Zvýšenie úrovne informačnej a kybernetickej bezpečnosti v prostredi PPA

dátum Tento dokument obsahuje x strán

Obsah

Zoznam tabuliek

1. Prehľad

Kto tvorí štúdiu, ktoré organizácie budú implementovať projekt, identifikácia organizácii v zriaďovateľskej pôsobnosti, identifikácia príslušného úseku verejnej správy, agendy verejnej správy a životnej situácie.
Tabuľka 1 Základné informácie - zhrnutie

Zdôvodnenie využitia národného projektu a vylúčenia výberu projektu prostredníctvom výzvy
Navrhovaný projekt, ktorý vychádza z predmetnej štúdie súvisí najmä s naplnením povinností definovaných najmä v zákone č. 69/2018 Z. z. Zákon o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov, ústredných orgánov a Organizácií verejnej moci spadajúcich pod podsektor informačné systémy verejnej správy, resp. informačné technológie verejnej správy podľa nového zákona č 95/2019 Z.z. Za účelom zvýšenia úrovne zavedených postupov a opatrení týkajúcich sa kybernetickej a informačnej bezpečnosti v PPA je potreba vybudovať novú, resp. konsolidovať existujúcu bezpečnostnú architektúru. Toto je možné dosiahnuť implementáciou nových, alebo inováciou existujúcich bezpečnostných nástrojov a procesov, a to najmä v nasledovných oblastiach: · ochrana pred útokmi z externého prostredia, · detekcia škodlivých aktivít a bezpečnostných incidentov, · ochrana dát, dátových prenosov a komunikácie, · budovanie bezpečnostného povedomia. PPA preto plánuje implementáciu preventívnych a reaktívnych opatrení v oblasti svojho pôsobenia a poskytovanie relevantných informácií o kybernetických incidentoch, aby bola zabezpečená efektívna spolupráca medzi vládnou jednotkou CSIRT a spoľahlivý výkon činností prostredníctvom vlastného systému riadenia informačnej a kybernetickej bezpečnosti pre plnenie bezpečnostných opatrení definovaných v § 20 zákone o KyB. Realizáciou projektu PPA prispeje k naplneniu nasledovných cieľov súvisiacich s údajmi v organizácií:

Oblasť	**Cieľ realizácia projektu**	**Áno / Nie**
Ochrana pred útokmi z externého prostredia,	Zabezpečenie primeranej ochrany a úrovne bezpečnosti informačných aktív, IS PPA	þ
Detekcia škodlivých aktivít a bezpečnostných incidentov,	Predchádzanie a riadenie bezpečnostných incidentov formálnym riadením rizík.	
Ochrana dát, dátových prenosov a komunikácie,	Bezpečnosť a ochrana digitálneho a kybernetického priestoru, monitoring a proaktívna ochrana kritickej infraštruktúry (agendové systémy) PPA..	
Budovanie bezpečnostného povedomia.	Budovanie komplexnej bezpečnostnej architektúry, ktorá bude založená na rovnakých princípoch a úrovniach bezpečnosti ako je budovaná národná horizontálna úroveň.	

PPA ako prevádzkovateľ základnej služby je povinná v súlade s §20 zákona o KyB prijať adekvátne bezpečnostné opatrenia (úlohy, procesy, roly a technológie v organizačnej, personálnej a technickej oblasti), ktorých cieľom je zabezpečenie kybernetickej bezpečnosti počas životného cyklu sietí a informačných systémov, ktoré sú v jej kompetencii. Bezpečnostné opatrenia realizované v závislosti od klasifikácie informácií a kategorizácie sietí a informačných systémov a v súlade s bezpečnostnými štandardami v oblasti kybernetickej bezpečnosti sa prijímajú s cieľom predchádzať kybernetickým bezpečnostným incidentom a minimalizovať vplyv kybernetických bezpečnostných incidentov na kontinuitu prevádzkovania základnej služby.

Dôvodom pre vypracovanie tejto štúdie uskutočniteľnosti je zámer PPA zaviesť elektronické služby pre formalizované riadenie informačnej a kybernetickej bezpečnosti na podporu v rámci programu digitálnej transformácie PPA (DT-PPA).

Informačná a kybernetická bezpečnostná podpora PPA je v súčasnosti riešená v rámci samostatných systémoch pre:

- Integrovaný administratívny kontrolný systém - IACS,
- Agrárny informačný systém - modul finančného riadenia - AGIS MFR,
- Agrárny informačný systém - spoločné organizácie trhu - AGIS SOT,
- Agrárny informačný systém - program rozvoja vidieka - AGIS PRV,
- Agrárny informačný systém - štátna pomoc - AGIS ŠP,
- Systém kontrol na mieste eKNM,
- Informačný systém účtovníctva fondov - ISUF,
- a značného počtu podporných systémov.

Z hľadiska naliehavosti situácie je možné rozdeliť potrebu uskutočnenia projektu na tieto hlavné skutočnosti:

Pre zabezpečenie a plnenie bezpečnostných opatrení definovaných v § 20 zákone o KyB v prostredí PPA je nevyhnuté implementovať komplexný systém kybernetickej ochrany a riadenia IB a KyB s prepojením na vládnu jednotku CSIRT a jednotný IS kybernetickej bezpečnosti prevádzkovaný NBÚ, ktorý bude reflektovať na bezpečnostnú architektúru (ciele, požiadavky, princípy, stavebných blokov a pod.) uvedenú v strategickej priorite „Informačná a kybernetická bezpečnosť".

Existujúci systém IB a KvB nepokrýva všetky opatrenia a požiadavky a nie je vytvorený systém vzdelávania špecialistov IB a KvB , aby boli schopní účinne rozvíjať detekčné mechanizmy v PPA na koľko nie všetky postupy a opatrenia KyB v PPA dosahujú potrebnú úroveň vyspelosti, ktorá je nevyhnutná pre znižovanie bezpečnostných rizík na prijateľnú úroveň zabezpečenia a ochrany pre všetky požiadavky legislatívy (najmä zákona o KyB)

V prostredí PPA IKT v súčasnosti obsahujú izolované prvky bezpečnostnej architektúry, ktoré primárne fungujú len na vybraných zariadeniach a systémoch, teda nie sú nasadené plošne, bezpečnostný systém nepokrýva všetky informačné aktíva a rovnako nie je implementovaný centrálny monitoring integrovaný na pripojenie do komunikačného systému pre hlásenie a riešenie kybernetických bezpečnostných incidentov vládnej jednotky CSIRT.

Prínosy projektu budú nasledovné :

- Možnosť nasadenia moderných, pokročilých bezpečnostných opatrení a sofistikovaných bezpečnostných mechanizmov, ktoré budú zaisťovať požadovanú úroveň ochrany všetkých bezpečnostne relevantných informačných aktív PPA a zároveň bude schopná na reflektovať vývoj v oblasti kybernetických hrozieb.
- Možnosť nasadenia prostriedkov a prvkov KyB ochrany a monitorovania, ktoré budú identifikovať možné bezpečnostné incidenty aj v reálnom čase.
- Zvýšenie úrovne bezpečnostných postupov a opatrení, ktorých výsledkom bude zníženie miery nových alebo stávajúcich rizík a hrozieb na prijateľnú úroveň.
- Možnosť vybavenia bezpečnostných tímov technickými prostriedkami a usporadúvania školení zamestnancov PPA a tým efektívne riešenie bezpečnostných incidentov v prostredí PPA
- Zlepšenie úrovne bezpečnostného povedomia u zamestnancov PPA a tým zníženie rizika útokov z kategórie sociálneho inžinierstva alebo rizika zlyhania ľudského faktoru.
- Zlepšenie prevencie kybernetických útokov používaním nástrojov a techník, ktoré odhalia zraniteľnosti a slabiny IS a aplikácií PPA skôr, ako dôjde k ich zneužitiu neoprávnenou osobou.
- Zlepšenie reakcie na kybernetické bezpečnostné incidenty, ich riadenie, zníženie na požadovanú úroveň, kategorizácia a evidencia.
- Umožnenie prístupu k vybraným logom a záznamom z rozhrania IKT PPA vládnej jednotke CSIRT priamo do monitorovacieho systému čím bude umožnený aj plošný monitoring bezpečnosti.
- Možnosť následného nasadenia analytických nástrojov nad veľkým množstvom údajov (Big-data) v reálnom čase, ktoré vyhodnocujú rizikovosť subjektov a ich správanie nielen na základe informácií previazaných s prostredím PPA, ale aj na základe jeho väzieb na okolité subjekty a ich správanie.

Vyššie zmienené fakty sú nielen prínosom pre samotných podnikateľov v agrosektore ale aj pre samotné zlepšenie procesov a činností vnútri PPA. Prínosy zároveň zabezpečia zvýšenie reputácie agentúry v očiach občanov ako aj zabezpečenie súladu s legislatívou SR a EU.

Prijímateľa/partnera národného projektu a dôvod jeho určenia

Príslušnosť národného projektu k relevantnej časti PO7 OPII

Predkladaná štúdia je štúdiou uskutočniteľnosti prepracovaného obdobie 2014až2022

	nosť,. Projekt je prísl ušný k špecifickým cieľom: 7.9 Zvýšenie kybernetickej bezpečnosti v spoločnosti
Indikatívna výška finančných prostriedkov určených na realizáciu národného projektu	

2. Dôvod

Dôvod vykonania štúdie uskutočniteľnosti. Definovanie IT stratégie a vízie architektúry organizácie verejnej správy.

3. Rozsah

Rozsah oblastí, v ktorom sa štúdia venuje projektu, do akej hĺbky sa venuje jednotlivým oblastiam.

V rámci PPA je potrebné realizovať všetky aktivity definované nižšie na naplnenie cieľa plnohodnotného zavedenia procesov na detekciu podvodov.

V nasledujúcej tabuľke sa žiadateľ zaväzuje realizovať nasledovné aktivity:

Výstup projektu:		**Áno / Nie**	**Odôvodnenie v prípade nerealizácie výstupu[1]**
A 1:	Vybudovanie systému riadenie informačnej bezpečnosti, návrh základných cieľov, stratégie, interných predpisov, postupov, vykonať bezpečnostné školenie, vypracovať bezpečnostné požiadavky na nové informačné systémy	þ	*Popis, prečo sa výstup nebude v projekte realizovať*
A 2:	Analýza rizík s návrhom primeraných a vhodných technických a procesných opatrení na ich minimalizovanie, vypracovať systém riadenia informačných aktív, popis a klasifikácia serverov, pracovných staníc, sieťových zariadení, zrealizovať audit aktuálneho stavu informačnej bezpečnosti z pohľadu najlepších bezpečnostných praktík, resp. noriem ISO 27000, zrealizovať gap analýzu aktuálneho stavu bezpečnosti technológií voči zákonu č. 95/2019 Z. z. o informačných technológiách vo verejnej správe	þ	*Popis, prečo sa výstup nebude v projekte realizovať*
A 3:	Gap analýza aktuálneho stavu bezpečnosti voči zákonu č. 69/2018 Z. z. o kybernetickej bezpečnosti a navrhnúť primerané technické a organizačné opatrenia	þ	*Popis, prečo sa výstup nebude v projekte realizovať*
A 9:	Gap analýza aktuálneho stavu voči požiadavkám nariadenia GDPR, vypacovanie chýbajúcej dokumentácie,	þ	*Popis, prečo sa výstup nebude v projekte realizovať*
A 4:	Penetračné testy	þ	*Popis, prečo sa výstup nebude v projekte realizovať*
A 5:	Vypracovanie BCM (riadenie kontinuity činností), vypracovanie analýzy dopadov, plánov kontinuity, plánov obnovy, havarijných plánov.	þ	*Popis, prečo sa výstup nebude v projekte realizovať*
A 6:	Zavedenie nástroja na monitorovanie a správu bezpečnostných udalostí SIEM	þ	*Popis, prečo sa výstup nebude v projekte realizovať*
A 7:	Zavedenie nástroja na riadenie privilegovaných identít (PIM)	þ	*Popis, prečo sa výstup nebude v projekte realizovať*
A 8:	Zavedenie nástroja pre analýzu anomálií dátových tokov	þ	*Popis, prečo sa výstup nebude v projekte realizovať*

A 9:	Nasadenie systému voči úniku citlivých dát DLP	þ	*Popis, prečo sa výstup nebude v projekte realizovať*
A 10:	Vybudovanie systému riadenie informačnej bezpečnosti, návrh základných cieľov, stratégie, interných predpisov, postupov, vykonať bezpečnostné školenie, vypracovať bezpečnostné požiadavky na nové informačné systémy	þ	*Popis, prečo sa výstup nebude v projekte realizovať*

[1] *Popis, prečo sa výstup nebude v projekte realizovať* **-** *V prípade, ak je pre zvolenú alternatívu nie je daná aktivita relevantná, je potrebné to zdôvodniť (napr. žiadateľ nebude mať v rámci realizovaného projektu údaje, ktoré sú referenčné)*

4. Použité skratky a značky

Tabuľka 2 Skratky a značky

Skratka / Značka	**Vysvetlenie**
R Analýza rizík	R Analýza rizík
BCM Riadenie kontinuity činností (Business Continuity Management)	BCM Riadenie kontinuity činností (Business Continuity Management)
BCP Plán riadenia kontinuity činností (Business Continuity Plan)	BCP Plán riadenia kontinuity činností (Business Continuity Plan)
BIA Analýza dopadov (Business Impact Analysis)	BIA Analýza dopadov (Business Impact Analysis)
CBA Nákladovo-prínosová analýza (Cost-Benefit Analysis)	CBA Nákladovo-prínosová analýza (Cost-Benefit Analysis)
CSIRT Computer Security Incident Response Team	CSIRT Computer Security Incident Response Team
CTI Cyber Threat Intelligence	CTI Cyber Threat Intelligence
DC Klasifikácia dát (Data Classification)	DC Klasifikácia dát (Data Classification)
DRP Plán obnovy po havárii (Disaster Recovery Plan)	DRP Plán obnovy po havárii (Disaster Recovery Plan)
EÚ Európska únia	EÚ Európska únia
EPP End Point Protection (Ochrana koncových zariadení používateľov)	EPP End Point Protection (Ochrana koncových zariadení používateľov)
FOB Fyzická a objektová bezpečnosť	FOB Fyzická a objektová bezpečnosť
Govnet Vládna sieť vybudovaná a spravovaná NASES	Govnet Vládna sieť vybudovaná a spravovaná NASES
HW Hardvér	HW Hardvér
IAM Správa identít a prístupov (Identity Access Management)	IAM Správa identít a prístupov (Identity Access Management)
IB Informačná bezpečnosť	IB Informačná bezpečnosť
IKT Informačno-komunikačné technológie	IKT Informačno-komunikačné technológie
IS Informačný systém	IS Informačný systém
IS VS Informačný systém verejnej správy	IS VS Informačný systém verejnej správy
IT Informačné technológie	IT Informačné technológie
ITP Informačno–technické prostriedky	ITP Informačno–technické prostriedky

JISKB Jednotný informačný systém kybernetickej bezpečnosti prevádzkovaný NBÚ	JISKB Jednotný informačný systém kybernetickej bezpečnosti prevádzkovaný NBÚ
KB DB Databáza znalostí (Knowledge Database)	KB DB Databáza znalostí (Knowledge Database)
KBI Kybernetický bezpečnostný incident	KBI Kybernetický bezpečnostný incident
KyB Kybernetická bezpečnosť	KyB Kybernetická bezpečnosť
NASES Národná agentúra pre sieťové a elektronické služby; organizácia zriadená v pôsobnosti Úradu vlády SR	NASES Národná agentúra pre sieťové a elektronické služby; organizácia zriadená v pôsobnosti Úradu vlády SR
NBÚ Národný bezpečnostný úrad	NBÚ Národný bezpečnostný úrad
NDA No Disclosure Agreement	NDA No Disclosure Agreement
NGFW Firewall novej generácie (Next-Generation Firewall)	NGFW Firewall novej generácie (Next-Generation Firewall)
NKIVS Národná koncepcia informatizácie verejnej správy	NKIVS Národná koncepcia informatizácie verejnej správy
OPII Operačný program Integrovaná infraštruktúra	OPII Operačný program Integrovaná infraštruktúra
OVM Orgány verejnej moci	OVM Orgány verejnej moci
PKI Infraštruktúra verejného kľúča (Public Key Infrastructure)	PKI Infraštruktúra verejného kľúča (Public Key Infrastructure)
SIEM Nástroj na manažment bezpečnostných informácií a udalostí (Security Information and Event Management)	SIEM Nástroj na manažment bezpečnostných informácií a udalostí (Security Information and Event Management)
SLA Service Level Agreement	SLA Service Level Agreement
SOC Pracovisko pre riadenie bezpečnosti (Security Operation Center)	SOC Pracovisko pre riadenie bezpečnosti (Security Operation Center)
SR Slovenská republika	SR Slovenská republika
SW Softvér	SW Softvér
ŠU Štúdia uskutočniteľnosti	ŠU Štúdia uskutočniteľnosti
ÚPVII Úrad podpredsedu vlády pre investície a informatizáciu	ÚPVII Úrad podpredsedu vlády pre investície a informatizáciu
R Analýza rizík	R Analýza rizík
BCM Riadenie kontinuity činností (Business Continuity Management)	BCM Riadenie kontinuity činností (Business Continuity Management)
BCP Plán riadenia kontinuity činností (Business Continuity Plan)	BCP Plán riadenia kontinuity činností (Business Continuity Plan)
BIA Analýza dopadov (Business Impact Analysis)	BIA Analýza dopadov (Business Impact Analysis)
CBA Nákladovo-prínosová analýza (Cost-Benefit Analysis)	CBA Nákladovo-prínosová analýza (Cost-Benefit Analysis)
CSIRT Computer Security Incident Response Team	CSIRT Computer Security Incident Response Team
CTI Cyber Threat Intelligence	CTI Cyber Threat Intelligence
DC Klasifikácia dát (Data Classification)	DC Klasifikácia dát (Data Classification)
DRP Plán obnovy po havárii (Disaster Recovery Plan)	DRP Plán obnovy po havárii (Disaster Recovery Plan)
EÚ Európska únia	EÚ Európska únia
EPP End Point Protection (Ochrana koncových zariadení používateľov)	EPP End Point Protection (Ochrana koncových zariadení používateľov)
FOB Fyzická a objektová bezpečnosť	FOB Fyzická a objektová bezpečnosť
Govnet Vládna sieť vybudovaná a spravovaná NASES	Govnet Vládna sieť vybudovaná a spravovaná NASES
HW Hardvér	HW Hardvér

IAM Správa identít a prístupov (Identity Access Management)	IAM Správa identít a prístupov (Identity Access Management)
IB Informačná bezpečnosť	IB Informačná bezpečnosť
IKT Informačno-komunikačné technológie	IKT Informačno-komunikačné technológie
IS Informačný systém	IS Informačný systém
IS VS Informačný systém verejnej správy	IS VS Informačný systém verejnej správy
IT Informačné technológie	IT Informačné technológie
ITP Informačno–technické prostriedky	ITP Informačno–technické prostriedky
JISKB Jednotný informačný systém kybernetickej bezpečnosti prevádzkovaný NBÚ	JISKB Jednotný informačný systém kybernetickej bezpečnosti prevádzkovaný NBÚ
KB DB Databáza znalostí (Knowledge Database)	KB DB Databáza znalostí (Knowledge Database)
KBI Kybernetický bezpečnostný incident	KBI Kybernetický bezpečnostný incident
KyB Kybernetická bezpečnosť	KyB Kybernetická bezpečnosť
NASES Národná agentúra pre sieťové a elektronické služby; organizácia zriadená v pôsobnosti Úradu vlády SR	NASES Národná agentúra pre sieťové a elektronické služby; organizácia zriadená v pôsobnosti Úradu vlády SR
NBÚ Národný bezpečnostný úrad	NBÚ Národný bezpečnostný úrad
NDA No Disclosure Agreement	NDA No Disclosure Agreement
NGFW Firewall novej generácie (Next-Generation Firewall)	NGFW Firewall novej generácie (Next-Generation Firewall)
NKIVS Národná koncepcia informatizácie verejnej správy	NKIVS Národná koncepcia informatizácie verejnej správy
OPII Operačný program Integrovaná infraštruktúra	OPII Operačný program Integrovaná infraštruktúra
OVM Orgány verejnej moci	OVM Orgány verejnej moci
PKI Infraštruktúra verejného kľúča (Public Key Infrastructure)	PKI Infraštruktúra verejného kľúča (Public Key Infrastructure)
SIEM Nástroj na manažment bezpečnostných informácií a udalostí (Security Information and Event Management)	SIEM Nástroj na manažment bezpečnostných informácií a udalostí (Security Information and Event Management)
SLA Service Level Agreement	SLA Service Level Agreement
SOC Pracovisko pre riadenie bezpečnosti (Security Operation Center)	SOC Pracovisko pre riadenie bezpečnosti (Security Operation Center)
SR Slovenská republika	SR Slovenská republika
SW Softvér	SW Softvér
ŠU Štúdia uskutočniteľnosti	ŠU Štúdia uskutočniteľnosti
ÚPVII Úrad podpredsedu vlády pre investície a informatizáciu	ÚPVII Úrad podpredsedu vlády pre investície a informatizáciu

Skratka / Značka	Vysvetlenie

Základné zhrnutie. Max 2400 znakov.
Priestor pre sumárny obrázok, nepovinná informácia: ArchiMate štandardný viewpoint – „Introductory viewpoint"

PPA ako orgán štátnej správy zabezpečuje administratívne činnosti súvisiace s poskytovaním podpôr pre poľnohospodárstvo a rozvoj vidieka formou finančných prostriedkov z fondov Európskej únie – Európskeho poľnohospodárskeho záručného fondu (ďalej len „EPZF"), Európskeho poľnohospodárskeho fondu pre rozvoj vidieka (ďalej len „EPFRV"), Európskeho námorného a rybárskeho fondu (ďalej len „ENRF") a zo štátneho rozpočtu (ďalej len „ŠR"). V PPA je spracúvaných množstvo citlivých informácie ako napr. osobné údaje majiteľov pozemkov, finančné dáta a iné. Tieto informácie a dáta sú kľúčovým, najdôležitejším a najcennejším aktívom, bez ktorého PPA nedokáže úspešne plniť svoje poslanie. Preto je potrebné a nevyhnutné zabezpečiť týmto informačným aktívam dostatočnú zákonom požadovanú ochranu. Informačné aktíva sa môžu vyskytovať v rôznych formách: v elektronickej, obrazovej, písomnej a snahou je zabezpečiť ich ochranu v celom životnom cykle ich spracovania: od získavania, cez prenášanie, uchovávanie (na prenosných zariadeniach, serveroch, na USB), archiváciu a až po ich zabezpečenú a riadenú likvidáciu.

Zámerom je návrh, vybudovanie a zavedenie systému riadenia informačnej (kybernetickej) bezpečnosti a implementácia vhodných a primeraných bezpečnostných opatrení, ktoré PPA a cieľovej skupine (žiadatelia o príspevok, verejnosť), zabezpečia minimalizovanie ohrozenia dostupnosti, pravosti, integrity alebo dôvernosti uchovávaných, prenášaných alebo spracúvaných údajov v informačných systémov, ktoré by mohli postihnúť používateľov, resp. žiadateľov o príspevky a v konečnom dôsledku zvýšia dôveryhodnosť štátnej inštitúcie.

Cieľom je zvýšenie ochrany pred útokmi z externého prostredia, zvýšenie schopnosti detekcie škodlivých aktivít, ochrana dát a budovanie bezpečnostného povedomia.

PPA si uvedomuje, že kybernetická a informačná bezpečnosť sa stáva nie len celospoločenským ale aj globálnym problémom a vníma ju ako jeden z kľúčových prvkov informačnej bezpečnosti. Základným cieľom informačnej bezpečnosti PPA je snaha prevádzkovať otvorený, bezpečný a chránený informačný systém, ako aj mať istoty, že informačné systémy budú plniť svoje funkcie a slúžiť aj v prípade kybernetického útoku. PPA prostredníctvom svojej Sekcie informačných technológií má snahu budovať aktívnu a riadenú informačnú bezpečnosť.

Krátkodobým cieľom (0 až 5 rokov) je vybudovanie riadeného systému kybernetickej a informačnej bezpečnosti, vypracovanie analýzy, ktorej cieľom je ukázať možnosti transformácie a konsolidácie doteraz vybudovaných informačných systémov PPA, čo v konečnom dôsledku povedie k ušetreniu prevádzkových ako aj investičných finančných prostriedkov, vybudovanie silného manažmentu rizík a venovanie trvalej pozornosti zvyšovaniu bezpečnostného povedomia v rámci PPA.

Štúdia uskutočniteľnosti pre projekt „Zvýšenie úrovne informačnej a kybernetickej bezpečnosti v PPA" je vypracovaná na základe požiadaviek definovaných vo Výzve č. OPII-2019/7/8-DOP na predkladanie Žiadostí o poskytnutie nenávratného finančného príspevku so zameraním na „Zvýšenie úrovne informačnej a kybernetickej bezpečnosti v podsektore ISVS / ITVS".

Predkladaná štúdia sa venuje otázke, ako efektívne využiť existujúce nástroje pre zabezpečenie vysokej úrovne informačnej a kybernetickej bezpečnosti informačných aktív a systémov PPA a bola vytvorená efektívna koordinácia s jednotkami CSIRT. Pri návrhu vhodného projektu, ktorý bude vychádzať z tejto štúdie sa bude sústrediť na výsledky a realizáciu ako boli posúdené nasledovné aspekty, ktoré si vyžaduje dopytová výzva a jej aktivity:

Pri príprave navrhovaného riešenia sme postupovali podľa vyššie uvedenej schémy, kedy sme:

- Stanovili základné témy a identifikovali dôležité problémy, ktoré vďaka zvýšeniu úrovne informačnej a kybernetickej bezpečnosti uvedených vo výzve dokážeme vyriešiť,
- Presne špecifikovali prípady použitia a stanovili ako budú implementované technologické riešenia a výsledky analýz a akým spôsobom,
- Identifikovali potrebné dátové zdroje a ďalšie vstupy, ktoré bude potrebné zabezpečiť počas implementácie projektu, ako i prevádzky riešenia,
- Stanovili, aké nástroje a technologické funkcie sú potrebné resp. vhodné v rámci danej metódy,
- Zamysleli sa nad používaním výsledkov riešenia v praxi,
- Pripravili plán zmien a nastaviť kroky pre ich implementáciu,
- Odhadli náklady projektu,
- Odhadli prínosy projektu.

Všetky vyššie uvedené kroky boli pretransformované do popísanú súčasného a budúce stav v oblasti legislatívy, biznis architektúry, architektúry IS, technologickej architektúry, bezpečnostnej architektúry. V rámci biznis architektúry sú popísané služby, ktoré v zmysle §20 zákona o KyB bude PPA realizovať za účelom vytvorenia efektívneho a spoľahlivého systému kybernetickej ochrany PPA a implementácie bezpečnostných opatrení vyžadovaných zákonom o KyB. Na základe tejto štúdie uskutočniteľnosti PPA vypracuje projekt, pomocou ktorého implementuje nové, resp. zefektívni staré postupy a opatrenia, a tým zvýši úroveň KIB v rámci IKT prostredia agentúry. Nutnosť realizácie projektu vyplýva z narastajúcej miery informatizácie spoločnosti a orgánov štátnej správy, z potreby dosiahnutia súladu so zákonom o KyB, z dôvodu dobrej pripravenosti na hrozby v oblasti informačnej a kybernetickej bezpečnosti, zo snahy o zefektívnenie riadenia informačnej bezpečnosti štátnej správy a z obmedzeného rozsahu finančných prostriedkov.

Cieľom projektu bude implementovať systémy ochrany kybernetickej bezpečnosti a bezpečnostné opatrenia definované zákonom o KyB, a to hlavne:

- zvýšením ochrany pred útokmi z externého prostredia,
- zvýšením schopnosti detekcie a reakcie na škodlivé aktivity a bezpečnostné incidenty,
- zvýšením úrovne ochrany dát, dátových prenosov a komunikácie,
- budovaním bezpečnostného povedomia a bezpečnostnej kultúry.

Takto koncipovaný projekt zabezpečí:

- efektívny prístup k informačnej a kybernetickej bezpečnosti PPA,
- súlad PPA s požiadavkami zákona o KyB,
- vysokú úroveň informačnej a kybernetickej bezpečnosti PPA,
- efektívne využitie finančných, technických prostriedkov a personálnych kapacít.

Na základe stanových cieľov bol pripravený projektový plán, ktorý vychádza z nasledovných oprávnených realizačných aktivít:

Aktivita	**Realizácia**
A1 vybudovanie systému riadenie informačnej bezpečnosti, návrh základných cieľov, stratégie, interných predpisov, postupov, vykonať bezpečnostné školenie, vypracovať bezpečnostné požiadavky na nové informačné systémy	þ
A2: Vykonať analýzu rizík s návrhom primeraných a vhodných technických a procesných opatrení na ich minimalizovanie, vypracovať systém riadenia informačných aktív, popis a klasifikácia serverov, pracovných staníc, sieťových zariadení, zrealizovať audit aktuálneho stavu informačnej bezpečnosti z pohľadu najlepších bezpečnostných praktík, resp. noriem ISO 27000, zrealizovať gap analýzu aktuálneho stavu bezpečnosti technológií voči zákonu č. 95 /2019 Z. z. o informačných technológiách vo verejnej správe	þ
A3: zrealizovať gap analýzu aktuálneho stavu bezpečnosti voči zákonu č. 69/2018 Z. z. o kybernetickej bezpečnosti a navrhnúť primerané technické a organizačné opatrenia	þ
A4: zrealizovať gap analýzu aktuálneho stavu voči požiadavkám nariadenia GDPR, vypacovanie chýbajúcej dokumentácie,	þ
A5: zrealizovať penetračné testy	þ
A6: vypracovanie BCM (riadenie kontinuity činností), vypracovanie analýzy dopadov, plánov kontinuity, plánov obnovy, havarijných plánov.	þ
A7: zavedenie nástroja na monitorovanie a správu bezpečnostných udalostí SIEM	þ
A8: zavedenie nástroja na riadenie privilegovaných identít (PIM)	þ
A9: zavedenie nástroja pre analýzu anomálií dátových tokov	þ
A10: nasadenie systému voči úniku citlivých dát DLP	þ

Projekt bude realizovaný 1 rok s podporou ďalších 12 mesiacov.

Merateľný ukazovateľ

- P0048 - Dodatočný počet informačných systémov verejnej správy s implementovaným nástrojom na rozpoznávanie, monitorovanie a riadenie bezpečnostných incidentov

Indikatívna cieľová hodnota 60 %

5. Motivácia

Tabuľka 3 Motivácia – budúci stav

Súhrnný popis
Úvodné informácie *(Max. 1600 znakov, pre detailný popis je potrebné využiť prílohy)* Dôvodom vypracovania predkladanej štúdie je analýza aktuálneho stavu súčasných procesov v oblastiach riadenia informačnej a kybernetickej bezpečnosti v PPA, najmä v oblasti detekcie a riešenia závažných kybernetických bezpečnostných incidentov. Zároveň táto štúdia predkladá špecifikáciu požiadaviek na nový stav, návrh riešenia na dosiahnutie nového stavu a na posúdenie možností a predpokladov jeho realizovateľnosti. Implementáciou nového, resp. inováciou starého systému kybernetickej ochrany dôjde k zvýšeniu informačnej a kybernetickej bezpečnosti v rámci PPA v súlade s NKIVS, predovšetkým v oblastiach: „Informačná a kybernetická bezpečnosť“. Zvýšenie kybernetickej bezpečnosti, prevencia kybernetických útokov, zefektívnenie výkonu, zníženie rizík a zníženie nákladov PPA patria k hlavným očakávaným prínosom informatizácie definovaných v NKIVS. Zákon o KyB vyžaduje, aby prevádzkovatelia IS VS (základných služieb) implementovali a dodržiavali konkrétne bezpečnostné procesy prostredníctvom moderných bezpečnostných technológií a ukladá im povinnosť odhaliť prípady ohrozenia informačnej a kybernetickej bezpečnosti vo svojom informačnom prostredí, ako aj zamedziť ďalšiemu výskytu týchto hrozieb. Z pohľadu potrieb Zákona o KyB je potrebné prijať bezpečnostné opatrenia, ktoré predstavujú úlohy, procesy, roly a technológie v organizačnej, personálnej a technickej oblasti, ktorých cieľom je zabezpečenie kybernetickej bezpečnosti počas životného cyklu sietí a informačných systémov PPA. Opatrenia je potrebné prijímať na základe klasifikácie informácií a kategorizácie sietí a informačných systémov na zabezpečenie predchádzania kybernetickým bezpečnostným incidentom a minimalizovanie vplyvov kybernetických bezpečnostných incidentov na kontinuitu prevádzkovania služieb, ktoré sú nevyhnutné pre plnenie úloh PPA. Hlavným cieľom je implementovať účinné opatrenia na vytvorenie bezpečného prostredia informačných systémov PPA a preto je hlavnou motiváciou realizácie projektu: Kybernetická ochrana a detekcia škodlivých aktivít a bezpečnostných incidentov Bezpečnostný monitoring, pozostávajúci z nasledovných procesov: • monitoring IS, platforiem, aplikácií a používateľských činností a aktivít, • monitoring sietí, • monitoring činností a aktivít privilegovaných používateľov, • analýza založená na big-data a machine learning algoritmoch; • Riadenie bezpečnostných incidentov, pozostávajúce z nasledovných procesov: • identifikácia a hlásenie bezpečnostných incidentov, • registrácia, kategorizácia a klasifikácia bezpečnostných incidentov, • akceptácia bezpečnostných incidentov a určenie riešiteľov, • analýza a vyšetrovanie bezpečnostných incidentov a zber dôkazov, • riešenie bezpečnostných incidentov a obnova prevádzky, • uzatvorenie bezpečnostných incidentov, • vyhodnotenie bezpečnostných incidentov, zavedenie do KB DB, spätná väzba a poučenie sa z bezpečnostného incidentu; • Ochrana dát, dátových prenosov a komunikácie:

- bezpečnosť virtualizovaných prostredí,
- ochrana dát na úrovni databáz a dátových úložísk (šifrovanie dát),
- ochrana dát na úrovni koncových zariadení (EPP - šifrovanie dát pri každom ich prenose alebo uchovávaní v lokálnom alebo centrálnom úložisku, kontrola a šifrovanie externých médií a pod.),
- riadenie prístupov (implementácia nástrojov IAM a remote access manažmentu),
- monitoring bezpečnosti na rozhraní s vyvedením logov do vládnej jednotky CSIRT.
- proces bezpečnej výmeny citlivých informácií s vládnou jednotkou CSIRT, prípadne inými spolupracujúcimi OVM (integráciou na JISKB prostredníctvom vládnej jednotky CSIRT)

Ďalšími podcieľmi motivácie pre realizáciu projektu sú:

- zabezpečenie dôvernosti, integrity a dostupnosti všetkých informačných aktív PPA,
- zabezpečenie efektívneho výkonu správy a riadenia informačnej a kybernetickej bezpečnosti vo svojej pôsobnosti,
- zabezpečenie efektívnej detekcie a riešenia bezpečnostných incidentov,
- zabezpečenie efektívnej, spoľahlivej a bezpečnej prevádzky IS a AS a aplikácií PPA,
- zabezpečenie efektívnej, spoľahlivej a bezpečnej komunikácie a výmeny informácií s vládnou jednotkou CSIRT.

Priestor pre sumárny obrázok: ArchiMate štandardný viewpoint – „Motivation viewpoint"

Ďalšie informácie
(Max. 1600 znakov, pre detailný popis je potrebné využiť prílohy)

Riziká	**Spresnenie identifikovaných rizík:** *Odkazy na relevantné identifikátory rizík v prílohe Riziká.*
Stručná charakteristika identifikovaných rizík (Max. 400 znakov)	

Prílohy	**Diagramy, modely, obrázky v plnom rozlíšení**
Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.	*Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.*

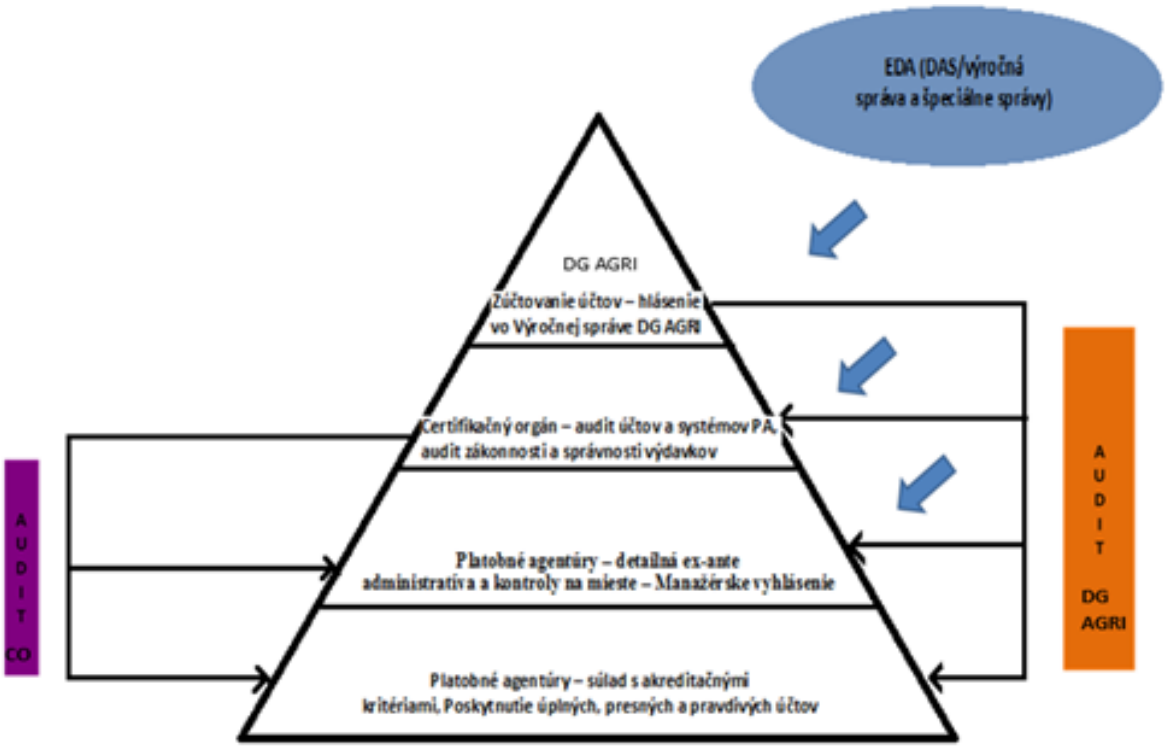
6. Popis aktuálneho stavu

Súčasná vláda SR považuje pôdohospodárstvo, potravinárstvo a lesníctvo za strategické odvetvia hospodárskej politiky štátu, ktoré majú nezastupiteľné miesto v štruktúre ekonomiky. Vo svojom programovom vyhlásení okrem iného uvádza: „Vláda si uvedomuje dôležitosť podpory rozvoja vidieka a zlepšovania životných podmienok vidieckeho obyvateľstva. Vláda považuje úspešné a transparentné čerpanie fondov Európskej únie za rozhodujúce vo vzťahu k poľnohospodárstvu a rozvoju vidieka."

K naplneniu vládnych zámerov a strategických cieľov Ministerstva pôdohospodárstva a rozvoja vidieka SR významným spôsobom prispieva Pôdohospodárska platobná agentúra (ďalej len „PPA"). Prostredníctvom svojich regionálnych pracovísk (ďalej len „RP PPA") je zároveň miestom kontaktu pre 41 571 žiadateľov o podporu v rezorte pôdohospodárstva.[1] V programovom období 2014 – 2020 PPA administruje finančné prostriedky štátneho rozpočtu a fondov EÚ v objeme 5 226 463 475,00 EUR.

PPA realizuje svoju činnosť v silne regulovanom prostredí. Vzhľadom na to, že 99 % výdavkov na Spoločnej poľnohospodárskej politike EÚ (ďalej len „SPP") je vyplácaných prostredníctvom členských krajín, Generálne riaditeľstvo pre poľnohospodárstvo a rozvoj vidieka Európskej komisie (ďalej len „DG AGRI") má zavedený veľmi prísny systém overovania zákonnosti a správnosti vyplatených finančných prostriedkov (obrázok 1).

Obrázok 1: Zdieľané riadenie výdavkov na SPP



Základnou podmienkou, aby PPA mohla administrovať podpory SPP, je udelenie akreditácie.[1] Na to, aby PPA mohla získať akreditáciu, musí spĺňať akreditačné kritériá v oblasti vnútorného prostredia (organizačná štruktúra, štandard ľudských zdrojov, delegovanie), kontrolných činností, informácií a oznamovania a monitorovania.

Pôdohospodárska platobná agentúra (ďalej len „platobná agentúra“) bola zriadená zákonom č. 473/2003 Z. z. o Pôdohospodárskej platobnej agentúre, o podpore podnikania v pôdohospodárstve a o zmene a doplnení niektorých zákonov v znení neskorších predpisov s účinnosťou od 1.12.2003. Základom platobnej agentúry sa stali regionálne odbory ministerstva pôdohospodárstva a rozvoja vidieka SR, k nim sa pripojila Intervenčná poľnohospodárska agentúra SR (IPA), ktorá sa zákonom zrušila a následne sa do platobnej agentúry začlenila aj Agentúra SAPARD, ktorá zabezpečovala vyplácanie podpory v rámci predvstupového programu SAPARD. Každá súčasť mala vybudovaný vlastný informačný systém, ktorý bolo potrebné zapracovať do jedného systému PPA. Uvedené informačné systémy boli budované na rôznych platformách a v rozličnom technologickom vybavení. Daný stav i v súčasnej dobe kladie vysoké požiadavky na udržiavanie stanovenej úrovne prevádzkovaných informačných systémov s efektívnym využitím finančných prostriedkov. Z dlhodobého pohľadu možno hovoriť o zastaranej technologickej infraštruktúry PPA.

Väčšina procesov v PPA je realizovaná s pomocou informačných a komunikačných technológií. Všetky tieto procesy (IT, právne, ľudské zdroje, finančné procesy a iné), ak majú byť vykonávané správne a v zmysle legislatívy, potrebujú využívať množstvo rôznych údajov, dát a informácií (informačné aktíva).

Každá činnosť PPA je úzko spojená s riadnym fungovaním IS a hardvérovej infraštruktúry, pričom bez dostatočných technologických kapacít by PPA nebola schopná zabezpečiť kľúčové činnosti spojené s vyplácaním platieb a komunikáciou medzi jednotlivými technologickými platformami.

Súčasná technologická platforma, na ktorej bežia jednotlivé IS PPA je na hranici svojich kapacít. Pravidelnou aktualizáciou a vývojom jednotlivých IS sa zvyšujú aj nároky na serverovú, databázovú a diskovú kapacitu hardvérového prostredia a tým sa vyvíja tlak na informačnú bezpečnosť.

V rámci sieťovej infraštruktúry PPA používa technologickú platformu, ktorá nespĺňa nároky na efektívne fungovanie súčasných procesov a kvalitné riadenie informačnej bezpečnosti. Z tohto dôvodu je nutné v prvej fáze aplikovať kvalitné riešenia a postupy pre maximálne využitie dát v definovanej problémovej oblasti a overenie definovaných spôsobov založených na dátovej vede a analytických prístupoch priamo v rozhodovaní v predmetnej oblasti, aplikovanie najlepších znalostí do procesov organizácie, ktorá na základe nich bude prijímať rozhodnutia a zavádzať modely dát a nástrojov, ktoré umožnia vytvárať analýzy, v ktorých je možné zlepšiť rozhodovanie. Táto skutočnosť vyvoláva naliehavú a nevyhnutnú potrebu riešiť zabezpečenie dostatočnej ochrany dát. Vyžaduje sa navrhnúť a implementovať komplexný systém riadenej informačnej bezpečnosti, ktorý zabezpečí ochranu aktív pred širokou škálou hrozieb s cieľom zabezpečiť kontinuitu činností, minimalizovať riziko krádeže alebo úniku údajov, ich zneužitia alebo neautorizovaných modifikácií.

Medzi kľúčové IS patria:

- IS – JRŽ spravuje základné kmeňové dáta o žiadateľoch. Z JRŽ sú posielané tieto údaje o žiadateľoch do jednotlivých IS. Z pohľadu spracovávania kmeňových dát ide o centralizovanú správu dát.
- IACS – je najväčším a najkomplexnejším IS PPA. Prebieha v ňom spracovávanie žiadostí o priame podpory. Technologicky je tento systém postavený na platforme Java. Avšak jeho staršie časti sú postavené na technológii, ktorá už nie je podporovaná.
- eKNM – IS využívaný na kontrolu podpôr. V súčasnosti nie je vybudovaný tak, aby bol plne prístupný z terénu na editáciu.
- AGIS SOT – Tento IS sa využíva na administrovanie trhových mechanizmov. Technologicky je systém postavený na dvoch platformách. Staršia je postavená na technológii Oracle Forms a nové súčasti sú naprogramované v Jave.
- AGIS PRV – je využívaný na administráciu projektových podpôr. Technologicky je postavený na platforme Java. V súčasnosti prebieha jeho integrácia.
- AGIS MFR – je využívaný na spracovanie žiadostí o platbu, započítavanie, nezrovnalostí a finančných vyrovnaní a vykazovanie na EK. Technologicky je postavený na platforme Java.
- AGIS ŠP – IS pre správu ŠP.
- ATIS – agrárny trhový informačný systém.

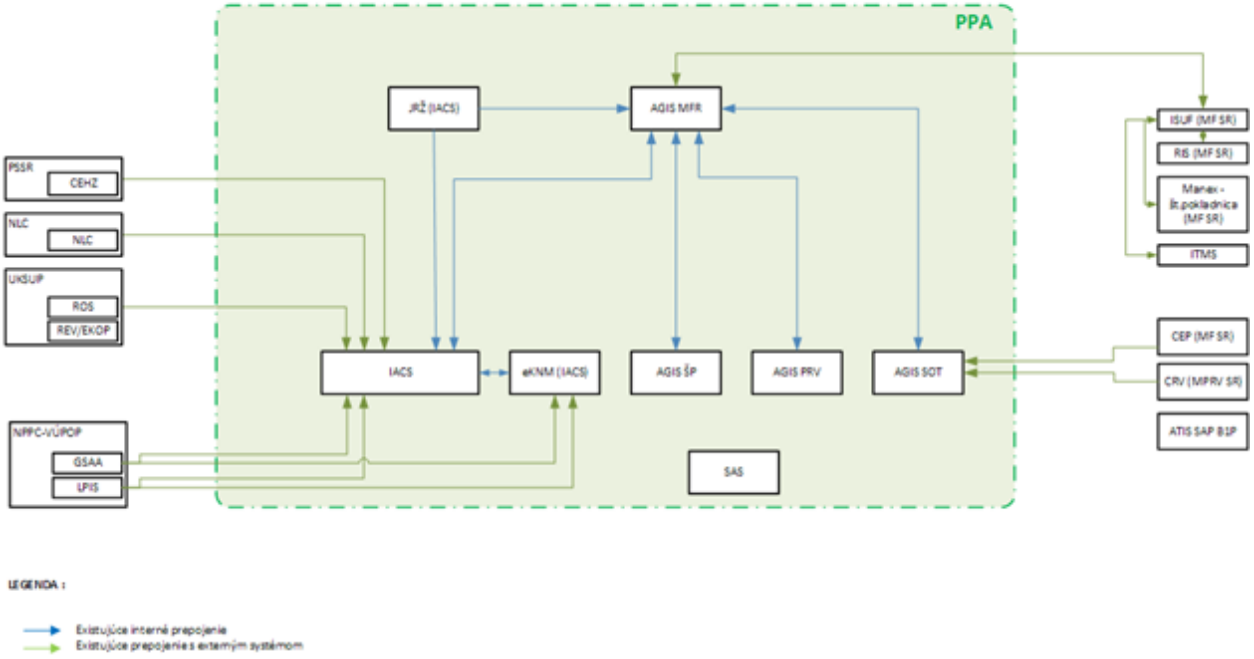
ITMS2014+ je platforma pre žiadosti, implementáciu a monitorovanie fondov EÚ, slúži žiadateľom zapojených do prípravy, administrácie, výberu, kontroly, analýzy, monitorovania a hodnotenia poskytovaných finančných prostriedkov z EŠIF. Skladá sa z verejnej a neverejnej zóny.

Ďalším kľúčovým IS PPA je ISUF - ISUF - integrovaný systém účtovania fondov - Integrovaný informačný systém účtovného, finančného a ekonomického riadenia prostriedkov. Účtovníctvo sa vedie v elektronickej forme s použitím softvéru SAP/R3 a je súčasťou informačného systému účtovania fondov EÚ. Systém ISUF je založený na spracovávaní procesov v prostredí SAP R/3 prostredníctvom viacerých modulov.

Logové hlásenia z jednotlivých IS sa replikujú na centrálny logovací server. Tým je zabezpečená nedotknuteľnosť a možnosť zmeny týchto záznamov dodávateľom. Chýba však automatizované vyhodnocovanie logových hlásení, nakoľko štruktúra logov je v každom IS rozdielna. Taktiež rozličnosť technológií sťažuje vyhodnocovanie týchto záznamov.

Súčasná technologická platforma, na ktorej bežia jednotlivé IS PPA je zastaraná. Z dôvodu neustálych legislatívnych zmien v jednotlivých agendových systémoch je nutné prispôsobovať a aktualizovať túto platformu a neustále tak vyvíjať jednotlivé IS, čím sa zvyšujú nároky na serverovú, databázovú a diskovú kapacitu hardvérového prostredia a je nutné zabezpečiť dostatočné technologické kapacity.

Súčasný stav IS PPA



6.0.1.

Významný finančný vplyv na prostriedky fondov majú zistenia z vyšetrovaní DG AGRI, z ktorých vyplývajú finančné korekcie. Na základe zistení z externých auditov a kontrol zameraných na overenie fungovania a výkon kontrolných činností pri plnení svojich úloh je PPA povinná prijať účinné opatrenia na zníženie miery chybovosti a dodržiavať legislatívu EÚ súvisiacu s SPP. Z analýzy príčin vysokej miery chybovosti za schémy EPFRV IACS a EPZF IACS ako aj zistení identifikovaných za oblasť EPFRV non-IACS nie je možné, aby samotná PPA prijala adekvátne opatrenia. Za účinné opatrenia považuje PPA predovšetkým zabezpečenie adekvátnych finančných zdrojov na dostatočné technické vybavenie, predovšetkým investície do IT systémov a navýšenie personálnych kapacít PPA.

[1] Delegované nariadenie Komisie (EÚ) č. 907/2014

[1] Údaj o počte registrovaných subjektov v Jednotnom registri žiadateľov, apríl 2018

6.1. Legislatíva

Tabuľka 4 Legislatíva – aktuálny stav

Súhrnný popis

Úvodné informácie
(Max. 1600 znakov, pre detailný popis je potrebné využiť prílohy)

PPA sa v súčasnosti riadi nasledovnými legislatívnymi zákonmi:

- Zákon č.280/2017 Z. z. o poskytovaní podpory a dotácie v pôdohospodárstve a rozvoji vidieka a o zmene zákona č. 292/2014 Z. z. o príspevku poskytovanom z európskych štrukturálnych a investičných fondov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
- Zákon č. 292/2014 Z. z. o príspevku poskytovanom z európskych štrukturálnych a investičných fondov a o zmene a doplnení niektorých zákonov,
- Zákon č. 543/2007 z 25. októbra 2007 o pôsobnosti orgánov štátnej správy pri poskytovaní podpory v pôdohospodárstve a rozvoji vidieka,
- Akreditačné kritéria definované delegovaným nariadením komisie (EÚ) č. 907/2014, ktorým sa dopĺňa nariadenie Európskeho parlamentu a Rady (EÚ) č. 1306/2013, pokiaľ ide o platobné agentúry a ostatné orgány, finančné hospodárenie, schvaľovanie účtovných závierok, zábezpeky a používanie eura,
- Pre riadenie informačnej bezpečnosti PPA používa medzinárodný štandard ISO/IEC 27001:2013,
- Definovanie bezpečnostných pravidiel je implementované v zmysle ISO/IEC 27002:2013,Všeobecný zákonný rámec pre oblasť IKT a údajov:
- Smernica Európskeho parlamentu a rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a
- informačných systémov v Únii.
- Vykonávacie nariadenie Komisie (EÚ) 2018/151 z 30. januára 2018, ktorým sa stanovujú pravidlá uplatňovania smernice Európskeho parlamentu a Rady
- (EÚ) 2016/1148, pokiaľ ide o bližšiu špecifikáciu prvkov, ktoré musia poskytovatelia digitálnych služieb zohľadňovať pri riadení rizík v oblasti bezpečnosti
- Zákon č. 69/2018 Z.z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov.
- Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov.
- Zákon č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente) v znení neskorších predpisov
- Zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov
- Výnos Ministerstva financií SR č. 55/2014 Z. z. o štandardoch pre informačné systémy verejnej správy v znení neskorších predpisov
- Zákon č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií) v znení neskorších predpisov
- Zákon č. 540/2001 Z. z. o štátnej štatistike v znení neskorších predpisov
- Vyhláška Štatistického úradu SR č. 306/2007 Z. z. ktorou sa vydáva Štatistická klasifikácia ekonomických činností
- Vyhláška Štatistického úradu SR č. 250/2017 Z. z., ktorou sa vydáva Program štatistických zisťovaní na roky 2018 až 2020 - povinnosti PPA v rámci štatistických zisťovaní
- Zákon č.69/2018 Z.z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov,
- a 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,
- Zákon č. 177/2018 Z.z. o niektorých opatreniach na znižovanie administratívnej záťaže využívaním informačných systémov verejnej správy a o zmene a doplnení niektorých zákonov (zákon proti byrokracii)
- Výnos Ministerstva financií SR č. 55/2014 o štandardoch pre informačné systémy verejnej správy, a výnos č. 137/2015 Z. z. ktorým sa mení a dopĺňa
- predošlý výnos č. 55/2014.
- Vyhláška NBÚ č. 164/2018 Z. z., ktorou sa určujú identifikačné kritériá prevádzkovanej služby (kritériá základnej služby).
- Vyhláška NBÚ č. 165/2018 Z. z., ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a
- podrobnosti hlásenia kybernetických bezpečnostných incidentov.
- Vyhláška NBÚ č. 166/2018 Z. z. o podrobnostiach o technickom, technologickom a personálnom vybavení jednotky pre riešenie kybernetických
- bezpečnostných incidentov.
- Vyhláška NBÚ č. 362/2018 Z. z. ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah
- všeobecných bezpečnostných opatrení.

Priestor pre sumárny obrázok / graf / diagram, nepovinná informácia.

Ďalšie informácie
(Max. 1600 znakov, pre detailný popis je potrebné využiť prílohy)

Riziká	**Spresnenie identifikovaných rizík:** *Odkazy na relevantné identifikátory rizík v prílohe Riziká.*

Stručná charakteristika identifikovaných rizík (Max. 400 znakov)

Prílohy	Diagramy, modely, obrázky v plnom rozlíšení
Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.	*Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.*

6.2. Architektúra

6.2.1. Biznis architektúra

Tabuľka 5 Biznis architektúra - aktuálny stav

Súhrnný popis
Úvodné informácie *(Max. 1600 znakov, pre detailný popis je potrebné využiť prílohy)* Popis súčasnej architektúry zachytáva IB a KyB v rámci PPA ako celku. Architektúra je popísaná z pohľadu: • Biznis architektúry – ide o zosumarizovanie výkonu biznis procesov ako preventívnych služieb v oblasti na prevenciu a detekciu kybernetických bezpečnostných incidentov a reaktívnych služieb v oblasti kybernetických bezpečnostných incidentov. Jedná sa o tie procesy, ktoré majú byť implementované v cieľovom stave. Zoznam procesov je konečný a každý z procesov je vyhodnotený z pohľadu, či je vôbec implementovaný a na druhej strane ako sa vykonáva. V rámci biznis architektúry sú zároveň popísané problémové oblasti a návrh na ich odstránenie. • Architektúry informačných systémov – predstavuje prehľad existujúcich informačných systémov a objektov evidencie, ktoré sú v daných informačných systémoch vedené. Zároveň sú popísané aj základné problémy vyplývajúce z nastavenej architektúry IS a definované návrhy na ich odstránenie. • Technologickej architektúry – z pohľadu technologického zabezpečenia je potrebné poznať súčasný stav najmä vo väzbe na budúce nastavenie technologickej architektúry a služieb, ktoré budú využívané. Rovnako je potrebné poznať existujúce limity a návrhy na ich odstránenie.
Priestor pre sumárny obrázok: ArchiMate štandardný viewpoint – „Product viewpoint", „Business Process Viewpoint"
Ďalšie informácie *(Max. 1600 znakov, pre detailný popis je potrebné využiť prílohy)* V nasledujúcej tabuľke je definovaný zoznam procesov, ktoré sú obligatórne v súvislosti s IB a KyB.. Zároveň je ku každému procesu, ktorý sa v súčasnosti v nejakej miere v organizácií vykonáva popísaný spôsob jeho výkonu.

Biznis proces	Úplnosť zavedenia [1]	Popis súčasného stavu pre daný proces
Vykonávanie preventívnych služieb, ktoré sú zamerané na prevenciu kybernetických bezpečnostných incidentov,	Čiastocne	V súčasnosti register JRŽ nie je integrovaný na žiadny referenčný register V súčasnej dobe sú zavedené v prostredí PPA antivírusové nástroja na produkčných serveroch a pracovných staniciach, sieťové firewally, systémy, centralizovaný systém riadenie prístupov s nepretržitým dohľadom
Vykonávanie reaktívnych služieb, ktoré sú zamerané na riešenie kybernetických bezpečnostných incidentov, poučovanie sa z bezpečnostných incidentov	Nezavedený	Uvedený proces nie je zavedený
Vytváranie bezpečnostného povedomia a vzdelávanie zamestnancov PPA	Nezavedený	Uvedený proces nie je zavedený
Nepretržité monitorovanie sieťovej bezpečnosti, detekcia bezpečnostných udalostí pomocou nástroja SIEM a nástroja na identifikovanie anomálií dátového toku a následná evidencia kybernetických bezpečnostných incidentov, ich odstraňovanie	Nezavedený	Uvedený proces nie je zavedený
Pravidelné posudzovanie stavu informačnej bezpečnosti, vykonávanie rizikovej analýzy, bezpečnostných auditov, gap analýz	Nezavedený	Uvedený proces nie je zavedený
Pravidelné a systematické posudzovanie súladu prostredia v PPA so zákonom o kybernetickej bezpečnosti a nariadením GDPR formou auditu	Nezavedený	Uvedený proces nie je zavedený
Vykonávanie penetračných testov	Nezavedený	Uvedený proces nie je zavedený
Vykonávanie pravideľnej klasifikácie informačných aktív,	Nezavedený	Uvedený proces nie je zavedený
Proces analytického spracovania dát pre účely detekcie podvodov	Nezavedený	Uvedený proces nie je zavedený
Pravidelné úprava a vylepšovanie bezpečnostnej dokumentácie, interných predpisov a pracovných postupov	Nezavedený	Uvedený proces nie je zavedený
Systematické testovanie plánov kontinuity a havarijných plánov	Nezavedený	Uvedený proces nie je zavedený
Proces automatickej transparentnej ochrany citlivých dát a informácií pomocou nástroja DLP	Nezavedený	Uvedený proces nie je zavedený
Proces systematického prideľovania privilegovaných prístupov interným používateľom aj externým dodávateľom pomocou nástroja na riadenie privilegovaných identít	Nezavedený	Uvedený proces nie je zavedený

[1] Jedná sa o mieru zavedenia v porovnaní s referenčnými procesmi manažmentu údajov definované v Strategickej priorite Manažment údajov

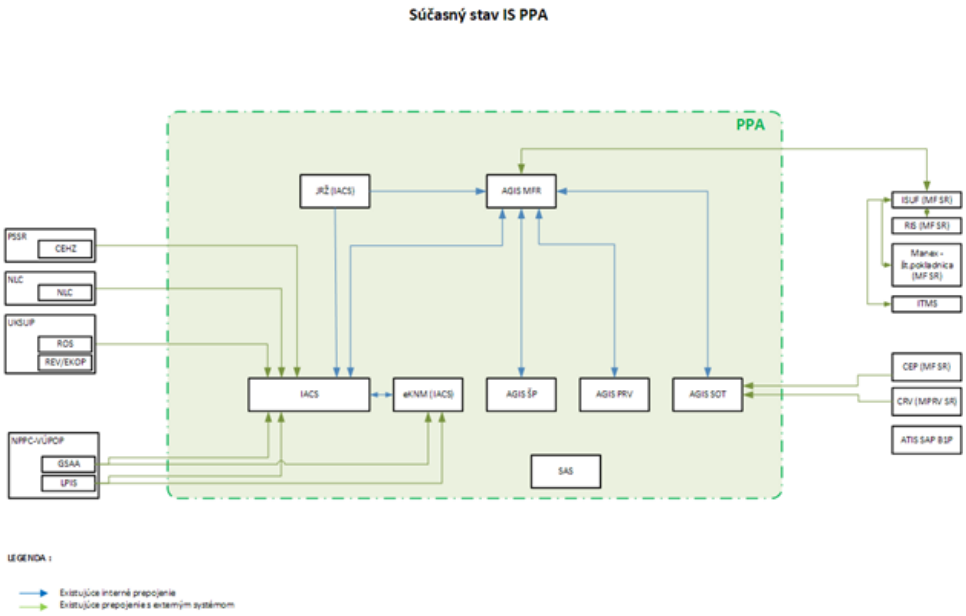
[A1]je to tak, existuje v PPA IDM alebo AD, treba to prípadne upraviť ?

Riziká	**Spresnenie identifikovaných rizík:** *Odkazy na relevantné identifikátory rizík v prílohe Riziká.*
Stručná charakteristika identifikovaných rizík (Max. 400 znakov)	

Prílohy	**Diagramy, modely, obrázky v plnom rozlíšení**
Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.	*Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.*

6.2.2. Architektúra informačných systémov

Tabuľka 6 Architektúra informačných systémov - aktuálny stav

Súhrnný popis
Úvodné informácie *(Max. 1600 znakov, pre detailný popis je potrebné využiť prílohy)* V tejto časti je popísaný súčasný stav vo väzbe na prevádzkovaný informačný systém. Pre účely rizikovej analýzy slúži informačný systém SAS , ktorý má špecifickú rolu a zabezpečuje samostatný funkčný celok s využitím dát z ostatných IS PPA. Systém je zahrnutý do údržby a plne podporovaný. Z pohľadu zabezpečenia cieľov tohto projektu sa počíta so zabezpečením podpory na ďalšie obdobie a rozšírením funkcionality na ostatné agendy. Z pohľadu zavedenia plnohodnotnej detekcie podvodov bude systém rozšírený o potrebné detekčné algoritmy, analytické modely a nevyhnutný transfer know-how zo strany dodávateľa/výrobcu.
Priestor pre sumárny obrázok: ArchiMate štandardný viewpoint – „Application Usage Viewpoint", „Application Co-operation Viewpoint"   
Ďalšie informácie *(Max. 1600 znakov, pre detailný popis je potrebné využiť prílohy)*

Riziká	**Spresnenie identifikovaných rizík:** *Odkazy na relevantné identifikátory rizík v prílohe Riziká.*
Stručná charakteristika identifikovaných rizík (Max. 400 znakov)	

Prílohy	**Diagramy, modely, obrázky v plnom rozlíšení**
Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.	*Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.*

6.2.3. Technologická architektúra

Tabuľka 7 Technologická architektúra - aktuálny stav

Súhrnný popis
Úvodné informácie *(Max. 1600 znakov, pre detailný popis je potrebné využiť prílohy)* Technologická architektúra dáva základné odpovede na otázky, ktorých zodpovedanie je potrebné pre budúce nastavenie technologickej architektúry. V súvislosti s realizáciou projektu bude nevyhnutné vyriešiť nasledovné problémy :

Problém	**Výber**	**Návrh riešenia**
Súčasné bezpečnostné systémy fungujú na zastaranej architektúre a nepokrývajú všetky informačné aktíva	þ	Nasadenia pokročilých bezpečnostných opatrení a sofistikovaných bezpečnostných mechanizmov, ktoré budú zaisťovať požadovanú úroveň ochrany všetkých bezpečnostne relevantných informačných aktív a IKT infraštruktúry PPA. Nasadenie prostriedkov a prvkov KyB ochrany a monitorovania, ktoré budú identifikovať možné bezpečnostné incidenty aj v reálnom čase
Infraštruktúra systémov PPA v súčasnosti obsahuje izolované prvky bezpečnostnej architektúry, ktoré primárne fungujú len na vybraných **zariadeniach a systémoch, teda nie sú nasadené plošne.**	þ	Zavedenie systému ochrany a bezpečnosti prevádzky informačných aktív a IKT infraštruktúry PPA, najmä použitím pokročilých bezpečnostných opatrení a sofistikovaných bezpečnostných mechanizmov a nástrojov, ktoré budú zaisťovať požadovanú bezpečnosť prevádzky a úroveň ochrany všetkých bezpečnostne relevantných informačných aktív a celej IKT infraštruktúry PPA.
Aktuálne systémy zabezpečenia a ochrany nespĺňajú všetky požiadavky legislatívy (najmä zákona o KyB)	þ	Aktualizácia interných aktov PPA a zabezpečenie súladu s požiadavkami aktuálnej legislatívy (najmä zákona o KyB) a prispôsobenie sa požiadavkám modernej a bezpečnej elektronickej verejnej správy.
Systémy nie sú prispôsobené na súčasné bezpečnostné požiadavky, čoho dôsledkom je, že nemusia byť identifikované všetky bezpečnostné incidenty.	þ	Implementácia nástrojov na ochranu dát, ich bezpečnú výmenu a komunikáciu. Vzdelávanie pre zamestnancov v oblasti kybernetickej a informačnej bezpečnosti

Priestor pre sumárny obrázok: ArchiMate štandardný viewpoint – „Infrastructure Usage Viewpoint", „Infrastructure Viewpoint"
Ďalšie informácie *(Max. 1600 znakov, pre detailný popis je potrebné využiť prílohy)*

Riziká	**Spresnenie identifikovaných rizík:** *Odkazy na relevantné identifikátory rizík v prílohe Riziká.*
Stručná charakteristika identifikovaných rizík (Max. 400 znakov)	

Prílohy	Diagramy, modely, obrázky v plnom rozlíšení
Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.	*Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.*

6.2.4. Bezpečnostná architektúra

Tabuľka 8 Bezpečnostná architektúra - aktuálny stav

Súhrnný popis	
Úvodné informácie *(Max. 1600 znakov, pre detailný popis je potrebné využiť prílohy)*	
Priestor pre sumárny obrázok / graf / diagram.	
Ďalšie informácie *(Max. 1600 znakov, pre detailný popis je potrebné využiť prílohy)*	
Riziká	**Spresnenie identifikovaných rizík:** *Odkazy na relevantné identifikátory rizík v prílohe Riziká.*
Stručná charakteristika identifikovaných rizík (Max. 400 znakov)	
Prílohy	**Diagramy, modely, obrázky v plnom rozlíšení**
Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.	*Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.*

6.3. Prevádzka

Tabuľka 9 Prevádzka - aktuálny stav

Súhrnný popis
Úvodné informácie *(Max. 1600 znakov, pre detailný popis je potrebné využiť prílohy)* V rámci prevádzky je súčasný stav nasledovný:

Služba/Požiadavka	**Aplikácia**	**Súčasný stav zabezpečenia**
Miera dostupnosti	þ	Prevádzka je realizovaná v dvoch lokalitách Hraničná a Devínska nová Ves.
Zálohovanie	þ	Príloha č. 1 k rozhodnutiu č. 93/2015 - Zálohovací predpis informačných systémov PPA
Podpora úrovne L1	þ	*Interná podpora z úrovne L1 (predovšetkým infraštruktúrne a technologické požiadavky)*
Podpora úrovne L2: aplikačná podpora	þ	*podpora z úrovne L2 je realizovaná internými a externými kapacitami*
Podpora úrovne L3	þ	*podpora z úrovne L3 (zabezpečovaná dodávateľmi jednotlivých riešení.)*
Počet interných pracovníkov, ktorí sa venujú podpore riešenia	þ	*2 AK pre IB a KyB*
Monitoring prevádzky	þ	*Realizované riešením Microsoft System Center Service Manager*
Kontinuálne zlepšovanie	þ	*Súčasné bezpečnostné systémy fungujú na zastaranej architektúre a nepokrývajú všetky informačné aktíva*
Bezpečnostný monitoring	þ	*Systémy nie sú prispôsobené na súčasné bezpečnostné požiadavky, čoho dôsledkom je, že nemusia byť identifikované všetky bezpečnostné incidenty.*
Realizovanie penetračných testov	þ	*Realizované internými a externými kapacitami*
Vykonávanie auditov, analýz a kontrol nezávislou treťou stranou	þ	*priebežné audity*
Riadenie incidentov	þ	*Infraštruktúra systémov PPA v súčasnosti obsahuje izolované prvky bezpečnostnej architektúry, ktoré primárne fungujú len na vybraných zariadeniach a systémoch, teda nie sú nasadené plošne*

Priestor pre sumárny obrázok / graf / diagram, nepovinná informácia.

Ďalšie informácie
(Max. 1600 znakov, pre detailný popis je potrebné využiť prílohy)

V súčasnosti je riešenie prostredí PPA realizovaná riešením Microsoft System Center Service Manager. Nižšie je popísaný celý proces od nahlásenia problému až po jeho uzavretie. Pre správne a efektívne fungovanie tohto procesu je dôležité používať pri mailovej komunikácii vždy len odpoveď resp. preposlanie na jednotlivé maily, aby sa zachovalo v predmete mailu jednoznačné číslo, ktoré identifikuje nahlásený problém.

Nahlásenie problému

Problém nahlasuje pracovník odbornej sekcie primárne v prostredí helpdesk portálu na web odkaze: http://helpdesk/Home. v príslušnej kategórii „Nefunguje /mám problém/problém s prevádzkou IS“.

Takto nahlásený problém dostane svoje unikátne číslo, na základe ktorého vieme riešenie problému jednoznačne identifikovať a na základe tohto čísla budeme viesť aj komunikáciu s dodávateľom. Číslo je vo formáte IRXXXXX, kde X sú číselné znaky.

Nahlasovateľ dostane notifikáciu o zaevidovaní jeho požiadavky a vidí podrobnosti nahláseného problému.

Priradenie problému riešiteľovi

Pracovník sekcie IT, ktorý má na starosti riešenie problémov s príslušným IS, si tento problém prevezme na riešenie a následne o tom dostane notifikáciu.

Monitoring

Cieľom monitorovania aktivít v informačných systémov v Pôdohospodárskej platobnej agentúre je výkon profylaxie s cieľom zistiť neautorizované aktivity a potencionálne hrozby IS PPA v súvislosti so spracúvaním informácií v súlade s ISO 27002 časť 10.10.

Monitoring aktivít v IS PPA vykonáva oddelenie informačnej bezpečnosti a správy kmeňových dát v pravidelných intervaloch s využitím existujúcich dostupných technológií.

Na všetkých pracovných staniciach a notebookoch musí byť zabezpečené monitorovanie aktivít cez existujúce technológie PPA (napr. TMG report, SCCM a pod.).

Zamestnanci sekcie informačných technológií sú povinní vykonávať záznamy do Help Desku, ktorý slúži ako zdroj riešenia bezpečnostných incidentov a zároveň sú povinní kontrolovať záznamy z HelpDesku ako možný zdroj bezpečnostných incidentov.

Zálohovanie

Organizácia má vypracovaný zálohovací predpis ktorý je uvedený v dokumente Príloha č. 1 k rozhodnutiu č. 93/2015 - Zálohovací predpis informačných systémov PPA. Predpis slúži pre riadené vytváranie a bezpečné ukladanie kópií údajov, programového vybavenia, konfiguračných a iných súborov, ktoré sa aktuálne vyskytujú v prostredí IS PPA.

Predmetom záloh sú určené médiá zaradené v skupinách podľa zálohovaných dát:

- Dokumenty PPA
- Domain Controllers
- Exhcange2013
- Hyper-V
- Mesačná
- PpaDpm01
- SAS Temp
- SQL_Db + System
- UsersFolders_Orto
- **Zálohovací softvér:**
- Microsoft Data Protection Manager 2012 R2 Verzia: 4.2.1338.0

Riziká	**Spresnenie identifikovaných rizík:** *Odkazy na relevantné identifikátory rizík v prílohe Riziká.*

Stručná charakteristika identifikovaných rizík (Max. 400 znakov)	
Prílohy	**Diagramy, modely, obrázky v plnom rozlíšení**
Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.	*Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.*

7. Alternatívne riešenia

7.1. Alternatíva A – „Názov"

Súhrnný popis
Úvodné informácie *(Max. 800 znakov)*
Priestor pre sumárny obrázok / graf / diagram, nepovinná informácia.
Ďalšie informácie *(Max. 800 znakov)*
Dôvod zamietnutia, alebo výberu riešenia (Max. 400 znakov)

7.2. Alternatíva B – „Názov"

Súhrnný popis
Úvodné informácie *(Max. 800 znakov)*
Priestor pre sumárny obrázok / graf / diagram, nepovinná informácia.
Ďalšie informácie *(Max. 800 znakov)*
Dôvod zamietnutia, alebo výberu riešenia (Max. 400 znakov)

8. Popis budúceho stavu

8.1. Legislatíva

Tabuľka 10 Legislatíva - budúci stav

Súhrnný popis	
Úvodné informácie *(Max. 1600 znakov, pre detailný popis je potrebné využiť prílohy)* Realizácia projektu si nevyžaduje legislatívne zmeny.	
Priestor pre sumárny obrázok / graf / diagram, nepovinná informácia.	
Ďalšie informácie *(Max. 1600 znakov, pre detailný popis je potrebné využiť prílohy)*	
Kritéria kvality	**Spresnenie kritérií kvality:** *Odkazy na relevantné identifikátory kritérií kvality v prílohe Kritéria kvality.*
Stručná charakteristika požadovanej kvality (Max. 400 znakov)	
Riziká	**Spresnenie identifikovaných rizík:** *Odkazy na relevantné identifikátory rizík v prílohe Riziká.*
Stručná charakteristika identifikovaných rizík (Max. 400 znakov)	
Prílohy	**Diagramy, modely, obrázky v plnom rozlíšení**
Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.	*Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.*

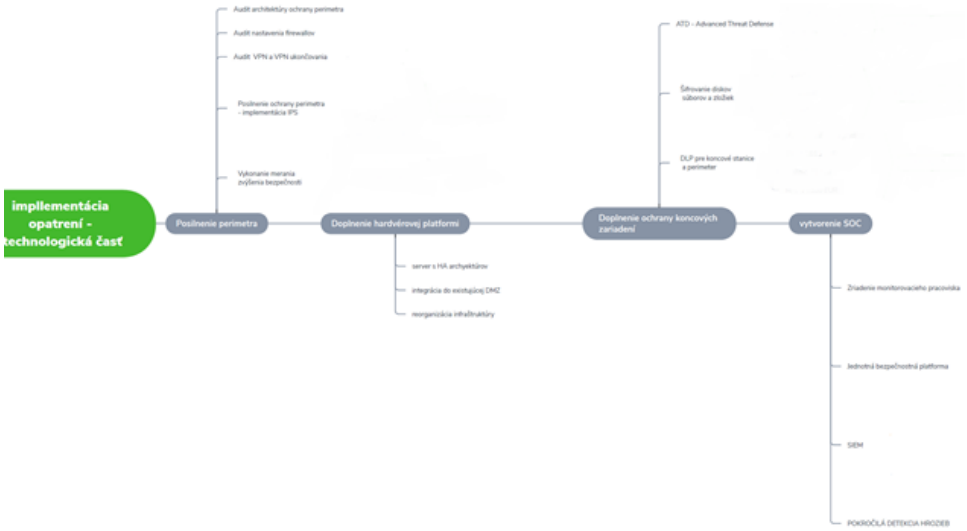
8.2. Architektúra

8.2.1. Biznis architektúra

Tabuľka 11 Biznis architektúra – budúci stav

Súhrnný popis
Úvodné informácie *(Max. 1600 znakov, pre detailný popis je potrebné využiť prílohy)* Budú vypracované a implementované bezpečnostné opatrenia. Samotný systém riadenia informačnej bezpečnosti bude implementovaný v súlade so štandardami platnými pre ISVS a bude spĺňať požiadavky Národnej koncepcie pre informatizáciu verejnej správy v súlade s požiadavkami Výnosu MF SR č. 55 /2014 Z.z. o štandardoch pre informačné systémy verejnej správy. Na základe vybudovaného Systému riadenia informačnej bezpečnosti môžu nasledovať ďalšie etapy ako napr. hardening serverov, vybudovanie operatívneho a bezpečnostného monitoringu, riadenie incidentov, implementovanie havarijných plánov a plánov kontinuity, alebo iné bezpečnostné projekty podľa potreby. Pre zabezpečenie dostatočnej ochrany bude navrhnutý a implementovaný komplexný systém informačnej bezpečnosti, ktorý zabezpečí ochranu aktív pred širokou škálou hrozieb s cieľom zabezpečiť kontinuitu činností, minimalizáciu rizika krádeže alebo úniku údajov, ich zneužitia alebo neautorizovaných modifikácií pred technologickými poruchami systémov, pred omylmi používateľov, pred nakazením pracovnej stanice vírusom alebo inštalovaním nelegálneho softvéru. Bezpečnostné hrozby môžu pochádzať od sofistikovaného útočníka na internete, ale hrozbu môže predstavovať aj zamestnanec svojim nezodpovedným správaním. Dobre nastavený systém riadenia bezpečnosti pomôže ochrániť aktíva pred všetkými týmito hrozbami. Na každé bezpečnostné riziko bude navrhnuté vhodné opatrenie. Realizácia projektu je návrh, vybudovanie a zavedenie systému riadenej informačnej (kybernetickej) bezpečnosti a implementácia vhodných a primeraných bezpečnostných opatrení: • vybudovanie, resp. zvýšenie úrovne informačnej bezpečnosti v PPA, to znamená vykonať všetky preventívne opatrenia, aby nedošlo k výskytu bezpečnostného incidentu • v prípade výskytu bezpečnostného incidentu, okamžitá detekcia a následné odstránenie problému • ochrana dôležitých a kritických informačných systémov • zabezpečenie dostupných kritických informačných systémov • zabezpečenie súladu s legislatívou SR • zabezpečenie zosúladenie so s legislatívou k ochrane osobných údajov • zvýšenie úrovne monitorovania, detekcie, analýzy a vyhodnocovania bezpečnostných udalostí a incidentov pomocou vhodnej technológie • zabezpečenie monitorovania privilegovaných prístupov (z interného aj externého prostredia)

Priestor pre sumárny obrázok: ArchiMate štandardný viewpoint – „Product viewpoint", „Business Process Viewpoint"



Ďalšie informácie
(Max. 1600 znakov, pre detailný popis je potrebné využiť prílohy)

Budú implementované nasledujúce technologické bezpečnostné opatrenia:

Riadené bezpečnostné služby (Managed Security Services), ktoré majú komplexný charakter, od architektúry bezpečnostných riešení, cez ich implementáciu, prevádzku, monitoring, aktualizácie a komplexné riadenie životných cyklov jednotlivých častí, priebežné testovanie, hodnotenie zraniteľností, udržiavanie funkčného a bezpečného stavu systémov s ohľadom na aktuálne hrozby a riziká, havarijné plánovanie a testovanie, riešenie bezpečnostných incidentov, konzultácie a forenzné analýzy.

Zoznam technológií spravovaných v rámci MSS

- Inteligentná ochrana koncových systémov voči neznámym hrozbám, Adaptive Threat Protection, Dynamické analýzy,
- Zabezpečenie súladu nastavení počítačov s normami (vrátane GDPR)
- Ochrana voči úniku citlivých dát - DLP (Data Loss Prevention)
- DLP ochrana na koncových počítačoch
- Riadené používanie vymeniteľných médií - DLP Device Control
- Riadené šifrovanie súborov, zložiek, vymeniteľných médií, celodiskové šifrovanie.
- Riadená klasifikácia citlivých dát
- DLP ochrana emailovej komunikácie
- DLP ochrana webovej komunikácie
- DLP ochrana na sieti
- Bezpečné zálohovanie dát – Backup
- Bezpečnosť emailovej komunikácie – Email Security
- Bezpečnosť webovej komunikácie – Web Security
- Ochrana publikovaných služieb, aplikačný firewall
- Sieťová bezpečnosť – Network Security
- Detekcia a ochrana voči prieniku - Intrusion Detection and Preventions
- Hodnotenie zraniteľností - Security Assessment and Analysis
- SIEM - Security Information and Event Monitoring
- Forenzné analýzy

Po organizačnej stránke budú zabezpečené nasledovné pozície:

Pozícia	Zabezpečené v projekte	Počet
IB špecialista	þ	1
KyB analytik	þ	1
Bezpečnostný špecialista	þ	1

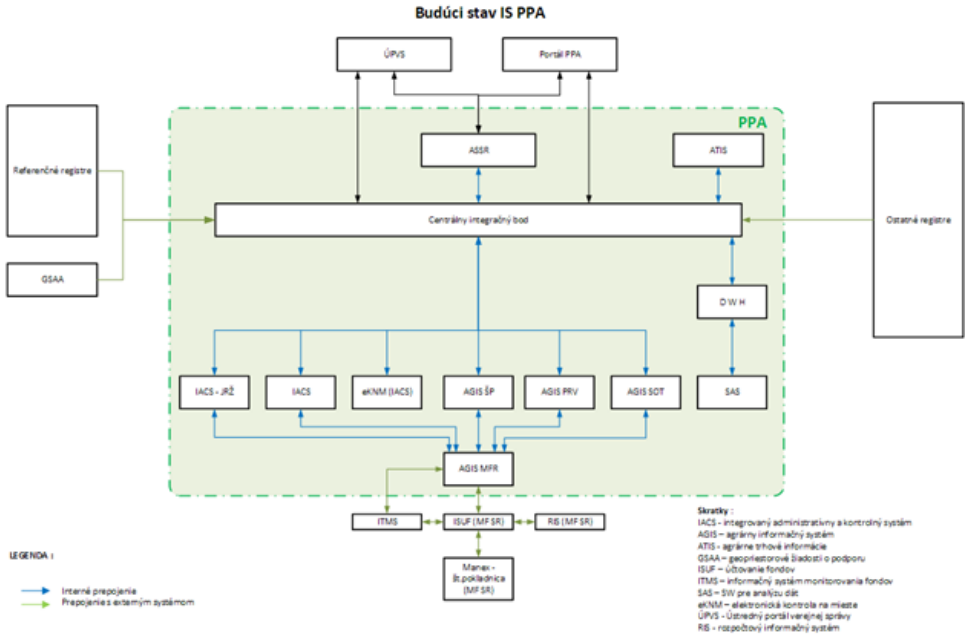
Kritéria kvality	**Spresnenie kritérií kvality:** *Odkazy na relevantné identifikátory kritérií kvality v prílohe Kritéria kvality.*
Stručná charakteristika požadovanej kvality (Max. 400 znakov)	

Riziká	**Spresnenie identifikovaných rizík:** *Odkazy na relevantné identifikátory rizík v prílohe Riziká.*
Stručná charakteristika identifikovaných rizík (Max. 400 znakov)	

Prílohy	**Diagramy, modely, obrázky v plnom rozlíšení**
Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.	*Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.*

8.2.2. Architektúra informačných systémov

Tabuľka 12 Architektúra informačných systémov - budúci stav

Súhrnný popis
Úvodné informácie *(Max. 1600 znakov, pre detailný popis je potrebné využiť prílohy)* Architektúra informačných systémov znázorňuje kompozíciu a integračné väzby systému s okolím: aké centrálne komponenty budú vytvorené a aké budú ich vlastnosti. Bezpečnostné hrozby môžu pochádzať od sofistikovaného útočníka na internete, ale hrozbu môže predstavovať aj zamestnanec svojim nezodpovedným správaním. Dobre nastavený systém riadenia bezpečnosti pomôže ochrániť aktíva pred všetkými týmito hrozbami. Na každé bezpečnostné riziko bude navrhnuté vhodné opatrenie. Budú implementované nasledujúce technologické bezpečnostné opatrenia. Zvýšenie schopnosti detekcie škodlivých aktivít a bezpečnostných incidentov • nástroj na monitorovanie a správu bezpečnostných udalostí SIEM, • nástroj na riadenie privilegovaných identít (PIM) • nástroj pre analýzu anomálií dátových tokov Ochrana dát, dátových prenosov a komunikácie • Systém voči úniku citlivých dát DLP Na nasledujúcom obrázku je znázornená architektúra IS po realizácii projektu:
Architektonické komponenty
Priestor pre sumárny obrázok: ArchiMate štandardný viewpoint – „Application Usage Viewpoint", „Application Co-operation Viewpoint" 
Prílohy	**Diagramy, modely, obrázky v plnom rozlíšení**

Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.	*Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.*

8.2.3. Technologická architektúra

Tabuľka 13 Technologická architektúra - budúci stav

Súhrnný popis	
Úvodné informácie *(Max. 1600 znakov, pre detailný popis je potrebné využiť prílohy)*	
Priestor pre sumárny obrázok: ArchiMate štandardný viewpoint – „Infrastructure Usage Viewpoint", „Infrastructure Viewpoint"	
Ďalšie informácie *(Max. 1600 znakov, pre detailný popis je potrebné využiť prílohy)*	
Prílohy	**Diagramy, modely, obrázky v plnom rozlíšení**
Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.	*Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.*

8.2.4. Implementácia a migrácia

Tabuľka 14 Implementácia a migrácia

Súhrnný popis	
Úvodné informácie *(Max. 1600 znakov, pre detailný popis je potrebné využiť prílohy)*	
Priestor pre sumárny obrázok: ArchiMate štandardný viewpoint – „Implementation and Migration Viewpoint"	
Ďalšie informácie *(Max. 1600 znakov, pre detailný popis je potrebné využiť prílohy)*	
Prílohy	**Diagramy, modely, obrázky v plnom rozlíšení**
Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.	*Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.*

8.2.5. Bezpečnostná architektúra

Tabuľka 15 Bezpečnostná architektúra - budúci stav

Súhrnný popis	
Úvodné informácie *(Max. 1600 znakov, pre detailný popis je potrebné využiť prílohy)*	
Priestor pre sumárny obrázok / graf / diagram.	
Ďalšie informácie *(Max. 1600 znakov, pre detailný popis je potrebné využiť prílohy)*	
Prílohy	**Diagramy, modely, obrázky v plnom rozlíšení**
Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.	*Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.*

8.3. Prevádzka

Tabuľka 16 Prevádzka - budúci stav

Súhrnný popis	
Úvodné informácie *(Max. 1600 znakov, pre detailný popis je potrebné využiť prílohy)* Realizácia riešenia si vyžiada zabezpečenie prevádzky, správy a údržby informačného systému v súlade s požiadavkami riadenia informačnej bezpečnosti. Prevádzka musí byť realizovaná v súlade s týmito predpismi: • Zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov; • Zákon č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente); • Výnos MV SR č. 525/2011 Z. z. o štandardoch pre elektronické informačné systémy na správu registratúry; • 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. • Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov. • Zákon č. 305/2013 o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o eGovernmente), v znení neskorších predpisov. • Zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov. • Smernica Európskeho parlamentu a rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii. • Vykonávacie nariadenie Komisie (EÚ) 2018/151 z 30. januára 2018, ktorým sa stanovujú pravidlá uplatňovania smernice Európskeho parlamentu a Rady • (EÚ) 2016/1148, pokiaľ ide o bližšiu špecifikáciu prvkov, ktoré musia poskytovatelia digitálnych služieb zohľadňovať pri riadení rizík v oblasti bezpečnosti sietí a informačných systémov, a parametrov na posudzovanie toho, či má incident závažný vplyv	
Priestor pre sumárny obrázok / graf / diagram, nepovinná informácia.	

Výsledok	**Výber**	**Popis výsledku**
zníži sa riziko prerušenia kritických procesov v PPA	þ	***súčasťou riadenia kontinuity procesov bude analýza rizík s opatreniami, ktoré budú minimalizovať možnosť narušenia kritických procesov a služieb***
zvýši sa úroveň dostupnosti systémov	þ	***stratégia ako súčasť riadenia kontinuity procesov popíše preventívne opatrenia na zabránenie výpadku systémov, aplikácií, služieb,***
zvýši sa úroveň ochrany dát a informácií	þ	***IS budú schopné odolať hrozbám (náhodným udalostiam) ale aj útokom (úmyselnému konaniu)***

zvýši sa úroveň integrity a autenticity údajov	þ	***každý uživateľ bude mať v zmysle základných bezpečnostných princípov a pravidieľ iba nevyhnutné privilégia a oprávnenia, systém na riadenie privilegovaných prístupov zaručí jednoznačný dôkaz za neoprávnenú modifikáciu údajov a súborov***
zlepšenie dobrej reputácie v dôsledku zníženia množstva bezpečnostných incidentov a ich dopadov na prevádzku	þ	***veľké percento udalostí a útokov bude odhalené a eliminované skôr než spôsobí vážne problémy***
zníži sa pravdepodobnosť platenia pokuty kvôli porušenia legislatívy	þ	***zosúladenie s kybernetickým zákonom a nariadením GDPR poskytne vedeniu PPA istotu, že v prípade kontroly alebo auditu nebude PPA udelená sankcia***
zníži sa pravdepodobnosť úniku citlivých (osobných, finančných) údajov	þ	***nasadením DLP systému a upravením procesov sa minimalizuje možnosť úniku citlivých dát***
školenia zabezpečia, že zamestnanci budú spoľahlivejší a budú viac chápať bezpečnostným hrozbám	þ	***zamestnanci sú najzraniteľnejší článok celého systému informačnej bezpečnosti***
ušetria sa finančné prostriedky, kvôli menšiemu počtu incidentov	þ	***rôzne zraniteľnosti, nedostatky a chyby budú odhalené ešte pred ich samotným zneužitím***
zníženia sa dôsledky incidentov,	þ	***dôsledkom z incidentu je že ho treba odstrániť a treba prijať preventívne opatrenia aby sa v budúcnosti opakovane nevyskytol***
kybernetická bezpečnosť ako katalyzátor zmien pomôže nových rozvojovým aktivitám	þ	***výsledkami analýz rizík môžu byť aj nové strategické projekty a iniciatívy*** ak o napr. digitálna transformácia, migrácia dát do cloudových služieb, využívanie mobilných zariadení ap.
s bezpečnosťou sa bude uvažovať už v úvodných fázach projektového vývoja nových aplikácií, systémov, čím sa znížia finančné náklady (v prípade zmien do bezpečnosti v neskorších etapách to už častokrát nie je možno, napr. zmena architektúry)	þ	***kybernetická bezpečnosť bude efektívne zvažovaná a posudzovaná ako integrálna súčasť každého procesu, každej zmeny***
Zvýši sa spokojnosť v agrosektore	þ	***bežní používatelia nebudú obmedzovaní a frustrovaní výpadkami a poruchami IS,***
Zvýši sa kvalita rozhodovania	þ	***vedenie IT bezpečnosti dostane dôležité vstupy na správne rozhodnutia***

8.4. Ekonomická analýza

Tabuľka 17 Ekonomická analýza - budúci stav

Súhrnný popis
Úvodné informácie *(Max. 1600 znakov, pre detailný popis je potrebné využiť prílohy)* **Čistá súčasná ekonomická hodnota (ENPV) =** 3 051 950 **Rok návratu investície (PBP) = 1** Ekonomické vyhodnotenie vychádza z realizovanej CBA, pričom výsledok predstavujú nasledovné ukazovatele a finančné toky:

Ukazovateľ efektivity	**Hodnota**	**Požadovaná hodnota**	**Vyhovuje**
Čistá súčasná hodnota (ENPV)	3 051 950	> 0 €	ÁNO
Ukazovatele ekonomickej výkonnosti pre životnosť projektu 3 roky	2,29	> 0 €	ÁNO
Vnútorné výnosové percento	5%	> 5.0 %	ÁNO
Doba návratnosti (3 roky trvá projekt)	1	< 10 rokov	ÁNO

Tabuľka 8: Prehľad ukazovateľov efektivity

Položka/Obdobie	**t1**	**t2**	**t3**
Náklad (€ s DPH)	2 400 000	646 800	550 800
Prínosy (€)	1 891 470	1 892 387	1 893 322
Finančný tok (€)	2 400 000	646 800	550 800

Na základe charakteru projektu, ktorý je definovaný v predchádzajúcich častiach štúdie, boli stanovené nasledovné náklady pre jednotlivé aktivity, pričom ku každej aktivite je stručne popísané zdôvodnenie stanovených nákladov pre danú aktivitu.

TCO	Spolu
SW produkty - sumár obstaranie	708000
SW produkty - sumár prevádzka	933 600
Aplikácie - sumár obstaranie	0
Aplikácie - sumár prevádzka	1 440 000
SW a Aplikácie - výstupné náklady	0
HW sumár obstaranie	300000
HW sumár prevádzka	144 000
Riadenie projektu	72 000
Spolu EUR s DPH	**3 597 600**

V rámci ekonomickej analýzy je kladený dôraz predovšetkým na definovanie prínosov navrhovaného projektu a to ako kvalitatívnych, tak aj kvantitatívnych. Zároveň sú v tejto časti definované aj náklady na realizáciu projektu pre jednotlivé aktivity. V nasledujúcej tabuľke je uvedené zaradenie projektu do finančného pásma, ktoré determinuje, či je potrebná detailná ekonomická analýza prostredníctvom CBA alebo postačuje len slovné vyhodnotenie a TCO analýza.

Celkové náklady	**Aplikácia**	**Miera závažnosti**
< 1,000,000.00 EUR s DPH		CBA nie je potrebná a v časti prínosov nie je potrebné vyčísliť jednotlivé prínosy
>= 1,000,000.00 EUR s DPH	þ	CBA je potrebná a v časti prínosov sú vyčíslené kvantitatívne prínosy

Priestor pre sumárny obrázok / graf / diagram, nepovinná informácia.

Ďalšie informácie
(Max. 1600 znakov, pre detailný popis je potrebné využiť prílohy)

V tejto časti sú popísané benefity ako aj riziká, ktoré vyplávajú z nerealizácie projektu. Prínosy sú definované do 5 základných kategórií a to:

- prínosy z prevencie incidentov (t. j. rôzne zraniteľnosti budú odhalené ešte pred samotným zneužitím). Tu odhadujeme, že v TOBE stave bude vďaka projektu možné odhaliť a tým pádom predísť väčšiemu počtu incidentov (expertný odhad je, že v súčasnosti je odhalených 5 % incidentov, pričom v TOBE stave bude vďaka projektu vyššia odhalenosť na úrovni 20 %). V prípade preventívne odhalených incidentov odhadujeme, že sa podarí zabrániť 60 % škodám. Tento odhad je prevzatý z CBA národného projektu CSIRT;
- prínosy zo zníženia dôsledkov incidentov, ktoré už nastali (odhalenie útoku ešte počas jeho priebehu, rýchle odstránenie chýb vedúcich k útoku atď). V tomto prípade odhadujeme, že sa zvýši počet incidentov, ktoré budú odhalené aj v kooperácii s CSIRT (rovnako ako pri preventívnych z 5 % na 10 %), pričom sa podarí zabrániť 20 % škodám. Tento odhad je polovičný oproti národnému projektu CSIRT (nie 20% ale 10%), pretože projekt má menší rozsah funkcionality v tejto oblasti oproti národnému projektu. pomocou škôd ako percenta z HDP. V prípade detegovaného incidnetu následne predpokladáme priemernú úsporu časti škody za daný incident. V prípade podielu škôd, ktorým sa zabránilo na základe detekcie (t. j. zistené ešte pred útokom) – 60 %, v prípade podielu škôd, ktorým sa zabránilo na základe reakcie (t. j. zistené už počas útoku) – 10 %
- (benefity z poučení do budúcnosti, zastavení priebehu útoku, zabránenie rovnakému útoku v budúcnosti).
- Výpočet výšky škôd (a tým pádom aj prínosov) je založený na výskume výšky škôd, ktoré kybernetické incidenty spôsobujú ekonomike. Táto výška je výskumom odhadovaná ako 0,8 % z národného HDP. Na základe súčasného počtu incidentov od národného CSIRT a odhade detekcie vieme následne určiť cenu incidentu a výšku zabránených škôd v súčasnom ako aj budúcom stave. Rozdiel týchto dvoch hodnôt predstavuje prínosy projektu, pričom v prípade reaktívnych incidentov je ako referenčná hodnota použitá výška HDP a v prípade preventívnych služieb je hodnotou výška štátneho rozpočtu. Výška ceny jedného incidentu je určená aj alternatívnym spôsobom ako rešerš priemernej ceny incidentu vo svete a následne bola normovaná podľa výšky HDP na obyvateľa. Výška škôd však v tomto prípade vychádzala pomerne vysoká, a preto ďalej vo výpočtoch konzervatívne používame cenu určenú
-

Vzhľadom na finančnú náročnosť projektu sú vyčíslené kvantitatívne prínosy z pohľadu ekonomickej hodnoty pre potreby Cost Benefit Analýzy. V nasledujúcich častiach sú rozpísané prínosy použité pre CBA.

Odhad úspory času vychádza z poznania súčasných procesov a náročnosti pričom v niektorých prípadoch môže ísť o úsporu viac než uvádzaných 50%, napriek tomu sa držíme konzervatívneho odhadu.

Kvalitatívne prínosy:

V tejto časti sú slovne popísané ďalšie prínosy, ktoré navrhované riešenie prináša:

- prínosy z prevencie incidentov (t. j. rôzne zraniteľnosti budú odhalené ešte pred samotným zneužitím). Odhad je, že vďaka projektu bude možné odhaliť a tým pádom predísť väčšiemu počtu incidentov (expertný odhad je, že v súčasnosti je odhalených 5 % incidentov, pričom vďaka projektu bude vyššia odhalenosť na úrovni 20 %). V prípade preventívne odhalených incidentov je odhad, že sa podarí zabrániť 60 % škodám. Tento odhad je prevzatý z CBA národného projektu CSIRT.
- prínosy zo zníženia dôsledkov incidentov, ktoré už nastali (odhalenie útoku ešte počas jeho priebehu, rýchle odstránenie chýb vedúcich k útoku atď). V tomto prípade je odhad, že sa zvýši počet incidentov, ktoré budú odhalené aj v kooperácii s CSIRT (rovnako ako pri preventívnych z 5 % na 10 %), pričom sa podarí zabrániť 20 % škodám. Tento odhad je polovičný oproti národnému projektu CSIRT (nie 20% ale 10%), pretože je predpoklad, že dopytové projekty budú mať menší rozsah funkcionality v tejto oblasti oproti národnému projektu.
- Výpočet prínosov pri projektoch tohto typu je zo svojej podstaty vždy iba odhadom (ako to je aj v tomto prípade), pričom to záleží najmä od incidentov, ktoré už nastali, boli zachytené a vyhodnotené v minulom období. Jednoznačným trendom je, že početnosť, sofistikovanosť a dopad kybernetických incidentov stále narastá.

8.5. Riziká

Riziko	Aplikácia	Miera závažnosti	Spôsob mitigácie
Náklady na prevádzku budú vyššie ako plánované resp. sa vymknú spod kontroly	þ	**Veľmi nízka**	*V súčasnosti PPA už využíva agendový systém a pozná doterajšiu úroveň nákladov na prevádzku*
Projekt nedosiahne očakávané prínosy	þ	**Veľmi nízka**	*PPA už v súčasnosti využíva rizikovú analýzy s preukázateľnými prínosmi a očakávame rovnakú úspešnosť aj pri rozšírení rizikovej analýzy na ostatné agendy. Vďaka internému know how vieme kontrolovať riziko.*
Nebudú k dispozícii údaje, aby sa dali overiť prínosy	þ	**Veľmi nízka**	*Dáta, ktoré potrebujeme včleniť do agendového systému sú k dispozícii len sa ešte nevyužívajú*
Náklady na implementáciu budú vyššie ako plánované resp. sa vymknú spod kontroly	þ	**Veľmi nízka**	*Odhadované náklady zodpovedajú náročnosti a nákladom vynaloženým na zavedenie existujúceho procesu rizikovej analýzy*
Neskúsení členovia tímu	þ	**Veľmi nízka**	*Požadované aktivity budú zabezpečené externými certifikovanými špecialistami*

Tabuľka 10: Ekonomické riziká

9. Časový rámec projektu

9.1. Harmonogram výstupov / míľnikov

V nasledujúcej tabuľke je znázornené, ako budú míľniky resp. výstupu dodávané v čase:

Aktivita	Aktivita podľa príručky	Míľnik / Výstup	Kvartál	Rok
A1 – A10	Analýza a návrh	Analýza existujúce stavu a návrh bezpečnostných opatrení	Q2	2020
	Nákup HW a SW	Obstaranie definovaných nástrojov, HW a SW	Q3	2020
	Implementácia	Implementácia riešenia, tvorba pravidiel a modelov, vytvorenie funkcionality podľa výstupov analýzy.	Q4	2020
	Testovanie	Nasadenie nástrojov / HW do testovacej prevádzky.	Q4	2020
	Nasadenie	Nasadenie do ostrej prevádzky / produkčného prostredia.	Q1	2021

Tabuľka 11: Harmonogram projektu

9.2. Harmonogram realizácie aktivít – GANT

Na nasledujúcej schéme je znázornené časové trvanie jednotlivých aktivít:

Výstup/funkcionalita projektu	Popis	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12	M13	M14
Aktivita															
Analýza a návrh						1									
Nákup HW a SW															
Implementácia															
Testovanie											1	1	1		
Nasadenie														1	

Prílohy

Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.