projekt_3001_Projektovy_zamer_detailny

PROJEKTOVÝ ZÁMER

Vzor pre manažérsky výstup I-02

podľa vyhlášky MIRRI č. 401/2023 Z. z.

Povinná osoba	DataCentrum elektronizácie územnej samosprávy Slovenska (DEUS)
Názov projektu	Kybernetická bezpečnosť pre samosprávy SR do 6000 obyvateľov prostredníctvom správcu informačného systému DCOM
Zodpovedná osoba za projekt	Ing. Peter Uhrík
Realizátor projektu	DataCentrum elektronizácie územnej samosprávy Slovenska (DEUS)
Vlastník projektu	Katarína Lešková, výkonná riaditeľka

Schvaľovanie dokumentu

Položka	Meno a priezvisko	Organizácia	Pracovná pozícia	Dátum	Podpis (alebo elektronický súhlas)
Vypracoval	Ing. Peter Uhrík	DataCentrum elektronizácie územnej samosprávy Slovenska (DEUS)		15.08.2024	

1. História DOKUMENTU

Verzia	Dátum	Zmeny	Meno
1.0	15.08.2024	Iniciálny dokument	Ing. Peter Uhrík

2. ÚČEL DOKUMENTU, SKRATKY (KONVENCIE) A DEFINÍCIE

V súlade s Vyhláškou č. 401/2023 Z.z. je dokument I-02 Projektový zámer určený na rozpracovanie detailných informácií prípravy projektu, aby bolo možné rozhodnúť o pokračovaní prípravy projektu, pláne realizácie, alokovaní rozpočtu a ľudských zdrojov.

Dokument Projektový zámer v zmysle vyššie uvedenej vyhlášky obsahuje manažérske zhrnutie, rozsah, ciele a motiváciu na realizáciu projektu, zainteresované strany, alternatívy, návrh merateľných ukazovateľov, detailný opis požadovaných projektových výstupov, detailný opis obmedzení, predpokladov, tolerancií a návrh organizačného zabezpečenia projektu, detailný opis rozpočtu projektu a jeho prínosov, nahľad architektúry a harmonogram projektu so zoznamom rizík a závislostí.

2.1 Použité skratky a pojmy

SKRATKA/POJEM	POPIS
HW	Hardvér

IKT	Informačno-komunikačné technológie (organizácie)
IS	Informačný systém
IT ROLA	Rola, ktorá definuje prístup do IS alebo definuje využívanie IT zdrojov
SD	Service Desk
SLA	Service Level Agreement – zmluva o podpore prevádzky, údržbe a rozvoji IS
SW	Softvér
NGFW	Next Generation Firewall
IPS	Intrusion Prevention System
DPH	Daň z pridanej hodnoty
ATD	Advanced Threat Detection
XDR/EDR	Extended Detection and Response/Endpoint Detection and Response
WAF	Web Apprilcation Firewall
PAM	Privileged Access Management
NDR	Network Detection and Response
AD server	Active Directory (adresárová služba)
CRZ	Centrálny register zmlúv
DEUS	DataCentrum elektronizácie územnej samosprávy Slovenska
RV	Riadiaci výbor projektu
ED	Externí dodávatelia
SIEM	Security Information and Event Management
NBÚ	Národný bezpečnostný úrad
MIRRI	Ministerstvo investícií, regionálneho rozvoja a informatizácie SR
ÚHP	Ministerstvo financií Slovenskej republiky – Útvar hodnoty za peniaze
ISO	Informačný Systém Obce

3. DEFINOVANIE PROJEKTU

3.1 Manažérske zhrnutie

Z hľadiska realizátora projektu bude projekt realizovaný združením DEUS, ktoré v zmysle § 9a odsek 1 zákona č. 305/2013 Z.z. o elektronickej podobe výkonu pôsobností orgánov verejnej moci (eGovernmente) vykonáva činnosti správcu a prevádzkovateľa IS DCOM. DEUS je záujmové združenie právnických osôb, ktorého jedinými členmi sú Ministerstvo financií SR (ďalej len „MF SR“) a Združenie miest a obcí Slovenska (ďalej len „ZMOS“). DEUS je špecifickým poskytovateľom cloudových služieb typu SaaS pre subjekty MÚS.

Informačný systém DCOM je nadrezortný informačný systém verejnej správy, prostredníctvom ktorého vykonávajú obce verejnú moc elektronicky.

Projekt je zameraný na posilnenie kybernetickej bezpečnosti v dvoch oblastiach:

1. **Posilnenie infraštruktúry ochrany dát obce v dátovom centre a zabezpečenie ochrany** pred stále rastúcimi kybernetickými hrozbami prostredníctvom upgrades a doplnenia centrálnej infraštruktúry. Implementáciou projektu sa zabezpečí modernizácia a posilnenie bezpečnostnej základne infraštruktúry IS DCOM. Projekt zároveň prinesie aktívny dohľad, analýzu prevádzky a priebežný monitoring bezpečnostných stavov IS DCOM. Celkovo sa týmto spôsobom zvýši úroveň ochrany, a tým aj schopnosť efektívne reagovať na rôzne typy kybernetických incidentov. Zvýšená schopnosť detekcie a prevencie hrozieb znižuje riziko kybernetických incidentov a znefunkčnenia IS DCOM. Zvýšenie kybernetickej bezpečnosti predstavuje kľúčový prvok projektu. Hlavným cieľom je zabezpečiť, že IS DCOM a úrady samospráv využívajúcich IS DCOM budú menej vystavené rizikám, ktoré sú spojené s rastúcimi a sofistikovanejšími kybernetickými hrozbami. Rozšírením kybernetickej bezpečnosti na vyššiu úroveň zabezpečíme ochranu aktív a dôveryhodnosti organizácie, čo je kritické pre klientov. Zvýšená kybernetická bezpečnosť je kľúčovým prínosom projektu a bude mať široký dosah na bezpečnosť miestnej samosprávy. Nakoľko súčasťou kybernetickej bezpečnosti je zachovanie vysokej dostupnosti základnej služby, súčasťou tohto cieľa je aj zabezpečenie komplexného monitoringu nielen bezpečnostných prvkov, ale aj všetkých komponentov IS DCOM. Zabezpečením integrovaného monitoringu od fyzickej až po aplikačnú vrstvu bude DEUS schopný efektívne identifikovať ohrozenia a zistiť, či sa jedná o ohrozenia dostupnosti spôsobené prevádzkou samotného IS DCOM, alebo či sa jedná o ohrozenie z dôvodu historického, alebo práve prebiehajúceho bezpečnostného útoku.
2. **Posilnenie bezpečnosti na samotných obciach.** v zmysle zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti, je každá obec s počtom obyvateľov viac než 1000 prevádzkovateľom základnej služby štátu a je povinná dodržiavať bezpečnostné opatrenia podľa §20 (1). Sú to úlohy, procesy, role a technológie v organizačnej, personálnej a technickej oblasti, ktorých cieľom je zabezpečenie kybernetickej bezpečnosti počas životného cyklu sietí a informačných systémov. Predmetom projektu je nastavenie úloh, procesov, rolí a technológií v organizačnej, personálnej a technickej oblasti, ktorých cieľom je zabezpečenie kybernetickej bezpečnosti. V zásade ide o opatrenia, ktoré majú za cieľ minimalizovať riziko vzniku negatívnej udalosti akými sú napríklad:
    a. Narušenie prevádzky siete alebo informačného systému, ktoré ohrozí integritu alebo dôvernosť spracovávaných osobných údajov,
    b. úniku osobných údajov v dôsledku čoho môže vzniknúť škoda na zdraví, či ujma na majetku,
    c. obmedzenie výkonu, alebo ohrozenie pôsobnosti obce, najmä s ohľadom na schopnosť zabezpečenia bezpečia, verejného poriadku alebo zvládnutia mimoriadnej udalosti.

Ciele projektu:

- Zvýšenie bezpečnostného štandardu v oblasti kybernetickej a informačnej bezpečnosti pre obce do 6.000 obyvateľov
- Na minimálne 1000 obciach obciach do 6000 obyvateľov využívajúcich IS DCOM zabezpečiť súlad s legislatívnymi požiadavkami KB kategórie I. podľa zákona č. 69/2018 Z. z. naprieč všetkými používanými informačnými systémami a internými procesmi.
- Zvyšovanie osvety a všeobecného povedomia o téme kybernetickej a informačnej bezpečnosti medzi zamestnancami a obyvateľmi samospráv /obcí.
- Zvýšenie bezpečnostného štandardu v oblasti kybernetickej a informačnej bezpečnosti IS DCOM v podobe procesného, technického, hardvérového vybavenia, aplikácií, SW a tým aj bezpečnosti samotných obcí.

Projekt bude realizovaný v rámci:

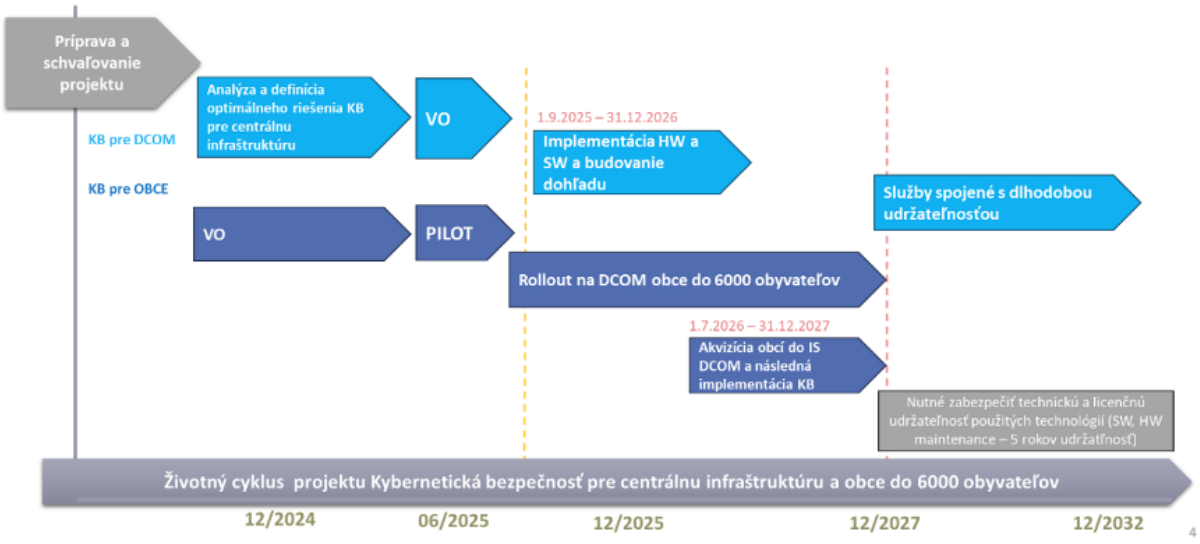
Špecifický cieľ: RSO1.2 Využívanie prínosov digitalizácie pre občanov, podniky, výskumné organizácie a orgány verejnej správy

Hlavné aktivity projektu:

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

Dĺžka projektu: je plánovaná na 39 mesiacov.

Rozdelenie projektu na dielčie súčasti zobrazuje nasledovná schéma:



Odhadované náklady: sú **14 273 031,48** EUR s DPH.

3.2 Motivácia a rozsah projektu

3.2.1. Problém, ktorý bude realizáciou projektu odstránený

Kybernetická a informačná bezpečnosť obcí s menej ako 6 000 obyvateľmi čelí značným výzvam. Podľa údajov NBÚ sa pri sektore „Verejná správa“, podsektor „Informačné systémy verejnej správy“, v ktorom sa nachádza najväčší počet PZS situácia v oblasti kybernetickej bezpečnosti dlhodobo nemení. Stále tu možno pozorovať až kritické zanedbávanie bezpečnosti. Najmä samosprávy a menší prevádzkovatelia si dostatočne neuvedomujú dôležitosť témy kybernetickej bezpečnosti, k problematike pristupujú povrchne a zameriavajú sa skôr na formálne aktivity. Celkové riadenie kybernetickej bezpečnosti pri PZS v tomto sektore často chýba, je chaotické alebo čiastkové.

Medzi najčastejšie auditné zistenia v sektore Verejná správa patria:

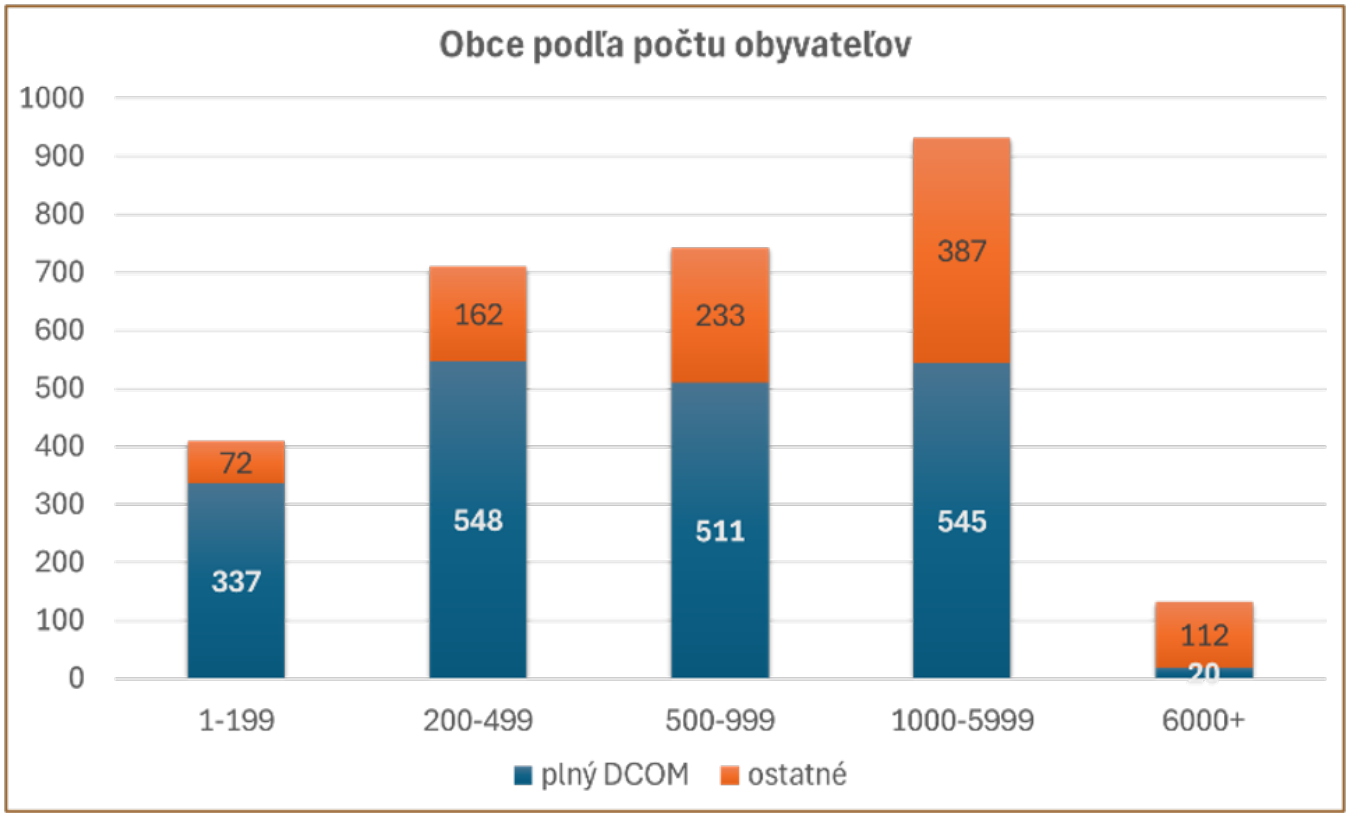
- nebol preukázaný systém riadenia kybernetickej bezpečnosti,
- bezpečnostná stratégia kybernetickej bezpečnosti ani ďalšia bezpečnostná dokumentácia nebola predložená,
- manažér kybernetickej bezpečnosti nie je formálne menovaný, je v konflikte záujmov a má nevhodne kumulované zodpovednosti,
- analýza rizík nie je zakotvená ako proces v interných predpisoch ani metodicky popísaná, nevykonáva sa,
- v organizácii sa nachádzajú vysoko privilegované účty, ktoré sú spoločné a nemajú definovaných vlastníkov a účel,
- v organizácii neexistuje definícia závažného kybernetického bezpečnostného incidentu, organizácia nevypracovala postupy a nemá dostatočné schopnosti na detekciu, zvládanie a poučenie sa z prípadných incidentov.

V súčasnosti sa na obciach do 6000 obyvateľov realizujú projekty kybernetickej bezpečnosti veľmi zriedka. Napriek mnohým zákonným požiadavkám platných najmä pre obce nad 1000 obyvateľov, ako poskytovateľov základnej služby štátu, je praktický prínos týchto aktivít minimálny. Najčastejšie dochádza len ku kopírovaniu existujúcej dokumentácie, bez aplikácie reálnej pridanej hodnoty pre špecifickú lokálnu potrebu a len výnimočne prebehne na obci aj relevantné školenie KB pre zamestnancov. Veľkou bariérou realizácie významnejších aktivít je najmä nedostatok finančných zdrojov a personálnych kapacít na obci. Povedomie o KB je tak na obciach minimálne.

Jedným z hlavných problémov, ktorý spôsobuje vyššie uvedené nedostatky je obmedzený rozpočet, čo znamená nedostatok finančných prostriedkov. Tieto obce často nedisponujú dostatočnými zdrojmi na zamestnanie odborníkov na kybernetickú bezpečnosť, čo vedie k nedostatočnému povedomiu a nedostatočnému zdokonaleniu bezpečnostných postupov. Okrem toho, staršie IT systémy a neaktualizovaný softvér predstavujú riziko, keďže obce nemajú prostriedky na modernizáciu svojej infraštruktúry. Nedostatok odborníkov na kybernetickú bezpečnosť a nedostatočné povedomie môžu zvyšovať riziko kybernetických hrozieb, čo môže ohroziť citlivé údaje a informačnú infraštruktúru obcí. Preto je dôležité venovať pozornosť týmto oblastiam a hľadať spôsoby, ako zlepšiť kybernetickú a informačnú bezpečnosť obcí tejto veľkosti. Najvyšší kontrolný úrad viackrát poukázal na to, že obce samostatne bez aktívnej podpory štátu nemajú dostatočné zdroje. Najmä v menších obciach absentuje akákoľvek infraštruktúra Informačnej a kybernetickej bezpečnosti a to hlavne z dôvodu obmedzených rozpočtových zdrojov. NKÚ opätovne konštatoval, že obce opäť uviedli nedostatok finančných prostriedkov ako jednu z významných bariér pri realizácii akýchkoľvek opatrení kybernetickej a informačnej bezpečnosti. Projekt si stanovuje primárne za cieľovú skupinu obce do 6000 obyvateľov, ktoré podľa Vyhlášky 179/2020 Z.z. spadajú do najnižšej kategórie I. no zároveň z pohľadu zdrojov sú najviac poddimenzované. Rozdelenie obcí na Slovensku podľa veľkostí a zapojenia do IS DCOM zobrazuje nasledovná tabuľka a graf:

	Počet obcí	Z toho plný DCOM	Z toho mimo DCOM
Skupina 199 obyvateľov alebo menej	409	337	72
Skupina Od 200 do 499 obyvateľov	710	548	162
Skupina Od 500 do 999 obyvateľov	744	511	233
Skupina Od 1 000 do 5 999 obyvateľov	932	545	387
Skupina nad 6000 obyvateľov	132	20	112
Spolu	**2927**	**1961**	**966**

Graf počtu obcí podľa veľkostnej kategórie:



Aby bolo možné zabezpečiť kybernetickú bezpečnosť zapojených obcí je zároveň potrebné prijať opatrenia na úrovni IS DCOM, ktorý spadá do III. kategórie. DEUS je špecifickým poskytovateľom cloudových služieb typu SaaS pre subjekty MÚS, a to s využitím IaaS a PaaS vládneho cloudu. IS DCOM spĺňa kritéria kybernetickej bezpečnosti požadované zákonom. IS DCOM je poskytovaný obciam ako SaaS služba, to znamená, že žiadne dáta, ktoré sú spracovávané v IS DCOM nie sú uložené na lokálnych zariadeniach na obciach. Lokálne zariadenia v tomto prípade slúži iba ako “terminály“ pre prístup na centrálne riešenie. V kontexte uvedeného je dôležité zdôrazniť, že viacero kritických bezpečnostných prvkov centrálneho riešenia IS DCOM je na hranici svojej životnosti a podpory. V priebehu najbližšieho obdobia bude nutné vykonať obnovu HW/SW komponentov. V rámci prostredia centrálnej infraštruktúry zatiaľ neboli implementované najmodernejšie SW nástroje pre ochranu prostredia. Ich budúcou implementáciou sa razantne zvýši celková odolnosť systému voči novým, sofistikovaným vektorom útoku. V súčasnosti je implementovaný monitoring nad základnými prvkami bezpečnostnej infraštruktúry, ktorý bol v minulosti plne postačujúci. Vzhľadom k narastajúcej komplexnosti hrozieb a taktiež komplexnosti ochranných nástrojov bude potrebné tento monitoring povýšiť na omnoho sofistikovanejšiu úroveň a zahrnúť do neho novo implementované vrstvy ochrany.

Implementáciou nových riešení sa dosiahne stav, kde aj dáta obcí, ktoré spadajú do kategórie I budú chránené na úrovni najvyšších bezpečnostných štandardov vyžadovaných pre celý IS DCOM.

3.2.2. Biznis procesy, ktoré sú predmetom projektu

Z pohľadu biznis procesov územná samospráva realizuje výkon vybraných procesov štátnej správy (tzv. prenesený výkon štátnej správy) a zodpovedá za metodické riadenie a výkon procesov samosprávy (tzv. originálne kompetencie). Z hľadiska originálnych kompetencií, sa opatrenia v oblasti kybernetickej bezpečnosti týkajú nasledovných originálnych kompetencií:

1. vykonáva úkony súvisiace s riadnym hospodárením s hnuteľným a nehnuteľným majetkom obce a s majetkom vo vlastníctve štátu prenechaným obci do užívania,
2. zostavuje a schvaľuje rozpočet obce a záverečný účet obce; vyhlasuje dobrovoľnú zbierku,
3. rozhoduje vo veciach miestnych daní a miestnych poplatkov a vykonáva ich správu,
4. usmerňuje ekonomickú činnosť v obci, a ak tak ustanovuje osobitný predpis, vydáva súhlas, záväzné stanovisko, stanovisko alebo vyjadrenie k podnikateľskej a inej činnosti právnických osôb a fyzických osôb a k umiestneniu prevádzky na území obce, vydáva záväzné stanoviská k investičnej činnosti v obci,
5. utvára účinný systém kontroly a vytvára vhodné organizačné, finančné, personálne a materiálne podmienky na jeho nezávislý výkon,
6. zabezpečuje výstavbu a údržbu a vykonáva správu miestnych komunikácií, verejných priestranstiev, obecného cintorína, kultúrnych, športových a ďalších obecných zariadení, kultúrnych pamiatok, pamiatkových území a pamätihodností obce,
7. zabezpečuje verejnoprospešné služby, najmä nakladanie s komunálnym odpadom a drobným stavebným odpadom, udržiavanie čistoty v obci, správu a údržbu verejnej zelene a verejného osvetlenia, zásobovanie vodou, odvádzanie odpadových vôd, nakladanie s odpadovými vodami zo žúmp a miestnu verejnú dopravu,
8. utvára a chráni zdravé podmienky a zdravý spôsob života a práce obyvateľov obce, chráni životné prostredie, ako aj utvára podmienky na zabezpečovanie zdravotnej starostlivosti, na vzdelávanie, kultúru, osvetovú činnosť, záujmovú umeleckú činnosť, telesnú kultúru a šport,
9. plní úlohy na úseku ochrany spotrebiteľa a utvára podmienky na zásobovanie obce; spravuje trhoviská,
10. obstaráva a schvaľuje územnoplánovaciu dokumentáciu obcí a zón, koncepciu rozvoja jednotlivých oblastí života obce, obstaráva a schvaľuje programy rozvoja bývania a spolupôsobí pri utváraní vhodných podmienok na bývanie v obci,
11. vykonáva vlastnú investičnú činnosť a podnikateľskú činnosť v záujme zabezpečenia potrieb obyvateľov obce a rozvoja obce,
12. zakladá, zriaďuje, zrušuje a kontroluje podľa osobitných predpisov svoje rozpočtové a príspevkové organizácie, iné právnické osoby a zariadenia,
13. organizuje miestne referendum o dôležitých otázkach života a rozvoja obce,
14. zabezpečuje verejný poriadok v obci,
15. zabezpečuje ochranu kultúrnych pamiatok v rozsahu podľa osobitných predpisov a dbá o zachovanie prírodných hodnôt,
16. plní úlohy na úseku sociálnej pomoci v rozsahu podľa osobitného predpisu,
17. vykonáva osvedčovanie listín a podpisov na listinách,
18. vedie obecnú kroniku v štátnom jazyku, prípadne aj v jazyku národnostnej menšiny.

3.2.3. Informácie o oblasti (OBSAH / AGENDA / ŽIVOTNÁ SITUÁCIA), ktorým sa projekt venuje

Z pohľadu životných situácií sa projekt venuje nasledovným životným situáciám:

Kód v číselníku (MetaIS)	Názov
068	Daň za užívanie verejného priestranstva
072	Miestny poplatok za komunálne odpady a drobné stavebné odpady
097	Šport
051	Demokracia

058	Účasť na veciach verejných
057	Štatistické informácie
030	Zatvorenie podniku
073	Odškodnenie
001	Dotácie
031	Odpadové hospodárstvo
093	Centrá voľného času
025	Služby
074	Poplatky za verejné služby
035	Udržateľnosť a ďalšie dimenzie
064	Daň z nehnuteľnosti
104	Základné umelecké školy
069	Daň za vjazd a zotrvanie motorového vozidla v historickej časti mesta
067	Daň za ubytovanie
094	Predškolské zariadenia
103	Základné školy
005	Oznamovacie povinnosti po registrácii podnikania
070	Dotácie
071	Dražby, exekúcie
034	Povolenia životného prostredia
020	Verejné obstarávanie
014	Ostatné dane
066	Daň za psa
016	Rozširovanie podnikania
013	Miestne dane a poplatky
061	Voľby
118	Uzavretie manželstva / rozvod manželstva
055	Slobodný prístup k informáciám, prístup k odtajneným skutočnostiam, archívy
112	Pomoc v hmotnej núdzi
160	Prenájom nehnuteľnosti
109	Narodenie
166	Odpadové hospodárstvo
111	Zdravotné postihnutie a podpora sociálneho začlenenia fyzickej osoby s ťažkým zdravotným postihnutím do spoločnosti
167	Ochrana ovzdušia
175	Civilná ochrana
157	Kataster nehnuteľností
153	Bytová politika
178	Požiar, povodeň a iné nebezpečenstvo

165	Územné plánovanie
176	Mestská polícia
171	Poľovníctvo a rybárstvo
003	Iná podpora, slobodný prístup k informáciám, prístup k odtajneným skutočnostiam, archívy
169	Ochrana prírody a krajiny
081	Cestná doprava a parkovanie
180	Kultúrne aktivity
163	Stavebné konanie
117	Úmrtie
119	Cirkev a náboženské spoločnosti
121	Pamiatky a zbierky múzeí a galérií
115	Sociálne služby
173	Zvieratá a rastliny

Tabuľka č. 1 - Zoznam projektom zlepšovaných životných situácií

Výnos MF SR č. 478/2010 Z. z. o základnom číselníku úsekov verejnej správy a agend verejnej správy nedefinoval pre samotný DEUS žiaden úsek. Avšak pre DEUS a tento projekt sú relevantné nasledovné úseky:

Kód v číselníku (MetaIS)	**Názov úseku**
U00024	Dane a poplatky
U00055	Stavebný poriadok a územné plánovanie okrem ekologických aspektov
U00169	Štátna starostlivosť o mládež a šport
U00165	Materské školy, základné školy, stredné školy, základné umelecké školy, jazykové školy a školské zariadenia
U00176	Vzťahy s cirkvami a náboženskými spoločnosťami
U00223	Vnútorná správa
U00097	Štátne symboly, heraldický register
U00077	Regionálny rozvoj okrem koordinácie využívania finančných prostriedkov z fondov Európskej únie
U00059	Cestovný ruch
U00100	Zhromažďovanie a združovanie vrátane registrácie niektorých právnických osôb, o ktorých to ustanoví osobitný zákon
U00080	Verejný poriadok, bezpečnosť osôb a majetku
U00144	Podpora sociálneho začlenenia fyzickej osoby s ťažkým zdravotným postihnutím do spoločnosti
U00012	Ochrana spotrebiteľa s výnimkou ochrany spotrebiteľa pri poskytovaní finančných služieb
U00143	Sociálne služby
U00157	Odpadové hospodárstvo
U00044	Cestná doprava
U00171	Ochrana pamiatkového fondu, kultúrne dedičstvo a knihovníctvo
U00149	Ochrana prírody a krajiny
U00154	Ochrana ovzdušia, ozónovej vrstvy a klimatického systému Zeme
U00083	Bezpečnosť a plynulosť cestnej premávky

U00122	Kontrola nad dodržiavaním podmienok organizovania a priebehu dobrovoľných dražieb
U00041	Hazardné hry
U00194	Štátna štatistika
U00091	Evidencia obyvateľov
U00098	Archívy a registratúry
U00145	Pomoc v hmotnej núdzi
U00094	Civilná ochrana a krízové riadenie
U00057	Tvorba a uskutočňovanie bytovej politiky
U00095	Ochrana pred požiarmi
U00073	Rybárstvo v oblasti akvakultúry a morského rybolovu
U00172	Umenie
U00046	Pozemné komunikácie

Tabuľka č. 2 - Zoznam projektom zlepšovaných úsekov

Vyššie uvedené úseky pozostávajú z veľkého počtu agend, pričom agendy priamo relevantné pre projekt sú uvedené v tabuľke nižšie:

Kód v číselníku (MetaIS)	**Názov úseku**
A0000224	Rozhodovanie vo veciach miestnych daní, miestnych poplatkov, verejnej dávky, prijatia úveru alebo pôžičky a vykonávanie ich správy
A0000700	Evidovanie a zabezpečenie ukladania územných rozhodnutí, stavebných povolení, kolaudačných rozhodnutí a iných opatrení
A0002454	Podporovanie organizovania športových podujatí miestneho významu
A0002352	Spracúvanie a poskytovanie informácií v oblasti výchovy a vzdelávania
A0000714	Spracovanie, schvaľovanie, zverejnenie a vyhodnotenie územného plánu
A0002594	Kontaktovanie sa s registrovanými cirkvami a náboženskými spoločnosťami
A0003185	Sprístupňovanie informácií z informačných systémov verejnej správy
A0003156	Sťažnosti
A0001410	Označovanie budovy, zasadacej miestnosti a úradnej miestnosti orgánov obce erbom a vlajkou
A0003117	Pripomienkovanie, vyhodnocovanie, zverejňovanie a sprístupňovanie nariadenia obce
A0003110	Zostavovanie, čerpanie, vykonávanie zmien a zverejňovanie rozpočtu obce
A0001171	Vypracúvanie programov rozvoja obcí
A0000772	Podpora rozvoja cestovného ruchu
A0003109	Zostavovanie a zverejňovanie záverečného účtu obce
A0001453	Zvolávanie verejného zhromaždenia občanov
A0001201	Zabezpečovanie verejného poriadku v obci
A0003157	Petičné právo
A0001912	Zabezpečovanie vyhotovenia preukazu fyzickej osoby s ťažkým zdravotným postihnutím, vyhotovenia preukazu fyzickej osoby s ťažkým zdravotným postihnutím so sprievodcom, parkovacieho preukazu
A0000048	Utváranie podmienok na zásobovanie obce, určovanie pravidiel času predaja v obchode, času prevádzky služieb a spravovanie trhovísk
A0003097	Poskytovanie dotácií z rozpočtu obce

A0001871	Poskytovanie finančného príspevku pri odkázanosti na pomoc inej osoby a finančného príspevku na prevádzku neverejným poskytovateľom sociálnych služieb
A0002243	Zabezpečovanie alebo umožňovanie zberu a prepravy komunálnych odpadov a zabezpečenie priestoru na odovzdávanie oddelených zložiek komunálnych odpadov občanmi v rámci separovaného zberu
A0002237	Poskytovanie informácie o umiestnení a činnosti zariadení na nakladanie s odpadmi držiteľovi odpadu na území obce
A0002380	Spracúvanie a poskytovanie informácií v oblasti výchovy a vzdelávania
A0000433	Schvaľovanie a ukladanie zmien cestovného poriadku
A0000434	Udeľovanie, zmena a odňatie dopravnej licencie
A0002541	Vydávanie záväzných stanovísk a stanovísk k úpravám uličného interiéru, drobnej architektúry, historickej zelene, verejného osvetlenia a reklamných zariadení
A0002082	Riadenie, vykonávanie a kontrola výkonu štátnej správy starostlivosti o životné prostredie
A0000431	Povoľovanie zriadenia autobusovej linky
A0003114	Hospodárenie a nakladanie s vlastným majetkom a s vlastnými príjmami obce
A0002203	Určovanie podmienok a kontrola dodržiavania povinností prevádzkovania malých zdrojov znečisťovania ovzdušia
A0001217	Odstraňovanie vozidiel ponechaných na ceste vrátane chodníka na náklady jeho prevádzkovateľa
A0001659	Kontrola dodržiavania podmienok organizovania a priebehu dražieb
A0003183	Zadávanie zákaziek na dodanie tovaru, zákazky na uskutočnenie stavebných prác alebo na poskytnutie služieb, zákazky na poskytnutie služieb a súťaž návrhov
A0000336	Rozhodovanie o udelení individuálnej licencie na úseku hazardných hier
A0000706	Obstarávanie, schvaľovanie, zmena a zverejnenie územnoplánovacej dokumentácie
A0000721	Určenie súpisného a orientačného čísla stavbám a vedenie ich evidencie
A0002777	Organizačné zabezpečenie volieb
A0001302	Evidovanie hlásení o uzavretí manželstva, o rozvode manželstva, o narodení, respektíve o úmrtí
A0001419	Umožňovanie prístupu k archívnym dokumentom
A0001938	Vykonávanie poradenstva pri zabezpečení základných životných podmienok a pomoci v hmotnej núdzi
A0001937	Rozhodovanie o jednorazovej dávke v hmotnej núdzi
A0001344	Oboznamovanie sa s havarijnými plánmi podnikov a prevádzok a informovanie obyvateľstva o postupe pri mimoriadnej udalosti
A0000765	Zabezpečovanie obstarávania a schvaľovania programov rozvoja bývania a spolupôsobenia pri utváraní vhodných podmienok na bývanie v obci
A0001383	Vypracovanie a vedenie dokumentácie ochrany pred požiarmi obce
A0001104	Vydávanie rybárskych lístkov a vedenie ich evidencie
A0002548	Vedenie evidencie pamiatkového fondu na území obce
A0002581	Prijímanie oznámenia usporiadateľa o zámere usporiadať podujatie
A0000476	Vedenie technickej evidencie o pozemných komunikáciách vo vlastníctve a správe obce
A0000486	Poskytovanie údajov o zjazdnosti miestnych komunikácií a údajov z technickej evidencie miestnych komunikácií
A0000445	Zabezpečovanie výstavby, údržby a výkonu správy miestnych komunikácií
A0000444	Zabezpečovanie miestnej verejnej dopravy
A0001856	Tvorba komunitného plánu sociálnych služieb
A0001861	Poskytovanie alebo zabezpečovanie sociálnej služby v nocľaháreň, v nízkoprahovom dennom centre, v nízkoprahovom dennom centre pre deti a rodinu, v zariadení pre seniorov, v zariadení opatrovateľskej služby, v dennom stacionári, opatrovateľskej služby, prepravnej služby, odľahčovacej služby

A0001857	Utváranie podmienok na podporu komunitného rozvoja v oblasti poskytovania sociálnych služieb

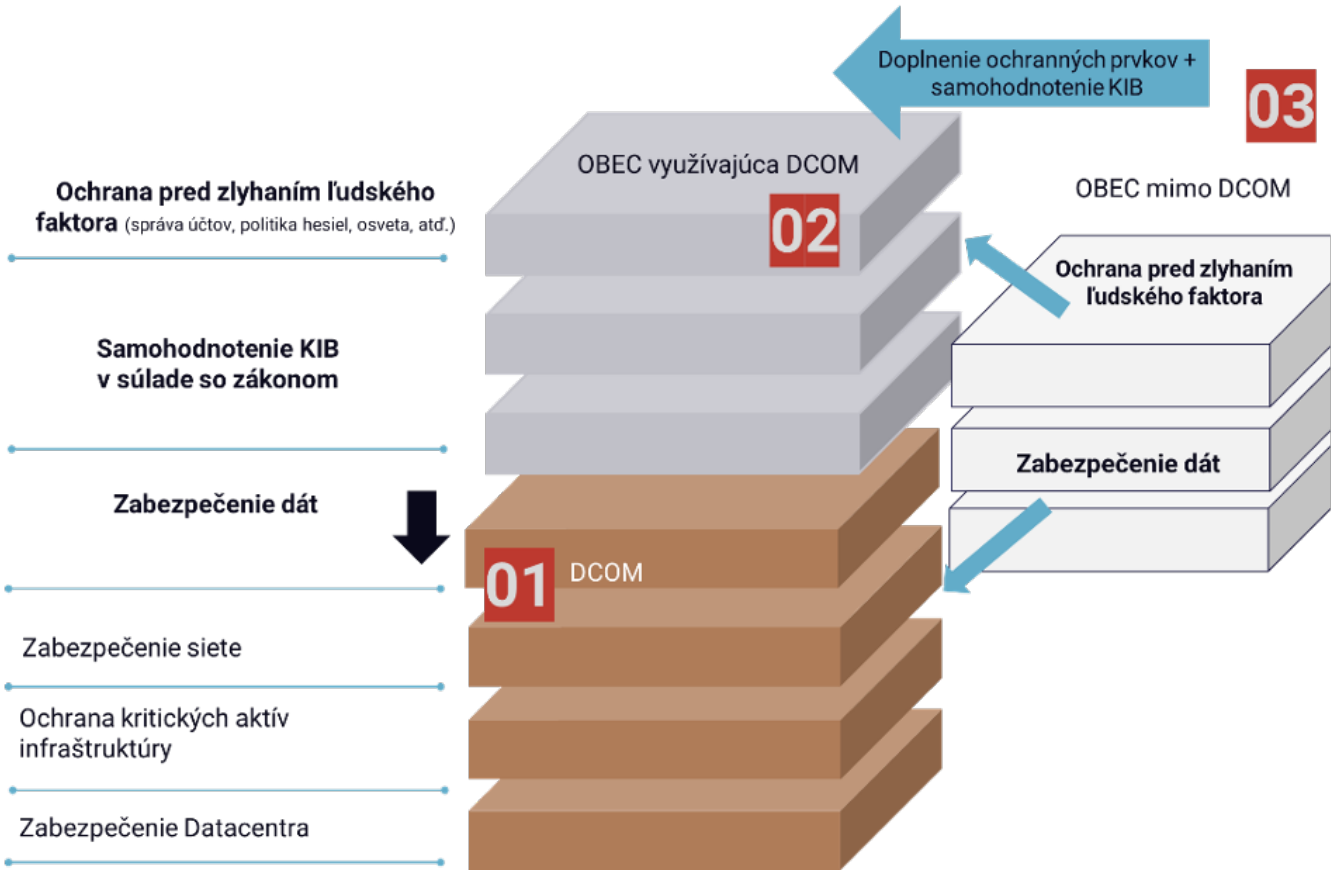
Tabuľka č. 3 - Zoznam agend relevantných pre projekt

3.2.4. ROZSAH PROJEKTU

Z hľadiska subjektu sa projekt týka DEUS. DEUS v zmysle § 9a odsek 1 zákona č. 305/2013 Z.z. o elektronickej podobe výkonu pôsobností orgánov verejnej moci (eGovernmente) vykonáva činnosti správcu a prevádzkovateľa IS DCOM. DEUS je záujmové združenie právnických osôb, ktorého jedinými členmi sú Ministerstvo financií SR (ďalej len „MF SR“) a Združenie miest a obcí Slovenska (ďalej len „ZMOS“). Zákon o eGovernmente zároveň vymedzuje IS DCOM ako nadrezortný informačný systém verejnej správy, ktorý poskytuje obciam technické a programové prostriedky na výkon verejnej moci elektronicky, na prevádzkovanie ISVS v ich správe a na zabezpečenie základných činností v oblasti elektronického výkonu vnútorných agend a prevádzku ostatných IS, ktoré obec používa.

Systém riadenia kybernetickej bezpečnosti v Slovenskej republike má niekoľko vrstiev, ktoré môžeme rozdeliť na národnú úroveň a sektorovú úroveň. Na sektorovej úrovni je podľa zákona definovaných 11 sektorov a 25 podsektorov. Za každý zo sektorov je zodpovedný ústredný orgán (ďalej len „ústredný orgán“), ktorý plní úlohy na úrovni poskytovania požadovanej súčinnosti s úradom, spolupráce s inými sektorovými ústrednými orgánmi a prevádzkovateľmi základných služieb vo svojej pôsobnosti, budovaní bezpečnostného povedomia, koordinovanej spolupráce na všetkých stupňoch riadenia kybernetickej bezpečnosti, aplikácie bezpečnostných opatrení, identifikácie základnej služby a prevádzkovateľa základnej služby a spolupráce so zahraničnou inštitúciou obdobného zamerania. Projekt sa priamo dotýka sektoru Verejnej správy a podsektorov Bezpečnosť a Informačné systémy verejnej správy. V každom sektore, na základe identifikácie podľa zákona, vystupujú prevádzkovatelia základných služieb. Títo majú povinnosti, vyplývajúce zo zákona a to najmä prijať a dodržiavať zákonne vymedzené bezpečnostné opatrenia, bezodkladne úradu hlásiť závažný kybernetický bezpečnostný incident, riešiť kybernetické bezpečnostné incidenty, zabezpečovať dôkazy o kybernetických bezpečnostných incidentoch, spolupracovať s úradom a ústredným orgánom, ako aj oznámiť orgánom činným v trestnom konaní, ak bol spáchaný trestný čin v súvislosti s kybernetickým bezpečnostným incidentom. Združenie DEUS, ako aj obce sú prevádzkovateľmi základnej služby.

Projekt kybernetickej bezpečnosti pre samosprávy do 6000 obyvateľov bude realizovaný v 3 častiach:



Projekt je rozdelený do troch základných častí:

1. **Infraštruktúra ochrany dát obce v dátovom centre.**

Upgrade a doplnenie centrálnej infraštruktúry IS DCOM na softvérovej a hardvérovej úrovni za účelom:

- udržania **vysokej bezpečnosti samotnej základnej služby** poskytovanej IS DCOM.
- **minimalizovanie výpadkov** poskytovanej služby z dôvodu kybernetického útoku
- **významného zníženia času obnovy** systému pri závažnom KB incidente a nutnosti obnovy systému zo zálohy (total recovery time IS DCOM)

Audit a kontrolné činnosti

- obstaranie auditu kybernetickej bezpečnosti v súlade so zákonom o KB pre IS DCOM

2. Zvýšenie kybernetickej bezpečnosti obcí v súčasnosti nezapojených do IS DCOM do 6000 obyvateľov

Pre zabezpečenie informačnej a kybernetickej bezpečnosti týchto obcí a ochranu dát je potrebné v prvom kroku realizovať migráciu obcí do IS DCOM. Po migrácii by tieto obce mali prostredníctvom IS DCOM zabezpečenú kompletnú agendu komunikácie cez elektronickú schránku obce, všetky rozhodnutia obce, všetky daňové informácie a rozhodnutia a množstvo inej agendy a integrácií na centrálne systémy verejnej správy ako Register fyzických osôb, sociálna poisťovňa, národná evidencia vozidiel a podobne. Všetky tieto dáta budú užívateľom obcí prístupné po dvojfaktorovej autorizácii – najskôr cez VPN a následne prostredníctvom aplikačných rolí v samotnej aplikácii. Okrem dát, ktoré sú evidované v IS DCOM, majú obce citlivejšie dáta evidované už iba v systémoch pre správu registratúry a účtovníctve. Veľká časť dát zo správy registratúry je prostredníctvom integrácií tiež synchronizovaná do IS DCOM za účelom optimálnej spolupráce oboch systémov. Obec by tak prostredníctvom IS DCOM mala chránené všetky kritické dáta, ktoré spravuje alebo uchováva.

a) Migrácia do IS DCOM

- Migrácia údajov súvisiacich so službami samosprávy poskytovanými verejnosti
- Asistencia pre obec/mesto po spustení do produkčnej prevádzky
- Školenie nových používateľov IS DCOM
- Zabezpečenie služieb ÚPVS pre obce
- Inštalácia a konfigurácia backup systému obce

b) Organizácia kybernetickej a informačnej bezpečnosti

- Vypracovanie alebo aktualizácia bezpečnostnej dokumentácie vrátane rozsahu a spôsobu plnenia všeobecných bezpečnostných opatrení;
- vypracovanie a implementácia špecifických interných riadiacich aktov pre vybrané oblasti kybernetickej a informačnej bezpečnosti;

c) Riadenie rizík

- Identifikácia všetkých aktív súvisiacich so zariadeniami na spracovanie informácií a centrálne zaznamenávanie inventáru týchto aktív podľa ich hodnoty vrátane určenia ich vlastníka, ktorý definuje požiadavky na ich dôvernosť, dostupnosť a integritu;
- riadenie rizík pozostávajúce z identifikácie zraniteľností, identifikácie hrozieb, identifikácie a analýzy rizík s ohľadom na aktívum, určenie vlastníka rizika, implementácie organizačných a technických bezpečnostných opatrení, analýzy funkčného dopadu a pravidelného preskúmavania identifikovaných rizík v závislosti od aktualizácie prijatých bezpečnostných opatrení;
- vypracovanie a implementácia interného riadiaceho aktu riadenia rizík kybernetickej a informačnej bezpečnosti.

d) Personálna bezpečnosť

- Vypracovanie postupov pri zaradení osoby do niektorých z bezpečnostných rolí, zavedenie plánu rozvoja bezpečnostného povedomia a vzdelávania, vypracovanie spôsobov hodnotenia účinnosti plánu rozvoja bezpečnostného povedomia, určenie pravidiel a postupov na riešenie prípadov porušenia bezpečnostnej politiky, zavedenie postupov pri skončení pracovnoprávneho vzťahu alebo iného obdobného vzťahu, zavedenie postupov pri porušení bezpečnostných politík;
- vypracovanie alebo aktualizácia interného riadiaceho aktu s bezpečnostnými zásadami pre koncových používateľov;
- vypracovanie a implementácia postupov a procesov upravujúcich personálnu bezpečnosť organizácie prostredníctvom interného riadiaceho aktu.

e) Riadenie prístupov

- Vypracovanie a implementácia zásad riadenia prístupov osôb k sieti a informačnému systému;
- vypracovanie a implementácia postupov a procesov upravujúcich riadenie prístupov organizácie.

f) Riadenie kybernetickej a informačnej bezpečnosti vo vzťahoch s tretími stranami

- Vypracovanie analýzy rizík tretích strán a celého dodávateľského reťazca, vrátane analýzy politických rizík;
- analýza a posúdenie súladu všetkých aktuálnych zmlúv s tretími stranami so zákonom o KB a dobrou praxou;
- vypracovanie návrhov dodatkov zmlúv s treťou stranou spolu s návrhom potrebných úprav na zabezpečenie súladu so zákonom KB;
- vypracovanie a implementácia interného riadiaceho aktu upravujúceho zásady kybernetickej a informačnej bezpečnosti vo vzťahoch s tretími stranami.

g) Bezpečnosť pri prevádzke informačných systémov a sietí

- obstaranie služieb pre potreby správy prevádzkovej zálohy, kópie archivačnej zálohy a kópie inštalačných médií, vrátane určenia spôsobu ich ukladania

h) Hodnotenie zraniteľností a bezpečnostné aktualizácie

- vypracovanie a implementácia interného riadiaceho aktu upravujúceho proces riadenia implementácie bezpečnostných aktualizácií a záplat;

i) Ochrana proti škodlivému kódu

- Vypracovanie interného riadiaceho aktu s požiadavkami na určenie zodpovednosti používateľov, pravidiel pre inštaláciu a monitorovania potenciálnych ciest prieniku škodlivého kódu;
- vypracovanie a implementácia pravidiel súvisiace s ochranou proti škodlivému kódu;

j) Sieťová a komunikačná bezpečnosť

- Implementácia nástrojov na ochranu integrity sietí, ktoré zabezpečujú riadenie bezpečného prístupu medzi vonkajšími a vnútornými sieťami, implementácia segmentácie sietí, implementácia alebo obnova firewall-u, revízia firewall pravidiel;
- vytvorenie alebo aktualizácia dokumentácie počítačovej siete, ktorá obsahuje evidenciu všetkých miest prepojenia sietí vrátane prepojení s externými sieťami, topológiu siete a využitie IP rozsahov;
- vypracovanie a implementácia interného riadiaceho aktu upravujúceho pravidlá sieťovej a komunikačnej bezpečnosti;

k) Riešenie kybernetických bezpečnostných incidentov

- Vypracovanie štandardov a postupov riešenia kybernetických bezpečnostných incidentov, vrátane definovania zodpovedností zamestnancov a ďalších povinností;
- vypracovanie plánov a spôsobov riešenia kybernetických bezpečnostných incidentov.

l) Kontinuita prevádzky

- Vypracovanie stratégie a krízových plánov prevádzky na základe analýzy vplyvov kybernetického bezpečnostného incidentu na základnú službu;
- vypracovanie interného riadiaceho aktu obsahujúceho a upravujúceho kontinuitu prevádzky následkom kybernetického bezpečnostného incidentu alebo inej krízovej situácie;
- implementácia systému zálohovania.

m) Samohodnotenie súladu opatrení obce s požiadavkami kybernetickej bezpečnosti

- Podpora pre obce pri vypracovaní prvého samohodnotenia obce

3. Zvýšenie kybernetickej bezpečnosti obcí zapojených do IS DCOM do 6000 obyvateľov

a) Organizácia kybernetickej a informačnej bezpečnosti

- Vypracovanie alebo aktualizácia bezpečnostnej dokumentácie vrátane rozsahu a spôsobu plnenia všeobecných bezpečnostných opatrení;
- vypracovanie a implementácia špecifických interných riadiacich aktov pre vybrané oblasti kybernetickej a informačnej bezpečnosti;

b) Riadenie rizík

- Identifikácia všetkých aktív súvisiacich so zariadeniami na spracovanie informácií a centrálne zaznamenávanie inventáru týchto aktív podľa ich hodnoty vrátane určenia ich vlastníka, ktorý definuje požiadavky na ich dôvernosť, dostupnosť a integritu;
- riadenie rizík pozostávajúce z identifikácie zraniteľností, identifikácie hrozieb, identifikácie a analýzy rizík s ohľadom na aktívum, určenie vlastníka rizika, implementácie organizačných a technických bezpečnostných opatrení, analýzy funkčného dopadu a pravidelného preskúmavania identifikovaných rizík v závislosti od aktualizácie prijatých bezpečnostných opatrení;
- vypracovanie a implementácia interného riadiaceho aktu riadenia rizík kybernetickej a informačnej bezpečnosti.

c) Personálna bezpečnosť

- Vypracovanie postupov pri zaradení osoby do niektorých z bezpečnostných rolí, zavedenie plánu rozvoja bezpečnostného povedomia a vzdelávania, vypracovanie spôsobov hodnotenia účinnosti plánu rozvoja bezpečnostného povedomia, určenie pravidiel a postupov na riešenie prípadov porušenia bezpečnostnej politiky, zavedenie postupov pri skončení pracovnoprávneho vzťahu alebo iného obdobného vzťahu, zavedenie postupov pri porušení bezpečnostných politík;
- vypracovanie alebo aktualizácia interného riadiaceho aktu s bezpečnostnými zásadami pre koncových používateľov;
- vypracovanie a implementácia postupov a procesov upravujúcich personálnu bezpečnosť organizácie prostredníctvom interného riadiaceho aktu.

d) Riadenie prístupov

- Vypracovanie a implementácia zásad riadenia prístupov osôb k sieti a informačnému systému;
- vypracovanie a implementácia postupov a procesov upravujúcich riadenie prístupov organizácie.

e) Riadenie kybernetickej a informačnej bezpečnosti vo vzťahoch s tretími stranami

- Vypracovanie analýzy rizík tretích strán a celého dodávateľského reťazca, vrátane analýzy politických rizík;
- analýza a posúdenie súladu všetkých aktuálnych zmlúv s tretími stranami so zákonom o KB a dobrou praxou;
- vypracovanie návrhov dodatkov zmlúv s treťou stranou spolu s návrhom potrebných úprav na zabezpečenie súladu so zákonom KB;
- vypracovanie a implementácia interného riadiaceho aktu upravujúceho zásady kybernetickej a informačnej bezpečnosti vo vzťahoch s tretími stranami.

f) Bezpečnosť pri prevádzke informačných systémov a sietí

- obstaranie služieb pre potreby správy prevádzkovej zálohy, kópie archivačnej zálohy a kópie inštalačných médií, vrátane určenia spôsobu ich ukladania

g) Hodnotenie zraniteľností a bezpečnostné aktualizácie

- vypracovanie a implementácia interného riadiaceho aktu upravujúceho proces riadenia implementácie bezpečnostných aktualizácií a záplat;

h) Ochrana proti škodlivému kódu

- Vypracovanie interného riadiaceho aktu s požiadavkami na určenie zodpovednosti používateľov, pravidiel pre inštaláciu a monitorovania potenciálnych ciest prieniku škodlivého kódu;
- vypracovanie a implementácia pravidiel súvisiace s ochranou proti škodlivému kódu;

i) Sieťová a komunikačná bezpečnosť

- Implementácia nástrojov na ochranu integrity sietí, ktoré zabezpečujú riadenie bezpečného prístupu medzi vonkajšími a vnútornými sieťami, implementácia segmentácie sietí, implementácia alebo obnova firewall-u, revízia firewall pravidiel;
- vytvorenie alebo aktualizácia dokumentácie počítačovej siete, ktorá obsahuje evidenciu všetkých miest prepojenia sietí vrátane prepojení s externými sieťami, topológiu siete a využitie IP rozsahov;
- vypracovanie a implementácia interného riadiaceho aktu upravujúceho pravidlá sieťovej a komunikačnej bezpečnosti;

j) Riešenie kybernetických bezpečnostných incidentov

- Vypracovanie štandardov a postupov riešenia kybernetických bezpečnostných incidentov, vrátane definovania zodpovedností zamestnancov a ďalších povinností;
- vypracovanie plánov a spôsobov riešenia kybernetických bezpečnostných incidentov.

k) Kontinuita prevádzky

- Vypracovanie stratégie a krízových plánov prevádzky na základe analýzy vplyvov kybernetického bezpečnostného incidentu na základnú službu;
- vypracovanie interného riadiaceho aktu obsahujúceho a upravujúceho kontinuitu prevádzky následkom kybernetického bezpečnostného incidentu alebo inej krízovej situácie;
- implementácia systému zálohovania.

l) Samohodnotenie súladu opatrení obce s požiadavkami kybernetickej bezpečnosti

- Podpora pre obce pri vypracovaní prvého samohodnotenia obce

Maximálny možný počet zapojených obcí do projektu uvádza nasledovná tabuľka:

samospráva do 6000 obyvateľov	SR	DCOM	Z toho do projektu	Mimo DCOM	Z toho do projektu 40%	Celkovo maximálne v projekte – kryté rozpočtom projektu	Minimálne KPI projektu
Spolu	**2795**	**1941**	**1455**	**854**	**350**	**1805**	**1000**

3.2.5. Motivácia stakeholderov projektu

Kybernetická bezpečnosť je s neustále rastúcou digitalizáciou spoločnosti jednou z najdôležitejších oblastí, ktorá priamo ovplyvňuje fungovanie modernej spoločnosti. Aby bolo možné ju efektívne riadiť, potrebuje strategické ukotvenie aj v rámci samosprávy. Komplexný prístup ku kybernetickej bezpečnosti s jasnými princípmi a cieľmi nie len zaručuje jasnú víziu, ale aj potvrdzuje jej dôležitosť v celom bezpečnostnom systéme. Previazanie kybernetickej bezpečnosti s problematikou počítačovej kriminality, kybernetického spravodajstva, kybernetickej obrany a kybernetickej diplomacie podčiarkuje multidimenzionálny presah kybernetickej bezpečnosti do viacerých významných oblastí, ktoré formujú kybernetický priestor.

Dňa 7. januára 2021 bola vládou schválená Národná stratégia kybernetickej bezpečnosti na roky 2021 až 2025 (ďalej len “Národná stratégia”), ktorá zakotvila smerovanie Slovenskej republiky (ďalej len „SR“) v oblasti kybernetickej bezpečnosti. V Národnej stratégii sú popísané princípy, na ktorých stojí systém riadenia kybernetickej bezpečnosti, ako aj hrozby, ktoré vplývajú na procesy a činnosti v oblasti kybernetickej bezpečnosti a majú významný dopad na bezpečnosť štátu, ako aj jeho obyvateľov. Ako reakcia na tieto hrozby Národná stratégia určila strategické ciele, na ktoré je potrebné sa najbližších minimálne 5 rokov zamerať:

1. Dôveryhodný štát pripravený na hrozby
2. Efektívne odhaľovanie a objasňovanie počítačovej kriminality
3. Odolný súkromný sektor
4. **Kybernetická bezpečnosť ako základná súčasť verejnej správy**
5. Silné partnerstvá
6. Vzdelaní odborníci a vzdelaná verejnosť
7. Výskum a vývoj v oblasti kybernetickej bezpečnosti

Aby mohla byť Národná stratégia a jej ciele vykonateľné, museli byť určené konkrétne úlohy a aktivity spolu s jasnými zodpovednosťami. Na tento účel slúži Akčný plán Národnej stratégie kybernetickej bezpečnosti na roky 2021 až 2025 (ďalej len “Akčný plán”), ktorý tieto úlohy definuje, určuje zodpovedné subjekty a takisto aj časové horizonty pre jednotlivé úlohy. Na národnú stratégiu, jej ciele a akčný plán nadväzuje ciel tohto národného projektu, ktorým je zvýšenie úrovne kybernetickej a informačnej bezpečnosti pre obce do 6 000 obyvateľov v podobe technických a organizačných opatrení a zabezpečenie súladu s legislatívnymi požiadavkami v oblasti kybernetickej bezpečnosti.

V IS DCOM majú obce kompletnú agendu komunikácie cez elektronickú schránku obce, všetky rozhodnutia obce, všetky daňové informácie a rozhodnutia a množstvo inej agendy a integrácií na centrálne systémy verejnej správy ako Register fyzických osôb, Sociálna poisťovňa, Národná evidencia vozidiel a podobne. Všetky tieto dáta sú užívateľom obcí prístupné po dvojfaktorovej autorizácii – najskôr cez VPN a následne prostredníctvom aplikačných rolí v samotnej aplikácii. Okrem dát, ktoré sú evidované v IS DCOM, majú obce citlivejšie dáta evidované už iba v systémoch pre správu registratúry a účtovníctve. Veľká časť dát zo správy registratúry je prostredníctvom integrácií tiež synchronizovaná do IS DCOM za účelom optimálnej spolupráce oboch systémov. Z vyššie uvedeného je zrejmé, že najväčší objem chúlostivých dát na obci (určite vieme povedať že viac ako 80%) prevádzkuje obec v IS DCOM. Na malých obciach sa v princípe jedná o 100%. Všetky tieto fakty potvrdzujú, že pokiaľ kvalitne ochránime centrálnu infraštruktúru IS DCOM v dátových centrách, ochránime tak vyše 80% dát a IT prevádzky obcí.

V zmysle zákona č.69/2018 Z.z. o kybernetickej bezpečnosti, je každá obec s počtom obyvateľov viac než 1000 prevádzkovateľom základnej služby štátu a je povinná dodržiavať bezpečnostné opatrenia podľa §20 (1). Sú to úlohy, procesy, role a technológie v organizačnej, personálnej a technickej oblasti, ktorých cieľom je zabezpečenie kybernetickej bezpečnosti počas životného cyklu sietí a informačných systémov. V zásade ide o opatrenia, ktoré majú za cieľ minimalizovať riziko vzniku negatívnej udalosti akými sú napríklad:

- Narušenie prevádzky siete alebo informačného systému, ktoré ohrozí integritu alebo dôvernosť spracovávaných osobných údajov,
- Úniku osobných údajov v dôsledku čoho môže vzniknúť škoda na zdraví, či ujma na majetku,
- Obmedzenie výkonu, alebo ohrozenie pôsobnosti obce, najmä s ohľadom na schopnosť zabezpečenia bezpečia, verejného poriadku alebo zvládnutia mimoriadnej udalosti.

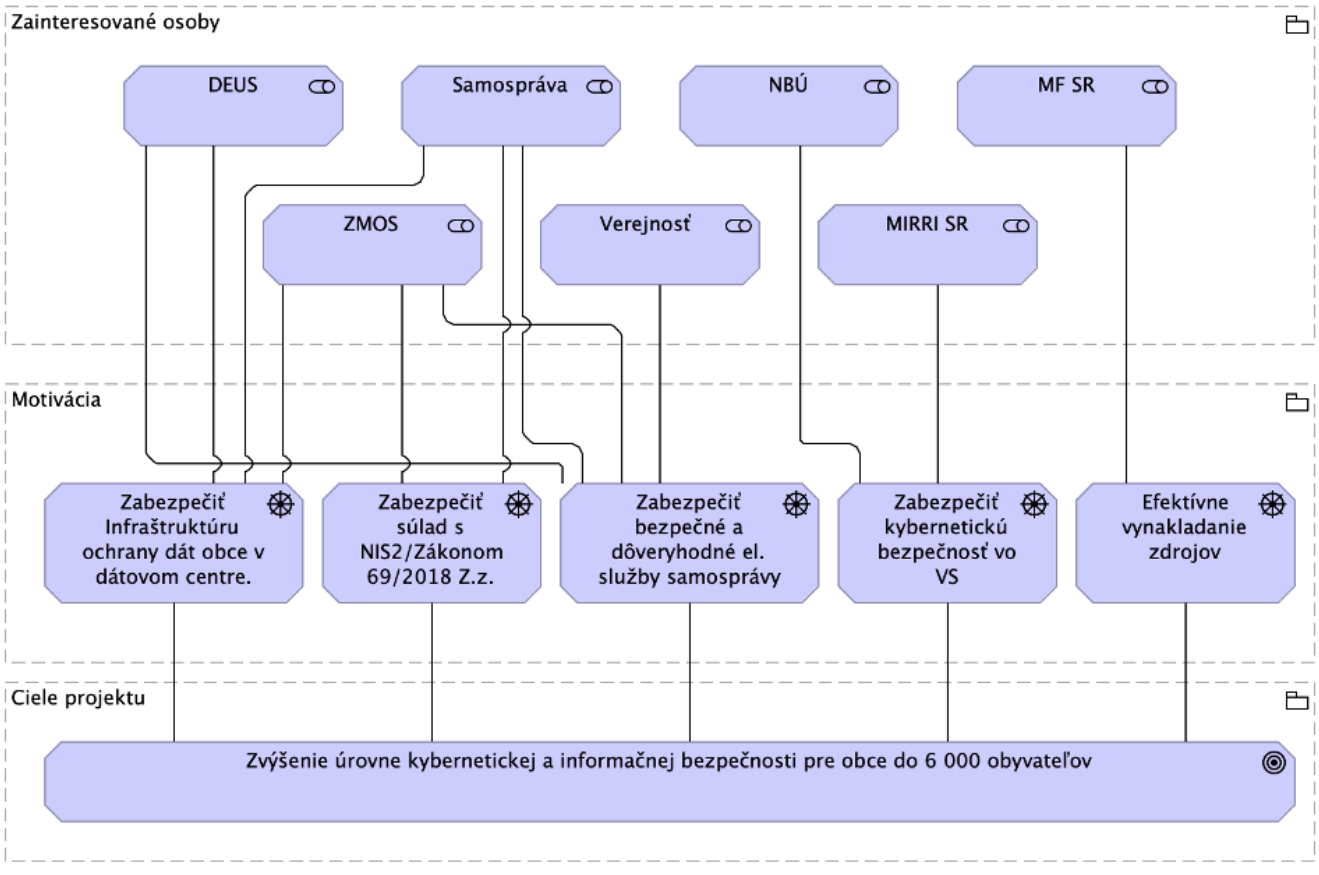
Zákon hovorí explicitne o obciach nad 1000 obyvateľov, až 1863 obcí na Slovensku, teda viac než 2/3 územia (!) má menej než tisíc obyvateľov a spolu tak v týchto obciach žije viac ako 800 000 obyvateľov. Z pohľadu kybernetickej bezpečnosti dáta týchto občanov a obcí nie sú chránené vôbec.

Štruktúra obcí podľa počtu obyvateľov a spôsobu zabezpečenia výkonu verejnej moci elektronicky

	Počet obcí	**Z toho plný DCOM**	**Z toho mimo DCOM**
Skupina 199 obyvateľov alebo menej	409	337	72

Skupina Od 200 do 499 obyvateľov	710	548	162
Skupina Od 500 do 999 obyvateľov	744	511	233
Skupina Od 1 000 do 5 999 obyvateľov	932	545	387
Skupina nad 6000 obyvateľov	132	20	112
Spolu	**2927**	**1961**	**966**

Cieľom aktivít projektu je vytvoriť prostredie na národnej úrovni v ktorom bude možné čo najefektívnejšie zvyšovať úroveň kybernetickej bezpečnosti pre samosprávy SR a občanov SR využívajúcich elektronické služby samospráv. Realizácia projektu prostredníctvom dopytovej výzvy na predkladanie žiadostí o NFP by bola neefektívna, nakoľko by nebolo možné naplniť všetky stanovené ciele predloženého projektu, ktorý bude mať dopad na organizácie samosprávy naprieč celým územím SR. Upgrade monitoringu prevádzky významne zlepší aj monitorovanie a detekciu hrozieb a umožní organizácii lepšie tieto hrozby identifikovať, analyzovať a v rýchlom čase prijať aktívne bezpečnostné opatrenia pre ochranu a zachovanie integrity dôverných informácií, ktoré systém spracováva. Implementáciou projektu sa významne zníži čas obnovy systému (recovery time) v prípade závažného bezpečnostného incidentu, čo predstavuje pre koncového užívateľa najväčší prínos projektu. Jedná sa tak o kontinuálnu investíciu do modernizácie IS DCOM a zabezpečenie jeho vysokej ochrany v dynamicky sa meniacom prostredí kybernetickej bezpečnosti.



Aktéri projektu, ich ciele, požiadavky a obmedzenia:

Aktér	Cieľ	Požiadavka	Obmedzenie

DEUS	Zabezpečiť infraštruktúru ochrany dát obce v dátovom centre Poskytovanie bezpečných a dôveryhodných elektronických služieb samosprávy Zníženie rizika kybernetických útokov v rámci samosprávy.	Realizácia projektu Kybernetická bezpečnosť pre samosprávy SR do 6000 obyvateľov prostredníctvom správcu informačného systému DCOM. Zamedziť riziku kybernetických útokov a výpadku eSlužieb MÚS.	Súčasné finančné zabezpečenie DEUS neumožňuje realizáciu projektu bez financovania zo zdrojov EÚ.
Obec (samosprávna)	Zabezpečiť infraštruktúru ochrany dát obce v dátovom centre Zabezpečiť súlad s nariadením NIS2, resp. zákonom č. 69/2018 Z.z. Poskytovanie bezpečných a dôveryhodných elektronických služieb samosprávy Zníženie rizika kybernetických útokov v rámci samosprávy.	Realizácia projektu Kybernetická bezpečnosť pre samosprávy SR do 6000 obyvateľov prostredníctvom správcu informačného systému DCOM.	Chýbajúce zdroje na zabezpečenie infraštruktúry. Dostupné finančné prostriedky sú smerované na zabezpečenie akútnych potrieb samosprávy.
ZMOS	Zabezpečiť infraštruktúru ochrany dát obce v dátovom centre Zabezpečiť súlad s nariadením NIS2, resp. zákonom č. 69/2018 Z.z. Poskytovanie bezpečných a dôveryhodných elektronických služieb samosprávy Zníženie rizika kybernetických útokov v rámci samosprávy.	Realizácia projektu Kybernetická bezpečnosť pre samosprávy SR do 6000 obyvateľov prostredníctvom správcu informačného systému DCOM. Minimalizácia administratívnej a finančnej záťaže na samosprávu.	Chýbajúce zdroje na zabezpečenie infraštruktúry. Dostupné finančné prostriedky sú smerované na zabezpečenie akútnych potrieb samosprávy.
MF SR	Efektívne vynakladanie zdrojov verejného rozpočtu (štátneho i samosprávneho).	Zabezpečenie kybernetickej bezpečnosti pre samosprávy SR do 6000 obyvateľov pri dodržaní podmienky VfM	Vzhľadom na prebiehajúce krízy a deficit v štátnom rozpočte sú zdroje štátneho rozpočtu výrazne obmedzené.
MIRRI SR	Zabezpečiť kybernetickú bezpečnosť vo VS Zabezpečiť súlad s nariadením NIS2, resp. zákonom č. 69/2018 Z.z. Zníženie rizika kybernetických útokov v rámci samosprávy.	Poskytovanie podpory samospráve.	Pre dosiahnutie cieľov na národnej úrovni je potrebný partner na úrovni samosprávy.

NBÚ	Zabezpečiť kybernetickú bezpečnosť vo VS Zabezpečiť súlad s nariadením NIS2, resp. zákonom č. 69/2018 Z.z. Zníženie rizika kybernetických útokov v rámci samosprávy.	Poskytovanie podpory samospráve.	Pre dosiahnutie cieľov na národnej úrovni je potrebný partner na úrovni samosprávy.
Verejnosť	Poskytovanie bezpečných a dôveryhodných elektronických služieb samosprávy. Zníženie rizika kybernetických útokov v rámci samosprávy.	Realizácia projektu Kybernetická bezpečnosť pre samosprávy SR do 6000 obyvateľov prostredníctvom správcu informačného systému DCOM. Minimalizácia administratívnej a finančnej záťaže na samosprávu.	N/A

Projekt je v súlade so strategickými dokumentmi v oblasti kybernetickej bezpečnosti a informatizácie samosprávy, pričom východiskovým rámcom pre realizáciu projektu sú dokumenty:

- Národná stratégia kybernetickej bezpečnosti na roky 2021 až 2025, ktorá zakotvila smerovanie Slovenskej republiky (ďalej len „SR“) v oblasti kybernetickej bezpečnosti. V Národnej stratégii sú popísané princípy, na ktorých stojí systém riadenia kybernetickej bezpečnosti, ako aj hrozby, ktoré vplývajú na procesy a činnosti v oblasti kybernetickej bezpečnosti a majú významný dopad na bezpečnosť štátu, ako aj jeho obyvateľov.
- Akčný plán realizácie Národnej stratégie kybernetickej bezpečnosti na roky 2021 až 2025. Cieľom Akčného plánu je vytvoriť ucelený koncept úloh a aktivít v oblasti kybernetickej bezpečnosti na najbližších 5 rokov. Navrhované úlohy sú adekvátne k potrebám naplnenia vízie a strategických cieľov stratégie a rešpektujú základné princípy, ktoré boli v stratégii zakotvené.
- Národná koncepcia informatizácie verejnej správy, definuje Informačnú a kybernetickú bezpečnosť ako jednu zo svojich priorít. Kybernetická a informačná bezpečnosť je horizontálna os, ktorá nastavuje ciele v záujme vybudovania ekosystému, legislatívneho, organizačného a technického prostredia schopného čeliť kybernetickým hrozbám

3.3 Zainteresované strany/Stakeholderi

ID	AKTÉR / STAKEHOLDER	SUBJEKT (názov / skratka)	ROLA (vlastník procesu/ vlastník dát/zákazník/ užívateľ …. člen tímu atď.)	Informačný systém (MetaIS kód a názov ISVS)
1.	Zamestnanec DEUS	DEUS	Správca a prevádzkovateľ nadrezortného informačného systému verejnej správy, ktorý poskytuje samospráve technické a programové prostriedky na výkon verejnej moci elektronicky, na prevádzkovanie ISVS v ich správe	IS DCOM (isvs_6391)
2.	Úradník samosprávy	samosprava	Používateľ G2G elektronických služieb IS DCOM	IS DCOM (isvs_6391)
3.	Zakladatelia združenia DEUS	ZMOS /MF SR	Governance DEUS	N/A
4.	Ministerstvo investícií, regionálneho rozvoja a informatizácie SR	MIRRI SR	Posudzovateľ projektu/ ÚOŠS pre Informačné systémy verejnej správy v oblasti kybernetickej bezpečnosti	N/A
5.	Národný bezpečnostný úrad	NBÚ	Riadi a koordinuje výkon štátnej správy v oblasti kybernetickej bezpečnosti.	N/A

6.	Občania/Podnikatelia	Verejnosť	Používateľ G2C a G2B elektronických služieb IS DCOM	IS DCOM (isvs_6391)
7.	Externí dodávatelia	ED	Dodávatelia	N/A

3.4 Ciele projektu

ID Názov cieľa	Názov strategického cieľa	Spôsob realizácie strategického cieľa
01 Zvýšenie a zlepšenie úrovne kybernetickej a informačnej bezpečnosti v prostredí samosprávy	Národná stratégia Kybernetickej bezpečnosti na roky 2021 – 2025: 4.1 Dôveryhodný štát pripravený na hrozby 4.4 Kybernetická bezpečnosť ako základná súčasť verejnej správy	- zavedením funkčných procesov riadenia rizík kybernetickej bezpečnosti, - kontinuálne posilňovaním technických, organizačných a personálnych kapacít pre detekciu a riešenie kybernetických bezpečnostných incidentov na národnej úrovni a v rámci jednotlivých sektorov, vrátane kritickej infraštruktúry, - rozvojom schopností v oblasti detekcie a zberu bezpečnostne relevantných udalostí v národnom kybernetickom priestore, ako aj rozvoj schopností v oblasti vyhodnocovania udalostí a detekcie incidentov modernými technikami v národnom kybernetickom priestore - uplatňovaním systematického prístupu ku kybernetickej bezpečnosti založeného na analýze a riadení rizík v každej dôležitej oblasti, pričom každá analýza musí vychádzať z plánu a metodiky jednotnej analýzy a riadenia rizík, - zvýšením ochrany prevádzkovateľov základných služieb vo verejnej správe z hľadiska kybernetickej bezpečnosti tak, aby ich audit a pravidelné kontroly vykonávaných opatrení trvalo preukazovali pozitívny trend zlepšovania stavu kybernetickej bezpečnosti vo verejnej správe, - poskytovaním bezpečných a dostupných elektronických služieb štátu každému občanovi s umožnením plnohodnotného rovného využitia elektronických nástrojov.

3.5 Merateľné ukazovatele (KPI)

ID ID/Názov cieľa	Názov ukazovateľa (KPI)	Popis ukazovateľa	Merná jednotka	AS IS merateľné hodnoty (aktuálne)	TO BE Merateľné hodnoty (cieľové hodnoty)	Spôsob ich merania	Pozn.
1. RSO1.2 Využívanie prínosov digitalizácie pre občanov, podniky, výskumné organizácie a orgány verejnej správy	Počet podporených obcí - Menej rozvinutý región (mimo BSK)	Zvýšenie bezpečnostného štandardu v oblasti kybernetickej a informačnej bezpečnosti pre obce do 6.000 obyvateľov v podobe procesného, technického, hardvérového vybavenia, aplikácií, SW - Menej rozvinutý región (mimo BSK)	Počet (ks)	0	990	Údaje DEUS /MS projektu	...
2. RSO1.2 Využívanie prínosov digitalizácie pre občanov, podniky, výskumné organizácie a orgány verejnej správy	Počet podporených obcí - Menej rozvinutý región (mimo BSK)	Zvýšenie bezpečnostného štandardu v oblasti kybernetickej a informačnej bezpečnosti pre obce do 6.000 obyvateľov v podobe procesného, technického, hardvérového vybavenia, aplikácií, SW - Menej rozvinutý región (mimo BSK)	Počet (ks)	0	10	Údaje DEUS /MS projektu	...
3. RSO1.2 Využívanie prínosov digitalizácie pre občanov, podniky, výskumné organizácie a orgány verejnej správy	Počet implementovaných centrálnych HW riešení pre zabezpečenie KIB	Implementácia riešenia centrálnych HW komponentov kybernetickej a informačnej bezpečnosti pre informačný systém DCOM	Počet (ks)	0	1	Údaje DEUS /MS projektu	...

4.	RSO1.2 Využívanie prínosov digitalizácie pre občanov, podniky, výskumné organizácie a orgány verejnej správy	Počet implementovaných centrálnych EDR systémov	Implementácia softvérového riešenia vrátane dohľadu pre oblasť endpoint detection and response vrátane inštalácie na koncové zariadenia spravované DEUSom	Počet (ks)	0	1	Údaje DEUS /MS projektu	
5.	RSO1.2 Využívanie prínosov digitalizácie pre občanov, podniky, výskumné organizácie a orgány verejnej správy	Verejné inštitúcie podporované v rozvoji kybernetických služieb, produktov a procesov (viac rozvinuté)	Počet verejných inštitúcií, ktoré sú podporované za účelom rozvoja a modernizácie kybernetických služieb, produktov, procesov a zvyšovania vedomostnej úrovne napríklad v kontexte opatrení smerujúcich k elektronickej bezpečnosti verejnej správy. Medzi verejné inštitúcie patria orgány štátnej správy, miestne orgány verejnej správy, orgány na nižšej ako celoštátnej úrovni alebo iné typy subjektov verejnej správy.	počet	0	10	Údaje DEUS /MS projektu	
6.	RSO1.2 Využívanie prínosov digitalizácie pre občanov, podniky, výskumné organizácie a orgány verejnej správy	Verejné inštitúcie podporované v rozvoji kybernetických služieb, produktov a procesov (viac rozvinuté)	Počet verejných inštitúcií, ktoré sú podporované za účelom rozvoja a modernizácie kybernetických služieb, produktov, procesov a zvyšovania vedomostnej úrovne napríklad v kontexte opatrení smerujúcich k elektronickej bezpečnosti verejnej správy. Medzi verejné inštitúcie patria orgány štátnej správy, miestne orgány verejnej správy, orgány na nižšej ako celoštátnej úrovni alebo iné typy subjektov verejnej správy.	počet	0	990	Údaje DEUS /MS projektu	

3.6 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. Pre koncového používateľa je nevyhnutné zabezpečiť bezpečné a dostupné riešenie eSlužieb MÚS. Projekt zabezpečuje implementáciu technickej/bezpečnostnej infraštruktúry bez dopadu na biznisovú a aplikačnú časť systému, preto žiadne nové potreby koncového používateľa nedefinuje.

3.7 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	Nedostatočné vyhodnotenie kvality	Neodhalenie slabých miest v jednotlivých fázach implementácie projektu.
11	Nesúčinnosť a nespoľahlivosť dodávateľa	Predčasné ukončenie projektu, alebo predĺženie doby realizácie projektu.
12	Nedostatok ľudských zdrojov	Predĺženie doby realizácie projektu. Výstupy projektu budú dodané v nedostatočnej kvalite.

Zoznam rizík a závislostí tvorí Prílohu č. 1 tohto dokumentu.

3.8 Stanovenie alternatív v biznisovej vrstve architektúry

Nakoľko sa jedná o projekt, v rámci ktorého nedochádza k budovaniu ani rozvoju ISVS, alternatívy neboli stanovené “štandardne” podľa biznisovej vrstvy architektúry ale porovnávali sme 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 komplexne.

1. **Zachovanie súčasného stavu bez realizácie projektu** - stav zostane nezmenený (v kritickom režime), kedy prípadný kybernetický/bezpečnostný incidentu môže viesť k nedostupnosti časti alebo celého riešenia.

1. **Realizácia Kybernetická bezpečnosť pre samosprávy SR do 6000 obyvateľov realizovaná prostredníctvom správcu informačného systému DCOM –** realizáciou projektu sa zabezpečí zvýšenie úrovne kybernetickej a informačnej bezpečnosti IS DCOM a obcí do 6000 obyvateľov, zároveň sa zvýši spoľahlivosť systému a zabezpečí podpora jednotlivých komponentov, prostredníctvom zabezpečenia efektívneho obstarania, inštalácie a ďalšej prevádzky zo strany DEUS, ktorý v zmysle § 9a odsek 1 zákona č. 305/2013 Z.z. o elektronickej podobe výkonu pôsobností orgánov verejnej moci (eGovernmente) vykonáva činnosti správcu a prevádzkovateľa IS DCOM.

1. **Kybernetická bezpečnosť realizovaná obcami samostatne -** alternatíva predstavuje zabezpečenia kybernetickej bezpečnosti zo strany samotných obcí. Samotné zabezpečenie súladu s legislatívnymi požiadavkami KB kategórie I. podľa zákona č. 69/2018 Z.z. naprieč všetkými používanými informačnými systémami a internými procesmi by bolo výlučne na pleciach príslušnej obce bez centrálnej podpory. Zároveň zvýšenie úrovne KIB IS DCOM by bolo taktiež realizované len čiastočne.

3.9 Multikriteriálna analýza

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

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

	KRITÉRIUM	ZDÔVODNENIE KRIÉRIA	Verejnosť	OBCE/ZMOS	DEUS	MFSR	MIRRI/NBÚ
STANOVENÉ ALTERNATÍVY	Kritérium A (KO) Zabezpečiť infraštruktúru ochrany dát obce v dátovom centre	Integrovaný informačný systém DCOM predstavuje kľúčový prostriedok pre elektronickú komunikáciu medzi obcami a mestami a ich obyvateľmi. Pre dosiahnutie optimálnej ochrany dát je nevyhnutné mať dostatočne robustnú a spoľahlivú infraštruktúru. Bez bezpečnostnej infraštruktúry by mohlo dôjsť k nedostatočnej dostupnosti systému, bezpečnostným incidentom, úniku dát alebo výpadkom, čo by závažne ovplyvnilo možnosť občanov a iných subjektov využívať elektronické služby a komunikovať s verejnými orgánmi. Zabezpečením potrebnej infraštruktúry pre IS DCOM sa teda zaisťuje neodlúčiteľný základ pre bezpečnú elektronickú komunikáciu v rámci samosprávy.		X	X		

	Kritérium B (KO) Zníženie rizika kybernetických útokov v rámci samosprávy.	Zabezpečenie dostatočných bezpečnostných opatrení a mechanizmov je nevyhnutné na minimalizovanie rizika kybernetických útokov, ktoré by mohli ohroziť nielen integritu údajov, ale aj dôveru verejnosti v správu a ochranu ich informácií. Implementácia potrebných bezpečnostných opatrení sa stáva kľúčovou súčasťou posilňovania odolnosti informačných systémov samosprávy voči kybernetickým hrozbám.	X	X	X	X	X
	Kritérium C (KO) Zabezpečiť súlad s nariadením NIS2, resp. zákonom č. 69 /2018 Z.z.	Citlivé údaje občanov a subjektov verejnej správy vyžadujú osobitnú ochranu, aby sa predišlo neoprávnenému prístupu, manipulácii alebo úniku údajov. Implementácia príslušných bezpečnostných opatrení a postupov je preto nevyhnutná na zabezpečenie integrity a dôvernosti údajov a na splnenie štandardov ochrany osobných údajov.	X	X	X	X	X
	Kritérium D (KO) Efektívne vynakladanie zdrojov	Efektívne hospodárenie so zdrojmi je kľúčové pre každú organizáciu, vrátane samosprávy. Investície do informačných technológií a bezpečnostných opatrení by mali byť usmerňované tak, aby prinášali maximálny prínos pri súčasnom minimalizovaní nákladov. Efektívnym vynakladaním finančných prostriedkov na implementáciu infraštruktúry a bezpečnostných opatrení sa dosahuje optimálny pomer medzi nákladmi a prínosmi.	X	X	X	X	X

Na základe stanovených kritérií boli vyhodnotené stanovené alternatívy. Sumár vyhodnotenia je uvedený v nasledujúcej tabuľke:

Zoznam kritérií	Alternatíva 1	Spôsob dosiahnutia	Alternatíva 2	Spôsob dosiahnutia	Alternatíva 3	Spôsob dosiahnutia
Kritérium A	nie	alternatíva 1 je zachovanie statusu quo bez realizácie projektu	áno	Implementáciou alternatívy 2 sa zabezpečí infraštruktúra pre správne fungovanie IS DCOM v rámci samosprávy.	nie	Implementáciou alternatívy 3 sa nezabezpečí infraštruktúra pre správne fungovanie IS DCOM v rámci samosprávy.
Kritérium B	nie	alternatíva 1 je zachovanie statusu quo bez realizácie projektu	áno	Realizáciou alternatívy 2 sa zníži riziko kybernetických útokov v rámci samosprávy.	áno	Realizáciou alternatívy 3 sa zníži riziko kybernetických útokov v rámci samosprávy.
Kritérium C	nie	alternatíva 1 je zachovanie statusu quo bez realizácie projektu	áno	Realizáciou alternatívy 2 sa sa zabezpečí naplnenie všetkých bezpečnostných požiadaviek	nie	Realizáciou alternatívy 3 sa nezabezpečí naplnenie všetkých bezpečnostných požiadaviek.
Kritérium D	nie	alternatíva 1 je zachovanie statusu quo bez realizácie projektu	áno	Realizáciou alternatívy 2 sa zabezpečí efektívne vynakladanie zdrojov	nie	Realizáciou alternatívy 3 sa nezabezpečí efektívne vynakladanie zdrojov.

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

3.10 Stanovenie alternatív v aplikačnej vrstve architektúry

Alternatívy na základe aplikačnej vrstvy architektúry neboli posudzované nakoľko nedochádza k zmene na úrovni aplikačnej vrstvy architektúry.

3.11 Stanovenie alternatív v technologickej vrstve architektúry

Výber alternatívy na úrovni technologickej a bezpečnostnej vrstvy architektúry kopíruje výber alternatívy č. 2 na základe MCA. Náklady na údržbu a prevádzku projektu sú uvedené v CBA analýze ako percentuálny pomer z obstarávacej ceny diela.

4. POŽADOVANÉ VÝSTUPY (PRODUKT PROJEKTU)

Predmetom projektu nie je vývoj softvérového diela. Na dodržanie štandardov sa použije M-04 Audit kvality zameraný na výstupy z iniciačnej, realizačnej a dokončovacej fázy projektu. Realizácia projektu bude pozostávať z uvedených etáp:

- Analýza a dizajn

- Nákup technických prostriedkov, programových prostriedkov a služieb
- Implementácia a testovanie,

DEUS bude pri implementácii postupovať v zmysle vyhlášky 401/2023 Z.z.

4.1 Zabezpečenie kybernetickej bezpečnosti pre centrálne prvky IS DCOM

1. HW vybavenie pre kybernetickú bezpečnosť

- Fyzické servery pre potreby bezpečnostného monitoringu 4ks iba pre primárne DC pre prevádzkovanie virtuálnych core FW, web aplikačných FW a ostatných SW nástrojov pre zabezpečenie kybernetickej bezpečnosti uvedených v kapitole 2 tohto dokumentu.

2. SW vybavenie pre kybernetickú bezpečnosť pre dátové centrá

- Core Firewally – 4 licencie
- Web Applications Firewally 4 virtuálne licencie
- EDR - Endpoint Detection and Response
- DNS firewall
- PAM - systém riadenia privilegovaných prístupov
- NDR – Network Detection and Response
- Antivírus pre centrálne virtuálne servery
- Vulnerability management
- Security Policy Automation
- Automatické penetračné testovanie - Nástroj na spúšťanie automatických penetračných testov nad centrálnou infraštruktúrou a nad koncovými zariadeniami
- Nástroj na riadenie rizík spojených s otvoreným zdrojovým kódom (OSS)

HW a SW vybavenie je bližšie popísané v prílohe Projektového zámeru – opise predmetu zákazky

3. Realizovaný audit kybernetickej bezpečnosti v súlade so zákonom o KB pre IS DCOM

4.2 Zabezpečenie kybernetickej bezpečnosti výkonom aktivít priamo na obciach

Výstupy projektu, ktoré sa týkajú aktivít kybernetickej bezpečnosti na obci do 6000 obyvateľov:

a) Migrácia do IS DCOM

- Migrácia SW súvisiacich s vnútornými agendami obce/mesta (účtovníctvo, mzdy a rozpočty, atď.)
- Migrácia údajov súvisiacich so službami samosprávy poskytovanými verejnosti
- Asistencia pre obec/mesto po spustení do produkčnej prevádzky
- Školenie nových používateľov IS DCOM
- Zabezpečenie služieb ÚPVS pre obce
- Inštalácia a konfigurácia backup systému obce

b) Organizácia kybernetickej a informačnej bezpečnosti

- Vypracovanie alebo aktualizácia bezpečnostnej dokumentácie vrátane rozsahu a spôsobu plnenia všeobecných bezpečnostných opatrení;
- vypracovanie a implementácia špecifických interných riadiacich aktov pre vybrané oblasti kybernetickej a informačnej bezpečnosti;

c) Riadenie rizík

- Identifikácia všetkých aktív súvisiacich so zariadeniami na spracovanie informácií a centrálne zaznamenávanie inventáru týchto aktív podľa ich hodnoty vrátane určenia ich vlastníka, ktorý definuje požiadavky na ich dôvernosť, dostupnosť a integritu;
- riadenie rizík pozostávajúce z identifikácie zraniteľností, identifikácie hrozieb, identifikácie a analýzy rizík s ohľadom na aktívum, určenie vlastníka rizika, implementácie organizačných a technických bezpečnostných opatrení, analýzy funkčného dopadu a pravidelného preskúmavania identifikovaných rizík v závislosti od aktualizácie prijatých bezpečnostných opatrení;

- vypracovanie a implementácia interného riadiaceho aktu riadenia rizík kybernetickej a informačnej bezpečnosti.

d) Personálna bezpečnosť

- Vypracovanie postupov pri zaradení osoby do niektorých z bezpečnostných rolí, zavedenie plánu rozvoja bezpečnostného povedomia a vzdelávania, vypracovanie spôsobov hodnotenia účinnosti plánu rozvoja bezpečnostného povedomia, určenie pravidiel a postupov na riešenie prípadov porušenia bezpečnostnej politiky, zavedenie postupov pri skončení pracovnoprávneho vzťahu alebo iného obdobného vzťahu, zavedenie postupov pri porušení bezpečnostných politík;
- vypracovanie alebo aktualizácia interného riadiaceho aktu s bezpečnostnými zásadami pre koncových používateľov;
- vypracovanie a implementácia postupov a procesov upravujúcich personálnu bezpečnosť organizácie prostredníctvom interného riadiaceho aktu.

e) Riadenie prístupov

- Vypracovanie a implementácia zásad riadenia prístupov osôb k sieti a informačnému systému;
- vypracovanie a implementácia postupov a procesov upravujúcich riadenie prístupov organizácie.

f) Riadenie kybernetickej a informačnej bezpečnosti vo vzťahoch s tretími stranami

- Vypracovanie analýzy rizík tretích strán a celého dodávateľského reťazca, vrátane analýzy politických rizík;
- analýza a posúdenie súladu všetkých aktuálnych zmlúv s tretími stranami so zákonom o KB a dobrou praxou;
- vypracovanie návrhov dodatkov zmlúv s treťou stranou spolu s návrhom potrebných úprav na zabezpečenie súladu so zákonom KB;
- vypracovanie a implementácia interného riadiaceho aktu upravujúceho zásady kybernetickej a informačnej bezpečnosti vo vzťahoch s tretími stranami.

g) Bezpečnosť pri prevádzke informačných systémov a sietí

- obstaranie služieb pre potreby správy prevádzkovej zálohy, kópie archivačnej zálohy a kópie inštalačných médií, vrátane určenia spôsobu ich ukladania

h) Hodnotenie zraniteľností a bezpečnostné aktualizácie

- vypracovanie a implementácia interného riadiaceho aktu upravujúceho proces riadenia implementácie bezpečnostných aktualizácií a záplat;

i) Ochrana proti škodlivému kódu

- Vypracovanie interného riadiaceho aktu s požiadavkami na určenie zodpovednosti používateľov, pravidiel pre inštaláciu a monitorovania potenciálnych ciest prieniku škodlivého kódu;
- vypracovanie a implementácia pravidiel súvisiace s ochranou proti škodlivému kódu;

j) Sieťová a komunikačná bezpečnosť

- Implementácia nástrojov na ochranu integrity sietí, ktoré zabezpečujú riadenie bezpečného prístupu medzi vonkajšími a vnútornými sieťami, implementácia segmentácie sietí, implementácia alebo obnova firewall-u, revízia firewall pravidiel;
- vytvorenie alebo aktualizácia dokumentácie počítačovej siete, ktorá obsahuje evidenciu všetkých miest prepojenia sietí vrátane prepojení s externými sieťami, topológiu siete a využitie IP rozsahov;
- vypracovanie a implementácia interného riadiaceho aktu upravujúceho pravidlá sieťovej a komunikačnej bezpečnosti;

k) Riešenie kybernetických bezpečnostných incidentov

- Vypracovanie štandardov a postupov riešenia kybernetických bezpečnostných incidentov, vrátane definovania zodpovedností zamestnancov a ďalších povinností;
- vypracovanie plánov a spôsobov riešenia kybernetických bezpečnostných incidentov.

l) Kontinuita prevádzky

- Vypracovanie stratégie a krízových plánov prevádzky na základe analýzy vplyvov kybernetického bezpečnostného incidentu na základnú službu;
- vypracovanie interného riadiaceho aktu obsahujúceho a upravujúceho kontinuitu prevádzky následkom kybernetického bezpečnostného incidentu alebo inej krízovej situácie;
- implementácia systému zálohovania.

m) Samohodnotenie súladu opatrení obce s požiadavkami kybernetickej bezpečnosti

- Podpora pre obce pri vypracovaní prvého samohodnotenia obce

5. NÁHĽAD ARCHITEKTÚRY

Biznis architektúra

Z pohľadu biznis procesov územná samospráva realizuje výkon vybraných procesov štátnej správy (tzv. prenesený výkon štátnej správy) a zodpovedá za metodické riadenie a výkon procesov samosprávy (tzv. originálne kompetencie). Ďalej z hľadiska originálnych kompetencií, obec pri výkone samosprávy najmä:

- vykonáva úkony súvisiace s riadnym hospodárením s hnuteľným a nehnuteľným majetkom obce a s majetkom vo vlastníctve štátu prenechaným obci do užívania,
- zostavuje a schvaľuje rozpočet obce a záverečný účet obce; vyhlasuje dobrovoľnú zbierku,
- rozhoduje vo veciach miestnych daní a miestnych poplatkov a vykonáva ich správu,
- usmerňuje ekonomickú činnosť v obci, a ak tak ustanovuje osobitný predpis, vydáva súhlas, záväzné stanovisko, stanovisko alebo vyjadrenie k podnikateľskej a inej činnosti právnických osôb a fyzických osôb a k umiestneniu prevádzky na území obce, vydáva záväzné stanoviská k investičnej činnosti v obci,
- utvára účinný systém kontroly a vytvára vhodné organizačné, finančné, personálne a materiálne podmienky na jeho nezávislý výkon,
- zabezpečuje výstavbu a údržbu a vykonáva správu miestnych komunikácií, verejných priestranstiev, obecného cintorína, kultúrnych, športových a ďalších obecných zariadení, kultúrnych pamiatok, pamiatkových území a pamätihodností obce,
- zabezpečuje verejnoprospešné služby, najmä nakladanie s komunálnym odpadom a drobným stavebným odpadom, udržiavanie čistoty v obci, správu a údržbu verejnej zelene a verejného osvetlenia, zásobovanie vodou, odvádzanie odpadových vôd, nakladanie s odpadovými vodami zo žúmp a miestnu verejnú dopravu,
- utvára a chráni zdravé podmienky a zdravý spôsob života a práce obyvateľov obce, chráni životné prostredie, ako aj utvára podmienky na zabezpečovanie zdravotnej starostlivosti, na vzdelávanie, kultúru, osvetovú činnosť, záujmovú umeleckú činnosť, telesnú kultúru a šport,
- plní úlohy na úseku ochrany spotrebiteľa a utvára podmienky na zásobovanie obce; spravuje trhoviská,
- obstaráva a schvaľuje územnoplánovaciu dokumentáciu obcí a zón, koncepciu rozvoja jednotlivých oblastí života obce,
- obstaráva a schvaľuje programy rozvoja bývania a spolupôsobí pri utváraní vhodných podmienok na bývanie v obci,
- vykonáva vlastnú investičnú činnosť a podnikateľskú činnosť v záujme zabezpečenia potrieb obyvateľov obce a rozvoja obce,
- zakladá, zriaďuje, zrušuje a kontroluje podľa osobitných predpisov svoje rozpočtové a príspevkové organizácie, iné právnické osoby a zariadenia,
- organizuje miestne referendum o dôležitých otázkach života a rozvoja obce,
- zabezpečuje verejný poriadok v obci,
- zabezpečuje ochranu kultúrnych pamiatok v rozsahu podľa osobitných predpisov a dbá o zachovanie prírodných hodnôt,
- plní úlohy na úseku sociálnej pomoci v rozsahu podľa osobitného predpisu,
- vykonáva osvedčovanie listín a podpisov na listinách,
- vedie obecnú kroniku v štátnom jazyku, prípadne aj v jazyku národnostnej menšiny.

IS DCOM umožňuje občanom komunikovať s obcou elektronicky, prostredníctvom tzv. elektronickej schránky. Verejnosť má dispozícii elektronické komunikačné rozhranie v podobe webových stránok pre všetkých 139 poskytovaných elektronických služieb. Občania majú prostredníctvom webového portálu DCOM prístup k elektronických službám, vrátane súkromnej zóny s informáciami o aktuálnej a predchádzajúcej komunikácii s obcou, či mestom. Zamestnanci úradov majú k dispozícii plne integrované a navzájom prepojené riešenia pre spracovanie agendy. Obce majú zároveň možnosť prevádzkovať svoje webové stránky v prostredí dátového centra (DCOM). Pracovníci obcí, rovnako ako aj pracovníci technickej podpory majú prístup na samostatný intranetový portál.

Používateľov systému DCOM možno rozdeliť nasledovne:

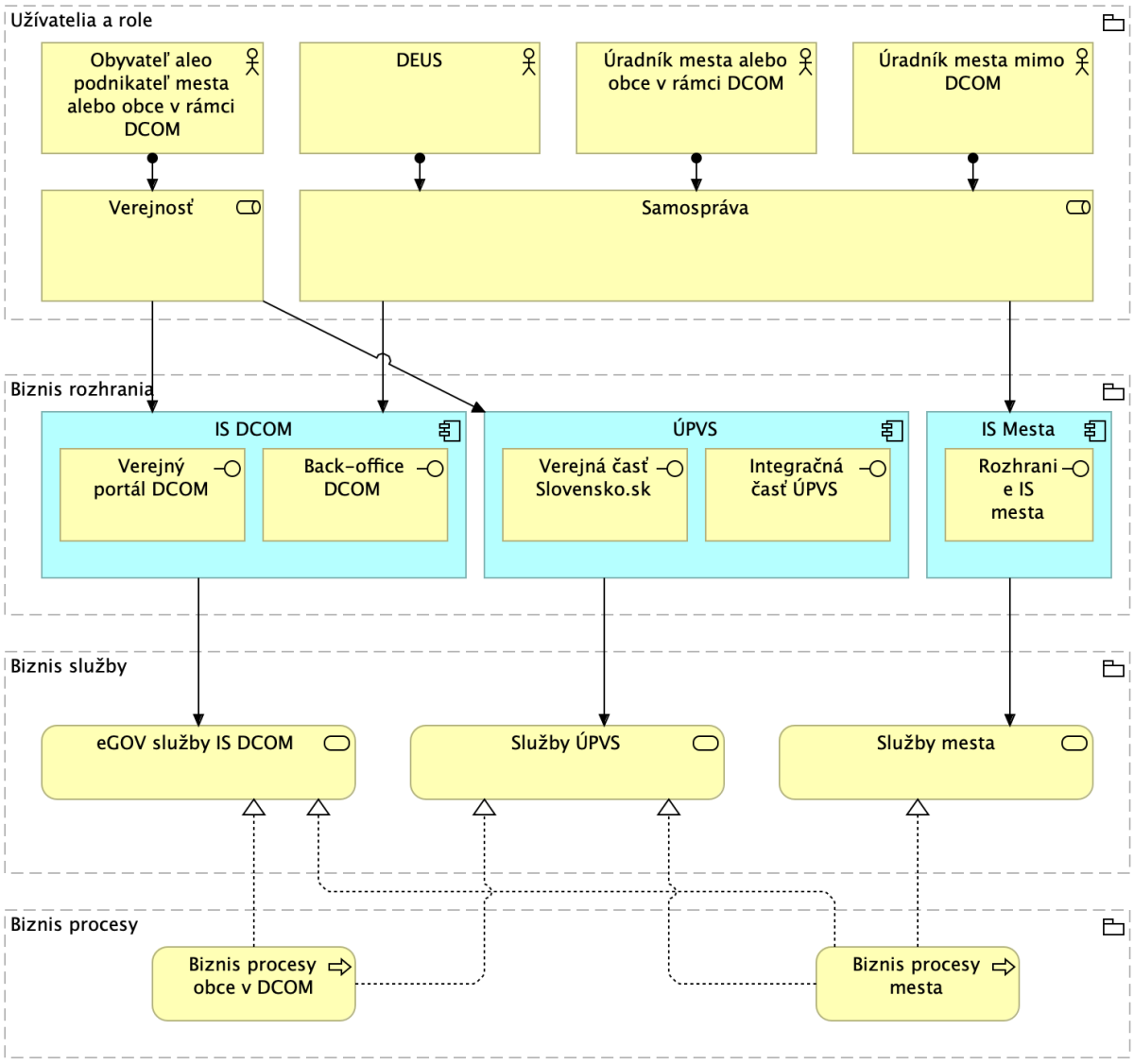
Externí používatelia – anonymná alebo autentifikovaná osoba, pristupujúca z externých verejných sietí a využívajúca služby portálu dcom.sk. Autentifikáciu externých používateľov zabezpečuje spoločný modul IAM ÚPVS.

- Obyvatelia (fyzické osoby)
- Podnikatelia

Interní používatelia – autentifikovaní používatelia pristupujúci z externých privátnych alebo verejných sietí do back-office DCOM. Používateľské účty, oprávnenia a autentifikačné prostriedky interných používateľov pre prístup k používateľským rozhraniam DCOM sú spravované v IAM DCOM.

- Reprezentant (úradník) obce alebo mesta - autentifikovaný zamestnanec obce alebo mesta, využívajúci služby IS DCOM
- Pracovník prevádzky - autentifikovaný zamestnanec DEUS, dodávateľa DEUS, dodávateľa ISM, poskytujúci podporu prevádzky DCOM.

Schéma biznis architektúry je nasledovná



Z pohľadu biznis architektúry nedôjde implementáciou projektu k zmenám v porovnaní AS IS a TO BE stavu.

Aplikačná architektúra

Z pohľadu súčasnej architektúry IS DCOM, tento poskytuje obciam a mestám potrebnú aplikačno-programovú podporu pri spracovaní jednotlivých agend samosprávy. Informačný systém DCOM zabezpečuje tiež prepojenie informačných systémov samospráv s inými Informačnými systémami verejnej správy (IS VS) a so základnými registrami. V rámci obce zapojenej do IS DCOM, Informačný systém obce (ISO) zabezpečuje funkcie vnútornej správy obce minimálne v súlade s rozsahom základných modulov ako sú účtovníctvo obce, finančný a rozpočtový systém, banka a pokladňa, personalistika a mzdy, registratúra, správa majetku obce a systém pre zastupiteľstvo, a IS DCOM zabezpečuje agendu súvisiacu s obsluhou verejnosti. Táto časť je prepojená na ÚPVS a zabezpečuje plnohodnotnú elektronickú komunikáciu. Prostredníctvom synchronizačnej vrstvy dátovej DCOM je riešenie prepojené s registrami verejnej správy.

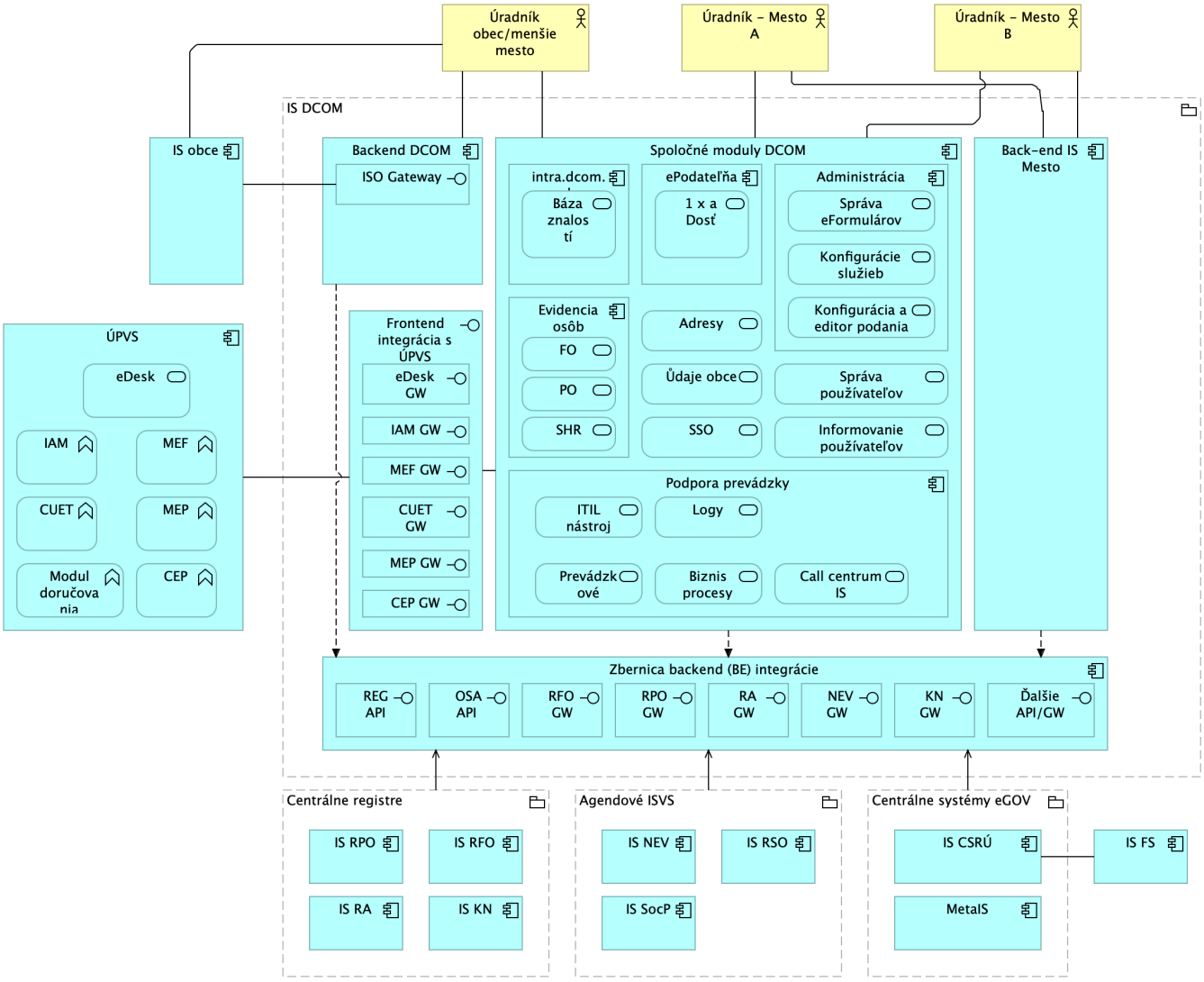
Architektúra riešenia DCOM vychádza z požiadaviek efektívneho prevádzkovania systémov a aplikácií obcí a miest, z požiadaviek vyššieho štandardu prevádzkovania aplikácií a z požiadavky flexibilného prispôsobovania potrebám budúcich aplikácií a modulom eGov. Riešenie IS DCOM možno rozdeliť do troch skupín – Front Office, Mid Office a Back Office. Informačný systém obce je časťou Back Office.

Front Office – prezentačná vrstva reprezentuje prezentačnú vrstvu, ktorá obsahuje interaktívne používateľské rozhrania aplikačných systémov pre používateľov IS DCOM. Front Office zabezpečuje interakciu IS DCOM s externými používateľmi, obsahuje interaktívne používateľské rozhranie pre občanov a podnikateľov a je integrovaný na ÚPVS. Prostredníctvom tejto vrstvy sú sprístupnené služby občanovi a referentovi obce v kompaktnej podobe. Je komponovaná s ohľadom na efektivitu jednotlivých konzumentov služieb a prostredníctvom silnej personalizačnej črty, kladie dôraz na rozdielny štýl práce jednotlivých rolí (občan / pracovník obce). Je adaptabilná pre používateľa a podľa kontextu vybavovanej agendy sa prispôsobuje a variuje od štýlu práce v koncepte portálu, cez koncept vybavenia služby, až po koncept práce v agendovom systéme.

Mid Office – procesno - integračná vrstva. Vrstva Mid Office je reprezentovaná procesno-integračnou vrstvou, prostredníctvom ktorej sa realizuje integračné a procesné riadenie. Komponenty BPM a Business Rules zastrešujú správu procesov a dennej agendy. Integračná platforma ESB zabezpečuje podpornú vrstvu pre integráciu systémov, orchestráciu služieb a manažment služieb podľa princípov SOA. Modul BAM zabezpečuje sledovanie a diagnostiku procesov, čo umožňuje následnú optimalizáciu.

Back Office – Aplikačná vrstva, ktorá zabezpečuje interakciu s internými používateľmi IS DCOM, úradníkmi obcí. Back Office predstavuje aplikačnú vrstvu tvorenú modulmi a komponentmi zabezpečujúcimi výkon elektronických služieb samosprávy prostredníctvom agendových systémov a podporných systémov. Obsahuje vrstvu integrácií na okolie IS DCOM, ako je napr. ISO, správu konsolidovanej dátovej vrstvy, správu cloudovej vrstvy a hardvérovej vrstvy. Súčasťou Back Office sú Informačné systémy obcí. Projekt DCOM poskytuje cloud platformu na prevádzku ISO modulov. Podporné moduly zastrešujú procesy podpory a prevádzky IS DCOM. Podporné moduly sú integrované do riešenia prostredníctvom integračnej vrstvy formou poskytovaných a konzumovaných služieb.

Schéma aplikačná architektúra:



Z pohľadu aplikačnej architektúry nedôjde implementáciou projektu k zmenám v porovnaní AS IS a TO BE stavu.

Technologická architektúra

Z pohľadu technologickej architektúry IS DCOM, základom riešenia je cloud infraštruktúra založená na princípoch ako sú redundancia lokality, redundancia funkčnosti, oddelenie sietí, obnoviteľnosť funkčnosti, modulárna infraštruktúra a štandardov pre dátové centrá a cloud infraštruktúru. Infraštruktúra pre prevádzku cloudu a aplikácií je vybudovaná ako vysoko dostupná, prevádzkovaná v dvoch nezávislých lokalitách a v prípade výpadku primárnej lokality je poskytujúca aplikácie z druhej, záložnej lokality, bez závislosti na dostupnosti komponentov a funkcií primárnej lokality. Cloud platforma umožňuje poskytovať služby IaaS (infraštruktúra ako služba) pre prevádzku ISO balíkov pre interné agendy obcí. Prístup používateľov (pracovníkov obcí a správcov ISO) k službám je štandardný, je definovaný spôsob, akým sú služby DCOM publikované pre obce. Pracovníci obcí pristupujú predovšetkým z koncových zariadení (PC alebo notebooky) dodaných v rámci projektu DCOM alternatívne cez privátnu komunikačnú sieť budovanú DataCentrom v rámci projektu FINNET, alebo cez internet.

Koncové zariadenia obsahujú operačný systém s potrebným softvérovým vybavením konfigurovaný, aktualizovaný a spravovaný centrálnym systémom. Z týchto pracovných staníc DCOM je možný aj alternatívny prístup cez sieť internet prostredníctvom zabezpečeného komunikačného kanálu. Tento stav sa v priebehu projektu a udržateľnosti môže zmeniť. Nesmie tým však utrpieť úroveň bezpečnosti samotného IS DCOM. Z dlhodobého pohľadu smeruje architektúra IS DCOM k riešeniu, kde nebude potrebné využívať zabezpečený kanál formou VPN, ale bezpečnosť bude riešená na úrovni ako infraštruktúry tak aj aplikácie tak, aby bolo aplikáciu možné používať ako úplne samostatnú SaaS službu so svojimi vlastnými bezpečnostnými riešeniami. Týmto postupom sa dlhodobo zruší závisloť na prevádzkovaní HW DEUSom a implementuje sa prístup “internetového bankovníctva“, teda dostupnosti riešenia z akéhokoľvek počítača pri zachovaní požadovanej bezpečnosti.

Súčasťou projektu je tiež doplnenie jednotlivých produktových položiek pre potreby rozšírenia Bezpečnostnej vrstvy. Položky sú vylistované v zozname uvedenom v dokumente BC/CBA na karte HW a licencie. Doplnením jednotlivých položiek nedochádza k zmene architektúry technologickej vrstvy.

Bezpečnostná architektúra

Návrh riešenia bezpečnostnej architektúry reflektuje cieľ projektu vytvoriť prostredie na národnej úrovni v ktorom bude možné čo najefektívnejšie zvyšovať úroveň kybernetickej bezpečnosti pre samosprávy SR a občanov SR využívajúcich elektronické služby samospráv. Predmetom projektu je implementácia riešenia ktoré zabezpečí dodržanie minimálnej požadovanej bezpečnostnej úrovne. Projekt kybernetickej bezpečnosti pre samosprávy do 6000 obyvateľov bude realizovaný v dvoch častiach:

I. Infraštruktúra ochrany dát obce v dátovom centre

IIa. Zvýšenie kybernetickej bezpečnosti obcí v súčasnosti nezapojených do IS DCOM do 6000 obyvateľov

IIb. Zvýšenie kybernetickej bezpečnosti obcí zapojených do IS DCOM do 6000 obyvateľov

I. Infraštruktúra ochrany dát obce v dátovom centre

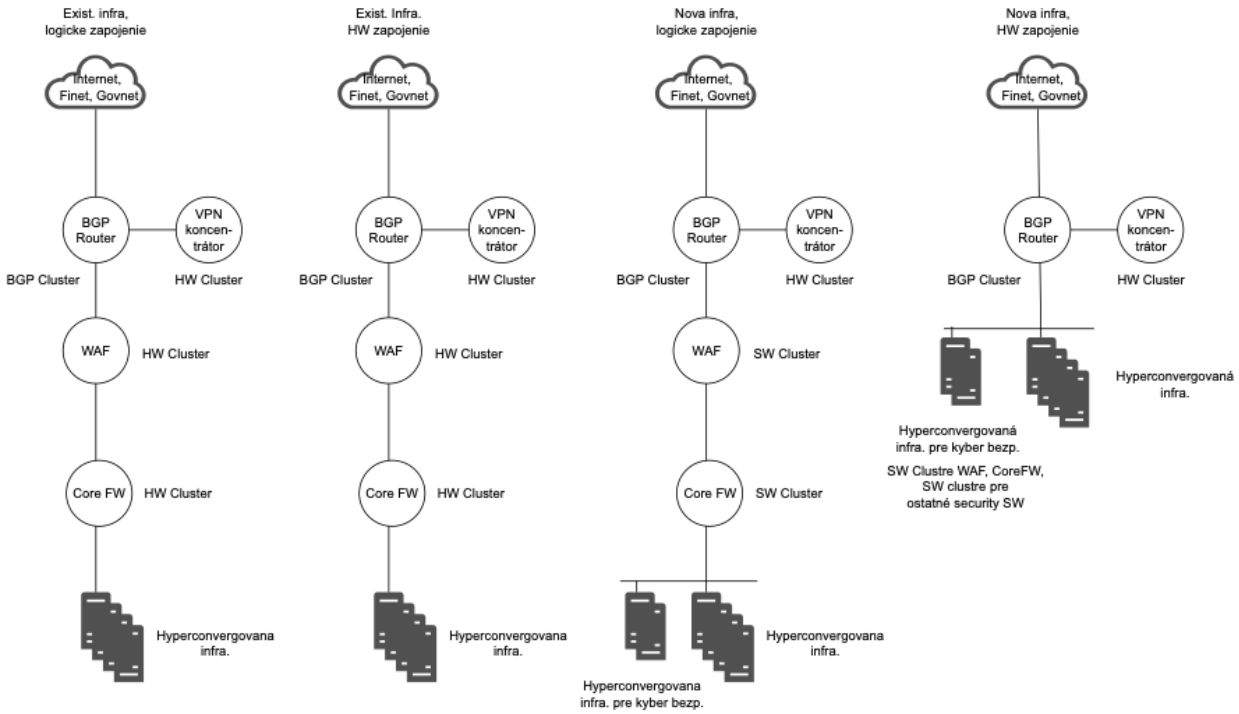
Táto časť projektu si dáva za cieľ poskytnúť maximálnu ochranu perimetru IS DCOM a zabezpečiť tak maximálnu ochranu procesov a najmä dát občanov všetkých obcí, ktoré v danom čase využívajú kompletné riešenie IS DCOM.

Návrh riešenia:

- Konzultačné práce pre podrobnú analýzu nutných požiadaviek na kybernetickú bezpečnosť systému DCOM, najmä vzhľadom k požiadavkám vyplývajúcim z novej smernice EU NIS2
- Nákup HW vybavenia pre zabezpečenie nutných požiadaviek KB vyplývajúcich z analýzy
- Nákup SW produktov pre zabezpečenie nutných požiadaviek KB vyplývajúcich z analýzy
- Implementačné práce spojené s realizáciou vyššie uvedených aktivít
- Posilnenie interného teamu bezpečnostného dohľadu pre zabezpečenie udržateľnosti riešenia a potrebné interné školenia

Výstupom časti projektu zvýšenie bezpečnosti IS DCOM bude dlhodobo udržateľný a kyberneticky bezpečný informačný systém DCOM.

Schéma navrhovanej bezpečnostnej architektúry:



Popis jednotlivých blokov bezpečnostnej architektúry a požiadaviek na jednotlivé technológie, ktoré budú obstarané:

HW

Iba 4ks výkonných serverov, ktoré sa zapoja do jedného clustra, na ktorom do budúcnosti budú bežať všetky bezpečnostné SW riešenia vrátane virtuálnych core firewallov, web aplikačných firewallov a všetkých ostatných SW aplikácií pre security. Tieto servery plánujeme nakúpiť iba do primárneho DC. V ostatných dvoch DC počítame, že security software nasadíme na serveroch poskytnutých ako IaaS.

SW

Core Firewally – 4 licencie

Web Applications Firewally 4 virtuálne licencie

Core aplikačné FW a WAF plánujeme nakúpiť ako virtuálne licencie pre primárne DC (Kopčianska) a pre záložné DC. To znamená, že počítame s jedným HA párom pre primár aj pre backup, teda z každej licencie po 4 kusy.

EDR - Endpoint Detection and Response

Riešenie EDR (Endpoint Detection and Response) zabezpečuje zber, koreláciu a analýzu údajov o udalostiach na endpointoch, vrátane upozornení a reakcií na bezprostredné hrozby.

DNS firewall

DNS rekurzívny resolver s bezpečnostnými funkcionalitami, ktoré zabezpečujú ochranu DNS prekladu. DNS firewall zabezpečuje ochranu voči cieleným phishingovým útokom (targeted phishing), poskytuje službu ochrany identít zamestnancov (identity protection) a alerting ich kompromitácie.

PAM - systém riadenia privilegovaných prístupov

Systém riadenia privilegovaných prístupov a vytvárania nahrávok a auditnej stopy. Riešenie umožní automatické prideľovanie oprávnení privilegovaných prístupov ku kritickým systémom, a riadi životný cyklus privilegovaných identity (vznik identity, priradenie práv, revízia práv a odňatie práv). Zároveň riešenie umožní riadiť a rotovať heslá k privilegovaným zdieľaným aj osobným účtom, aby spĺňalo požiadavky na komplexnosť a unikátnosť. Heslá si vie užívateľ vyzdvihnúť alebo sa vedia riešením priamo vložiť do relácie a užívateľ ich nemusí zadávať zo svojej pracovnej stanice.

Riešenie umožní pri citlivých reláciách alebo využitia nadštandardných oprávnení užívateľom schvaľovací workflow emailom na zodpovedných pracovníkov.

NDR – Network Detection and Response

Nástroj na analýzu sieťovej prevádzky a bezpečnostný monitoring v prostredí technologickej a klasickej siete, ktorý okamžite identifikuje bezpečnostné riziká. Jedná sa o systém zložený z HW/SW zariadení, ktorý monitoruje sieťovú aktivitu v reálnom čase a identifikuje potenciálne kybernetické hrozby, bezpečnostné riziká a anomálne správanie a vytvára o nich upozornenia v reálnom čase. NDR analyzuje sieť na základe zrkadlenej sieťovej prevádzky zo SPAN portov alebo TAPov a zároveň analyzuje obsah dátových paketov v reálnom čase a detekuje protokol alebo aplikáciu na základe obsahu prevádzky prostredníctvom DPI (Deep Packet Inspection). NDR analyzuje sieť na základe spracovania štatistických protokolov typu NetFlow, IPFIX, NetStream, Cisco NSEL a prípadne ďalších. Network Detection and Response umožňuje spracovanie a ukladanie sieťových tokov vo formáte, ktorý umožňujé analýzu sieťovej komunikácie na úrovni jednotlivých tokov, vrátane vyhľadania informácií o aplikačných transakciách a ich metadátach z L2 až L7, obsiahnutých v danom sieťovom toku, zároveň umožňuje analýzu aplikačných a systémových logov. NDR bude zbierať a analyzovať aplikačné a systémové logy vo formáte syslog z monitorovaných zariadení a identifikovať nebezpečné alebo potenciálne škodlivé aktivity.

Antivírus pre centrálne virtuálne servery

Všetky centrálne servery riešenia IS DCOM budú zabezpečené antivírusovým programom, ktorý zabezpečí ochranu centrálnych serverov IS DCOM v rozsahu:

- Ochrana pred ransomvérom
- Centrálna správa všetkých chránených serverov
- Prevencia Zero-day hrozieb
- Pokročilá kontrola pamäte
- Sandboxing podozrivých vzoriek
- Ochrana pred botnetmi
- Ochrana pred malvérom

Vulnerability management

Jedná sa o nástroj na automatické spúšťanie skenovania zraniteľností a získavanie údajov. Riešenie bude vykonávať automatizované testovanie zraniteľností zariadení a umožňovať testovanie dynamicky pridelených IP adries prostredníctvom služby DHCP. Taktiež bude monitorovať históriu týchto adries a podávať správy pomocou DNS alebo Host name. Konzola pre centrálnu správu a skener bude kompatibilná s operačnými systémami Windows a Linux. Riešenie bude podporovať hybridné nasadenie v rôznych prostrediach, ako sú fyzické, virtualizované a cloudové prostredia. Vulnerability management bude umožňovať automatickú aktualizáciu tagov v databáze aktív na základe dynamických označení. Taktiež bude podporovať automatické aktualizácie všetkých softvérových komponentov celej architektúry s najnovšími dostupnými verziami počas celého obdobia predplatného. Riešenie bude umožňovať centralizovanú správu všetkých nájdených aktívnych systémov a ich atribútov, vrátane verzií operačného systému, aplikácií, otvorených portov TCP a UDP a sieťových protokolov. taktiež bude zahŕňať definovanie statických a dynamických hierarchických tagov na filtrovanie aktív, testovanie a vykazovanie výsledkov.

Súčasťou vulnerability managementu bude podpora automatického zisťovania aktív s minimálnymi parametrami, ako sú IP adresy, MAC adresy a názvy hostiteľov, aby sa predišlo duplicite a zároveň bude podporovať centrálnu správu v geograficky rozptýlenom nasadení skenerov a podporovať prístup založený na rôznych rolách, vrátane vlastných rolí. Riešenie bude podporovať automatizáciu pracovných postupov, ako je plánovanie skenovania, upozornenia na udalosti a zraniteľnosti, ako aj generovanie a distribúcia správ. Plánované skenovanie bude podporovať opakované skenovanie v určitých časových intervaloch.

Súčasťou riešenia je podpora neinvazívnej aj invazívnej kontroly a umožnenie používateľom upraviť výkon skenovania a vykonávaných kontrol. Administratívne poverenia budú môcť byť použité na hĺbkové autentifikované skenovanie, ktoré kontroluje aktíva na širší rozsah zraniteľností alebo porušení bezpečnostných politík.

Riešenie bude označovať nebezpečné kontroly a umožní používateľom ich vypnúť na základe jednotlivých skenov. Bude podporovať overené skenovanie a integrovať sa so SIEM riešením a platformami na penetračné testovanie. Riešenia bude zabezpečovať identifikáciu a správu výnimiek zo zraniteľnosti a podporovať vytváranie používateľom definovaných zraniteľností a kontrol zraniteľnosti. Riešenie umožní používateľom definovať kritickosť aktív, ktoré sa musí zohľadniť v hodnotení rizík, a poskytne viacero modelov hodnotenia rizík vrátane vlastných modelov.

Vulnerability management bude podporovať integráciu s produktmi na analýzu topológie siete a rizík, virtuálnymi prostrediami a umožní stanoviť ciele nápravných opatrení na základe rôznych kritérií.

Security Policy Automation

Security Policy Automation je inovatívne riešenie navrhnuté na centralizovanú a modernú správu bezpečnostných politík na rôznych sieťových zariadeniach, vrátane firewall systémov. Toto riešenie poskytuje minimálne požiadavky, ktoré zahŕňajú dynamické mapovanie topológie siete v reálnom čase, segmentáciu politík, optimalizáciu a čistenie politík, monitorovanie a upozornenia v reálnom čase, riešenie problémov s pripojením a auditovanie súladu s predpismi. Navyše, riešenie umožňuje automatizovanú správu komplexných infraštruktúr, integráciu s rôznymi systémami tretích strán a poskytuje samoobslužný portál pre používateľov. Security Policy Automation je efektívny nástroj pre správu a zlepšenie kybernetickej bezpečnosti v komplexných sieťových prostrediach.

Automatické penetračné testovanie

Nástroj na spúšťanie automatických penetračných testov nad centrálnou infraštruktúrou a nad koncovými zariadeniami. Systém vie automaticky alebo manuálne vyberať vhodné exploity a nastavenia pre objavené hostiteľské počítače. Systém organizuje údaje pomocou back-endovej databázy a automaticky sleduje hostiteľov, dôkazy a informácie o tom, ako boli hostitelia kompromitovaní. Systém poskytuje rýchly a intuitívny spôsob automatizácie skupín úloh prostredníctvom funkcie nazývanej reťazenie úloh. Umožňuje používateľom automatizovať alebo plánovať úlohy, ako je napríklad exploitácia, bruteforcing. Systém bude umožňovať používateľom testovať 20000 počítačov súčasne a vytvoriť viac ako 500 relácií naraz. Ďalšie požiadavky na systém automatického penetračného testovania:

Nástroj na riadenie rizík spojených s otvoreným zdrojovým kódom (OSS)

Nástroj na efektívne riadenie rizík spojených s používaním otvoreného zdrojového softvéru, zabezpečenie súladu s licenčnými požiadavkami a zlepšenie celkovej bezpečnosti svojich softvérových produktov. Jedná sa o nástroj na správu softverových komponentov automaticky skenuje kód a identifikuje otvorené zdrojové komponenty, ich verzie a ich závislosti.

OSS identifikuje známe bezpečnostné zraniteľnosti v skenovaných otvorených zdrojových komponentoch. Umožňuje týmto spôsobom tímom rýchlo reagovať na potenciálne hrozby. Nástroj identifikuje licencie spojené s otvoreným zdrojovým kódom a pomáha organizáciám zabezpečiť, aby boli v súlade s licenčnými požiadavkami zároveň umožňuje organizáciám vytvárať a uplatňovať politiky týkajúce sa otvoreného zdrojového kódu a automaticky generovať upozornenia, keď sú tieto politiky porušené. Okrem povrchovej analýzy môže nástroj na správu softverových komponentov vykonať hĺbkové skenovanie kódu na zistenie skrytých závislostí.

Nástroj na správu softverových komponentov sa môže integrovať do existujúcich procesov kontinuálnej integrácie a kontinuálneho dodávania, umožňujúc automatické skenovanie počas vývoja a zároveň ponúka integráciu s mnohými ďalšími nástrojmi a platformami, vrátane nástrojov na správu zraniteľností, repozitárov kódu a platformami DevOps.

Nástroj na správu softverových komponentov umožňuje organizáciám sledovať a spravovať riziká spojené s otvoreným zdrojovým kódom prostredníctvom vizuálnych dashboardov.

II. Realizácia aktivít kybernetickej bezpečnosti na obci do 6000 obyvateľov

Zadefinovanie 3 základných segmentov obcí vzhľadom k ich špecifikám s ohľadom na rôzne IS, ktoré sú na obciach využívané:

1. Segment: DCOM obce využívajúce služby registratúry a účtovníctva firiem plne integrovaných s IS DCOM a prevádzkovaných na infraštruktúre DCOM *(najhlbšia integrácia)*;
2. Segment: DCOM obce využívajúce služby registratúry a účtovníctva partnerov, ktorí prevádzkujú vlastné IS lokálne, ale sú certifikovaní na prepojenie s IS DCOM;
3. Segment: DCOM obce bez certifikovaných partnerov, alebo bez identifikovaných prevádzkovateľov (typicky segment najmenších obcí, dáta sú ukladané v rôznych nástrojoch).

Pre samosprávu z pohľadu pripravovanej novely zákona o KB bude platiť delenie na obce a mestá.

1. KB obce : Vzťahujú sa na ňu minimálne bezpečnostné opatrenia Kategórie I. podľa zákona č. 69/2018 Z.z. a **obec je povinná absolvovať sebahodnotenie.**
2. KB mesta: Vzťahujú sa na neho minimálne bezpečnostné opatrenia Kategórie I. a je povinné absolvovať audit KB. (predmetom projektu nie je audit KB)

V rámci tejto časti budú realizované nasledovné aktivity kybernetickej bezpečnosti na obci do 6000 obyvateľov:

- Odladenie procesu implementácie aktivít na jednotlivých typoch obcí s cieľom potvrdenia ich užitočnosti a využitia na obciach,
- Automatizácia procesov, a výkon úloh tak, aby sa do projektu mohlo zapojiť maximum obcí so záujmom zabezpečenia vlastnej KB a súladu so zákonom o KB,
- Konzultačné práce na jednotlivých typoch obcí, pre zadefinovanie optimálnej sady opatrení KB pre každý jednotlivý typ obce,
- Vypracovanie štandardov pre rollout v spolupráci s MIRRI, pre využitie existujúcich podkladov, materiálov a vzorovej dokumentácie,
- Rollout na jednotlivé DCOM obce – kontrola procesov, aktualizácia dokumentácie, príprava na certifikáciu KB,

5.1 Prehľad e-Government komponentov

5.1.1 Prehľad koncových služieb – budúci stav:

Vzhľadom na charakter a rozsah projektu nebudú výsledkom projektu nové požiadavky na koncové služby.

5.1.2 Prehľad budovaných/rozvíjaných ISVS v projekte – budúci stav:

Vzhľadom na charakter a rozsah projektu nebudú budované ani rozvíjané informačné systémy ako také. Budú nepriamo rozvíjané implementáciou licenčných riešení s pozitívnym dopadom na úroveň kybernetickej bezpečnosti a prevádzku systémov poskytovateľa základnej služby.

5.1.3 Prehľad budovaných aplikačných služieb – budúci stav:

Vzhľadom na charakter a rozsah projektu nebudú budované aplikačné služby ako také. Počas realizácie projektu bude dopĺňaná hardvérová infraštruktúra poskytovateľa základnej služby ako aj doplnené licenčné proprietárne softvéry s pozitívnym dopadom na úroveň kybernetickej bezpečnosti a prevádzku systémov poskytovateľa základnej služby.

5.1.4 Prehľad integrácii ISVS na spoločné ISVS[1] a ISVS iných OVM alebo IS tretích strán

Vzhľadom na charakter a rozsah projektu nebudú výsledkom projektu nové požiadavky na integrácie na spoločné ISVS či ISVS iných OVM a tretích strán.

5.1.5 Aplikačné služby na integráciu

Vzhľadom na charakter a rozsah projektu nebudú výsledkom projektu nové požiadavky na budované aplikačné služby a ich využitie na integráciu na spoločné moduly a iné ISVS alebo ich poskytovanie na externú integráciu ani nie je plánované vybudovanie cloudových služieb “softvér ako služba“ (SaaS).

5.1.6 Poskytovanie údajov z ISVS do IS CSRÚ

Vzhľadom na charakter a rozsah projektu nebudú výsledkom projektu nové požiadavky na poskytovanie údajov do CSRÚ.

5.1.7 Konzumovanie údajov z IS CSRÚ

Vzhľadom na charakter a rozsah projektu nebudú výsledkom projektu nové požiadavky na konzumovanie údajov z CSRÚ.

5.1.8 Prehľad plánovaného využívania infraštruktúrnych služieb (cloudových služieb) – budúci stav:

Vzhľadom na charakter a rozsah projektu nebudú výsledkom projektu nové požiadavky na využívanie kapacít ktorejkoľvek časti vládneho cloudu.

6. LEGISLATÍVA

Projekt nemá žiadny legislatívny dopad. Nové riešenie musí byť v súlade s platnou legislatívou a to najmä:

- Zákon č. 95/2019 Z.z. o informačných technológiách vo verejnej správe Zákon č. 69/2018 Z.z. o kybernetickej bezpečnosti
- Zákon č. 45/2011 Z.z. o kritickej infraštruktúre
- Zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
- 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),
- Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov
- Vyhláška NBÚ č. 492/2022 Z. z. ktorou sa ustanovujú znalostné štandardy v oblasti kybernetickej bezpečnosti
- Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 78/2020 Z. z. o štandardoch pre informačné technológie verejnej správy
- Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 179/2020 Z. z., ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy
- Vyhláška Úradu na ochranu osobných údajov Slovenskej republiky č. 158/2018 Z. z. o postupe pri posudzovaní vplyvu na ochranu osobných údajov
- Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
- Zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.

7. ROZPOČET A PRÍNOSY

NÁKLADY

Sumarizácia nákladov:

Typ aktivity	Oblasť výdavku	Suma	OPEX / CAPEX	Int / ext	Suma	Zdroj finacovania - %				
						Suma %	Vlastné OPEX	Vlastné CAPEX	ESIF OPEX	ESIF CAPEX
Hlavné aktivity	Vývoj aplikácií	8 216 337 €	OPEX	Externé	- €					
			CAPEX	Externé	6 952 182 €	100%				100%
			OPEX	Interné	1 264 155 €	100%			100%	
	Nákup HW a SW	5 122 944 €	OPEX	Externé	- €					
			CAPEX	Externé	5 122 944 €	100%				100%
			OPEX	Interné	- €					
Prevádzka	Aplikácie	0 €	OPEX	Externé	- €					
			CAPEX	Externé	- €					
			OPEX	Interné	- €					
	HW a SW	1 939 920 €	OPEX	Externé	1 229 507 €	100%	100%			
			CAPEX	Externé	710 413 €	100%		100%		
			OPEX	Interné	- €					
Podporné aktivity	Projekový manažment	360 653 €	OPEX	Externé	0 €					
			OPEX	Interné	360 653 €	100%			100%	
	Publicita	573 097 €	OPEX	Externé	- €					
			OPEX	Interné	21 638 €	100%			100%	
	Ostatné výdavky		Ostatné zmiešané výdavky		551 459 €	100%			100%	
Výstupné náklady		0 €		Externé	- €					
				Interné	- €					
SPOLU		16 212 952 €		-	16 212 952 €					

Sumarizácia nákladov a prínosov riešenia za obdobie 10 rokov:

TO BE - AS IS (€, SUM)			Spolu	Externé služby (2FTE)	HW vybavenie pre kybernetickú bezpečnosť	PAM	NDR	Antivírus pre centrálne virtuálne servery	Security Policy Automation	Automatické penetračné testovanie	Riadenie rizík OSS	EDR	DNS Firewall	Vulnerability management	Dokumentácia KB pre samosprávu	Migrácia obce do IS DCOM
Náklady s DPH			**16 212 952 €**	**1 202 940 €**	**2 833 384 €**	**134 702 €**	**327 709 €**	**404 699 €**	**408 585 €**	**176 034 €**	**57 879 €**	**592 217 €**	**2 180 850 €**	**305 412 €**	**5 118 002 €**	**2 470 539 €**
	Všeobecný materiál		-€	-€	-€	-€	-€	-€	-€	-€	-€	-€	-€	-€	-€	-€
	IT - CAPEX		*12 785 540 €*	*951 268 €*	*2 162 889 €*	*107 762 €*	*262 167 €*	*323 759 €*	*326 868 €*	*140 827 €*	*46 303 €*	*473 773 €*	*1 744 680 €*	*244 330 €*	*4 047 245 €*	*1 953 668 €*
		Aplikácie	*6 952 182 €*	*951 268 €*	-€	-€	-€	-€	-€	-€	-€	-€	-€	-€	*4 047 245 €*	*1 953 668 €*
		SW	*3 670 469 €*	-€	-€	*107 762 €*	*262 167 €*	*323 759 €*	*326 868 €*	*140 827 €*	*46 303 €*	*473 773 €*	*1 744 680 €*	*244 330 €*	-€	-€
		HW	*2 162 889 €*	-€	*2 162 889 €*	-€	-€	-€	-€	-€	-€	-€	-€	-€	-€	-€
	IT - OPEX		*2 493 662 €*	*172 975 €*	*519 093 €*	*20 857 €*	*50 742 €*	*62 663 €*	*63 265 €*	*27 257 €*	*8 962 €*	*91 698 €*	*337 680 €*	*47 290 €*	*735 934 €*	*355 247 €*
		Aplikácie	*1 264 155 €*	*172 975 €*	-€	-€	-€	-€	-€	-€	-€	-€	-€	-€	*735 934 €*	*355 247 €*
		SW	*710 413 €*	-€	-€	*20 857 €*	*50 742 €*	*62 663 €*	*63 265 €*	*27 257 €*	*8 962 €*	*91 698 €*	*337 680 €*	*47 290 €*	-€	-€
		HW	*519 093 €*	-€	*519 093 €*	-€	-€	-€	-€	-€	-€	-€	-€	-€	-€	-€
	Riadenie projektu		933 750 €	78 697 €	151 402 €	6 083 €	14 800 €	18 277 €	18 452 €	7 950 €	2 614 €	26 745 €	98 490 €	13 793 €	334 823 €	161 624 €
	Výstupné náklady		-€	-€	-€	-€	-€	-€	-€	-€	-€	-€	-€	-€	-€	-€
Prínosy			**- 34 860 000 €**	**- 12 000 000 €**	**- 2 160 000 €**	**- 20 700 000 €**	**-€**	**-€**	**-€**	**-€**	**-€**	**-€**	**-€**	**-€**	**-€**	**-€**
	Finančné prínosy		-€	-€	-€	-€	-€	-€	-€	-€	-€	-€	-€	-€	-€	-€
		Administratívne poplatky	-€	-€	-€	-€	-€	-€	-€	-€	-€	-€	-€	-€	-€	-€
		Ostatné daňové a nedaňové príjmy	-€													
	Ekonomické prínosy		*- 34 860 000 €*	*- 12 000 000 €*	*- 2 160 000 €*	*- 20 700 000 €*	-€	-€	-€	-€	-€	-€	-€	-€	-€	-€
		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*	*N/A*	*N/A*
		Kvalitatívne prínosy	*- 34 860 000 €*	*- 12 000 000 €*	*- 2 160 000 €*	*- 20 700 000 €*	-€	-€	-€	-€	-€	-€	-€	-€	-€	-€

Interpretácia výsledkov:

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

- Pomer prínosov a nákladov (BCR): 4,03

Celkové náklady na riešenie boli vypočítané prostredníctvom UCP analýzy a zároveň PHZ oslovením dodávateľov. Vypočítané náklady projektu cez UCP analýzu a výšku rozpočtu môžeme rozdeliť nasledovne:

Rozpočet projektu celkom

Externé služby	6 952 182,00 €
HW a licencie	5 122 944,40 €

Interné mzdové náklady	1 264 155,36 €
907 - Paušálna sadzba na nepriame výdavky podľa článku 54 písm. a) NSU	933 749,72 €
Projekt Celkom	**14 273 031,48 €**

Položka Externé služby sa v zmysle CBA delia nasledovne

Implementačné práce pre centrálnu infraštruktúru	951 268,42 €
Implementačné práce priamo na obciach	6 000 913,58 €

Pri výpočte implementačných prác môžeme počítať s tým, že jednotkový náklad na implementáciu kybernetickej bezpečnosti je pre obec už zapojenú v IS DCOM 2781,6 EUR a pre obec, ktorá počas projektu iba vstúpi do IS DCOM 5581,9. Tieto čísla vychádzajú z predbežných analýz celkovej nákladovosti projektu a počtu pripojených obcí.

V prípade, že nebude realizovaný plný počet obcí (1805) na ktoré je stanovený rozpočet, bude lineárne ponížený rozpočet projektu o násobok menšieho počtu pripojených obcí. To znamená, že náklady na implementačné práce na obciach sa správajú ako čistý variabilný náklad.

PRÍNOSY:

KVANTITATÍVNE PRÍNOSY:

Kvantifikovanie prínosov v oblasti kybernetickej bezpečnosti a informačných technológií môže byť zložité, nakoľko tieto prínosy sa často prejavujú v závislosti od mnohých faktorov. V projekte boli kvantifikované dve hlavné skupiny prínosov.

A. DCOM – zamedzenie výpadku elektronických služieb IS DCOM

B. Obec – Neobstaranie prípravy riadiacej dokumentácie obcou ale centrálne DEUSom

A. DCOM – zamedzenie výpadku elektronických služieb IS DCOM

1.) Zníženie % výpadku služieb IS DCOM a s tým súvisiaceho „prestoja" zamestnancov samosprávy

% zníženia výpadkov infraštruktúry z dôvodu výmeny a doplnenie niektorých kľúčových bezpečnostných komponentov infraštruktúry.

Prínos sme vypočítali ako rozdiel medzi nedostupnosťou infraštruktúry v AS-IS a TO-BE stave.

2.) Zamedzenie bezpečnostného incidentu

Pravdepodobnosť DDoS podľa štatistík nasadeného vulnerability manažementu je na úrovni 80% per rok. Prínos je vypočítaný ako rozdiel pravdepodobností dopadov DDoS útoku *počet používateľov používajúcich IS *%alokácia zamestnanca *priemerná dĺžka trvania výpadku pri DDoS v hod. * priemerná superhrubá hodinová mzda. Model predpokladá s postupným zavádzaním opatrení (HW a SW) do prevádzky. Pravdepodobnosť DDoS po nasadení opatrení je viac ako 7x nižšia.

3.) Zamedzenie výpadku z dôvodu bezpečnostného incidentu a nutného recovery

Riziko dopadu veľmi závažného incidentu podľa VM je v súčasnosti 10%. Z praxe vyplýva, že periodicita takéhoto incidentu je 1x za obdobie 10 rokov. V prípade závažného výpadku sa predpokladá výpadok v dĺžke 3 mesiacov. Nasadením riešenia dôjde k zníženiu pravdepodobnosti dopadu závažného incidentu o polovicu. Zároveň zmenou bezpečnostnej architektúry, zálohovania a zavedením Business continuty manažmentu a zmeny disaster recovery dôjde k zníženiu doby obnovy z 60 prac. dní na 5 dní.

B. Obec – Neobstaranie jednotlivých opatrení obcou ale centrálne DEUSom

1) Úspora z rozsahu pri verejnom obstarávaní

Prínos je vypočítaný ako rozdiel medzi sumárom nákladov pri individuálnom obstarávaní obcou a sumou nákladov pri centrálnom verejnom obstarávaní. Úspora pri centrálnom verejnom obstarávaní je na úrovni 4%.

2) Úspora času zamestnanca OÚ (zamestnanec VO)

Cieľová hodnota MU projektu je 1000 obcí. Tú sme použili aj pre výpočet prínosu úspory času zamestnanca OÚ. Prínos úspory času zamestnanca VO počítame ako počet obcí* super hrubá hod. mzda* počet VO per obec *počet hodín zamestnanca strávených realizovaním 1 VO.

3) Úspora z centrálnej prípravy riadiacej dokumentácie, ktorá obsahuje o.i., metodiku a riadiace akty, pre obce do 6000 obyvateľov

Prínos je vypočítaný ako úspora z centrálnej prípravy riadiacej dokumentácie, ktorá obsahuje o.i., metodiku a riadiace akty, pre obce do 6000 obyvateľov. Náklad na prípravy riadiacej dokumentácie KIB na základe priemeru predpokladaných nákladov na ISMS dokumentáciu v predložených projektoch v rámci DOP PSK-MIRRI-611-2024-DV-EFRR.

KVALITATÍVNE PRÍNOSY:

Zvýšenie kybernetickej bezpečnosti

Projekt prinesie zlepšenie ochrany samospráv a obcí pred stále rastúcimi kybernetickými hrozbami. Upgrades a doplnenia centrálnej infraštruktúry informačného systému DCOM zabezpečujú modernizáciu a posilnenie bezpečnostnej základne. 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 evolvujú a stávajú sa čoraz zložitejšími a nebezpečnejšími. Útoky sa objavujú na nových frontoch a využívajú nové techniky na prekonanie 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.

Centralizovaná podpora

Vytvorenie centrálnych bezpečnostných riešení a služieb prináša výhodu efektívnej a centralizovanej podpory v oblasti kybernetickej bezpečnosti pre obce. Toto znamená, že obce si nebudú musieť jednotlivo zabezpečovať a spravovať komplexné bezpečnostné opatrenia, čo by mohlo byť časovo náročné a nákladné. Týmto spôsobom projekt znižuje administratívne zaťaženie samospráv.

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 metódami. 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.

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:

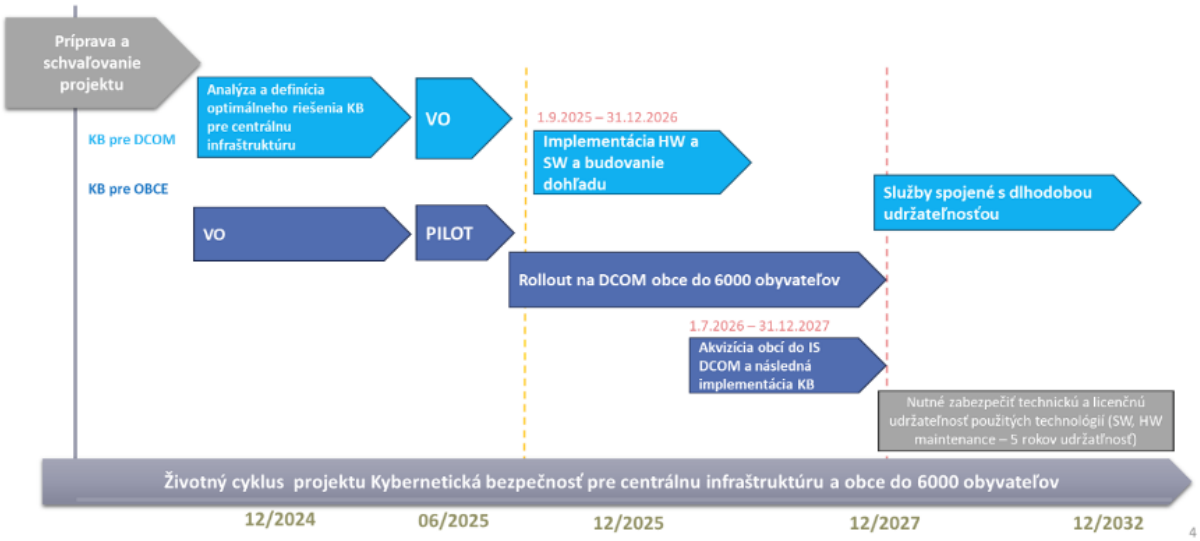
Rýchla identifikácia nových hrozieb

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.

Projekt sa zabezpečí, že organizácia nebude iba pasívnym príjemcom informácií o hrozbách, ale aktívnym účastníkom v boji proti nim. Tým sa DEUS stane schopný 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 samospráve, ale aj pre celý štát.

8. HARMONOGRAM JEDNOTLIVÝCH FÁZ PROJEKTU a METÓDA JEHO RIADENIA

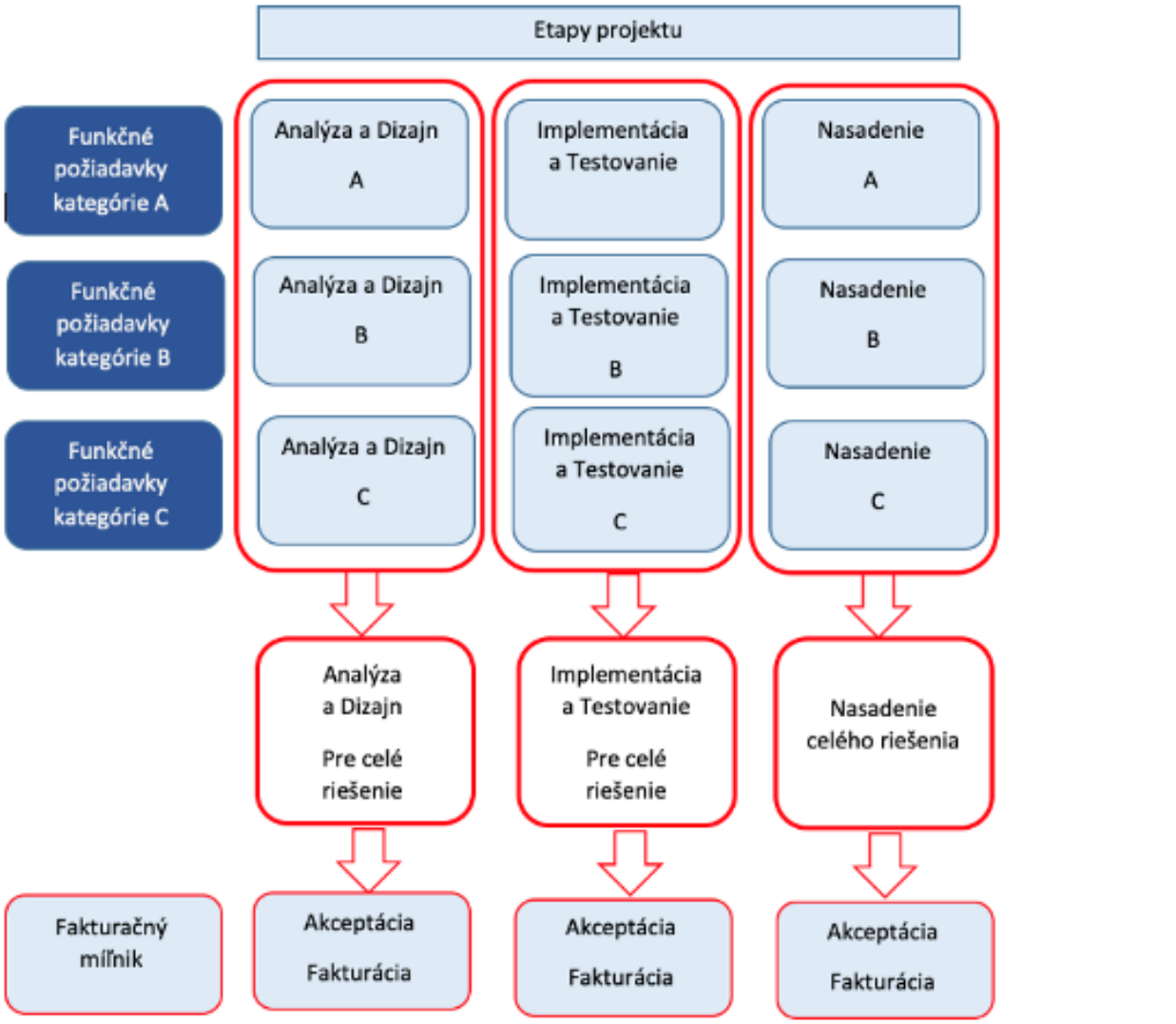
Orientačný časový harmonogram:



HARMONOGRAM RoZDELENÝ NA ETAPY V ZMYSLE VYHLÁŠKY 401/2023 Z. z.:

ID	FÁZA/AKTIVITA	ZAČIATOK (odhad termínu)	KONIEC (odhad termínu)	POZNÁMKA
1.	Prípravná a iniciačná fáza	05/2024	10/2024	Vlastné kapacity DEUS. Predpokladom je, že prípravná fáza je ukončená s kladným výsledkom z riadiaceho výboru. Iniciačná fáza končí vypísaním Verejného obstarania.
2.	Realizačná fáza	10/2024	12/2027	vlastné kapacity DEUS a dodávateľ
2a	Analýza a Dizajn	10/2024	9/2025	vlastné kapacity DEUS a dodávateľ
2b	Nákup technických prostriedkov, programových prostriedkov a služieb	10/2024	12/2026	vlastné kapacity DEUS a dodávateľ
2c	Implementácia a testovanie	09/2025	12/2027	vlastné kapacity DEUS a dodávateľ
2d	Nasadenie a PIP	09/2025	12/2027	vlastné kapacity DEUS a dodávateľ
3.	Dokončovacia fáza	11/2027	12/2027	vlastné kapacity DEUS a dodávateľ

Projekt Kybernetická bezpečnosť pre samosprávy SR do 6000 obyvateľov prostredníctvom správcu informačného systému DCOM bude v DEUS realizovaný metódou Waterfall.



Realizácia aktivít kybernetickej bezpečnosti na obci do 6000 obyvateľov bude prebiehať v dvoch fázach.

Pilot:

Pilotné návštevy podľa jednotlivých kategórií obcí a implementácia navrhovaných aktivít, prípadné úpravy rozsahu pre celonárodný rollout najmä:

- odladenie procesu implementácie aktivít na jednotlivých typoch obcí s cieľom potvrdenia ich užitočnosti a využitia na obciach
- automatizácia procesov, a výkon úloh tak, aby sa do projektu mohlo zapojiť maximum obcí so záujmom zabezpečenia vlastnej KB a súladu so zákonom o KB.
- Konzultačné práce na jednotlivých typoch obcí, pre zadefinovanie optimálnej sady opatrení KB pre každý jednotlivý typ obce
- Vypracovanie štandardov pre rollout v spolupráci s MIRRI, pre využitie existujúcich podkladov, materiálov a vzorovej dokumentácie

Rollout:

- Rollout na jednotlivé DCOM obce – kontrola procesov, aktualizácia dokumentácie, príprava na certifikáciu KB
- Rollout podpory zvýšenia KB na obce, ktoré nevyužívajú IS DCOM bude realizovaný v dvoch krokoch:
  - migrácia do IS DCOM
  - implementácia aktivít projektu KB

9. PROJEKTOVÝ TÍM

Projekt sa bude riadiť v súlade s platnou legislatívou v oblasti riadenia projektov IT. Pre potreby riadenia projektu bude vytvorený riadiaci výbor projektu a budú menovaní členovia Riadiaceho výboru projektu (ďalej len „RV“), projektový manažér a členovia projektového tímu.

Najvyššou autoritou projektu je RV, ktorý tvorí:

- predseda RV
- zástupca vlastníkov procesov - zástupca predsedu RV (podpredseda RV)
- zástupca kľúčových používateľov
- manažér kybernetickej a informačnej bezpečnosti
- Projektový manažér
- zástupca dodávateľa

Zloženie riadiaceho výboru:

ID	MENO A PRIEZVISKO	POZÍCIA	ORGANIZAČNÝ ÚTVAR	ROLA V PROJEKTE S UVEDENÍM HLASOVACIEHO PRÁVA
1.	Ing. Katarína Lešková	výkonná riaditeľka	DEUS	Predseda RV (HP)
2.	TBD	TBD	DEUS	Zástupca predsedu RV (HP) - zástupca vlastníkov procesov
2.	Ing. Peter Uhrík	manažér oddelenia IT	DEUS	Zástupca predsedu RV (HP) - zástupca vlastníkov procesov
3.	TBD	TBD	DEUS	Zástupca kľúčových používateľov (HP)
4.	TBD	TBD	DEUS	Manažér kybernetickej a informačnej bezpečnosti (HP)
5.	TBD	projektový manažér	DEUS	Zástupca dodávateľa
2.	TBD	projektový manažér	NBÚ	zástupca vlastníkov procesov

Zloženie projektového tímu:

- IT projektový manažér,
- IT architekt,
- IT analytik,
- Vlastník procesov,
- Kľúčový používateľ,
- Špecialista pre infraštruktúrny/HW špecialista,
- Manažér kybernetickej a informačnej bezpečnosti,
- IT/IS konzultant,
- Manažér kvality,
- Finančný manažér,
- Špecialista pre bezpečnosť IT
- Technik kybernetickej bezpečnosti
- Špecialista na publicitu
- Architekt sieťovej infraštruktúry

ID	MENO A PRIEZVISKO	POZÍCIA	ORGANIZAČNÝ ÚTVAR	PROJEKTOVÁ ROLA
1.	TBD	IT projektový manažér	DEUS	IT projektový manažér
2.	TBD	IT architekt	DEUS	IT architekt
3.	TBD	IT analytik	DEUS	IT analytik
4.	TBD	Vlastník procesov	DEUS	Vlastník procesov

5.	TBD	Kľúčový používateľ	DEUS	Kľúčový používateľ
6.	TBD	Špecialista pre infraštruktúrny/HW špecialista	DEUS	Špecialista pre infraštruktúrny/HW špecialista
7.	TBD	Manažér kybernetickej a informačnej bezpečnosti	DEUS	Manažér kybernetickej a informačnej bezpečnosti
8.	TBD	IT/IS konzultant	DEUS	IT/IS konzultant
9.	TBD	Manažér kvality	DEUS	Manažér kvality
10.	TBD	Finančný manažér	DEUS	Finančný manažér
14.	TBD	Manažér kvality	NBÚ	Manažér kvality
15.	TBD	Finančný manažér	NBÚ	Finančný manažér
17.	TBD	Technik kybernetickej bezpečnosti	DEUS	Technik kybernetickej bezpečnosti
18.	TBD	Špecialista na publicitu	DEUS	Špecialista na publicitu
19.	TBD	Architekt sieťovej infraštruktúry	DEUS	Architekt sieťovej infraštruktúry

9.1 PRACOVNÉ NÁPLNE

RV je riadiaci orgán projektu, ktorý zodpovedá najmä za splnenie stanovených cieľov projektu, rozhoduje o zmenách, ktoré majú zásadný význam a prejavujú sa hlavne dopadom na časový harmonogram a finančné prostriedky projektu. Reprezentuje najvyššiu akceptačnú autoritu projektu. Rokovací poriadok a štatút Riadiaceho výboru projektu upravuje najmä úlohy, zloženie a pôsobnosť RV, ako aj práva a povinnosti členov RV pri riadení a realizácii predmetného projektu.

Projektový manažér riadi projekt, kvalitu a riziká projektu a zabezpečuje plnenie úloh uložených RV. Členovia projektového tímu zabezpečujú plnenie úloh uložených projektovým manažérom, alebo RV.

Ďalšie povinnosti členov RV, projektového manažéra a členov projektového tímu sú uvedené vo Vyhláške č. 401/2023 Z. z. a v doplňujúcich vzoroch a šablónach zverejnených na webovom sídle MIRRI SR.

Projektová rola:	**PROJEKTOVÝ MANAŽÉR**
Detailný popis ozsahu 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 aefektívne využívanie projektových zdrojov (ľudských a finančných), - zodpovedá za splnenie všetkých legislatívnych požiadaviek (právne predpisy SR a EK), 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 azabezpečenie 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 DEUS, 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 aspolupracuje 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 ozsahu 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 užívateľov a 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 ozsahu 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 v zmysle organizačného poriadku , 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 ahodnovernosti 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 DEUS 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 DEUS, - 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 DEUS a dokumentoch týkajúcich sa bezpečnosti DEUS, - 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 ozsahu zodpovedností, povinností a kompetencií	- zodpovedá za špecifikovanie: • štandardov, princípov a stratégií v oblasti informačnej bezpečnosti („IB“) akybernetickej 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", • požiadavieknadodaniepotrebnejdokumentáciesúvisiacejsIBaKBkontrolujeichimplementáciu 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)“, • požiadavieknabezpečnosť ITaKB vrámci 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.

10. ODKAZY

Táto verzia neobsahuje odkazy, budú doplnené pri ďalšej aktualizácií.

11. PRÍLOHY

Príloha 1: Zoznam rizík a závislostí

Príloha 2: Dokumentácia k stanoveniu PHZ pre HW/SW

Koniec dokumentu

[1] Spoločné moduly podľa zákona č. 305/2013 e-Governmente