*	- €	*679 142 €*	*206 606 €*	*66 720 €*	*558 948 €*	- €	*10 511 €*	*240 203 €*	*147 594 €*	*160 735 €*	- €
		HW	*1 833 522 €*	- €	*597 786 €*	*35 640 €*	- €	- €	*862 383 €*	*130 391 €*	- €	- €	- €	*207 322 €*
	IT - OPEX		2 691 237 €	1 668 924 €	355 932 €	61 491 €	16 174 €	135 502 €	275 963 €	44 273 €	58 231 €	35 780 €	38 966 €	- €
		Aplikácie	*1 668 924 €*	*1 668 924 €*	- €	- €	- €	- €	- €	- €	- €	- €	- €	- €
		SW	*501 929 €*	- €	*164 640 €*	*50 086 €*	*16 174 €*	*135 502 €*	- €	*2 548 €*	*58 231 €*	*35 780 €*	*38 966 €*	- €
		HW	*520 384 €*	- €	*191 291 €*	*11 405 €*	- €	- €	*275 963 €*	*41 725 €*	- €	- €	- €	- €
	Riadenie projektu		229 068 €	107 017 €	39 904 €	6 894 €	1 813 €	15 191 €	30 939 €	4 964 €	6 528 €	4 011 €	4 369 €	7 438 €
	Výstupné náklady		- €	- €	- €	- €	- €	- €	- €	- €	- €	- €	- €	- €
Prínosy			- **18 466 212 €**	- **7 200 000 €**	- **1 980 000 €**	- **1 584 000 €**	- **7 702 212 €**	**- €**	**- €**	**- €**	**- €**	**- €**	**- €**	**- €**
	Finančné prínosy		- €	- €	- €	- €	- €	- €	- €	- €	- €	- €	- €	- €
		Administratívne poplatky	- €	- €	- €	- €	- €	- €	- €	- €	- €	- €	- €	- €
		Ostatné daňové a nedaňové príjmy	- €											
	Ekonomické prínosy		- 18 466 212 €	- 7 200 000 €	- 1 980 000 €	- 1 584 000 €	- 7 702 212 €	- €	- €	- €	- €	- €	- €	- €
		Občania (€)	- €	- €	- €	- €	- €	- €	- €	- €	- €	- €	- €	- €
		Úradníci (€)	- €	- €	- €	- €	- €	- €	- €	- €	- €	- €	- €	- €
		Úradníci (FTE)	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
		Kvalitatívne prínosy	- *18 466 212 €*	- *7 200 000 €*	- *1 980 000 €*	- *1 584 000 €*	- *7 702 212 €*	- €	- €	- €	- €	- €	- €	- €
	Nevyčíslené spoločenské prínosy													
		(prosíme doplniť)...												

Interpretácia výsledkov:

Ekonomická a finančná efektívnosť projektu je v analýze prínosov a nákladov hodnotená kvantitatívne pomocou nasledujúcich ukazovateľov:

Pomer prínosov a nákladov (BCR): 2,19

Rozpočet projektu: 6 614 091,15 € €
Výška žiadosti o PPM: **6 614 091,15 €**

Náklady projektu a výšku rozpočtu môžeme rozdeliť nasledovne:

Hlavné aktivity:

- **Externé služby:** 1 314 048,00 €
- **Nákup technických prostriedkov, programových prostriedkov a služieb:** 3 402 051,15 €
- **Interné kapacity:** 1 668 924,00 €

Podporné aktivity: 229 068,00 €

PRÍNOSY

Bližší výpočet prínosov je definovaný v dokumente BC/CBA.

Na základe analýzy a v nej použitých konzervatívnych odhadov projekt je návratnou investíciou a BCR projektu je 2,19

Zamedzenie výpadku eSlužieb eZdravia z dôvodu doplnenia HW infraštruktúry:
% zníženia výpadkov infraštruktúry z dôvodu výmeny a doplnenie niektorých kľúčových HW komponentov infraštruktúry. Prínos je počítaný ako rozdiel medzi % výpadkov infraštruktúry AS-IS a TO-BE *počet používateľov *vyťaženie používateľov *superhrubá mzda/hod *počet hodín za rok (počet pracovných dní * počet hodín/deň).

Zdroj výpadkov AS-IS: Monitoring sieťových komponentov a serverov
Zdroj výpadkov TO-BE: Interne nastavená úroveň dostupnosti 99,5%, čo je aj úroveň dostupnosti vládneho cloudu, táto dostupnosť bude garantovaná aj rezortným organizáciám
Zdroj vyťaženie používateľov: Meranie realizované NCZI

Zníženie pravdepodobnosti DDoS
Projekt predpokladá postupné zavedenie opatrení (HW a SW) do prevádzky. Pravdepodobnosť odvrátenia DDoS útoku po nasadení opatrení je viac ako o 50-80% vyššia. Prínos je počítaný ako zvýšenie odolnosti bezpečnostného perimetra voči pravdepodobnému DDoS útoku. Prínos je vypočítaný ako pravdepodobnosť DDoS podľa štatistík minulých incidentov (DDoS útokov) *počet používateľov používajúcich IS *% alokácia zamestnanca *priemerná dĺžka trvania výpadku pri DDoS v hod. *priemerná superhrubá hodinová mzda.
Zdrojové údaje pravdepodobností vychádzajú z predchádzajúcich incidentov a monitorovacích zariadení na sieťovom perimetri

Zdroj pravdepodobnosti DDoS AS-IS: početnosť a efektivita DDoS útokov počas predchádzajúcich incidentov
Zdroj pravdepodobnosti DDoS TO-BE: zníženie počtu a efektivity nadchádzajúcich DDoS útokov naNCZI zavedením opatrení
Zdroj priemerná dĺžka trvania výpadku pri DDoS: Expertný odhad Manažéra kybernetickej bezpečnosti vychádzajúci z minulého výpadku pri DDoS útoku na infraštruktúru NCZI.

Zamedzenie výpadku infraštruktúry z dôvodu zníženia pravdepodobnosti dopadu závažného kybernetického útoku
Riziko dopadu veľmi závažného incidentu podľa internej rizikovej analýzy je v súčasnosti 5%. Aj keď z praxe vyplýva, že periodicita takéhoto incidentu je 1 krát za 10r. Nasadením riešenia dôjde k zníženiu pravdepodobnosti dopadu závažného incidentu o polovicu. Zároveň zmenou bezpečnostnej architektúry, zálohovania a zavedením Bussiness continuty manažmentu dôjde k zníženiu doby obnovy z 10 (8 prac.) dní na 5 dní.
Zdrojové údaje a pravdepodobností vychádzajú z rizikovej analýzy a plánu kontinuity činností (BCP)

Zdroj pravdepodobnosti výpadku AS-IS: predchádzajúce incidenty a ich dopad na prevádzku Zároveň ½ z Expertného odhadu Manažéra kybernetickej bezpečnosti NCZI.
Zdroj pravdepodobnosti výpadku TO-BE: zníženie počtu incidentov a ich efektivity na prevádzku systémov zavedením opatrení.
Zdroj priemerná dĺžka trvania výpadku pri dopade závažného kybernetického útoku AS-IS: Expertný odhad Manažéra kybernetickej bezpečnosti na základe súčasného stavu infraštruktúry NCZI.
Zdroj priemerná dĺžka trvania výpadku pri dopade závažného kybernetického útoku TO-BE: Expertný odhad Manažéra kybernetickej bezpečnosti na základe plánovaného budúceho stavu infraštruktúry NCZI.

Zabránenie riziku narušenia údajov implementáciou EDR
Prínos je vypočítaný ako rozdiel medzi sumárom pravdepodobných priemerných nákladov v prípade narušenia údajov medzi prostredím bez implementovaného riešenia EDR a prostredím s implementovaným EDR. Priemerné náklady pre AS_IS sú vypočítané ako priemerné náklady pri úspešnom porušení údajov* pravdepodobnosť úniku údajov za 2 roky / počet rokov (2). Implementácia riešenia EDR počíta so znížením rozsahu dopadu o 97%.

Zdroj pre výpočet prínosu: https://www.fortinet.com/demand/gated/esg-economic-validation-fortinet-security-operations

Kvalitatívne prínosy

Projekt budovania kapacít a zvýšenia spôsobilosti pracoviska bezpečnostných operácii (SOC) NCZI prináša viaceré významné kvalitatívne prínosy v oblasti kybernetickej bezpečnosti a ochrany kritických informačných systémov:

Zvýšená kybernetická ochrana
Projekt prispieva k posilneniu ochrany pred kybernetickými hrozbami a útokmi. Zvýšená schopnosť detekcie a prevencie hrozieb pomáha minimalizovať riziko kybernetických incidentov a znefunkčnenia kritických systémov. Zvýšenie kybernetickej bezpečnosti predstavuje kľúčový prvok projektu. Hlavným cieľom je zabezpečiť, že organizácia bude vystavená menej rizikám, ktoré sú spojené s rastúcimi a sofistikovanejšími kybernetickými hrozbami. Súčasné kybernetické hrozby neustále evoluujú a stávajú sa čoraz zložitejšími a nebezpečnejšími. Útoky sa objavujú na nových frontoch a využívajú nové techniky na obehnanie existujúcich obranných mechanizmov. Tieto hrozby predstavujú závažné riziká pre organizáciu, ktoré môžu mať vážne dôsledky na jej činnosť a povesť. V rámci projektu investujeme do nových technológií, nástrojov a stratégií, ktoré organizácii umožnia identifikovať a eliminovať tieto hrozby na najvyššej úrovni. Vytvoríme širší a komplexnejší prístup k kybernetickej bezpečnosti, ktorý zabezpečí, že organizácia bude dobre pripravená na kybernetické hrozby všetkých druhov. Rozšírením kybernetickej bezpečnosti na najvyššiu úroveň budeme mať možnosť brániť sa najnáročnejším útokom a minimalizovať ich škodlivé účinky. Tým zabezpečíme ochranu aktív a dôvernosti organizácie, čo je kritické pre našich klientov, zamestnancov a partnerov. Zvýšená kybernetická bezpečnosť je kľúčovým prínosom projektu a bude mať široký dosah na bezpečnosť a prosperitu organizácie.

Rýchlejšia reakcia na hrozby
Implementácia technologických riešení a automatizácia procesov v pracovisku SOC umožní rýchlejšiu identifikáciu, analýzu a riešenie kybernetických hrozieb. Tým sa zabezpečí včasná reakcia a minimalizácia potenciálnych škôd. V rámci projektu budeme implementovať najmodernejšie technológie a nástroje, ktoré umožnia okamžité rozpoznanie potenciálnych hrozieb a ich priradenie do správnych kategórií. Implementáciou projektu dôjde k okamžitejšom nasadení potrebných opatrení na minimalizáciu potenciálnych škôd. To znamená, že vďaka implemnetácii projektu budeme schopní zareagovať na hrozby rýchlejšie a účinnejšie. Výsledkom je nielen zníženie rizika pre organizáciu, ale aj minimalizácia možných škôd, ktoré by takéto hrozby mohli spôsobiť. Zvýšená rýchlosť a efektivita reakcie na kybernetické hrozby prinesie organizácii významný prínos, a to v podobe zníženia rizika straty dôveryhodnosti, finančných strát a poškodenia povesť. Týmto spôsobom sa projekt stáva kľúčovým opatrením v oblasti kybernetickej bezpečnosti a ochrany organizácie pred hrozbami v dnešnom digitálnom svete.

Hĺbková analýza hrozieb
Projekt zahŕňa zdokonalenie analytických schopností pracoviska SOC, vrátane analýzy malvéru a sledovania správania útočníkov. Tým sa zvýši schopnosť odhaľovať sofistikované hrozby a budúce kybernetické útoky. Hĺbková analýza je kritická v identifikácii a porozumení novým a komplexným hrozbám, ktoré sa vyvíjajú v kybernetickom prostredí. Prostredníctvom projektu investujeme do školenia našich expertov a do moderných nástrojov na analýzu malvéru, čo umožní získať hlbší pohľad do štruktúry hrozieb a ich metód. Okrem toho, sledovanie správania útočníkov je ďalším významným prvkom hĺbkovej analýzy. S týmito nástrojmi sme schopní sledovať, ako sa útočníci pohybujú v našej sieti a aké kroky podnikajú na dosiahnutie svojich cieľov. Toto je kľúčové pri rozpoznaní sofistikovaných útokov, ktoré môžu byť skryté a ťažko detekovateľné tradičnými metodami. Zlepšená schopnosť hĺbkovej analýzy hrozieb prinesie organizácii výhody v podobe predchádzania novým, ešte neznámym útokom a rýchlejšiemu vytváraniu ochranných opatrení. Týmto spôsobom projekt prispieva k dlhodobejšiemu zabezpečeniu organizácie pred kybernetickými hrozbami a znižuje pravdepodobnosť závažných incidentov.

Spolupráca a komunikácia
Zlepšená spolupráca a komunikácia medzi rôznymi tímami v organizácii pomáha včasnému zdieľaniu informácií o hrozbách a koordinácii reakcií na kybernetické incidenty. Zlepšená spolupráca znamená, že tímy zamerané na bezpečnosť, IT, a všetky ďalšie príslušné oddelenia budú mať jednoduchší prístup k informáciám o kybernetických hrozbách. To umožní včasné a rýchle zdieľanie informácií o identifikovaných rizikách a aktuálnych situáciách. Týmto spôsobom môžeme predchádzať izolovaným silám a skrátiť čas, ktorý by inak bol stratený na vyhľadávanie dôležitých informácií. V prípade kybernetických incidentov, kedy každá sekunda záleží, umožňuje tento projekt okamžitú komunikáciu a koordináciu reakcií. Rôzne tímy sú schopné okamžite reagovať na situácie, spolupracovať na náprave incidentu a obnoviť normálnu prevádzku bez neprimeraného omeškania. Spolupráca a komunikácia sú kľúčom k efektívnemu kybernetickému bezpečnostnému procesu, a ich zdokonalenie v rámci tohto projektu posilňuje obranu organizácie proti hrozbám. Zabezpečuje to, že organizácia je jednotným tímom, ktorý je schopný reagovať na kybernetické hrozby s jednotným úsilím, čo vedie k zníženiu rizika a minimalizácii škôd.

Zvýšená odbornosť
Projekt zahŕňa odborné školenia a certifikácie pre personál pracoviska SOC, čo vedie k zvýšeniu znalostného štandardu tímu a udržiavaniu odbornosti v oblasti kybernetickej bezpečnosti.

Kontinuálne zlepšovanie procesov
Pracovisko SOC bude pravidelne preskúmavať a zlepšovať pracovné postupy a procesy na základe skúseností získaných počas riešenia kybernetických incidentov. Tým sa dosiahne efektívnejšia a zohľadnená reakcia na hrozby.

Sledovanie právnych a regulačných požiadaviek
Projekt zabezpečí, že činnosti pracoviska SOC budú v súlade s platnými právnymi a regulačnými požiadavkami týkajúcimi sa ochrany údajov a kybernetickej bezpečnosti, čo znižuje riziko porušenia predpisov a potenciálne sankcie.

Zvýšená reputácia a dôvera

Dôsledné opatrenia v oblasti kybernetickej bezpečnosti pomáhajú zvýšiť dôveru v štát a reputáciu krajiny. Zabezpečením integrity, dôvernosti a dostupnosti dôležitých informácií a služieb v kybernetickom priestore sa zlepšuje vnímaná kvalita a spoľahlivosť verejnej správy.

Proaktivita v reakcii na kybernetické hrozby
Projekt umožňuje rozšírenie služieb SOC o proaktívne opatrenia, čím sa organizácia stáva menej zraniteľnou voči novým hrozbám a útokom. Projekt prispieva k zvýšeniu proaktívnych opatrení v oblasti kybernetickej bezpečnosti a umožňuje organizácii lepšie reagovať na nové hrozby a útoky. Implementácia tohto projektu rozširuje služby Security Operations Center (SOC) o proaktívne opatrenia, čo organizácii umožňuje aktívnejšie reagovať na kybernetické hrozby. Proaktivita spočíva v predvídavých krokoch, ktoré organizácia vykonáva, aby sa stala menej zraniteľnou voči novým a rozvíjajúcim sa hrozbám a útokom. Tu je niekoľko kľúčových prínosov projektu:

Rýchla identifikácia nových hrozieb - Vďaka zdokonaleným nástrojom a schopnostiam v rámci SOC organizácia môže rýchlejšie identifikovať nové kybernetické hrozby. S novými technológiami a analýzou správania útočníkov môžeme odhaliť aj rafinovanejšie útoky, ktoré by mohli uniknúť tradičným bezpečnostným systémom.

Včasné varovania - Proaktívna kybernetická bezpečnostná stratégia umožňuje organizácii generovať včasné varovania a upozornenia na potenciálne hrozby. To dáva tímom viac času na prípravu a predchádzanie útokom.

Preventívne opatrenia - Projekt zahŕňa implementáciu preventívnych opatrení na základe včasného rozpoznania hrozieb. Tieto opatrenia môžu zahŕňať aktualizácie zraniteľných systémov, zvýšenú monitorovanie, a iné kroky na minimalizáciu rizika.

Znižuje zraniteľnosť organizácie - Proaktivita v reakcii na kybernetické hrozby robí organizáciu menej zraniteľnou voči novým hrozbám. Tým sa minimalizuje potenciálna škoda, ktorú by organizácia mohla utrpieť v dôsledku kybernetického útoku.

Projekt sa zabezpečí, že organizácia nebude iba pasívnym príjemcom informácií o hrozbách, ale aktívnym účastníkom v boji proti nim. Tým sa NCZI stane schopnou predvídať a čeliť hrozbám s vyššou efektivitou a dôslednosťou, čím sa posilňuje celková kybernetická bezpečnosť.

Celkovo projekt prispeje k vytvoreniu moderného a efektívneho systému včasnej reakcie na kybernetické hrozby v oblasti verejnej správy. Zvýšená kybernetická ochrana a reaktívna schopnosť pomôžu minimalizovať riziká, ktoré kybernetický priestor predstavuje pre dôležité informácie a služby, a to nielen v oblasti zdravotníctva, ale aj pre celý štát.

8. HARMONOGRAM JEDNOTLIVÝCH FÁZ PROJEKTU A METÓDA JEHO RIADENIA

Projekt bude dodávaný v 1 Inkremente z tohoto dôvodu uvádzame Harmonogram na úrovni 1 Etapy/ 1 Inkrementu.

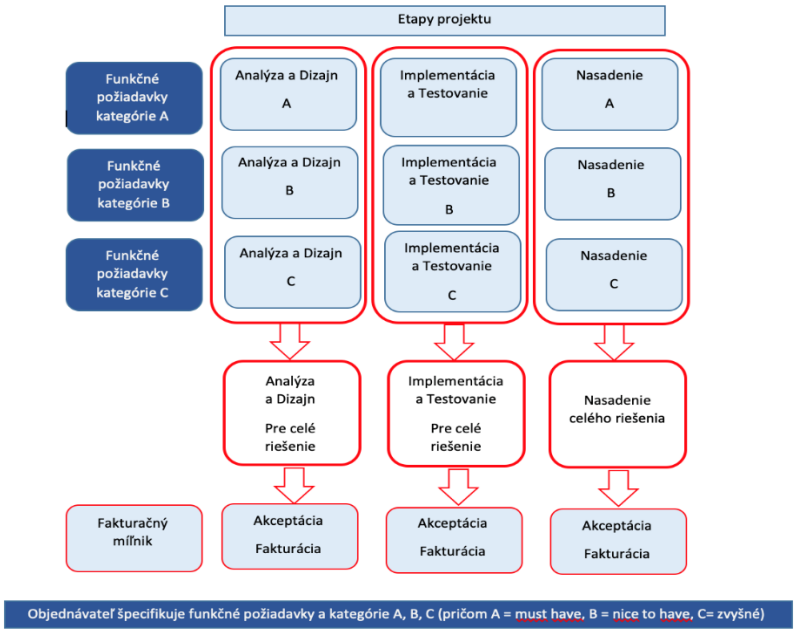
Tabuľka č.10 – Harmonogram jednotlivých fáz projektu

ID	FÁZA/AKTIVITA	ZAČIATOK (odhad termínu)	KONIEC (odhad termínu)	POZNÁMKA
1.	Prípravná fáza	01/2023	05/2023	
2.	Iniciačná fáza	05/2023	03/2024	
3.	Realizačná fáza	04/2024	03/2026	
3a	Analýza a Dizajn	04/2024	08/2024	Analýza súčasných potrieb, súčasného stavu, návrh dizajnu služieb a modulov pre integráciu
3b	Nákup technických prostriedkov, programových prostriedkov a služieb	04/2024	11/2024	Nákup technických prostriedkov HW a SW a služieb
3c	Implementácia a testovanie	09/2024	11/2024	Zavedenie riešenia do prevádzky, Míľnik 12/24 - naplnenie merateľného ukazovateľa č.1 na úrovni minimálne 80 %
3d	Nasadenie a PIP	12/2024	03/2026	Nasadenie a post implementačná podpora
4.	Dokončovacia fáza	03/2026	03/2026	Odovzdávanie výstupov a administratívna finalizácia

5.	Podpora prevádzky (SLA)	04/2026	03/2030	Trvanie SLA kontraktu

Projekt bude realizovaný metódou waterfall.

Waterfall- vodopádový prístup počíta s detailným naplánovaním jednotlivých krokov a následnom dodržiavaní postupu pri vývoji alebo realizácii projekty. Projektovému tímu je daný minimálny priestor na zmeny v priebehu realizácie. Vodopádový prístup je vhodný a užitočný v projektoch, ktorý majú jasný cieľ a jasne definovateľný postup a rozdelenie prác.



9. PROJEKTOVÝ TÍM

Riadiaci výbor projektu tvorí predseda riadiaceho výboru projektu a vlastníci procesov alebo nimi poverení zástupcovia.

Riadiaci výbor sa riadi "Štatútom riadiaceho výboru", ktorý je popísaný v dokumente Štatút RV projektu ako najvyšší riadiaci orgán na účely realizácie projektu na základe schválenej projektovej dokumentácie v podmienkach rezortu zdravotníctva.
Štatút Riadiaceho výboru upravuje najmä jeho pôsobnosť, úlohy, zloženie, zasadnutie a hlasovanie. Členom riadiaceho výboru projektu môže byť aj zástupca dodávateľa. Väčšina členov riadiaceho výboru projektu s hlasovacím právom sú osoby navrhnuté objednávateľom a zastupujú záujmy objednávateľa. Riadiaci výbor projektu dozerá na hospodárnosť, efektívnosť a účelové využívanie finančných prostriedkov a môže prispôsobiť štandardy projektového riadenia na realizovaný projekt.
Riadiaci výbor má minimálne 5 členov, vrátane predsedu Riadiaceho výboru (ďalej len „predseda") :

Riadiaci výbor projektu môžu tvoriť:

a) **predseda** Riadiaceho výboru projektu,
b) **podpredseda** Riadiaceho výboru projektu,
c) **vlastník alebo vlastníci procesov NCZI** (biznis vlastník infraštruktúra) alebo nimi poverený zástupca alebo zástupcovia,
d) **zástupcu kľúčových používateľov** (end user),
e) zástupca za Dodávateľa v zmysle Zmluvy o Dielo s Dodávateľom.

f) projektový manažér prijímateľa PPM.

Riadiaci výbor je riadený predsedom, ktorým je zástupca Objednávateľa. V prípade neprítomnosti predsedu na zasadnutí Riadiaceho výboru, predseda musí na toto konkrétne zasadnutie písomne delegovať svoju funkciu v rozsahu svojich práv a povinností formou splnomocnenia na zástupcu, ktorým môže byť aj iný člen Riadiaceho výboru s hlasovacím právom. Na rokovanie Riadiaceho výboru môžu byť v prípade potreby prizvaní aj iní účastníci tak zo strany Objednávateľa alebo za stranu Dodávateľa.

Riadiaci výbor zasadá pravidelne, spravidla raz za mesiac avšak najmenej jedenkrát za tri (3) po sebe nasledujúce kalendárne mesiace. Zasadnutie Riadiaceho výboru zvoláva predseda. Závery zo zasadnutia Riadiaceho výboru a jednotlivé body zo zasadnutia Riadiaceho výboru sa prijímajú súhlasným hlasovaním nadpolovičnej väčšiny prítomných členov Riadiaceho výboru s hlasovacím právom. Hlas predsedu má v prípade rovnosti hlasov hodnotu dvoch hlasov.

Hlavné dokumenty spojené s činnosťou Riadiaceho výboru sú program zasadnutia, pracovný materiál a záznam zo zasadnutia Riadiaceho výboru, ktorého prílohou musí byť aj prezenčná listina, prípadne aj písomné splnomocnenia členov Riadiaceho výboru.

Program zasadnutia a pracovné materiály Riadiaceho výboru distribuuje Asistent projektového manažéra na základe podkladov a inštrukcií predsedu alebo toho člena Riadiaceho výboru, ktorý požiadal o zasadnutie Riadiaceho výboru.
Asistent projektového manažéra zabezpečí ich distribúciu členom Riadiaceho výboru najneskôr 3 pracovné dni pred zasadnutím Riadiaceho výboru. Za vecnú správnosť distribuovaného materiálu zodpovedá člen Riadiaceho výboru, ktorý ho predkladá.

Riadiaci výbor zaniká ukončením plnohodnotnej implementácie projektu a jeho uvedením do produktívnej prevádzky. Zoznam členov Riadiaceho výboru je súčasťou dokumentu Komunikačná matica uloženom na zdieľanom projektovom úložisku.

ID	MENO A PRIEZVISKO	POZÍCIA	ORGANIZAČNÝ ÚTVAR	ROLA V PROJEKTE S UVEDENÍM HLASOVACIEHO PRÁVA
1.	Ing. Vladimír Daňo	TBD	TBD	Predseda RV (HP)
2.	Ing. Martin Laubert	TBD	TBD	Podpredseda RV (HP)
3.	Ing. Martin Puchalík	TBD	TBD	Zástupca vlastníkov procesov (HP)
4.	TBD	TBD	TBD	Zástupca vlastníkov procesov II. (HP)
5.	Ing. Martin Székely	TBD	TBD	Zástupcu kľúčových používateľov
6.	TBD	TBD	TBD	Zástupca Dodávateľa
7.	Mgr. Silvia Strešková	Projektový manažér	Odbor projektového riadenia	Projektový manažér prijímateľa

Riadenie projektu zo strany Objednávateľa bude zabezpečené prostredníctvom Projektového manažéra a Finančného manažéra a bude trvať počas celej doby realizácie projektu. Bude pokrývať oblasť projektového riadenia (projektový manažment, celková koordinácia projektu, celkový dohľad nad vývojom dodávaného Diela, vrátane kvality), finančného riadenia a monitorovania realizácie projektu v zmysle riadenia podľa vyhlášky UPVII č. 85/2020 Z. z. o riadení projektov v platnom znení.
Projektový tím bude pozostávať z pozícií:

- Povinné projektové role:
  - Projektový manažér,
  - Kľúčový používateľ,
  - Vlastník procesov,
  - IT analytik,
  - IT architekt,
  - Manažér kvality,
  - Manažér kybernetickej a informačnej bezpečnosti,
  - Špecialista pre bezpečnosť IT.
- Povinné plánované kapacity:

- Manažér SOC,
- Špecialista bezpečnosti SOC,
- Bezpečnostný analytik (úroveň L1, L2),
- Incident Responder (úroveň L3),
- Špecialista Threat intelligence,
- Platform support engineer.

- Ďalšie projektové role:
  - Finančný manažér
  - Asistent PM

V súlade s výzvou NCZI zabezpečí, aby počas implementácie projektu a po jeho skončení (počas obdobia udržateľnosti) bol k dispozícii interný personál na obsluhu, prevádzku a rozvoj riešenia. Zároveň bude minimálne počas obdobia udržateľnosti zabezpečené financovanie tohto personálu zo zdrojov NCZI.

Projektový manažér Objednávateľa bude zabezpečovať koordináciu projektových činností a manažment v súlade s metodikou PRINCE2 (hlavné dokumenty, priebežné manažérske výstupy, a pod.).
Projektový manažér Objednávateľa bude riadiť, administratívne a organizačne zabezpečovať implementáciu projektu, komunikovať s dodávateľmi, sledovať plnenie harmonogramu projektu a zabezpečovať dokumenty požadované MIRRI. Zároveň bude v spolupráci s projektovým manažérom dodávateľa koordinovať realizáciu hlavných aktivít, činností a úloh projektu.

Zodpovednosťou projektového manažéra je v spolupráci s finančným manažérom (objednávateľa) finančné riadenie projektu kontrolu rozpočtu projektu a jeho súlad s účtovnými dokladmi. Kontrolu podpornej účtovnej dokumentácie a poradenstvo pri definovaní oprávnených výdavkov bude zabezpečovať finančný manažér Objednávateľa.

Súčasťou projektového riadenia bude tiež operatívna projektová podpora zabezpečujúca administratívnu podporu pre písomnú komunikáciu, administratívne vedenie projektovej dokumentácie a prípravu podkladov pre členov projektového tímu, organizáciu stretnutí a pod.. V rámci aktivity budú taktiež zabezpečovaný manažment a hodnotenie kvality zo strany Objednávateľa.

ID	MENO A PRIEZVISKO	POZÍCIA	ORGANIZAČNÝ ÚTVAR	PROJEKTOVÁ ROLA
1.	Mgr. Silvia Strešková	Projektový manažér	Odbor projektového riadenia	Projektový manažér
2.	Ing. Vladimír Daňo	Riaditeľ odboru bezpečnostného monitoringu	Odbor bezpečnostného monitoringu	Kľúčový používateľ
3.	TBD	TBD	TBD	Vlastník procesov
4.	TBD	TBD	TBD	IT analytik
5.	TBD	TBD	TBD	IT architekt
6.	TBD	TBD	TBD	Manažér kvality
7.	TBD	TBD	TBD	Manažér kybernetickej a informačnej bezpečnosti
8.	TBD	TBD	TBD	Špecialista pre bezpečnosť IT
9.	TBD	TBD	TBD	Manažér SOC
10.	TBD	TBD	TBD	Špecialista bezpečnosti SOC
11.	TBD	TBD	TBD	Bezpečnostný analytik (úroveň L1, L2)
12.	TBD	TBD	TBD	Incident Responder (úroveň L3)
13.	TBD	TBD	TBD	Špecialista Threat intelligence
14.	TBD	TBD	TBD	Platform support engineer

15.	TBD	TBD	TBD	Finančný manažér

10. PRACOVNÉ NÁPLNE

Projektová rola:	**PROJEKTOVÝ MANAŽÉR**
Detailný popis rozsahu zodpovedností, povinností a kompetencií:	- zodpovedá za každodenné riadenie projektu v mene RV, za monitorovanie projektu, za plánovanie aktivít, za informovanie o projekte, atď., - zodpovedá za určenie pravidiel, spôsobov, metód a nástrojov riadenia projektu a získanie podpory RV pre riadenie, plánovanie a kontrolu projektu a efektívne využívanie projektových zdrojov (ľudských a finančných), - zodpovedá za splnenie všetkých legislatívnych požiadaviek (právne predpisy SR), metodických požiadaviek súvisiacich s implementáciou projektu a formálnu administráciu projektu súvisiacu s riadením, organizovaním, finančným zúčtovaním, sledovaním čiastkových a celkových výsledkov (monitorovaním) a hodnotením výsledkov, - integrovane riadi prípravu a uskutočnenie projektu, nasadenie disponibilných prostriedkov, zabezpečuje koordináciu dodávateľov a zhotoviteľov jednotlivých výstupov projektu, zabezpečuje koordináciu partnerov, časový priebeh a kvalitu výstupov projektu, zmeny projektu a rieši konflikty s okolím projektu, - prijíma rozhodnutia a riadi projekt tak, aby sa splnili stanovené ciele projektu, a aby projekt dodával dohodnuté produkty v dohodnutej kvalite, v čase, a v rámci rozpočtu, - zodpovedá RV za plnenie cieľov projektu a celkový postup prác v projekte, - informuje RV o stave a priebehu projektu, predkladá návrhy na zlepšenie, - riadi strategické a projektové riziká, vrátane vývojových a rezervných plánov, - zodpovedá za identifikovanie kritických miest projektu a navrhovanie ciest k ich eliminácii, - aktívne komunikuje s dodávateľom, zástupcom dodávateľa a projektovým manažérom dodávateľa s cieľom zabezpečiť úspešné dodanie a nasadenie požadovaných projektových výstupov, - zabezpečuje kontrolu dodržiavania a plnenia míľnikov v zmysle zmluvy s dodávateľom, - zabezpečuje vecnú administráciu zúčtovania dodávateľských faktúr, - predkladá požiadavky dodávateľa na rokovanie RV, - zodpovedá za koordináciu a zabezpečenie podkladov pre oddelenie komunikačné pre potreby medializácie projektu, - zodpovedá za informovanie zamestnancov a verejnosti o začatí a ukončení projektu v závislosti od jeho charakteru, - zodpovedá za zabezpečenie vypracovania, priebežnej aktualizácie a verzionovania manažérskej a špecializovanej dokumentácie a produktov, - pripravuje a predkladá stanovené dokumenty na schválenie RV, - navrhuje zaradiť projekt alebo jeho časť do režimu utajenia, - zabezpečuje permanentný dohľad a zvýšenú mieru kontroly a ochrany tokov informácií pri realizácii utajovaného projektu alebo utajovanej časti projektu, - zodpovedá za vypracovanie požiadaviek na zmenu, návrh ich prioritizácie a predkladanie zmenových požiadaviek na rokovanie RV, - zabezpečuje podanie žiadosti o rozpočtové opatrenie MF SR cez Rozpočtový informačný systém na projekt IT podľa potreby, - zodpovedá za riadenie zmeny a prípadné požadované riadenie konfigurácií, - navrhuje členov projektového tímu po dohode s líniovým vedúcim a tímovým manažérom a tiež navrhuje rozsah ich zodpovedností a činností, - organizuje, riadi, motivuje projektový tím a deleguje úlohy členom projektového tímu, - hodnotí členov projektového tímu, - udeľuje pokyny na výkon činností projektovej kancelárie, - podľa potreby deleguje svoje povinnosti a práva na tímových manažérov a koordinuje ich činnosť, - plní úlohy tímového manažéra (vedúceho projektového tímu), ak takáto rola v projekte nie je obsadená –viď činnosť projektovej role „Tímový manažér", - monitoruje výkonnosť projektu, to znamená, že sleduje pokrok vo vybraných ukazovateľoch (KPI) projektu a predkladá ho na schválenie RV,

	- zabezpečuje evidenciu v informačných systémoch pre štandardizované procesy programové a projektového riadenia, napr. IT monitorovací systém pre európske štrukturálne a investičné fondy, - zodpovedá za publikovanie RV schválených projektových výstupov v MetaIS chronologicky, z každej fázy životného cyklu projektu, - zodpovedá za publikovanie zápisov RV v MetaIS, - počas celej doby realizácie projektu štandardne zabezpečuje nasledovné prierezové činnosti: 1. kontinuálne zdôvodňovanie projektu, ktoré zahŕňa posúdenie, či je projekt požadovaný a dosiahnuteľný, potrebné na rozhodovanie o pokračovaní vynakladania prostriedkov počas všetkých fáz projektu, vypracované aspoň po ukončení každej fázy projektu, 2. plánovanie a operatívne riadenie dodávania projektových produktov, 3. riadenie rizík a závislostí, ktoré zahŕňa identifikáciu, hodnotenie a riadenie rizík, závislostí a hrozieb na úspešnú realizáciu projektu, - zabezpečuje dodržiavanie legislatívno-metodických zásad pre riadenie projektov, - zodpovedá za formálnu administráciu projektu, riadenie centrálneho úložiska projektovej dokumentácie NCZI, správu a archiváciu projektovej dokumentácie, - sleduje dodržiavanie interných riadiacich aktov.

Projektová rola:	**MANAŽÉR KVALITY**
Stručný popis:	- zodpovedá za úvodné nastavenie pravidiel riadenia kvality a za následné dodržiavanie a kontrolu kvality, - kontroluje, či sa riadenie a proces zabezpečenia kvality vykonáva správnym spôsobom, v správnom čase a správnymi osobami, - počas celej doby realizácie projektu zabezpečuje riadenie kvality projektových výstupov a zhodu projektových výstupov s požiadavkami definovaním merateľných výkonnostných parametrov na vytváranie, overovanie projektových produktov, definovanie akceptačných kritérií, ktoré sú vhodné na požadovaný účel, - počas celej doby realizácie projektu zodpovedá za priebežné vyžadovanie, hodnotenie a kontrolu kvality (vecnej aj formálnej), za plánovanie, zabezpečovanie, kontrolu, operatívne riadenie, zlepšovanie a vyhodnocovanie kvality projektu, - aktívne sa zúčastňuje stretnutí projektového tímu a spolupracuje na vypracovaní manažérskej a špecializovanej dokumentácie a produktov v minimálnom rozsahu určenom Prílohou č.1 tejto smernice, - plní pokyny PM a dohody zo stretnutí projektového tímu, - spolupracuje s PM, - zodpovedá sa PM, - informuje PM o stave plnenia úloh, o zisteniach a o rizikách, - sleduje a hodnotí kvalitatívne ukazovatele projektových výstupov, - zabezpečuje zhodnotenie kvality projektu zamerané na výstupy iniciačnej a realizačnej fázy projektu formou auditu na mieste, ktorého výsledky spracuje v produkte M-04 Audit kvality.
Detailný popis rozsahu zodpovedností, povinností a kompetencií	• návrh a zavádzanie do praxe postupov, techník, nástrojov a pravidiel, ktoré maximalizujú efektivitu práce a kvalitatívne parametre vývoja softwaru/produktu/IS, resp. IT projektu, • definovanie politiky kvality (stratégie kvality), meranie kvality, analýzu a spracovanie plánov kvality, • riadenie a monitorovanie dosahovania cieľov kvality, • špecifikáciu požiadaviek na kvalitu vyvíjaných funkcionalít systému, • špecifikáciu požiadaviek pre ďalší rozvoj, • definovanie akceptačných kritérií, • zabezpečenie súladu so štandardmi, normami, právnymi požiadavkami, požiadavkami užívateľova prevádzkovateľov systémov, • posúdenie BC/CBA – odôvodenie projektu s katalógom funkčných, nefunkčných a technických požiadaviek, • kontrolu kvality plnenia vecných požiadaviek definovaných v zmluve s dodávateľom alebo v požiadavkách na zmenu, • akceptáciu splnenia vecných a kvalitatívnych požiadaviek v projekte svojím podpisom na akceptačnom protokole pri odovzdávaní jednotlivých fáz projektu/čiastkových projektov alebo pri odovzdávaní zmien vykonaných v rámci zmenových konaní, • monitoring a vyhodnocovanie kvality údajov a návrh nápravných opatrení za účelom zabezpečenia správnosti a konzistentnosti údajov, • definovanie postupov, navrhovanie a vyjadrovanie sa k plánom testov a testovacích scenárov, • analyzovanie výsledkov testovania, • kontrolu plnenia projektových úloh a časového harmonogramu projektu, • 15. kontrolu plnenia finančného plánu projektu,

Projektová rola:	**KĽÚČOVÝ POUŽÍVATEĽ**
Stručný popis:	- reprezentuje záujmy budúcich koncových používateľov projektových produktov alebo projektových výstupov, - poskytuje súčinnosť pri spracovaní interného riadiaceho aktu upravujúceho prevádzku, servis a podporu IT, - aktívne sa zúčastňuje stretnutí projektového tímu a spolupracuje na vypracovaní manažérskej a špecializovanej dokumentácie a produktov v minimálnom rozsahu určenom Prílohou č.1 tejto smernice, - plní pokyny PM a dohody zo stretnutí projektového tímu.
Detailný popis rozsahu zodpovedností, povinností a kompetencií	• návrh a špecifikáciu funkčných, nefunkčných a technických požiadaviek, potreby, obsahu, kvalitatívnych a kvantitatívnych prínosov projektu, požiadaviek koncových používateľov na prínos systému a požiadaviek na bezpečnosť, • jednoznačnú špecifikáciu požiadaviek na jednotlivé projektové výstupy (špecializované produkty a výstupy) z pohľadu vecno-procesného a legislatívy, • návrh a definovanie rizík, rozhraní a závislostí, • vykonanie používateľského testovania funkčného používateľského rozhrania (UX testovania) a za finálne odsúhlasenie používateľského rozhrania, • návrh a definovanie akceptačných kritérií, • akceptačné testovanie (UAT) a návrh na akceptáciu projektových produktov alebo projektových výstupov a finálny návrh na spustenie do produkčnej prevádzky, • 7. predkladanie požiadaviek na zmenu funkcionalít produktov,

Projektová rola:	**PROJEKTOVÁ KANCELÁRIA („PMO“)**
Projektovou kanceláriou je príslušný organizačný útvar FR SR v zmysle organizačného poriadku FR SR, ktorý zabezpečuje podporu riadenia projektu, najmä:	- administratívnu a technickú podporu v jednotlivých fázach životného cyklu projektu, - vypracovanie a odovzdanie menovacích dekrétov a odvolacích dekrétov pre predsedu RV, členov RV, PM a podpísaných predsedom RV pre členov projektového tímu a PMO, - zabezpečenie oboznámenia predsedu RV, členov RV, a členov projektového tímu s projektom, ich úlohami a rozsahom ich zodpovedností, atď. podľa pokynu PM, - organizačné zabezpečenie zasadnutí RV, spracovanie zápisov zo zasadnutí RV a zabezpečenie ich zverejnenia prostredníctvom MetaIS, ak je to potrebné, - organizačné zabezpečenie stretnutí realizovaných v rámci projektu, spracovanie zápisov z týchto stretnutí, - vykonávanie úloh na základe pokynov PM, - vypracovanie a aktualizácia zoznamov úloh, rizík, otvorených otázok a iných manažérskych správ, reportov, zoznamov a požiadaviek, - organizačné zabezpečenie pripomienkového konania projektovej dokumentácie, - správu projektov, monitorovanie stavu projektu, udržiavanie aktuálnosti a hodnovernosti údajov o projektoch a podľa potreby optimalizáciu projektov, - prípravu informácií o stave realizácie projektu podľa potreby, - zhromaždenie, analyzovanie a vyhodnotenie poznatkov z implementácie projektov a definovanie ponaučenia za účelom predchádzania a opakovania chýb z minulosti, - zabezpečenie zverejnenia projektových výstupov jednotlivých fáz životného cyklu projektu na centrálnom úložisku projektovej dokumentácie NCZI a v MetaIS, ak je to potrebné, - poskytuje súčinnosť PM pri predkladaní projektových produktov na posúdenie ekonomickej výhodnosti a súladu s programovým riadením MIRRI SR, ak je to potrebné, - organizáciu procesov súvisiacich s výkazmi práce členov projektových tímov jednotlivých projektov, - vytvorenie a spravovanie centrálneho úložiska projektovej dokumentácie NCZI, - vytvorenie komunikačnej platformy v rámci projektu a medzi projektami navzájom, - zabezpečenie interakcie medzi zainteresovanými stranami, ich spokojnosť a realizáciu požiadaviek spojených s implementáciou projektu, - spoluprácu s metodickou podporou projektového riadenia, - zabezpečenie uloženia originálov projektovej dokumentácie.

Projektová rola:	**MANAŽÉR KYBERNETICKEJ A INFORMAČNEJ BEZPEČNOSTI („KIB“)**
Stručný popis:	- má neobmedzený aktívny prístup ku všetkým projektovým dokumentom, nástrojom a výstupom projektu, v ktorých sa opisuje predmet projektu z hľadiska jeho architektúry, funkcií, procesov, manažmentu informačnej bezpečnosti a spôsobov spracúvania dát, ako aj dát samotných,

	- má sprístupnené všetky informácie o bezpečnostných opatreniach zavádzaných projektom v zmysle § 20 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a v zmysle ustanovení zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, - zodpovedá za posúdenie možných alternatív realizácie projektu za oblasť IB a KB, - zodpovedá za posúdenie požiadaviek agendy IB a KB na rozhrania a spoločné komponenty, na integrácie a procesy konverzie a migrácie, identifikácia nesúladu a návrh riešenia, - poskytuje konzultácie a súčinnosť pre problematiku IB a KB, - poskytuje konzultácie pri tvorbe šablón a vzorov dokumentácie pre oblasť IB a KB, - poskytuje konzultácie a vykonáva kontrolnú činnosť zameranú na obsah a komplexnosť dokumentácie z hľadiska IB a KB, - dohliada na zosúladenie projektu s princípmi definovanými v interných riadiacich aktoch NCZI a dokumentoch týkajúcich sa bezpečnosti NCZI, - zabezpečuje získavanie a spracovanie informácií nutných pre plnenie úloh v oblasti IB a KB, - aktívne sa zúčastňuje stretnutí projektového tímu a spolupracuje na vypracovaní manažérskej a špecializovanej dokumentácie a produktov v minimálnom rozsahu určenom Prílohou č.1 tejto smernice, - plní pokyny PM a dohody zo stretnutí projektového tímu.
Detailný popis rozsahu zodpovedností, povinností a kompetencií	- zodpovedá za špecifikovanie: • štandardov, princípov a stratégií v oblasti informačnej bezpečnosti („IB“) a kybernetickej bezpečnosti („KB“) a ich dodržiavanie, • funkčných, nefunkčných a technických požiadaviek na IB a KB a za ich analýzu, • požiadaviek na IB a KB, kontroluje ich implementáciu v realizovanom projekte, • požiadaviek na bezpečnosť vývojového, testovacieho a produkčného prostredia, • požiadaviek na bezpečnosť v rámci bezpečnostnej vrstvy, • požiadaviek na školenia pre oblasť IB a KB, • požiadaviek na bezpečnostnú architektúru riešenia a technickú infraštruktúru pre oblasť IB a KB, • požiadaviek na dostupnosť, zálohovanie, archiváciu a obnovu IS vzťahujúce sa na IB a KB, • požiadaviek na IB a KB, bezpečnostný projekt a riadenie prístupu, • požiadaviek na opis vývojového, testovacieho a produkčného prostredia za oblasť IB a KB, • požiadaviek na testovanie z hľadiska IB a KB, realizáciu kontroly zapracovania a retestu, • požiadaviek na obsah dokumentácie v zmysle legislatívnych požiadaviek pre oblasť IB a KB, ako aj v zmysle "best practies", • požiadaviek na dodanie potrebnej dokumentácie súvisiacej s IBaKB kontroluje ich implementáciu v realizovanom projekte, • požiadaviek a konzultácie pri návrhu riešenia za agendu IB a KB v rámci procesu „Mapovanie a analýza technických požiadaviek - detailný návrh riešenia (DNR)“, • požiadaviek nabezpečnosť ITaKB v rámci procesu "akceptácie, odovzdania a správy zdrojových kódov“, • akceptačných kritérií za oblasť IB a KB, • pravidiel pre publicitu a informovanosť s ohľadom na IB a KB, • podmienok na testovanie, reviduje výsledky a výstupy z testovania za oblasť IB a KB, • požiadaviek na bezpečnostný projekt pre oblasť IB a KB, - zodpovedá za realizáciu kontroly: • zameranej na naplnenie požiadaviek definovaných v bezpečnostnom projekte za oblasť IB a KB, • zameranú na správnosť nastavení a konfigurácii bezpečnosti jednotlivých prostredí, • zameranú na realizáciu procesu posudzovania a komplexnosti bezpečnostných rizík, bezpečnosť a kompletný popis rozhraní, správnu identifikácia závislostí, • naplnenia definovaných požiadaviek pre oblasť IB a KB, • zameranú na implementovaný proces v priamom súvise s IB a KB, • súladu s platnou legislatívou v oblasti IB a KB (obsahuje aj kontrolu legislatívnych požiadaviek), • zameranú na zabezpečenie procesu, interfejsov, integrácii, kompletného popisu rozhraní a spoločných komponentov a posúdenia z pohľadu bezpečnosti,

Projektová rola:	**ČLEN PROJEKTOVÉHO TÍMU**

Stručný popis:	- vykonáva odbornú prácu v projekte a poskytuje odborné stanoviská a konzultácie za príslušnú oblasť, - aktívne sa zúčastňuje odborných stretnutí tímu, ako aj konzultácií, - zabezpečuje vypracovanie, priebežnú aktualizáciu a verzionovanie manažérskej a špecializovanej dokumentácie a produktov v minimálnom rozsahu určenom Prílohou č.1 tejto smernice v súčinnosti a podľa pokynov tímového manažéra a PM, - plní úlohy uložené tímovým manažérom a PM v požadovanej kvalite a v stanovených termínoch, - plní dohody zo stretnutí projektového tímu, - odpočtuje plnenie úloh tímovému manažérovi a PM, - predkladá námety, podnety, požiadavky a upozorňuje na problémy a riziká súvisiace s projektom tímovému manažérovi a PM, - spolupracuje s projektovým tímom na strane dodávateľa, - zodpovedá za splnenie všetkých legislatívnych požiadaviek (právne predpisy SR a EK) a metodických a administratívnych požiadaviek súvisiacich s implementáciou projektu.

11. ODKAZY

12. PRÍLOHY

Príloha 1: Zoznam rizík a závislostí

Koniec dokumentu