Ministerstvo financií Slovenskej republiky
Sprostredkovateľský orgán OPIS

Európska únia

Strategická priorita Bezpečnosť

Pracovná verzia

(Verzia 0.2)

Informácia o dokumente

Názov:	Strategická priorita Bezpečnosť
Stav:	Pracovná verzia
Pripravil:	AKVS
Verzia:	0.2
Dátum:	7.12.2015
Pripomienkoval:	AKVS
Dátum revízie:	29.1.2016

Distribučný zoznam

Od	Dátum	Kontakt

Pre	Akcia*	Dátum (do)	Kontakt

** Akcia: Schváliť, Pripomienkovať, Informovať, Realizovať, iné (uveďte)*

História verzií

Verzia	Dátum verzie	Pripravil/ Zmenil	Pripomienkoval	Kľúčové zmeny
0.1	13.7.2015			Úvodné predstavenie strategickej priority
0.2	30.9.2015			Draft na pripomienky MF

Obsah

1 Úvod

Národná koncepcia informatizácie verejnej správy (2016) ustanovuje 10 strategických priorít informatizácie verejnej správy:

1 Multikanálový prístup
2 Interakcia s verejnou správou, životné situácie a výber služby navigáciou
3 Integrácia a orchestrácia
4 Rozvoj agendových informačných systémov
5 Využívanie centrálnych spoločných blokov
6 Riadenie údajov a Big data
7 Otvorené údaje
8 Vládny cloud
9 Komunikačná infraštruktúra
10 Informačná a kybernetická bezpečnosť

NKIVS ku každej strategickej priorite informatizácie verejnej správy vysvetľuje jej cieľ, prístup k riešeniu a tiež rámcový architektonický model.

Tento dokument predstavuje prvý návrh a high-level analýzu priority informatizácie verejnej správy **Informačná a kybernetická bezpečnosť upravenú v kapitole 6.2.10 NKIVS,** pripravenú v rámci Architektonickej kancelárie verejnej správy. Dokument ešte môže byť z pozície architektonickej kancelárie verejnej správy upravovaný a dopĺňaný aj na základe pripomienok a komunikácie s gestorom tejto strategickej priority.

Zodpovednosť za ďalšie detailné riešenie konkrétnej priority, vypracovanie štúdie jej realizovateľnosti a následnú realizáciu formou zabezpečenia implementácie príslušného projektu, resp. projektov, má gestor podľa jemu prislúchajúcej kompetencie.

Strategická priorita Bezpečnosť predstavuje základný a kľúčový komponent navrhovanej cieľovej architektúry 2020. Vytvorenie prostredia bezpečného pre občana, podnikateľa aj verejnú správu je jedným zo základných cieľov celej budovanej vízie architektúry. Medzi základné úlohy oblasti patrí najmä:

- Zabezpečenie primeranej ochrany a úrovne bezpečnosti informačných aktív, IS VS a poskytovaných elektronických služieb formalizovaným riadením informačnej bezpečnosti. Predchádzanie a riadenie bezpečnostných incidentov formálnym riadením rizík.
- Bezpečnosť a ochrana digitálneho a kybernetického priestoru, monitoring a proaktívna ochrana kritickej infraštruktúry štátu.
- Budovanie komplexnej bezpečnostnej architektúry, ktorá bude založená na rovnakých princípoch a úrovniach bezpečnosti tak na centrálnej, ako aj na rezortných a lokálnych úrovniach.

Tento dokument definuje základný návrh riešenia a prístup k riešeniu strategickej priority informatizácie verejnej správy, ktorou je oblasť informačnej a kybernetickej bezpečnosti.

1.1 Skratky a definície

1.1.1 Skratky

Skratka	Popis
IB	Informačná bezpečnosť
IS VS	Informačný systém verejnej správy
KIBVS	Kancelária informačnej bezpečnosti verejnej správy

Skratka	Popis
KyB	Kybernetická bezpečnosť
NBÚ	Národný bezpečnostný úrad
SKI	Spoločná komunikačná infraštruktúra
SP	Strategická priorita
VS	Verejná správa

2 Predstavenie a cieľ priority

Zaistenie informačnej a kybernetickej bezpečnosti naprieč celým spektrom vybudovanej technologickej infraštruktúry štátu predstavuje dlhodobý kľúčový cieľ, osobitne zohľadnený aj v rámci programového obdobia 2014-2020. Všetky základné ciele stanovené pre cieľovú architektúru 2020 sú kriticky závislé od dôveryhodného a bezpečného prostredia, v ktorom budú prevádzkované, a ktorým budú zároveň chránené.

Vízia rozvoja sa zameriava na niekoľko základných oblastí bezpečnosti, z ktorých najvýznamnejšie sú:

- služby správy a riadenia informačnej bezpečnosti,
- služby zaistenia kybernetickej bezpečnosti,
- služby akreditácie a certifikácie a
- služby zaistenia súladu s regulačnými predpismi.

Z pohľadu definovania základných politík a pravidiel pre správu a riadenie informačnej bezpečnosti v rámci IS VS bude potrebné, v súčinnosti s Národným bezpečnostným úradom (ďalej len „NBÚ“), ako gestorom pre oblasť kybernetickej bezpečnosti, zabezpečiť správu, definovanie a publikovanie základných bezpečnostných politík a štandardov pre všetky sub-oblasti informačnej bezpečnosti vrátane dozoru a kontroly v rámci inštitúcií verejnej správy vo forme auditovania a rovnako aj zabezpečenia procesu výkonu akreditácií a certifikácií v jednotlivých oblastiach bezpečnosti. Pre tento účel by mala byť v rámci verejnej správy zriadená osobitná kancelária informačnej bezpečnosti verejnej správy, ktorá bude plne pokrývať oblasti:

- riadenia a metodiky,
- akreditácie a certifikácie,
- auditu,
- bezpečnostnej architektúry,
- bezpečnosti pre cloud a
- bezpečnosti pri riadení zmluvných vzťahov.

Z pohľadu ochrany kybernetického priestoru sa rozvoj zameria v prvom rade na definovanie a sprevádzkovanie služieb, ktoré zaistia bezpečnosť a ochranu kybernetického priestoru, s primárnym zameraním na ochranu kritickej infraštruktúry SR. Všetky činnosti súvisiace s riadením, rozvojom a správou oblasti kybernetickej bezpečnosti, ako aj monitoringom kritickej infraštruktúry, vyšetrovaním a aktívnou obranou budú v kompetencii NBÚ a plánovanej organizačnej jednotky kybernetickej bezpečnosti v gescii NBÚ.

Oblasť informačnej a kybernetickej bezpečnosti bude potrebné rozvíjať na centrálnej úrovni ale rovnako aj na úrovni jednotlivých povinných osôb a na úrovni konkrétnych riešení – informačných systémov, aplikácií, mobilných zariadení a iných IKT riešení.

2.1 Stakeholderi a ich záujmy

Oblasť bezpečnosti sa prierezovo dotýka všetkých poskytovaných služieb na všetkých úrovniach. Z tohto dôvodu sú touto oblasťou dotknuté všetky relevantné strany v rámci navrhovanej strategickej architektúry.

2.1.1 Občan

Základnou požiadavkou z pohľadu občana je možnosť bezpečného prístupu a využívania budovaných elektronických služieb štátu a zároveň uistenie, že jeho citlivé informácie a dáta budú spracúvané tak, aby nebola ohrozená ich dôvernosť a integrita.

- Ochrana citlivých dát a informácií spracúvaných a uložených v rámci ISVS.
- Zaistenie bezpečného procesu identifikácie a autentifikácie voči ISVS.
- Zabezpečenie procesu autorizácie rozhodnutí občanom v rámci ISVS.

2.1.2 Prevádzkovatelia IS

Z pohľadu prevádzkovateľov jednotlivých IS je informačná bezpečnosť kľúčovou pre zaistenie bezpečného a plynulého fungovania budovaných služieb. Jednotlivé organizácie nevyhnutne potrebujú bezpečné a dôveryhodné prostredie ktoré zaručí, že svoje služby môžu poskytovať v požadovanom čase a kvalite.

- Vybudovanie bezpečnej infraštruktúry pre poskytovanie služieb v gescii prevádzkovateľa a jej následná ochrana pred neželaným narušením bezpečnosti infraštruktúry a spracúvaných dát.
- Zaistenie integrity, dostupnosti a dôvernosti dát v závislosti od ich typu a spôsobu ich použitia.

2.1.3 Ústredné orgány dohliadajúce na oblasť IB (MF SR a NBÚ)

- Centralizácia bezpečnostných riešení s priamym dopadom na ochranu kritických prvkov infraštruktúry prevádzkovateľa, respektíve štátu.
- Vybudovanie jednotnej architektúry umožňujúcej zosúladenie dodržiavania bezpečnostných požiadaviek naprieč orgánmi VS – vytvorenie a dohľad nad tzv. základnou úrovňou bezpečnosti, ktorú musí dodržiavať každý orgán VS.
- Zabezpečenie kybernetickej ochrany štátu.

3 Návrh stratégie riešenia

3.1 Organizačný pohľad

Stratégia riešenia sa zameriava najmä na vybudovanie a prepojenie odborných kapacít v jednotlivých navrhovaných oblastiach. Vytvorenie Útvaru kybernetickej bezpečnosti pod NBÚ a kancelárie bezpečnosti VS vytvorí základ pre prácu expertných skupín zameraných na reálny výkon činností potrebných pre zaistenie bezpečnosti či už v rámci ISVS, ale aj v rámci ochrany kritickej infraštruktúry štátu.

Z pohľadu organizácie a usporiadania tejto priority je možné oblasť informačnej a kybernetickej bezpečnosti rozdeliť na tri základné úrovne:

- úroveň centrálnej správy,
- úroveň centralizovaných nástrojov a podmienok na podporu riadenie bezpečnosti v rámci jednotlivých povinných osôb,
- lokálnu úroveň špecifickú pre konkrétny rezort, resp. inštitúciu verejnej správy a jej informačné systémy.

Úroveň centrálnej správy zahŕňa najmä definovanie základných politík, pravidiel a normatívnych dokumentov, ktoré umožnia vytvorenie jednotného bezpečného prostredia v definovaných úrovniach bezpečnosti. Takáto centrálna správa umožní jednoduché porovnanie a vyhodnocovanie bezpečnosti v ľubovoľnom systéme, resp. organizácii a umožní tak rýchlo a efektívne navrhnúť na lokálnej úrovni vhodné mechanizmy a postupy, ktoré zaistia bezpečnosť prevádzkovanej infraštruktúry a spracúvaných dát.

Na úrovni centralizovaných nástrojov a podmienok pre podporu riadenia a výkonu IB sa predpokladá vybudovanie a prevádzka centrálnych systémov umožňujúcich riadenie informačnej bezpečnosti tak na centrálnej úrovni štátu, ako na úrovni pripojených organizácií. Typickým príkladom je napríklad vytvorenie nástroja na centrálny monitoring siete, potrebného tak pre riadenie prevádzky, ako aj pre monitoring z pohľadu ochrany kybernetického priestoru krajiny. K takýmto nástrojom môžu priamo pristupovať a využívať ich správcovia na úrovni povinných osôb, ktorí ich môžu začleniť do svojej bezpečnostnej architektúry a sprístupniť okrem iného aj na centrálnej úrovni samostatným zložkám, napr. kybernetickej ochrany.

Najnižšia úroveň bude realizovaná samotnými povinnými osobami, ktoré budú povinné vytvoriť vlastnú bezpečnostnú architektúru v súlade s centrálnymi pravidlami, ale aj osobitnými požiadavkami špecifickými pre každý rezort, resp. inštitúciu. Dohľad nad budovaním takýchto architektúr bude vykonávať centrálna architektonická kancelária v správe MF SR, samotná realizácia a prevádzka ale už bude plne v gescii jednotlivých organizácií.

3.1.1 Strategický prístup k riešeniu

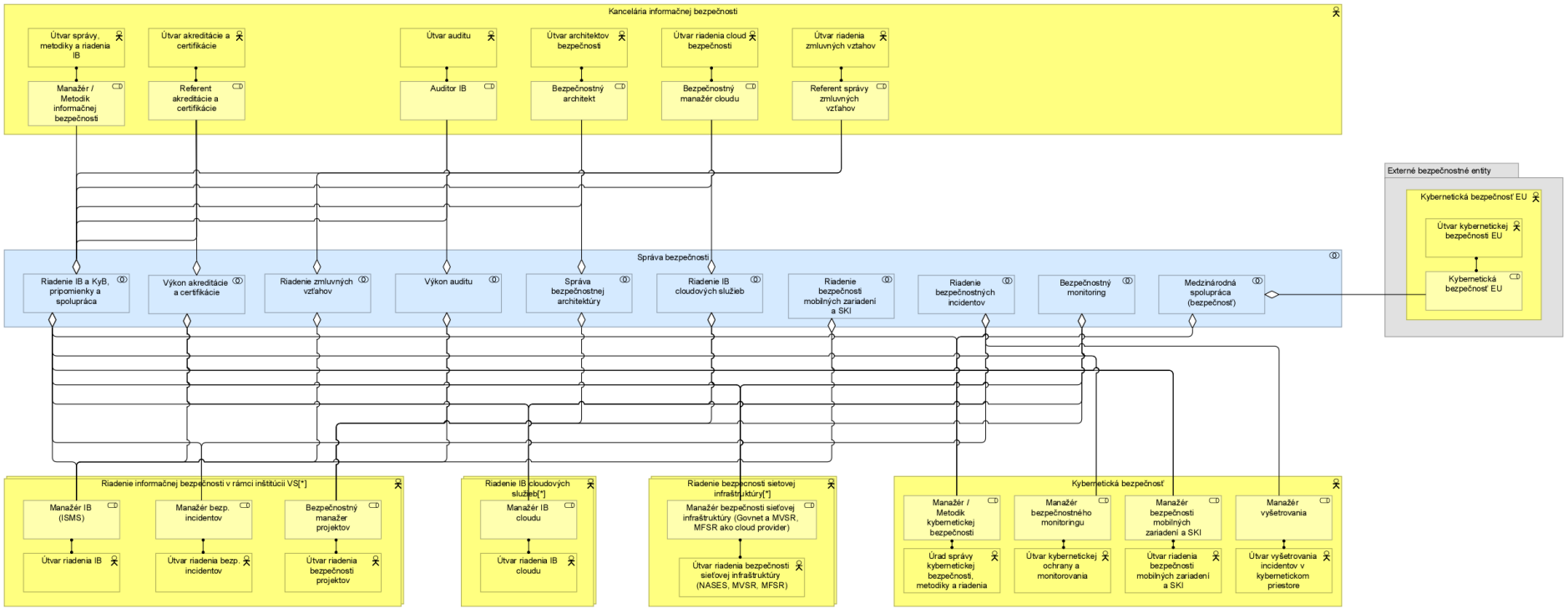
Podobne ako správa architektúry VS, aj správa informačnej a kybernetickej bezpečnosti VS by mala byť riešená kaskádovým spôsobom. Na najvyššej úrovni musí existovať centrálna entita s medzirezortnou pôsobnosťou (kancelária informačnej bezpečnosti verejnej správy – KIBVS), ktorá je vlastníkom a správcom strategickej bezpečnostnej architektúry verejnej správy a zároveň sa podieľa na metodickom riadení informačnej bezpečnosti („IB“) v rámci celej verejnej správy. Okrem uvedených dvoch základných funkcií plní aj iné „centrálne“ úlohy, ako je napr. metodické riadenie a udeľovanie akreditácií a certifikácií v oblasti informačnej bezpečnosti, metodické riadenie a zabezpečovanie výkonu auditov informačnej bezpečnosti, metodické riadenie a usmerňovanie informačnej bezpečnosti v rámci cloud datacentier verejnej správy a centrálna správa zmluvných vzťahov (súvisiacich s informačnou bezpečnosťou) medzi jednotlivými poskytovateľmi eGov služieb verejnej správy.

Samotný výkon riadenia IB a realizácia konkrétnych opatrení informačnej bezpečnosti je ponechaný na jednotlivé inštitúcie verejnej správy, správcov sieťových komunikačných infraštruktúr (najmä ÚVSR ako správcu siete Govnet, MVSR ako správcu siete MVNet a MFSR ako správcu siete MFNet) a správcov cloud datacentier verejnej správy (MFSR a MVSR).

Okrem výkonu riadenia IB je potrebné na centrálnej úrovni zabezpečiť aj aktivity a úlohy súvisiace s ochranou digitálneho a kybernetického priestoru (najmä v súvislosti s ochranou kritickej infraštruktúry SR a v súvislosti

s medzinárodnou spoluprácou v oblasti bezpečnosti digitálneho a kybernetického priestoru), s centrálnym bezpečnostným monitoringom a centrálnou správou bezpečnosti mobilných zariadení používaných vo verejnej správe. Ide o aktivity, ktoré dnes čiastočne zastrešuje CSIRT SK, ktorý je súčasťou organizácie DataCentra MFSR. Uvedené aktivity by však vzhľadom na aktuálne schválenú koncepciu kybernetickej bezpečnosti mali prejsť pod NBÚ, ktorý by mal okrem roly Manažér kybernetickej bezpečnosti útvaru správy kybernetickej bezpečnosti, zabezpečiť aj výkon navrhovaných ďalších troch útvarov. Ide o činnosti a funkcie, ktoré by mal zastrešiť navrhovaný útvar kybernetickej ochrany a monitorovania, útvar vyšetrovanie incidentov v kybernetickom priestore a útvar bezpečnosti mobilných zariadení a spoločnej komunikačnej infraštruktúry (SKI).

Grafický návrh organizačnej štruktúry, jednotlivých rolí, príslušných zodpovedností a činností KIBVS a útvaru správy a riadenia KyB pod NBÚ je znázornený na nasledujúcom obrázku.



Obrázok 1: Štruktúra správy bezpečnosti VS SR - detail

V nasledujúcej tabuľke je uvedený stručný popis jednotlivých rolí KIBVS a útvaru správy a riadenia KyB pod NBÚ spolu s uvedením odporúčaného minimálneho „štartovacieho“ počtu FTE. Úlohou jednotlivých rolí bude najmä vytvoriť personálne, materiálne, technické, organizačné a iné podmienky pre plnohodnotné naštartovanie činnosti a realizáciu konkrétnych úloh jednotlivých navrhovaných útvarov a doplnenie týchto útvarov o adekvátny počet pracovníkov zabezpečujúcich výkon jednotlivých činností.

Funkcia (útvar)	Dop. min. FTE	Rola	Stručný popis
Na úrovni KIBVS			
Útvar správy, metodiky a riadenia IB	1	Manažér informačnej bezpečnosti	Správa a riadenie informačnej bezpečnosti verejnej správy.
	1	Metodik IB	Správa a riadenie informačnej bezpečnosti verejnej správy, najmä príprava a definovanie metodík, politík, štandardov, regulácií a pod.
Útvar akreditácie a certifikácie	0,5	Referent akreditácie a certifikácie	Správa a definovanie procesu a požiadaviek akreditácie a certifikácie a udeľovanie akreditácií a certifikácií v oblasti informačnej bezpečnosti.
Útvar architektov bezpečnosti	1	Bezpečnostný architekt	Riadenie bezpečnostnej enterprise architektúry verejnej správy.
Útvar auditu IB	1	Audítor IB	Správa a definovanie procesu a požiadaviek auditu v oblasti informačnej bezpečnosti.
Útvar riadenia cloud bezpečnosti	1	Bezpečnostný manažér cloudu	Správa a usmerňovanie bezpečnosti v rámci cloud datacentier verejnej správy.
Útvar riadenia zmluvných vzťahov	0,25	Referent správy zmluvných vzťahov	Správa a definovanie požiadaviek na zmluvné vzťahy medzi poskytovateľmi služieb (najmä SLA a NDA).
Spolu:	**5,75**		
Na úrovni entity kybernetickej bezpečnosti a bezpečnostného monitoringu pod NBÚ			
Útvar správy kybernetickej bezpečnosti, metodiky a riadenia	1	Manažér kybernetickej bezpečnosti	Správa a riadenie kybernetickej bezpečnosti verejnej správy.
	1	Metodik KyB	Správa a riadenie kybernetickej bezpečnosti verejnej správy, najmä príprava a definovanie metodík, politík, štandardov, regulácií a pod.
Útvar vyšetrovania incidentov	0,5	Manažér vyšetrovania	Správa a metodické riadenie vyšetrovania bezpečnostných incidentov v kybernetickom priestore.

Funkcia (útvar)	Dop. min. FTE	Rola	Stručný popis
v kybernetickom priestore		bezpečnostných incidentov	
Útvar kybernetickej ochrany a monitorovania	1	Manažér bezpečnostného monitoringu	Správa a výkon centrálneho bezpečnostného monitoringu používania služieb verejnej správy. Zabezpečenie primeranej úrovne ochrany národnej informačnej a komunikačnej infraštruktúry (NIKI) a kritickej informačnej infraštruktúry. (Poskytuje služby spojené so zvládnutím bezpečnostných incidentov, odstraňovaním ich následkov a následnou obnovou činnosti informačných systémov v spolupráci s vlastníkmi a prevádzkovateľmi NIKI, telekomunikačnými operátormi, poskytovateľmi internetových služieb (ISP) a inými štátnymi orgánmi. Podieľa sa na budovaní a rozširovaní poznania verejnosti vo vybraných oblastiach informačnej bezpečnosti, aktívne kooperuje so zahraničnými organizáciami a reprezentuje SR v oblasti informačnej bezpečnosti na medzinárodnej úrovni.)
	(n)	Aktuálne role CSIRT SK týkajúce sa ochrany a monitorovania	Presun rolí CSIRT SK pod správu NBÚ alebo v prípade, že CSIRT SK bude plniť rolu rezortného CSIRT pre MFSR, tak vytvorenie rovnakých rolí na NBÚ
Útvar riadenia bezpečnosti mobilných zariadení a SKI	0,5	Manažér bezpečnosti mobilných zariadení	Riadenie kybernetickej bezpečnosti verejnej správy v rámci oblasti mobilných zariadení a usmerňovanie riadenia a používania mobilných zariadení vo VS.
	0,5	Manažér bezpečnosti SKI	Riadenie kybernetickej bezpečnosti verejnej správy v rámci SKI a usmerňovanie riadenia prevádzkovateľov SKI v oblasti kybernetickej bezpečnosti.
Spolu:	**4,50+ (n)**		

Tabuľka 1: Role a zodpovednosti KBVS

V ďalšom období bude potrebné jednotlivé útvary rozšíriť o adekvátny počet pracovníkov, ktorí budú realizovať úlohy konkrétneho útvaru.

3.1.2 Prístup k riešeniu IB a KyB na úrovni jednotlivých inštitúcií

V rámci jednotlivých inštitúcií VS musí byť zriadená a obsadená rola Manažér IB a rola Bezpečnostného manažéra projektov zastrešujúca informačnú bezpečnosť v rámci jednotlivých IKT projektov. Manažér IB na úrovni inštitúcie verejnej správy metodicky podlieha útvaru Metodiky a riadenia IB, ktorý je súčasťou KIBVS. Z pohľadu

monitorovania a následného riadenia bezpečnostných incidentov, ktoré presahujú rámec inštitúcie verejnej správy, je potrebné, aby každá inštitúcia mala definovanú rolu Manažér bezpečnostných incidentov, ktorá z pohľadu metodického riadenia bude podliehať útvaru kybernetickej bezpečnosti a bezpečnostného monitoringu NBÚ (terajší CSIRT SK).

Na úrovni jednotlivých rezortov a organizácií budú zadefinované a obsadené samostatné role v oblasti informačnej a kybernetickej bezpečnosti podľa medzinárodných štandardov tak, aby bola zabezpečená minimálna akceptovaná úroveň bezpečnosti naprieč verejnou správou.

Zodpovední rezortní architekti IB budú pod dohľadom kancelárie bezpečnosti zabezpečovať, aby bolo vždy, v rámci existujúcich aj vznikajúcich systémov a projektov, osobitne kontrolované a vynucované dodržiavanie definovaných bezpečnostných politík a pravidiel. Okrem budovania celkovej bezpečnostnej architektúry svojej inštitúcie, resp. rezortu sa tvorba lokálnych bezpečnostných oddelení zameria aj na prípravu nových projektov a ich posudzovania z pohľadu všeobecne definovaných pravidiel pre verejnú správu ako aj lokálnych obmedzení. Rezortní bezpečnostní architekti budú zodpovední za definovanie bezpečnostných požiadaviek na každý nový systém alebo aplikáciu v súlade so strategickou a rezortnou bezpečnostnou architektúrou. Rezortný architekt bude zodpovedať za definovanie funkčných požiadaviek a bezpečnostný rezortný architekt za definovanie bezpečnostných požiadaviek. Osobitne tiež budú zodpovední v súčinnosti s centrálnou kanceláriou bezpečnosti za výkon testovania bezpečnosti novo dodávaných systémov a riešení a za kontrolu odstránenia identifikovaných zistení.

3.1.2.1 Zabezpečenie definovania bezpečnostných požiadaviek na aplikácie v procese verejného obstarávania

Základnou úlohou rezortných architektov by malo byť stanovenie opatrení a potrebných krokov pre zabezpečenie definovania bezpečnostných požiadaviek na novo obstarávané informačné systémy verejnej správy v procese ich verejného obstarávania a ich následného testovania v rámci príslušnej realizačnej fázy projektu.

Cieľom implementácie projektov by mala byť, okrem implementácie funkčných požiadaviek, aj implementácia bezpečnostných funkcií a vlastností, ktoré dokážu zabezpečiť základné bezpečnostné požiadavky, ktorými sú dôvernosť, integrita a dostupnosť informačných aktív a zároveň aj súlad s bezpečnostnými štandardmi, najmä s požiadavkami výnosu MFSR č. 55/2014 Z. z. o štandardoch pre informačné systémy verejnej správy (ďalej len „Výnos o štandardoch“).

Nastavenie jednotného rámca bezpečnostných požiadaviek a funkcií, ktoré by mali byť implementované v rámci realizovaných projektov, je nevyhnutné najmä za účelom efektívneho a jednotného postupu pri zachovaní požadovanej úrovne bezpečnosti. Zároveň sa zabezpečí efektívne overenie potrebného legislatívneho súladu s definovanými požiadavkami. V rámci prípravy procesu verejného obstarávania projektu je potrebné zo strany obstarávateľa zabezpečiť, aby súčasťou súťažných podkladov a následne aj návrhu zmluvy s budúcim dodávateľom bola definícia konkrétnych bezpečnostných požiadaviek na aplikácie, ktoré budú predmetom dodania v rámci príslušného projektu. Týmto sa budúci dodávateľ zaviaže, že dodá systém nie len s požadovanými funkčnými vlastnosťami, ale zároveň aj s požadovanými bezpečnostnými funkciami a vlastnosťami, ktoré musia byť implementovaná na úrovni konkrétnych aplikácií. Definícia konkrétnych bezpečnostných požiadaviek a funkcií musí vychádzať najmä zo štandardu (Common Criteria) uvedeného v predchádzajúcej kapitole. Tento štandard definuje základný rámec bezpečnostných funkcií, ktoré je potrebné zohľadniť pri definovaní konkrétnych bezpečnostných požiadaviek na základe výsledkov analýzy rizík novo obstarávanej aplikácie, resp. systému. Ide najmä o nasledovné bezpečnostné funkcie:

- bezpečnostný audit,
- komunikácia,
- kryptografická podpora,
- nepopierateľnosť (non-repudiation),
- bezpečnosť používateľských údajov,
- identifikácia a autentifikácia,
- ochrana súkromia,
- ochrana bezpečnostných funkcií aplikácie,

- prístup do aplikácie.

Okrem uvedených bezpečnostných funkcií, ak je to relevantné, sa odporúča zohľadniť aj bezpečnostné požiadavky na vývoj web aplikácií, ktoré by mali zahŕňať najmä požiadavky z pohľadu bezpečnosti:

- aktívneho kódu,
- architektúry web aplikácie,
- webovej aplikácie na strane používateľa,
- webovej aplikácie na strane servera.

Zároveň sa odporúča zohľadniť aj iné všeobecné bezpečnostné požiadavky na web aplikácie, napr. poznámky vývojárov v kóde aplikácie, pravidelné implementovanie bezpečnostných „záplat“, indexovanie adresárov, použitie vhodných kryptografických algoritmov s primeranými parametrami a pod..

To aké konkrétne bezpečnostné funkcie budú pre príslušnú aplikáciu požadované je plne v kompetencii samotných obstarávateľov, ktorí by mali vychádzať najmä z analýzy rizík a mali byť zohľadniť prístup, ktorý vychádza z identifikovaných rizík a zraniteľností príslušných aplikácií (tzv.“Risk Based Approach“).

3.1.2.2 Zabezpečenie testovania bezpečnostných požiadaviek na aplikácie v rámci príslušnej fázy implementácie projektu

Počas realizácie fázy projektu „testovanie“ je zo strany obstarávateľov potrebné zabezpečiť, nie len otestovanie funkčných požiadaviek, ale aj otestovanie implementácie a kvality implementácie definovaných bezpečnostných požiadaviek a funkcií jednotlivých aplikácií systému. Súčasťou uvedenej fázy musí byť aj návrh testov a testovacích scenárov, ktoré okrem testovania funkčných vlastností, pokryjú aj oblasť bezpečnosti. Výsledky testov z oblasti bezpečnosti musia byť uvedené vo formálnom akceptačnom protokole.

V prípade potreby vykonania niektorých testov systému priamo na produkčných dátach, napr. v testovacom prostredí dodávateľa, je potrebné zabezpečiť bezpečnosť produkčných dát použitých na testovanie najmä z pohľadu ich dôvernosti vhodným spôsobom ich „anonymizácie“. Takto upravené dáta by nemali mať žiadnu nechcenú vypovedaciu hodnotu, ale zároveň by mali spĺňať požiadavky potrebné na samotné testovanie funkčnosti systému. Z uvedeného dôvodu je potrebné venovať zvýšenú pozornosť analýze a výberu správnej „anonymizačnej“ metódy a zabezpečeniu prostredia, v ktorom bude „anonymizácia“ vykonaná.

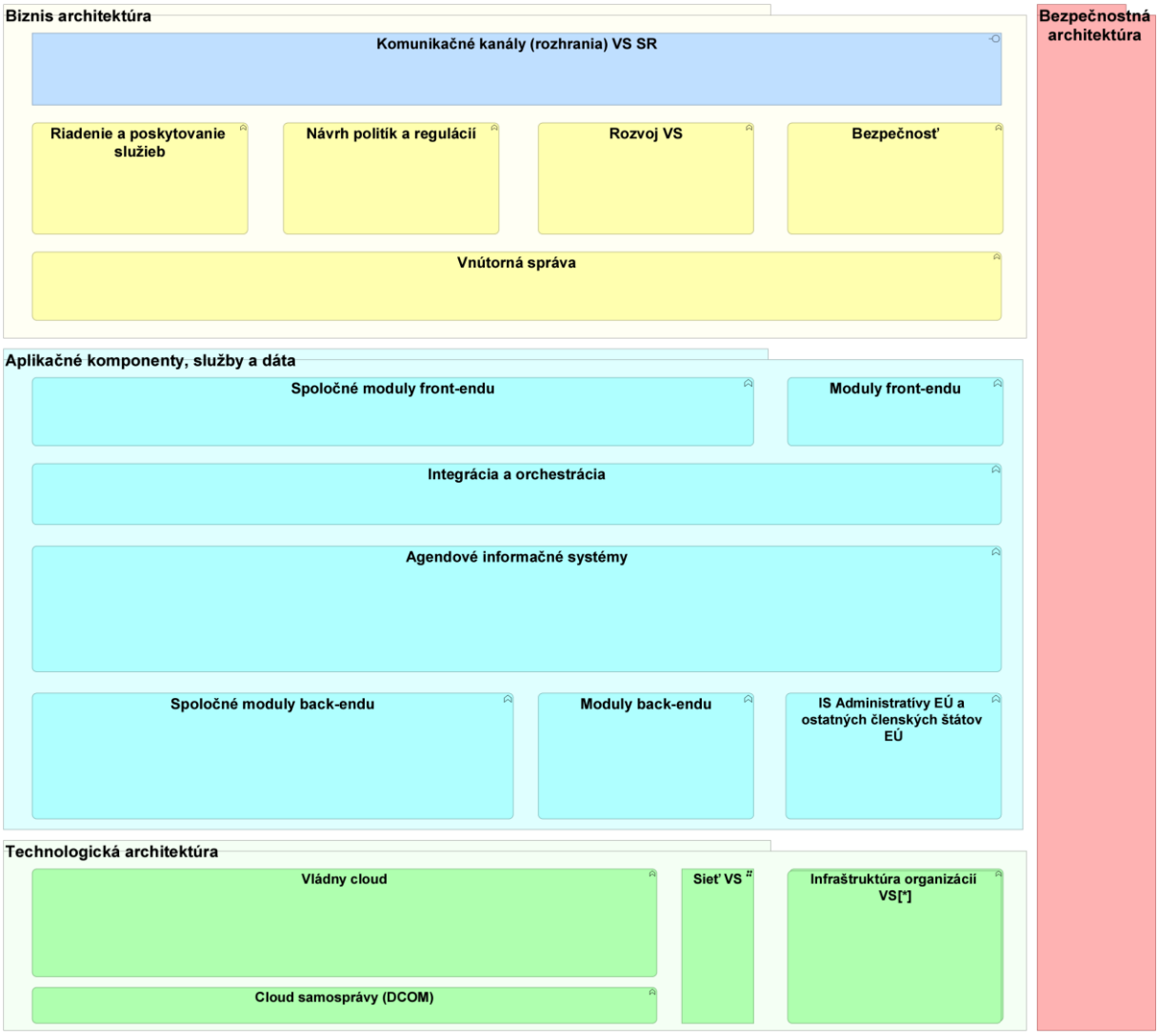
V prípade testovania zložitejších informačných systémov, resp. systémov, ktorých súčasťou nie je len produkčné prostredie, ale napr. aj vývojové alebo minimálne testovacie prostredie je potrebné v požiadavkách zadefinovať aj príslušné bezpečnostné požiadavky vyplývajúce z uvedenej skutočnosti, t.j. napr. požiadavky na bezpečnosť infraštruktúry a sieťového prostredia, prípadne aj požiadavky na fyzické oddelenie jednotlivých prostredí a pod.

Okrem uvedených skutočností sa pred ukončením, odovzdaním a akceptovaním samotného diela, t.j. pred jeho uvedením do prevádzky, odporúča zabezpečiť komplexné preverenie bezpečnosti formou vykonania, na dodávateľovi nezávislého, bezpečnostného auditu a penetračného testovania. Zároveň je vhodné vykonať aj audit súladu so všetkými oblasťami štandardizácie uvedenými vo Výnose o štandardoch.

3.2 Architektonický pohľad

3.2.1 Vzťah k modelu architektonickej vízie

Strategická priorita bezpečnosť je kľúčovým prvkom Architektonickej vízie verejnej správy 2020 a prechádza všetkými vrstvami a priamo ovplyvňuje všetky budované bloky v rámci ostatných strategických priorít ako samostatný pohľad na architektúru či už v biznis, aplikačnej, alebo technologickej vrstve.



Obrázok 2: Vzťah bezpečnosti a strategickej architektúry

S ohľadom na široký rámec, ktorý SP „Bezpečnosť" pokrýva by sa mala realizovať postupne, pričom kľúčové komponenty musia byť realizované prakticky okamžite, nakoľko budú mať priamy dopad na všetky plánované projekty a ostatné SP.

3.2.2 Architektonické ciele

Táto kapitola obsahuje špecifikáciu architektonických cieľov[1], ktoré by mali byť dosiahnuté prostredníctvom realizácie strategickej priority.

Cieľ	Pod-cieľ	Stručný popis
Bezpečnosť digitálneho a kybernetického priestoru	Zvýšenie ochrany digitálneho a kybernetického priestoru	Zvýšenie ochrany digitálneho a kybernetického priestoru je jedným zo základných cieľov EÚ v oblasti potláčania počítačovej kriminality. Bezpečnosť a ochrana digitálneho a kybernetického priestoru je jedným zo základných aspektov efektívneho a najmä bezpečného používania služieb verejnej

[1] Pozri dokument - Biznis kontext a motivačný aspekt EA

Cieľ	Pod-cieľ	Stručný popis
		správy a komunikácie občanov a podnikateľov s verejnou správou a opačne.
Bezpečnosť údajov a transakcií	Existencia a presnosť údajov	Existencia a presnosť údajov v rámci elektronickej komunikácie, resp. elektronických transakcií sú jedným zo základných aspektov zaručenia a zabezpečenia efektívneho, bezpečného a spoľahlivého výkonu činností verejnej správy.
	Úplnosť údajov	Úplnosť údajov v rámci elektronickej komunikácie, resp. elektronických transakcií je jedným zo základných aspektov zaručenia a zabezpečenia efektívneho, bezpečného a spoľahlivého výkonu činností verejnej správy.
	Platnosť a pravosť údajov	Platnosť a pravosť údajov v rámci elektronickej komunikácie, resp. elektronických transakcií sú jedným zo základných aspektov zaručenia a zabezpečenia efektívneho, bezpečného a spoľahlivého výkonu činností verejnej správy.
Bezpečnosť informačných aktív - základné aspekty bezpečnosti	Dôvernosť údajov	Zachovanie dôvernosti údajov, t.j. zabezpečenie prístupu k údajom len pre oprávnené osoby je jedným zo základných aspektov zaručenia a zabezpečenia efektívneho, bezpečného a spoľahlivého výkonu činností verejnej správy.
	Integrita údajov	Zachovanie integrity údajov, t.j. zabezpečenie ich celistvosti voči neautorizovaným zmenám alebo chybám je jedným zo základných aspektov zaručenia a zabezpečenia efektívneho, bezpečného a spoľahlivého výkonu činností verejnej správy.
	Dostupnosť údajov	Zabezpečenie definovanej dostupnosti údajov pre oprávnené subjekty v požadovanom čase je jedným zo základných aspektov zaručenia a zabezpečenia efektívneho, bezpečného a spoľahlivého výkonu činností verejnej správy.
	Neodmietnuteľnosť	Zabezpečenie aspektu neodmietnuteľnosti úkonu a nepopretia obsahu údajov jeho pôvodcom je jedným zo základných aspektov zaručenia a zabezpečenia efektívneho, bezpečného a spoľahlivého výkonu činností verejnej správy.

Tabuľka 2: Architektonické ciele v oblasti bezpečnosti

3.2.3 Architektonické princípy

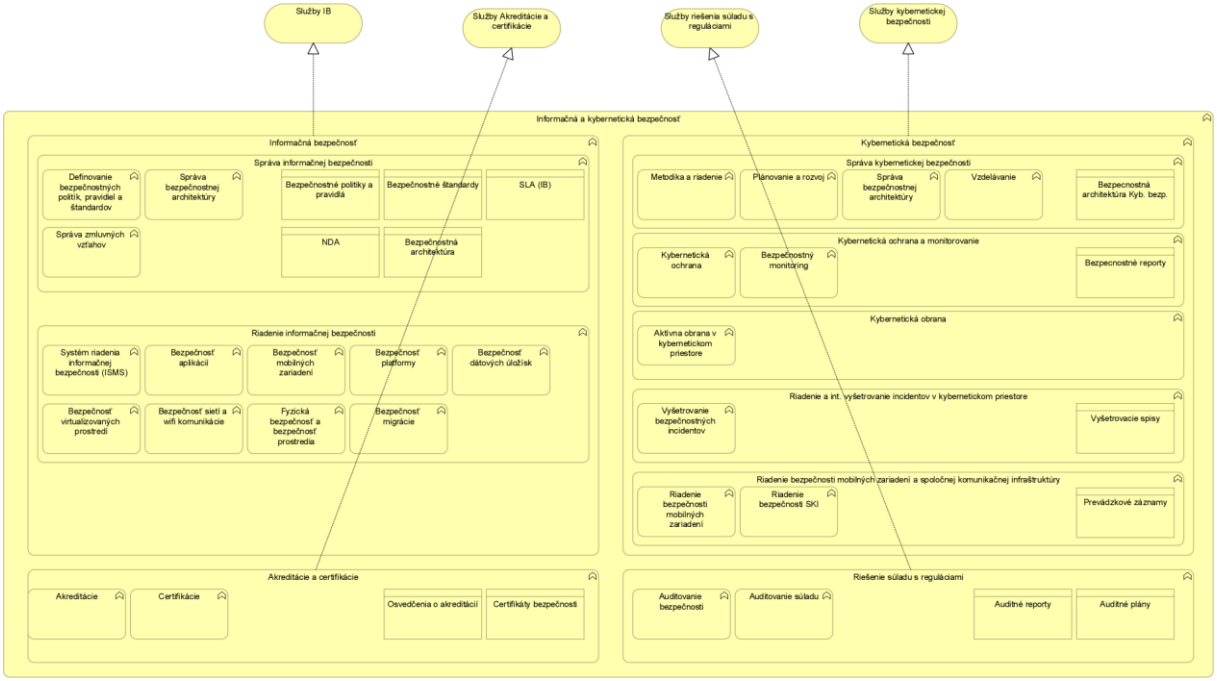
Naplnenie vyššie uvedených cieľov by malo byť dosiahnuté najmä naplnením nasledovných architektonických princípov v oblasti bezpečnosti:

- BEZPEČNOSŤ ÚDAJOV - Údaje sú chránené najmä pred neoprávneným prístupom, manipuláciou, použitím a zverejnením (zachovanie dôvernosti údajov), ich úmyselnou alebo neúmyselnou modifikáciou (zachovanie integrity údajov) a sú dostupné v požadovanom čase a v požadovanej kvalite (zachovanie dostupnosti údajov).
- PRAVOSŤ A DÔVERYHODNOSŤ ÚDAJOV - Používateľ pracuje len s údajmi, ktorých hodnovernosť a pôvod sú zabezpečené napríklad ich autorizáciou. Používateľ pracuje len s údajmi, ktoré sú z dôveryhodného zdroja s garantovanou identitou

- TRANSPARENTNOSŤ A OPAKOVATEĽNOSŤ - Riadenie informačnej bezpečnosti, najmä výkon dohľadu a kontroly, musí byť zabezpečený postupmi, ktoré garantujú ich transparentnosť a opakovateľnosť.
- AUDITOVATEĽNOSŤ - Riadenie informačnej bezpečnosti rovnako ako aj iných aktivít vo verejnej správe musí používať princípy a pravidlá, ktoré umožňujú výkon kontroly a zároveň umožňujú generovanie auditných a iných log záznamov s požadovanou úrovňou ich ochrany.

3.2.4 Biznis architektúra

Nakoľko oblasť informačnej bezpečnosti je prierezovou oblasťou a dotýka sa všetkých prvkov budovanej infraštruktúry, v rámci architektonického pohľadu je dôležité najmä zobrazenie jednotlivých biznis služieb a funkcií, ktoré ich budú pokrývať.



Obrázok 3: Rámcový pohľad na bloky realizujúce architektonickú prioritu

Pre oblasť informačnej bezpečnosti sú základnými blokmi správa informačnej bezpečnosti, ktorá predovšetkým definuje základné politiky, bezpečnostné pravidlá a odporúčania pre jednotlivých prevádzkovateľov a následne samotné riadenie informačnej bezpečnosti, v rámci ktorého už expertné skupiny priamo zasahujú a zabezpečujú konkrétne procesy a systémy v súlade so základnými cieľmi, ktoré si oblasť bezpečnosti vyžaduje. Ďalšími blokmi sú oblasť akreditácie a certifikácie, ktorá zaistí jednotné kritériá certifikácii v oblasti IB naprieč rezortmi a stavebný blok riešenia súladu, zameraný najmä na kontrolu a audit súladu so stanovenými požiadavkami v reálnom prostredí.

Pravidlá, politiky a požiadavky budú vytvárané na základe aktuálneho stavu vývoja IT a medzinárodne platných a uznávaných noriem a pravidiel (ISO, NIST). Po vydaní budú všetky požiadavky periodicky aktualizované a dopĺňané o nové oblasti. Medzi základné oblasti, ktorých sa bude oblasť riadenia IB týkať a ktoré bude plošne v rámci celej VS vynucovať, patria najmä Riadenie prístupu; Ochrana médií; Vzdelávanie a budovanie bezpečnostného povedomia; Fyzická a objektová bezpečnosť; Oblasť auditu; Plánovanie a rozvoj; Personálna bezpečnosť; Konfiguračný manažment; Riadenie rizík; Krízové plánovanie; Riadenie výberu systémov a služieb; Oblasť identifikácie a autentifikácie; Pravidlá autorizácie; Zvládanie incidentov; Riadenie integrity systémov a údržba.

Z pohľadu kybernetickej bezpečnosti je požadované pokrytie štyroch základných oblastí. Obdobne ako pri informačnej bezpečnosti je prvým blokom správa kybernetickej bezpečnosti zameraná najmä na vydávanie metodických pokynov, základných pravidiel a politík, ale aj na správu bezpečnostnej architektúry a rozvoj v tejto

oblasti. Kriticky dôležitou je oblasť kybernetickej ochrany a monitorovania, teda proaktívneho monitorovanie a aktívna obrana proti kybernetickým útokom, najmä voči kritickej infraštruktúre štátu. To zahŕňa okrem vybudovania vhodného centra obrany aj požiadavku na vzdelávanie naprieč celým verejným aj dotknutým súkromným sektorom so zameraním na kybernetickú bezpečnosť, jej ciele a pravidlá. Ďalším blokom je oblasť vyšetrovania bezpečnostných incidentov a oblasť riadenia bezpečnosti prevádzky spoločnej komunikačnej infraštruktúry, ktorá má vzhľadom na prepojenie systémov kritický dosah na všetky aspekty prevádzky IS.

3.2.4.1 Základné stavebné bloky

Základné stavebné bloky sú zobrazené v nasledovnej tabuľke. Všeobecne je možné ich rozdeliť podľa oblasti na Informačnú bezpečnosť a Kybernetickú bezpečnosť.

Stavebný blok	Stručný popis
Informačná bezpečnosť	Základná biznis funkcia v rámci bezpečnosti, ktorá zoskupuje nasledovné oblasti informačnej bezpečnosti: • Správa informačnej bezpečnosti. • Riadenie informačnej bezpečnosti. • Auditovanie informačnej bezpečnosti. • Akreditácie a certifikácie v oblasti informačnej bezpečnosti.
Správa informačnej bezpečnosti	Biznis funkcia zoskupujúca funkcie adresujúce: • definovanie bezpečnostných politík, pravidiel a štandardov, • správu (najmä definovanie, udržiavanie, plánovanie a dohľad) bezpečnostnej architektúry, • správu zmluvných vzťahov (najmä SLA z pohľadu bezpečnostných aspektov a NDA) a správu vzťahov s dodávateľmi.
Riadenie informačnej bezpečnosti	Biznis funkcia zoskupujúca funkcie adresujúce: • systém riadenia informačnej bezpečnosti (ISMS), • bezpečnosť aplikácií, • bezpečnosť mobilných zariadení, • bezpečnosť platformy, • bezpečnosť dátových úložísk, • bezpečnosť virtualizovaných prostredí, • bezpečnosť sietí a wifi komunikácie, • fyzická bezpečnosť a bezpečnosť prostredia.
Akreditácie a certifikácie	Biznis funkcia zoskupujúca funkcie adresujúce: • akreditáciu (metodické riadenie a udeľovanie akreditácií v oblasti informačnej bezpečnosti), • certifikáciu (metodické riadenie a udeľovanie certifikácií v oblasti informačnej bezpečnosti).
Auditovanie informačnej bezpečnosti	Biznis funkcia zoskupujúca funkcie adresujúce: • auditovanie informačnej bezpečnosti (metodické riadenie a zabezpečovanie výkonu auditov informačnej bezpečnosti), • auditovanie súladu.
Kybernetická bezpečnosť	Biznis funkcia zoskupujúca funkcie adresujúce: • správu kybernetickej bezpečnosti,

Stavebný blok	Stručný popis
	• kybernetickú ochranu a monitorovanie, • kybernetickú obranu, • riadenie a interné vyšetrovanie incidentov v kybernetickom priestore, • riadenie bezpečnosti mobilných zariadení a spoločnej komunikačnej infraštruktúry.

Tabuľka 3: Základné stavebné bloky

3.2.4.1.1 IB - Správa informačnej bezpečnosti

3.2.4.1.1.1 Definovanie bezpečnostných politík, pravidiel a štandardov

Funkcia definovanie bezpečnostných politík, pravidiel a štandardov zabezpečí jednotné a centrálne metodické riadenie informačnej bezpečnosti celej verejnej správy.

Hlavnou činnosťou v rámci tejto funkcie bude predovšetkým definovanie politík, pravidiel a štandardov v oblasti riadenia IB vo verejnej správe a rovnako regulácia oblasti riadenia IB najmä formou definovania metodík a publikovaním usmernení. Súčasťou dokumentačnej podpory prijímateľov by mala byť, okrem uvedených skutočností, aj podpora vo forme:

- správy (najmä tvorby a udržiavania) bezpečnostnej architektúry,
- podporných kontrolných zoznamov a iných pracovných dokumentov a šablón,
- podpory pri implementácii prostredníctvom kolaboračných nástrojov,
- správy, podpory a riadenia informačných aktív,
- riadenia konfigurácií.

Výkonná časť kancelárie bezpečnosti bude priamo pomáhať s implementáciou a nastavením bezpečnosti v rámci inštitúcií verejnej správy, najmä na projektoch prijímateľov OPII.

3.2.4.1.1.2 Správa zmluvných vzťahov

Súčasťou funkcie správa zmluvných vzťahov bude prostredníctvom schvaľovania dohôd o poskytovaní služieb (SLA) najmä zabezpečovanie súladu dohôd s potrebami jednotlivých zainteresovaných a zároveň dohliadanie na SLA medzi objednávateľom a poskytovateľom služby v rámci projektov OPII na podporu eGovernmentu. Správa SLA musí obsahovať najmä nasledujúce body:

- jednotlivé strany kontraktu, predmet kontraktu a rozsah dohody,
- časovú dĺžku poskytovania služieb,
- používateľskú podporu, kontakty a eskalačný mechanizmus,
- správa zmien, zabezpečenie a nadväznosť služby,
- výkonnostné a bezpečnostné parametre služby,
- zodpovednosti.

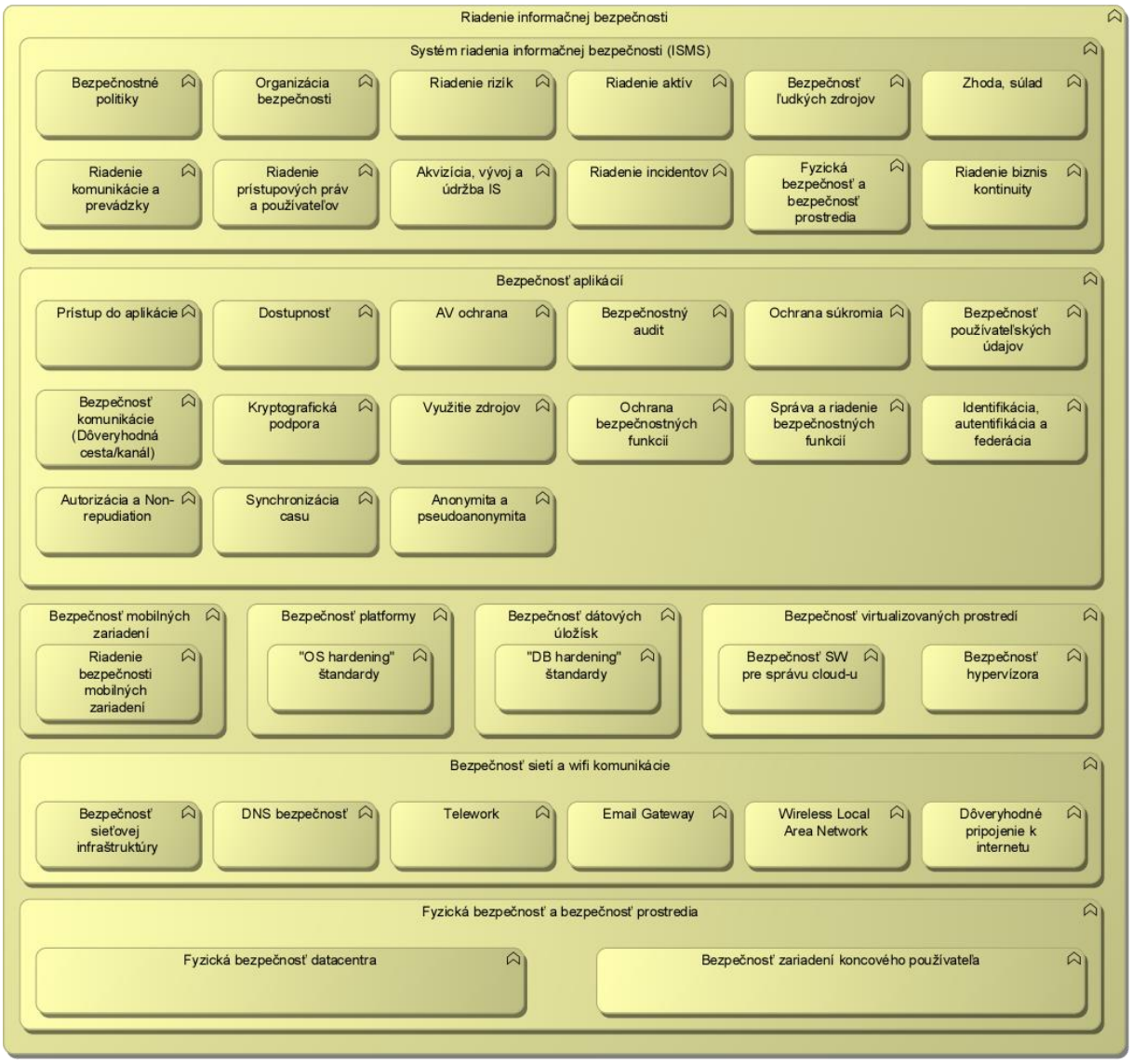
Okrem SLA bude súčasťou centrálnej správy zmluvných vzťahov aj oblasť správy zmlúv ohľadom zachovania mlčanlivosti (tzv. NDA) a oblasť správy softvérových licencii verejnej správy.

3.2.4.1.1.3 Správa bezpečnostnej architektúry

Funkcia správa bezpečnostnej architektúry zabezpečí najmä definovanie, udržiavanie, analyzovanie, plánovanie a dohľad bezpečnostnej architektúry. Bezpečnostná architektúra bude vytváraná v úzkej spolupráci s AKVS ako súčasť enterprise architektúry VS SR.

3.2.4.1.2 IB - Riadenie informačnej bezpečnosti

Detailný pohľad na stavebné bloky riadenia IB je znázornený na nasledujúcom obrázku.



Obrázok 4: Riadenie IB - detailný pohľad

3.2.4.1.2.1 Systém riadenia informačnej bezpečnosti (ISMS)

Funkcia systém riadenia informačnej bezpečnosti (ISMS) musí pokrývať všetky oblasti riadenia definované v normách ISO/IEC 27001 a ISO/IEC 27002. Ide najmä o oblasť:

- bezpečnostnej politiky,
- organizácie bezpečnosti,
- riadenia rizík,
- riadenie incidentov,
- riadenie aktív,
- bezpečnosť ľudských zdrojov,
- riadenie komunikácie a prevádzky,
- riadenie prístupových práv a používateľov,

- akvizícia, vývoj a údržba IS,
- fyzická bezpečnosť a objektová bezpečnosť,
- riadenie vzťahov s dodávateľmi,
- šifrovanie,
- riadenie kontinuity biznis činností,
- súlad.

3.2.4.1.2.2 Bezpečnosť aplikácií

Funkcia bezpečnosť aplikácií musí integrovať najmä nasledovné funkcie dôležité z pohľadu zabezpečenia dôvernosti, integrity, autentickosti a dostupnosti dát vytváraných, spracovávaných, uchovávaných alebo prenášaných prostredníctvom aplikácií a systémov, vychádzajúcich najmä zo štandardu ISO/IEC 15408:

- prístup do aplikácie,
- dostupnosť,
- antivírusová ochrana,
- bezpečnostný audit a logovanie,
- ochrana súkromia,
- bezpečnosť používateľských údajov,
- bezpečnosť komunikácie (dôveryhodná cesta a dôveryhodný komunikačný kanál),
- kryptografická podpora,
- využitie zdrojov,
- ochrana bezpečnostných funkcií,
- správa a riadenie bezpečnostných funkcií,
- identifikácia, autentifikácia a federácia,
- autorizácia a neodmietnuteľnosť úkonov (non-repudiation),
- synchronizácia času,
- anonymita a pseudoanonymita.

3.2.4.1.2.3 Bezpečnosť mobilných zariadení

V rámci funkcie bezpečnosti mobilných zariadení je potrebné pokryť najmä riadenie bezpečnosti mobilných zariadení používaných v rámci VS, vrátane ich vzdialenej správy, monitoringu a kontroly (tzv. Mobile device management), ktorý rieši ich bezpečné používanie a zároveň ochranu v prípade odcudzenia alebo straty týchto zariadení. Ide o bezpečnostné funkcie umožňujúce napr. realizáciu vynútenia šifrovania dát nachádzajúcich sa v pamäti zariadenia, používanie PKI identifikácie a autentifikácie, vytváranie virtuálnych privátnych sietí, kontrolovanie, či nebol narušený firmvér telefónu, vynútenie a aktualizácia antivírusovej ochrany alebo aktualizácií OS, kontrola inštalovania nedovoleného SW, vymazanie pamäte zariadenia v prípade jeho straty alebo ukradnutia, prípadne lokalizovanie polohy zariadenia na základe GPS a pod.

3.2.4.1.2.4 Bezpečnosť platformy a bezpečnosť dátových úložísk

Súčasťou funkcií bezpečnosť platformy a bezpečnosť dátových úložísk musí byť najmä zabezpečenie definovania, aktualizácie a udržiavania tzv. hardening štandardov pre jednotlivé operačné a databázové systémy, riadenie servisných a bezpečnostných záplat, riadenie zraniteľností a ochrana pred škodlivým kódom.

3.2.4.1.2.5 Bezpečnosť virtualizovaných prostredí

Funkcia bezpečnosť virtualizovaných prostredí musí pokryť komplexne problematiku bezpečnosti dátových úložísk verejnej správy, vrátane bezpečnosti SW pre správu cloudových služieb, bezpečnosti hypervízora, zabezpečenie

integrity údajov a aplikácií bežiacich na cloudových službách, zabezpečenie dostupnosti a zabezpečenie dôvernosti údajov fungujúcich na cloud službách.

3.2.4.1.2.6 Bezpečnosť sietí, bezdrôtovej a mobilnej komunikácie

Bezpečnosť sietí, bezdrôtovej (wifi) a mobilnej komunikácie musí zahŕňať komplexnú problematiku bezpečnosti sieťových infraštruktúr, bezdrôtovej a mobilnej komunikácie. Musí pokryť najmä oblasť DNS bezpečnosti, vzdialenej práce, emailových sieťových brán, dôveryhodných sieťových a internetových spojení a oblasť zabezpečenia lokálnych wifi sietí.

3.2.4.1.2.7 Fyzická bezpečnosť a bezpečnosť prostredia

Posledná z funkcií riadenia IB, funkcia fyzickej bezpečnosti a bezpečnosti prostredia, musí integrovať najmä oblasť fyzickej bezpečnosti a zabezpečenia ochrany cloud datacentier verejnej správy a rovnako aj fyzickú bezpečnosť zariadení a prostredia koncových používateľov. Cloud datacentrá verejnej správy musia byť budované a prevádzkované najmä v súlade s ANSI/TIA 942 štandardom telekomunikačnej infraštruktúry pre dátové centrá, ktorý definujú štyri základné úrovne (vrstvy) dátových centier a v súlade s pripravovaným štandardom ISO/IEC 27017.

3.2.4.1.3 Kybernetická bezpečnosť

Základnými bezpečnostnými požiadavkami, ktorým bude potrebné venovať pozornosť, je najmä zabezpečenie:

- dostupnosti, integrity a najmä dôvernosti jednotlivých údajov a služieb,
- povolenia prístupu k jednotlivým údajom a službám len dôveryhodným a oprávneným subjektom na základe princípu „need to know“,
- bezpečnej a dôveryhodnej komunikácie oprávnených subjektov,
- existencie bezpečnej a dôveryhodnej komunikačnej infraštruktúry, ktorá zabezpečuje komunikáciu medzi jednotlivými entitami, resp. systémami,
- odpojenie entít, ktoré sa stali nedôveryhodné, prípadne bol v rámci nich identifikovaný relevantný bezpečnostný incident, alebo entít, ktoré prestali spĺňať definované bezpečnostné požiadavky a pod..

3.2.4.1.3.1 Správa kybernetickej bezpečnosti

Funkcia správa kybernetickej bezpečnosti zabezpečí jednotné a centrálne metodické riadenie kybernetickej bezpečnosti celej verejnej správy. Hlavnou činnosťou v rámci tejto funkcie bude predovšetkým definovanie politík, pravidiel a štandardov v oblasti riadenia kybernetickej bezpečnosti vo verejnej správe a rovnako regulácia oblasti riadenia kybernetickej bezpečnosti najmä formou definovania metodík a publikovaním usmernení.

Funkcia správa kybernetickej bezpečnosti musí zabezpečiť a pokryť aktivity a úlohy súvisiace s bezpečnosťou a ochranou kybernetického priestoru, najmä v súvislosti s ochranou kritickej infraštruktúry SR a v súvislosti s medzinárodnou spoluprácou v oblasti bezpečnosti kybernetického priestoru. Funkcia vzdelávanie v oblasti kybernetickej bezpečnosti musí zabezpečiť podmienky a samotný výkon vzdelávania inštitúcií VS a iných subjektov v oblasti zvyšovania povedomia o kybernetickej bezpečnosti a ochrane. Ide najmä o nasledovné aktivity:

- metodika a riadenie kybernetickej bezpečnosti,
- plánovanie a rozvoj kybernetickej bezpečnosti a ochrany,
- správa bezpečnostnej architektúry pre oblasť kybernetickej bezpečnosti,
- vzdelávanie a zvyšovanie bezpečnostného povedomia.

3.2.4.1.3.2 Kybernetická ochrana a monitorovanie

Funkcia kybernetická ochrana musí zabezpečiť úlohy a činnosti spojené s ochranou kybernetického priestoru, ochranou kritickej infraštruktúry SR. Ide najmä o úlohy v oblasti správy a riadenie kybernetickej ochrany.

V rámci funkcie bezpečnostný monitoring bude potrebné zabezpečiť najmä ochranu a monitorovanie poskytovaných eGov služieb verejnej správy a výmeny dokumentov, údajov a informácií medzi jednotlivými inštitúciami verejnej správy. Uvedené bude možné dosiahnuť najmä implementáciou nasledovných funkcií:

- centrálny bezpečnostný monitoring – monitoring a riadenie incidentov,
- monitorovanie, identifikovanie, vyhodnocovanie a reakcia na identifikované bezpečnostné incidenty,
- manažment oprávnení a prístupových práv k službám jednotlivých inštitúcií verejnej správy (umožnenie prístupu k dátam jednej inštitúcie len pre také inštitúcie, ktoré spĺňajú požadované bezpečnostné požiadavky pre príslušný klasifikačný stupeň predmetných dát / bezpečnostná politika a prijaté bezpečnostné opatrenia komunikujúcich inštitúcií by mali byť na rovnakej úrovni),
- riadenie prevádzky a dátových tokov,
- štatistiky a reporting (poskytovanie štatistických reportov používania a vyťaženia jednotlivých služieb a systémov),
- prehľad o lustráciách nad údajmi používateľov,
- ďalšie podporné úlohy potrebné pre zabezpečenie dostupnosti, integrity a dôvernosti dát, ako je napr. definovanie, sledovanie a následné vyhodnocovanie výskytu rôznych vzorov (z angl. „patterns“) z pohľadu identifikovania neprimeraného, resp. neoprávneného prístupu k údajom (napr. sťahovanie, resp. žiadanie neprimeraného množstva údajov, prípadne neprimeraného množstva údajov ohľadom jednej osoby z viacerých systémov naraz a pod.).

3.2.4.1.3.3 Kybernetická obrana

Táto funkcia zabezpečí aktívnu obranu v prípade identifikovania útokov v kybernetickom priestore na prvky a systémy, ktoré budú predmetom kybernetickej ochrany a monitorovania.

Prostredníctvom operačného centra kybernetickej bezpečnosti budú riadené aktivity týkajúce sa obrany na prebiehajúce útoky.

3.2.4.1.3.4 Riadenie a interné vyšetrovanie incidentov v kybernetickom priestore

Funkcia riadenie a vyšetrovanie bezpečnostných incidentov musí zabezpečiť dostatočné zdroje a kapacity pre výkon procesov riadenia a riešenia bezpečnostných incidentov a obnovy systémov do pôvodného stavu a zároveň pre účely interného vyšetrovania bezpečnostných incidentov v kybernetickom priestore, v súlade s platnými právnymi predpismi, musí zabezpečiť dostatočné prostriedky a kapacity na vyšetrenie bezpečnostných incidentov, prípadne aj s použitím forenzných techník a nástrojov.

3.2.4.1.3.5 Riadenie bezpečnosti mobilných zariadení a spoločnej komunikačnej infraštruktúry

Funkcia riadenie bezpečnosti mobilných zariadení a spoločnej komunikačnej infraštruktúry musí zabezpečiť dostatočné zdroje a kapacity pre riadenie bezpečnosti a prevádzky spoločnej komunikačnej infraštruktúry a mobilných zariadení používaných vo VS na výkon činností VS.

3.2.4.1.4 Akreditácie a certifikácie

3.2.4.1.4.1 Akreditácia

Funkcia akreditácia umožní metodické riadenie a udeľovanie akreditácií v oblasti informačnej bezpečnosti. Zabezpečí definovanie akreditačných postupov a pravidiel pre proces akreditácie audítorov informačnej bezpečnosti, metód, postupov a pravidiel v oblasti informačnej bezpečnosti a v oblasti bezpečnej výmeny informácií medzi jednotlivými inštitúciami a samotný výkon a udeľovanie príslušných akreditácií.

Proces akreditácie bude vykonávaný treťou stranou (skúšobňa, prípadne iná oprávnená autorita), ministerstvo bude tento proces len formálne zastrešovať, definovať a kontrolovať akreditačné postupy, preberať výsledky a bude udeľovať samotné certifikáty o akreditácii.

3.2.4.1.4.2 Certifikácia

Podobne ako predchádzajúca funkcia aj funkcia certifikácia umožní metodické riadenie a udeľovanie certifikácií v oblasti informačnej bezpečnosti. Zabezpečí definovanie certifikačných postupov a pravidiel pre proces certifikácie informačných systémov, zariadení, SW, firmvér, OS, DB systémov a pod. a samotný výkon a udeľovanie príslušných certifikácií.

Proces certifikácie bude vykonávaný treťou stranou (skúšobňa, prípadne iná oprávnená autorita), ministerstvo bude tento proces len formálne zastrešovať, definovať a kontrolovať certifikačné postupy, preberať výsledky a bude udeľovať samotné certifikácie HW a SW produktov.

3.2.4.1.5 Auditovanie informačnej bezpečnosti

Funkcia auditovanie informačnej bezpečnosti umožní najmä:

- metodické riadenie auditov informačnej bezpečnosti a auditov súladu,
- plánovanie auditov informačnej bezpečnosti a auditov súladu,
- definovanie rozsahu a požiadaviek na audit informačnej bezpečnosti a audit súladu,
- definovanie požiadaviek na audítorov informačnej bezpečnosti a audítorov súladu a
- zabezpečovanie výkonu auditov informačnej bezpečnosti a auditov súladu.

Auditovanie bezpečnosti je zamerané predovšetkým na transparentný a opakovateľný proces výkonu bezpečnostných a iných auditov (napr. auditov súladu a pod.). Kľúčovou úlohou je definovanie jednotných postupov a najmä plánov týchto auditov na najvyššej úrovni tak, aby v rámci definovaného obdobia boli pokryté všetky kritické informačné systémy verejnej správy (najmä systémy kritickej infraštruktúry) a samozrejme aj zvyšné informačné systémy verejnej správy.

Správa auditov informačnej bezpečnosti je okrem manažmentu plánov auditov zameraná aj na výsledky z jednotlivých auditov, správu akčných plánov na odstránenie identifikovaných nedostatkov, nesúladov alebo rizík, zabezpečovanie výkonu „follow-up“ aktivít za účelom zistenia aktuálneho stavu odstránenia identifikovaných nedostatkov a pod.

V rámci definovania jednotlivých plánov auditov je potrebné zvažovať najmä nasledovné oblasti:

- procesná oblasť (napr. ISMS, PKI a súlad s vydanými štandardami),
- nastavenia systémov a komponentov (aplikácie, IKT komponenty a súlad s vydanými štandardami v relevantnej oblasti),
- aplikačných a infraštruktúrnych penetračných testov,
- testov zraniteľností,
- a iných testov súvisiacich s riadením informačnej bezpečnosti, prevádzkou ISVS a poskytovaním elektronických služieb.

Samotný výkon auditov informačnej bezpečnosti by mal byť zabezpečovaný najmä prostredníctvom nezávislých externých zdrojov (certifikovaných audítorov informačnej bezpečnosti).

3.2.5 Aplikačná architektúra

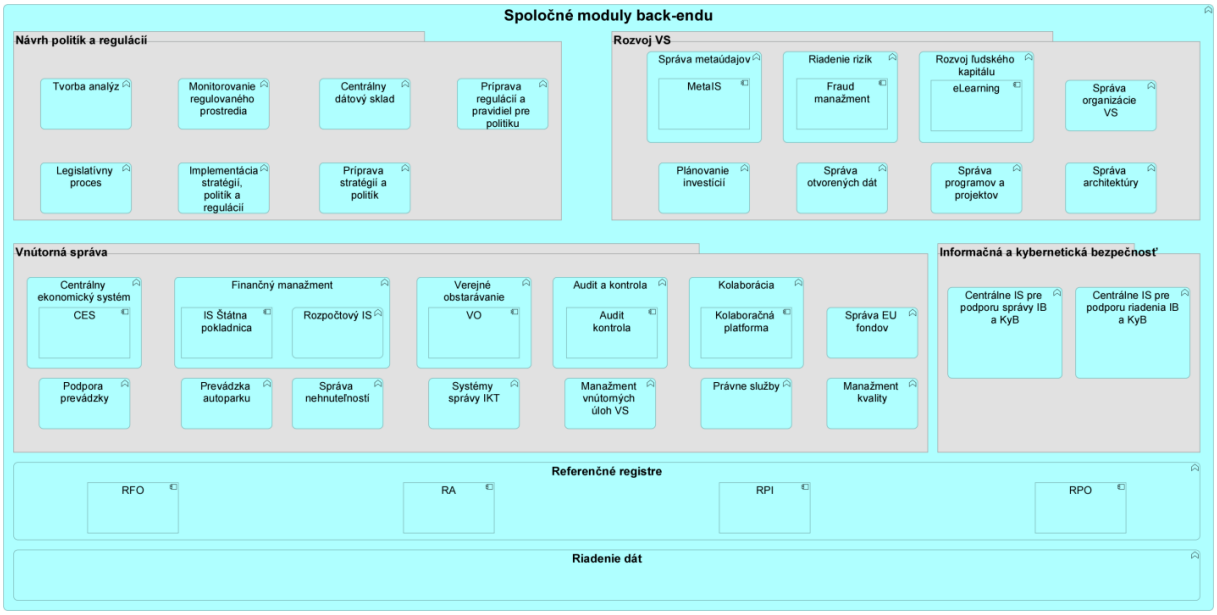
Na aplikačnej úrovni bude implementácia informačných systémov a iných bezpečnostných riešení rozdelená nasledovne:

- Centrálna úroveň IS a bezpečnostných riešení za účelom zabezpečenia podpory pre správu informačnej a kybernetickej bezpečnosti – primárne určené pre subjekty, ktoré budú riešiť správu (governance) uvedených dvoch oblastí (najmä NBÚ).
- Centrálna úroveň IS a bezpečnostných riešení za účelom zabezpečenia podpory riadenia a výkonu informačnej a kybernetickej bezpečnosti pre jednotlivé inštitúcie VS. Ide o centralizované riešenia, ktoré zabezpečia:

- Požadovanú úroveň bezpečnosti (najmä ochrany, bezpečnostného monitoringu, kontroly a pod.) pre centrálne komponenty architektúry VS (ako sú napr. spoločné moduly, integračné platformy, spoločné bloky, vládny cloud a pod.).
- Požadované bezpečnostné funkcie, ktoré je efektívnejšie implementovať centralizovane (napr. testovanie zraniteľnosti, identifikácia a autentifikácia, a pod.) pre jednotlivé inštitúcie VS.

■ Decentralizovaná úroveň IS a bezpečnostných riešení za účelom zabezpečenia podpory riadenia a výkonu informačnej a kybernetickej bezpečnosti pre jednotlivé inštitúcie VS. Ide o implementáciu bezpečnostných funkcií na úrovni jednotlivých projektov a riešení jednotlivých inštitúcií VS, ktoré nie je možné (najmä z pohľadu bezpečnosti) realizovať centralizovaným spôsobom. Táto úroveň je plne v gescii a kompetencii jednotlivých inštitúcií VS.

Zaradenie centrálnych komponentov realizujúcich bezpečnostnú architektúru informačnej a kybernetickej bezpečnosti do celkovej strategickej architektúry (aplikačná úroveň) je uvedené na nasledujúcom obrázku.



Obrázok 5: Aplikačná architektúra – zaradenie IB a KyB

4 Plánovanie a migrácia

V rámci oblasti je potrebné realizovať viacero projektov min. v nasledovných oblastiach:

- zriadenie KIBVS,
- oblasť správy IB,
- oblasť riadenia IB,
- oblasť kybernetickej bezpečnosti,
- oblasť bezpečnosti cloudu,
- podporné projekty.

4.1 Zriadenie KIBVS

Popis a cieľ

Cieľom projektu je vybudovanie centrálnej kancelárie informačnej bezpečnostnej verejnej správy, ktorá by metodicky riadila a dohliadala nad celou oblasťou informačnej bezpečnosti.

Aktivity

- Vytvorenie podkladov a odborných materiálov, najmä:
  - náplne práce jednotlivých pracovníkov kancelárie informačnej bezpečnosti,
  - metodiky práce,
  - organizačné pokyny a pod.
- Definovanie úloh a povinností jednotlivých rolí KIB:
  - v oblasti definovania politík, štandardov a regulácie riadenia IB,
  - v oblasti riadenia ISMS,
  - v oblasti návrhu a udržiavania bezpečnostnej architektúry,
  - v oblasti akreditácie a certifikácie v rámci IB,
  - v oblasti bezpečnostných auditov IS,
  - v rámci centrálneho riadenia SLA a NDA.
- Premapovanie existujúcich úloh a rolí existujúceho útvaru, ktorý bude riešiť zriadenie KIB na úlohy kancelárie bezpečnosti.
- Zabezpečenie dostatočného počtu interných a externých pracovníkov na výkon jednotlivých rolí kancelárie bezpečnosti, a kooperáciu s architektonickou kanceláriou (AK) prostredníctvom roly bezpečnostný architekt architektúry verejnej správy SR.

Navrhovaný realizátor

- MFSR

Navrhovaní partneri

- NBÚ

Odhadovaná dĺžka realizácie projektu (projektov)

- 1 rok

Závislosti na iných projektoch a prioritách (OPII a OPIS)

- Projekt je možné realizovať samostatne.

4.2 Oblasť správy IB

4.2.1 IS správy akreditácií, IS správy certifikácií v oblasti bezpečnosti, IS správy bezpečnostných auditov

Popis a ciel

Cieľom projektov je vybudovanie troch samostatných informačných systémov zabezpečujúcich definovanie, monitorovanie a riadenie súboru akreditácií a certifikácií systémov, aplikácií, osôb, prípadne služieb z pohľadu informačnej bezpečnosti a samostatného systému pre riadenie a porovnávanie bezpečnostných auditov realizovaných v rámci IS VS. Systémy budú navzájom nezávislé, ale veľmi príbuzné a pri vhodnom definovaní požiadaviek je možné ich realizáciu spájať a optimalizovať tým finančné, časové aj personálne náklady.

Aktivity

- Analýza a návrh riešenia.
- Analýza existujúcich foriem akreditácií, certifikácií a typov auditov a analýza budúcich potrieb.
- Integrácia zdrojov dát.
- Testovanie.

Navrhovaný realizátor

- MFSR

Navrhovaní partneri

- NBÚ

Odhadovaná dĺžka realizácie projektu (projektov)

- 2 roky

Závislosti na iných projektoch a prioritách (OPII a OPIS)

- Projekty predpokladajú zriadenie KIBVS,

4.3 Pre oblasť riadenia IB

4.3.1 IS riadenia rizík, manažmentu aktív a používateľov

Popis a ciel

Cieľom projektu je vybudovanie centrálneho informačného systému zameraného na riadenie aktuálnych rizík naprieč infraštruktúrou verejnej správy. Okrem priebežného monitorovania existujúcich a novo vznikajúcich rizík na centrálnej úrovni, umožní systém riadenie rizík a súvisiacu správu aktív a používateľov na jednotlivých orgánoch štátnej správy. Z pozície BKVS sa tak docieli ucelený prehľad o aktuálnom stave zabezpečenia eGovernmentu a z pohľadu podriadených organizácií sa tak docieli zabezpečenie expertného nástroja na riadenia rizík v rámci organizácie.

Aktivity

- Analýza a návrh riešenia.
- Analýza existujúcich systémov riadenia rizík, aktív a používateľov.
- Integrácia zdrojov dát.
- Testovanie.
- Prevádzka na centrálnej úrovni.
- Prevádzka na podriadených organizáciách.

Navrhovaný realizátor

- MFSR

Navrhovaní partneri

- Všetky ústredné orgány VS

Odhadovaná dĺžka realizácie projektu (projektov)

- 3 roky

Závislosti na iných projektoch a prioritách (OPII a OPIS)

- Centrálne IAM.
- IS PKI.
- IS manažmentu a správy zraniteľností.

4.3.2 IS riadenia obnovy

Popis a ciel

Cieľom projektu je vybudovanie centrálneho informačného systému zameraného na riadenie obnovy ako činnosti potrebnej pre všetky IS naprieč infraštruktúrou verejnej správy. Systém umožní na centrálnej úrovni stanoviť základné predpoklady a požiadavky na jednotlivé organizácie a zároveň im dá možnosť zabezpečiť si riadenie obnovy v prípade neočakávaných udalostí v prevádzke ich IS pomocou jednotného nástroja.

Aktivity

- Analýza a návrh riešenia.
- Analýza existujúcich postupov riadenia obnovy IS a potrieb jednotlivých organizácií.
- Integrácia zdrojov dát.
- Testovanie.
- Prevádzka na centrálnej úrovni.
- Prevádzka na podriadených organizáciách.

Navrhovaný realizátor

- MFSR

Navrhovaní partneri

- NBÚ a všetky ústredné orgány VS

Odhadovaná dĺžka realizácie projektu (projektov)

- 3 roky

Závislosti na iných projektoch a prioritách (OPII a OPIS)

- Systém riadenia obnovy sa priamo dotýka prevádzky každého prevádzkovaného IS.

4.3.3 IS security awareness (eLearning)

Popis a ciel

Cieľom projektu je vybudovanie centrálneho informačného systému zameraného na vzdelávanie zamestnancov štátnej správy, udržiavanie vysokého bezpečnostného povedomia naprieč organizáciami verejnej správy a stanovovanie meraní a hodnotenie existujúceho bezpečnostného povedomia. Vytvorenie centrálneho systému umožní na jednej strane monitorovať úroveň povedomia naprieč všetkých organizáciami, rovnako umožní okamžite reagovať na novo vznikajúce hrozby a adresovať expertné informácie všetkým používateľom v konkrétnych roliach (napríklad vzdelávanie len pre správcov systémov, zodpovedné osoby za ochranu osobných údajov a pod.).

Aktivity

- Analýza a návrh riešenia.

- Analýza existujúcich dostupných materiálov a postupov zvyšovania bezp. Povedomia.
- Integrácia zdrojov dát.
- Testovanie.
- Prevádzka na centrálnej úrovni.
- Prevádzka na podriadených organizáciách.

Navrhovaný realizátor

- MFSR

Navrhovaní partneri

- Všetky ústredné orgány VS.

Odhadovaná dĺžka realizácie projektu (projektov)

- 3 roky

Závislosti na iných projektoch a prioritách (OPII a OPIS)

- Systém predpokladá existenciu KIBVS a dostatku expertov schopných pripravovať podklady a monitorovať výstupy.

4.3.4 Centrálne IAM (pre cloud)

Popis a ciel

Cieľom projektu je vybudovanie centrálneho informačného systému umožňujúceho riadenie prístupu ku cloudovým službám vybudovaným v rámci eGovernmentu. To predpokladá bezpečný proces identifikácie a autentifikácie osôb a prevádzku systému rozhodujúceho o povoleniach pre prístup konkrétnych používateľov, resp. systémov.

Aktivity

- Analýza a návrh riešenia.
- Integrácia zdrojov dát – informácie o používateľoch.
- Testovanie.
- Prevádzka na centrálnej úrovni.

Navrhovaný realizátor

- MFSR, MVSR

Navrhovaní partneri

- -

Odhadovaná dĺžka realizácie projektu (projektov)

- 2 roky

Závislosti na iných projektoch a prioritách (OPII a OPIS)

- TBD

4.3.5 IS manažmentu a správy zraniteľností

Popis a ciel

Cieľom projektu je vybudovanie centrálneho informačného systému zameraného na manažment a správu zraniteľností systémov naprieč infraštruktúrou verejnej správy. Systém bude určený predovšetkým pre podriadené organizácie a bude priamo viazaný na IS riadenia rizík. Z pozície KIBVS sa tak docieli ucelený prehľad o aktuálnych a typických zraniteľnostiach systémov v rámci eGovernmentu a z pohľadu podriadených organizácií sa tak docieli zabezpečenie expertného nástroja na manažment zraniteľností v rámci organizácie.

Aktivity

- Analýza a návrh riešenia.
- Analýza existujúcich systémov manažmentu zraniteľností.
- Integrácia zdrojov dát.
- Testovanie.
- Prevádzka na centrálnej úrovni.
- Prevádzka na podriadených organizáciách.

Navrhovaný realizátor

- MFSR

Navrhovaní partneri

- Všetky ústredné orgány VS

Odhadovaná dĺžka realizácie projektu (projektov)

- 3 roky

Závislosti na iných projektoch a prioritách (OPII a OPIS)

- IS riadenia rizík, manažmentu aktív a používateľov.

4.3.6 Govnet 2.0

Popis a ciel

Cieľom projektu je rozšírenie a obnova siete Govnet. Predpokladá sa rozšírenie prenosových kapacít, implementácia nových sieťových a bezpečnostných nástrojov a zariadení a celkové zlepšenie prevádzky siete.

Aktivity

- Analýza a návrh riešenia.
- Testovanie.

Navrhovaný realizátor

- ÚV SR (NASES)

Navrhovaní partneri

- MF SR, MV SR, NBÚ

Odhadovaná dĺžka realizácie projektu (projektov)

- 2 roky

Závislosti na iných projektoch a prioritách (OPII a OPIS)

- Priamy dopad na celé prostredie eGovernmentu.

4.3.7 Mobile Device Management

Popis a ciel

Cieľom projektu je vybudovanie centrálneho informačného systému zameraného na manažment a správu mobilných zariadení používaných zamestnancami štátnej správy. Typicky by systém mal umožniť bezpečný prístup k citlivému obsahu (sandboxing dát), vzdialenú správu aplikácií, vzdialené vymazanie obsahu zariadenia v prípade straty alebo krádeže a pod. V rámci systému by mali mať prístup jednotlivé organizácie VS s možnosťou určiť si konkrétne pravidlá a požiadavky na zariadenia vlastných zamestnancov. Z pohľadu centrálneho riadenia bude možné v rámci riešenia zabezpečiť rovnakú baseline bezpečnostnej úrovne pre mobilné zariadenia naprieč celou VS.

Aktivity

- Analýza a návrh riešenia.
- Analýza existujúcich systémov MDM využívaných v štátnej správe.
- Integrácia zdrojov dát.
- Testovanie.
- Prevádzka na centrálnej úrovni.
- Prevádzka na podriadených organizáciách.

Navrhovaný realizátor

- MFSR, NBÚ?

Navrhovaní partneri

- Všetky ústredné orgány VS.

Odhadovaná dĺžka realizácie projektu (projektov)

- 3 roky

Závislosti na iných projektoch a prioritách (OPII a OPIS)

- IS riadenia rizík, manažmentu aktív a používateľov.

4.4 Pre oblasť kybernetickej bezpečnosti

4.4.1 Vytvorenie útvaru kybernetickej ochrany

Popis a ciel

Cieľom projektu je vybudovanie centrálneho útvaru zabezpečujúceho riadenie kybernetickej bezpečnosti a ochrany kybernetického priestoru štátu. Medzi základné úlohy útvaru bude patriť najmä:

- Vytvorenie návrhu príslušných politík, štandardov, usmernení a legislatívnych aktov v oblasti riadenia KyB, vrátene definovania metrík a hodnôt jednotlivých parametrov, prioritne pre oblasť riadenie incidentov a riadenie kontinuity činností (BCM).
- Definovanie organizačného a kompetenčného postavenia jednotlivých subjektov zapojených do riešenia problematiky informačnej a kybernetickej bezpečnosti, t.j. definovanie tzv. „bezpečnostnej organizačnej štruktúry štátu“, ktorá bude riešiť oblasť informačnej a kybernetickej bezpečnosti, vrátane orgánov dohľadu, dozoru a kontroly.
- Definovanie úloh, kompetencií a zodpovedností pre jednotlivé subjekty podieľajúce sa na správe (governance) a na riadení (management) IB a KyB.
- Zavedenie systému koordinácie a riadenia informačných incidentov presahujúcich rámec organizácie (jednotný rámec riadenia BCM prioritne nad systémami KI).
- Vytvorenie technických a organizačných podmienok pre:
  - monitoring a ochranu kybernetického priestoru,
  - efektívnu obranu v prípade výskytu kybernetických útokov v kybernetickom priestore,
  - vyšetrovanie bezpečnostných incidentov v kybernetickom priestore, najmä formou:
    - zabezpečenia vytvorenia ŠU pre IT projekty potrebné pre podporu činností KyB,
    - zabezpečenia realizácie IT projektov potrebných pre podporu činnosti KyB.
- Zvyšovanie bezpečnostného povedomia zamestnancov VS v oblasti KyB a zabezpečenie R&D.
- Zabezpečenie koordinácie a podpory v oblasti medzinárodnej spolupráce a vzájomnej komunikácie.
- Dohľad, dozor, podporné činnosti a QA

- Príprava a spolupráca na podkladoch ohľadom metodického riadenia, štandardizácie, tvorby stratégie, koncepcie a plánovania.
- Príprava materiálov a spolupráca v oblasti definovania, modelovania a udržiavania bezpečnostnej architektúry VS SR.
- Vytvorenie základných obsahových šablón dokumentov z oblasti riadenia KyB.

Aktivity

- Vytvorenie podkladov a odborných materiálov, najmä:
  - náplne práce jednotlivých pracovníkov,
  - metodiky práce,
  - organizačné pokyny a pod.
- Definovanie úloh a povinností jednotlivých rolí.
- Zabezpečenie dostatočného počtu interných a externých pracovníkov na výkon jednotlivých rolí a kooperáciu s KIB a AK prostredníctvom roly bezpečnostný architekt pre príslušnú oblasť.

Navrhovaný realizátor

- NBÚ

Navrhovaní partneri

- MF SR,

Odhadovaná dĺžka realizácie projektu (projektov)

- 1 rok

Závislosti na iných projektoch a prioritách (OPII a OPIS)

- Projekt je možné realizovať samostatne.

4.4.2 IS centrálny komunikačný bod

Popis a ciel

Cieľom projektu je vybudovanie centrálneho informačného systému umožňujúceho efektívnu, rýchlu a bezpečnú výmenu informácií naprieč kybernetickým priestorom SR aj voči externým partnerom.

Aktivity

- Analýza a návrh riešenia.
- Integrácia zdrojov dát.
- Testovanie.

Navrhovaný realizátor

- NBÚ, NASES?, MFSR?

Navrhovaní partneri

- Datacentrum a následne všetky ústredné orgány VS.

Odhadovaná dĺžka realizácie projektu (projektov)

- 3 roky

Závislosti na iných projektoch a prioritách (OPII a OPIS)

- IS riadenia rizík, manažmentu aktív a používateľov.

4.4.3 IS centrálneho monitoringu kybernetického priestoru

Popis a ciel

Cieľom projektu je vybudovanie centrálneho informačného systému umožňujúceho na jednom mieste monitorovať aktuálny stav ochrany a zabezpečenia kybernetického priestoru štátu. Systém je dôležitý najmä pre zabezpečenie komplexného prehľadu v prípade krízových situácií, kedy globálny pohľad na existujúci stav zabezpečenia umožní vhodne rozhodnúť o budúcich krokoch.

Aktivity

- Analýza a návrh riešenia.
- Integrácia zdrojov dát.
- Testovanie.

Navrhovaný realizátor

- NBÚ

Navrhovaní partneri

- MFSR, Všetky orgány VS

Odhadovaná dĺžka realizácie projektu (projektov)

- 3 roky

Závislosti na iných projektoch a prioritách (OPII a OPIS)

- IS riadenia rizík, manažmentu aktív a používateľov.
- Centrálny SOC.
- Centrálny CMR.
- Centrálny SIEM.

4.4.4 Riadenie a nahlasovanie bezpečnostných incidentov

Popis a ciel

Cieľom projektu je vybudovanie centrálneho informačného systému zameraného na manažment a správu bezpečnostných incidentov naprieč systémami verejnej správy. Systém bude určený predovšetkým pre podriadené organizácie a bude priamo viazaný na IS riadenia rizík a následne na centrálny monitoring kybernetického priestoru. Z pozície ÚKO sa tak docieli ucelený prehľad o aktuálnom stave naprieč organizáciami a možnosť sledovať korelácie medzi vznikajúcimi incidentmi.

Aktivity

- Analýza a návrh riešenia.
- Analýza existujúcich systémov riadenia bezpečnostných incidentov.
- Integrácia zdrojov dát.
- Testovanie.
- Prevádzka na centrálnej úrovni.
- Prevádzka na podriadených organizáciách.

Navrhovaný realizátor

- NBÚ

Navrhovaní partneri

- MFSR, Všetky ústredné orgány VS.

Odhadovaná dĺžka realizácie projektu (projektov)

- 3 roky

Závislosti na iných projektoch a prioritách (OPII a OPIS)

- IS riadenia rizík, manažmentu aktív a používateľov.

4.4.5 Vulnerability management

Popis a ciel

Cieľom projektu je vybudovanie centrálneho informačného systému zameraného na manažment a správu zraniteľností a ohrození naprieč infraštruktúrou verejnej správy. Súčasťou projektu by malo byť predovšetkým vybudovanie centrálneho systému poskytujúceho možnosť priebežného skenovania zariadení v rámci jednotlivých organizácií a priebežného porovnávania aktuálneho stavu zabezpečenia. Z pozície ÚKO sa tak docieli ucelený prehľad o aktuálnych a typických zraniteľnostiach systémov v rámci eGovernmentu a z pohľadu podriadených organizácií sa tak docieli zabezpečenie expertného nástroja na manažment zraniteľností v rámci organizácie.

Aktivity

- Analýza a návrh riešenia.
- Analýza existujúcich systémov manažmentu zraniteľností.
- Integrácia zdrojov dát.
- Testovanie.
- Prevádzka na centrálnej úrovni.
- Prevádzka na podriadených organizáciách.

Navrhovaný realizátor

- NBÚ

Navrhovaní partneri

- MFSR, Všetky ústredné orgány VS.

Odhadovaná dĺžka realizácie projektu (projektov)

- 3 roky

Závislosti na iných projektoch a prioritách (OPII a OPIS)

- IS riadenia rizík, manažmentu aktív a používateľov.

4.4.6 Centrálny SOC, Centrálny CMR, Centrálny SIEM

Popis a ciel

Cieľom projektov je vybudovanie centrálnych systémov poskytujúcich služby SOC, CMR a SIEM pre jednotlivé organizácie verejnej správy. Z pohľadu centrálneho monitoringu tak získa centrálny orgán ucelený prehľad o aktuálnej bezpečnostnej situácii v rámci jednotlivých organizácií aj celkového kybernetického priestoru SR. Samotné organizácie zároveň získajú prístup k expertným nástrojom, ktorých použitie im umožní efektívne a bezpečne riadiť IB vo svojich podmienkach.

Aktivity

- Analýza a návrh riešenia.
- Analýza existujúcich a zavedených systémov a požiadaviek dotknutých organizácií.
- Integrácia zdrojov dát.
- Testovanie.
- Prevádzka na centrálnej úrovni.

- Prevádzka na podriadených organizáciách.

Navrhovaný realizátor

- NBÚ

Navrhovaní partneri

- MFSR, Všetky ústredné orgány VS.

Odhadovaná dĺžka realizácie projektu (projektov)

- 3 roky

Závislosti na iných projektoch a prioritách (OPII a OPIS)

4.4.7 IS ILP

Popis a ciel

Cieľom projektov je vybudovanie centrálneho systému umožňujúceho správu informácií o lustráciách nad údajmi používateľov (ILP).

Aktivity

- Analýza a návrh riešenia.
- Analýza požiadaviek dotknutých organizácií.
- Integrácia zdrojov dát.
- Testovanie.

Navrhovaný realizátor

- NBÚ, MFSR?, NASES?

Navrhovaní partneri

- Všetky ústredné orgány VS.

Odhadovaná dĺžka realizácie projektu (projektov)

- 2 roky

Závislosti na iných projektoch a prioritách (OPII a OPIS)

4.5 Pre oblasť bezpečnosti cloudu

4.5.1 IS riadenia IB v rámci datacentier

Popis a ciel

Cieľom projektu je vybudovanie systému pre podporu riadenia informačnej bezpečnosti v rámci cloud datacentier. Systém musí byť mapovaný na požiadavky a pravidlá definované KIBVS a zároveň musí poskytnúť expertné nástroje a riadenie IB cloudovej infraštruktúry.

Aktivity

- Analýza a návrh riešenia.
- Analýza existujúcich a zavedených systémov a požiadaviek dotknutých organizácií.
- Integrácia zdrojov dát.
- Testovanie.

Navrhovaný realizátor

- MV SR, MF SR

Navrhovaní partneri

- NBÚ?

Odhadovaná dĺžka realizácie projektu (projektov)

- 3 roky

Závislosti na iných projektoch a prioritách (OPII a OPIS)

- Monitoring bezpečnosti na úrovni cloudu

4.5.2 Monitoring bezpečnosti na úrovni cloudu

Popis a ciel

Projekt priamo nadväzuje na predchádzajúci. Umožní vybudovanie expertného kontrolného systému, ktorý zabezpečí monitoring celej vybudovanej cloudovej infraštruktúry v rámci datacentier štátu.

Aktivity

- Analýza a návrh riešenia.
- Analýza existujúcich a zavedených systémov a požiadaviek dotknutých organizácií.
- Integrácia zdrojov dát.
- Testovanie.

Navrhovaný realizátor

- MV SR, MF SR

Navrhovaní partneri

- NBÚ?

Odhadovaná dĺžka realizácie projektu (projektov)

- 2 roky

Závislosti na iných projektoch a prioritách (OPII a OPIS)

- IS riadenia IB v rámci Datacentier.

4.6 Podporné komponenty

4.6.1 IS PKI

Popis a ciel

Cieľom projektu je vybudovanie centrálneho informačného systému zabezpečujúceho poskytovanie služieb PKI infraštruktúry pre všetky orgány štátnej správy. Systém by mal umožniť kompletnú správu životného cyklu vydávania všetkých definovaných typov certifikátov pre zamestnancov štátnej správy a systémových certifikátov. Systém by mal umožniť organizáciám a systémom eGovernmentu automaticky žiadať o vydávanie potrebných certifikátov a umožniť integráciu voči spoliehajúcim sa systémom (napríklad pre potreby autentifikácie používateľov a systémov).

Aktivity

- Analýza a návrh riešenia.
- Analýza existujúcich a zavedených systémov a požiadaviek dotknutých organizácií.
- Integrácia zdrojov dát.
- Testovanie.

Navrhovaný realizátor

- MV SR, NBÚ?

Navrhovaní partneri

- Všetky orgány VS

Odhadovaná dĺžka realizácie projektu (projektov)

- 3 roky

Závislosti na iných projektoch a prioritách (OPII a OPIS)

4.6.2 IS AltA

Popis a ciel

Cieľom projektu je vybudovanie centrálneho systému zabezpečujúceho vydávanie a distribúciu prostriedkov v rámci tzv. Alternatívneho autentifikátora, ktorý by mal v zmysle Zákona o eGovernmente slúžiť ako náhradný prostriedok autentifikácie voči systémom verejnej správy.

Aktivity

- Analýza a návrh riešenia.
- Analýza existujúcich a zavedených systémov a požiadaviek dotknutých organizácií.
- Integrácia voči existujúcim IAM riešeniam (predovšetkým ÚPVS).
- Testovanie.

Navrhovaný realizátor

- MV SR

Navrhovaní partneri

- -

Odhadovaná dĺžka realizácie projektu (projektov)

- 2 roky

Závislosti na iných projektoch a prioritách (OPII a OPIS)

- IS ÚPVS
- IS Centrálne IAM

4.6.3 Centrálne NTP

Popis a ciel

Cieľom projektu je vybudovanie centrálneho systému zabezpečujúceho poskytovanie NTP služieb všetkým systémom eGovernmentu. Predpokladá sa vytvorenie robustného riešenia dôveryhodne poskytujúceho presný čas žiadateľom.

Aktivity

- Analýza a návrh riešenia.
- Analýza existujúcich a zavedených systémov a požiadaviek dotknutých organizácií.
- Testovanie.

Navrhovaný realizátor

- MV SR, NBÚ?

Navrhovaní partneri

- -

Odhadovaná dĺžka realizácie projektu (projektov)

- 2 roky

Závislosti na iných projektoch a prioritách (OPII a OPIS)

- Systém je možné realizovať samostatne.

5 Legislatívne požiadavky

Pre zaistenie odpovedajúcej právnej sily a vhodných podmienok pre vymáhanie požiadaviek stanovených pre oblasti bezpečnosti je potrebné prijať aj odpovedajúce právne predpisy, najmä Zákon o informačnej a kybernetickej bezpečnosti a novelizovať existujúce legislatívne predpisy v oblasti riadenia a správy informačnej bezpečnosti. Terajšie pravidlá a požiadavky na oblasť bezpečnosti, definované v rámci Výnosu MF SR č. 55/2014 o štandardoch pre ISVS, budú vyňaté a definované nanovo v rámci vyššie uvedeného zákona. Pravidlá budú výrazne bližšie spresnené a rozšírené o doteraz nepokryté oblasti.

Realizácia strategickej priority je závislá na prijatí samostatného zákona pokrývajúceho plne požiadavky tak v oblasti informačnej bezpečnosti, ako aj v oblasti kybernetickej bezpečnosti a ochrany. Praktická realizácia môže byť buď vo forme dvoch legislatívnych predpisov (IB v gescii MF SR, KyB v gescii NBÚ), alebo po dohode oboch organizácií vo forme jedného centrálneho zákona o informačnej a kybernetickej bezpečnosti v rámci verejnej správy.

Terajší stav riadenia informačnej bezpečnosti je založený najmä na existencii Výnosu č. 55/2014 Z. z. o štandardoch pre ISVS, ktorý obsahuje aj samostatné požiadavky venované oblasti informačnej bezpečnosti. Navrhuje sa tieto ustanovenia z Výnosu vyňať a vydať ich v rámci samostatného vykonávacieho predpisu už podľa požiadaviek stanovených novým zákonom o informačnej bezpečnosti.

Legislatívny predpis	Navrhované opatrenie
Zákon o informačnej bezpečnosti	Predstavenie a publikovanie zákona pokrývajúceho základné oblasti správy a riadenia informačnej bezpečnosti
Zákon o kybernetickej bezpečnosti	Vytvorenie a publikovanie zákona pokrývajúceho jednak oblasť kybernetickej ochrany a bezpečnosti, ale aj štatút monitoringu a osobitných práv pri ochrane kybernetického priestoru a kritickej infraštruktúry SR s dôrazom na ochranu a práva občanov a ich slobody
Výnos o informačnej a kybernetickej bezpečnosti	Legislatívny predpis priamo definujúci požiadavky kladené na jednotlivé orgány verejnej správy, ako aj na organizácie súkromnej sféry, ktoré spadajú do kritickej infraštruktúry štátu

6 Možné problémy a riziká

6.1 Dôsledky

Realizácia SP „Bezpečnosť“ bude vplývať na všetky orgány verejnej správy, pričom medzi najvýznamnejšie dôsledky na organizácie možno zaradiť:

- Potreba zamestnania špecialistu v oblasti návrhu a revízii bezpečnostnej architektúry na úrovni jednotlivých rezortov, prípadne inštitúcií.
- Nutnosť prevádzkovania samostatných kancelárií informačnej bezpečnosti a kybernetickej bezpečnosti v rámci MF SR, resp. NBÚ s dostatkom expertných personálnych kapacít.
- Nutnosť zapracovať procesy monitoringu a hlásenia podozrivých aktivít a následného vyšetrovania incidentov aj pre súkromné subjekty spadajúce do oblasti kritickej infraštruktúry štátu.
- CSIRT.SK musí prejsť do pôsobnosti NBÚ, alebo musí značnú časť svojich kompetencií odovzdať NBÚ.

6.2 Problémy

Je možné popísať nasledujúce predpokladané problémy s realizáciou priority bezpečnosť:

- Oblasť informačnej bezpečnosti a najmä kybernetickej ochrany sa nepretržite mení a nové riziká sa objavujú prakticky každým dňom. Nakoľko ide o nesmierne dynamickú oblasť, je možné predpokladať, že niektoré z definovaných projektov a plánov nebudú odzrkadľovať potreby zaistenia bezpečnosti v roku 2020.
- Nakoľko sa oblasť bude pravdepodobne kompetenčne deliť medzi dve rôzne inštitúcie, musí vzniknúť vhodný mechanizmus výmeny informácií a rozhodovací proces v prípade nekonzistencie požiadaviek kladených MFSR alebo NBÚ.
- Už niekoľko rokov meška publikovanie odpovedajúcich legislatívnych predpisov, najmä zákona o informačnej bezpečnosti, ktorý by oblasť legislatívne podporil a dal jej potrebnú legislatívnu silu na presadzovanie jej cieľov. Pokiaľ nebudú potrebné legislatívne predpisy vydané a schválené v blízkom čase, nebude možné efektívne riadiť bezpečnosť v rámci vznikajúcich projektov a spätné dopracovanie si môže vyžiadať neúmerne vysoké náklady, prípadne vôbec nemusí byť realizovateľné.

6.3 Riziká

Vzhľadom na široký dosah navrhovaných činností v rámci SP „Bezpečnosť“ a rozdelenie kompetenčných oblastí medzi dvoch základných gestorov je možné medzi hlavné riziká začleniť najmä:

- Príliš široký záber – s ohľadom na množstvo viazaných projektov a potrebu väčšieho množstva skúsených bezpečnostných expertov existuje reálne riziko, že sa nepodarí výstupy a požiadavky z oblasti vhodne rozšíriť na celú oblasť verejnej správy, resp. na všetky realizované projekty v rámci jednotlivých strategických priorít.
- Nezhody medzi informačnou a kybernetickou bezpečnosťou – oblasti informačnej a kybernetickej bezpečnosti majú niekoľko spoločných aj rozdielnych cieľov a vzhľadom na dve gesčné organizácie môže vzniknúť spor v napĺňaní niektorých požiadaviek z ľubovoľnej oblastí.
- Neskoré nasadenie – toto riziko súvisí s prvým popísaným rizikom a zohľadňuje skutočnosť nedostatku dostatočne skúseného personálu v oblasti bezpečnosti. Príprava jednotlivých bezpečnostných architektúr tak môže meškať až po realizácií samotných projektov, čo môže vyústiť do nekonzistencie a nevhodnosti navrhovaných riešení z pohľadu ich zabezpečenia.