ÚRAD PODPREDSEDU VLÁDY SR
PRE INVESTÍCIE
A INFORMATIZÁCIU

Doplňujúce informácie k štúdii uskutočniteľnosti národného projektu:

„Národný systém riadenia incidentov kybernetickej bezpečnosti vo verejnej správe“

V Bratislave, 25.07.2018

Informácie o dokumente

Názov:	Doplňujúce informácie k štúdii uskutočniteľnosti národného projektu: „Národný systém riadenia incidentov kybernetickе bezpečnosti vo verejnej správe“.
Stav:	Finálna verzia
Pripravil:	Ján Bačko
Verzia:	1.0

Obsah

1 Úvod

Aktuálne hrozby v oblasti kybernetickej bezpečnosti sú obrovské, neustále narastajú a môžu mať na krajinu a jej obyvateľov nedozierné následky.
Napríklad sa môže stať:

- že pacientovi niekto skompromituje zdravotné záznamy,
- že dôchodcom a ľuďom v núdzi nebudú vyplatené dôchodky,
- že podnikateľ príde o svoj denný či mesačný príjem,
- že veľká korporácia nebude môcť vykonávať svoju činnosť a príde o milióny príjmov a tisícky zákazníkov,
- že veľká časť krajiny môže zostať bez elektriny,
- že bude narušená likvidita alebo dôveryhodnosť štátu a doplatia na to ďalšie generácie.

Uvedené príklady sú poukázaním na skutočnú dennú realitu v celosvetovom meradle a nevynímajúc ani najvyspelešie štáty.

Máme tu neviditeľné armády útočníkov, ktorí napádajú krajiny a ich inštitúcie ako aj firmy a jednotlivcov. Ich najhlavnejším cieľom je ekonomický prospech alebo kompromitácia. Najväčším rizikom pre nás všetkých je možná strata majetku, dôveryhodnosti či dokonca vlastnej identity. Prípadná obnova reputácie krajiny, ktorá je súčasťou medzinárodných zoskupeni ako EÚ a NATO by mala na ekonomiku štátu nevyčísliteľné dopady a to aj pre ďaľšie generácie.

Vláde SR na bezpečnosti krajiny a našich občanov záleží, a preto sa tejto téme venuje systematicky a s veľkou vážnosťou. Je absolútne nevyhnutné, aby Slovenská republika bola chránená pred kybernetickou hrozbou, a to je vláda odhodlaná aj dosiahnuť.

2 Cieľ / Súlad so stratégiou a špecifickým cieľom 7.9 v rámci PO7

Hlavným cieľom národného projektu je vytvorenie siete adekvátne odborne a technicky vybavených jednotiek CSIRT pre riešenie kybernetických bezpečnostných incidentov na celonárodnej úrovni. Úlohou jednotiek CSIRT bude vykonávanie preventívnych a reaktívnych opatrení v oblasti svojho pôsobenia a poskytovanie relevantných informácií o kybernetických incidentoch národnej jednotke CSIRT a vládnej jednotke CSIRT.

Projekt je v súlade s Národnou stratégiou kybernetickej bezpečnosti na roky 2015 – 2020 a jej Akčným plánom ako aj so Špecifickým cieľom 7.9 v rámci OPII PO7 - Zvýšenie kybernetickej bezpečnosti v spoločnosti.

Národná stratégia pre kybernetickú bezpečnosť je aktuálne rozpracovaná do dvoch strategických dokumetov:

- Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015 - 2020, ktorá bola schválená 17. júna 2015.
- Akčný plán realizácie Koncepcie kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020, ktorý bol schválený 2. marca 2016.

Národná stratégia pre kybernetickú bezpečnosť je uvedená na nasledovnom linku: http://www.nbusr.sk/kyberneticka-bezpecnost/strategicke-dokumenty/index.html .

Cieľom Koncepcie je dosiahnutie stavu, kedy:

- Ochrana národného kybernetické priestoru je systémom fungujúcim koncepčne, koordinovane, efektívne, účinne a na právnom základe.
- Bezpečnostné povedomie všetkých zložiek spoločnosti sa systematicky zvyšuje.
- Súkromný a akademický sektor, ako aj občianska spoločnosť sa aktívne zúčastňujú na formovaní a realizácii politiky Slovenskej republiky v oblasti kybernetickej bezpečnosti.
- Je zabezpečená efektívna spolupráca na národnej, ako aj medzinárodnej úrovni.
- Prijaté opatrenia sú primerané a rešpektujú ochranu súkromia a základné ľudské práva a slobody.

Koncepcia navrhuje prijať a prioritne riešiť nasledujúcich sedem kľúčových opatrení:

- Opatrenie 1: Vytvorenie inštitucionálneho rámca riadenia kybernetickej bezpečnosti.
- Opatrenie 2: Vytvorenie a prijatie legislatívneho rámca kybernetickej bezpečnosti.
- Opatrenie 3: Rozpracovanie a aplikácia základných mechanizmov zabezpečenia správy kybernetického priestoru.
- Opatrenie 4: Podpora, vypracovanie a zavedenie systému vzdelávania v oblasti kybernetickej bezpečnosti.
- Opatrenie 5: Stanovenie a aplikácia kultúry riadenia rizík a systému komunikácie medzi zainteresovanými stranami.
- Opatrenie 6: Aktívna medzinárodná spolupráca.
- Opatrenie 7: Podpora vedy a výskumu v oblasti kybernetickej bezpečnosti.

Koncepcia a jej jednotlivé opatrenia sú detailnešie rozpracové do úloh definovaných v Akčnom pláne. Veľkú časť úloh v rámci opatrení č.1 a č.2 sa už podarilo splniť aj vďaka nedávnemu prijatiu Zákona o kybernetickej bezpečnosti č. 69/2018 Z.z., ktorý podpísal prezident Slovenskej republiky 22.2.2018.

Momentálne sa štát intenzívne venuje aj opatreniu č.3, v rámci ktorého plánuje implementovať systém včasného varovania a reakcie na incidenty ako aj funkcionalitu na bezpečnostné opatrenia pre jednotlivé kategórie informačných aktív. Na realizáciu je však potrebná transformačná investícia, ktorá vychádza z nového inštitucionálneho rámca a nových kompetencií a zodpovedností jednotiek CSIRT podľa Zákona o kybernetickej bezpečnosti ako aj z aktuálnej úrovne a kapacity ich technologického vybavenia.

Projekt je v plnom súlade so špecifickým cieľom 7.9 vo všetkých 4 oblastiach:

A. Výsledky:

- Zníženie finančných dopadov a dopadov na inštitúcie verejnej správy pri bezpečnostných incidentoch.
- Zvýšenie vyspelosti trhu s bezpečnostnými riešeniami zvýšením výdavkov na bezpečnosť verejného sektora.
- Zvýšenie kybernetickej bezpečnosti a aplikovanie najnovších poznatkov v európskom priestore.
- Zvýšenie miery inovácie v oblasti bezpečnostných opatrení.
- Zvýšenie dôvery občanov a podnikateľov v digitálny priestor.
- Zvýšenie transparentnosti pri riešení bezpečnostných incidentov a kybernetických útokov.

B. Aktivity:

Zabezpečenie komplexnej kybernetickej bezpečnosti v spoločnosti:

- Vytvorenie nástrojov na rozpoznanie, monitorovanie a riadenie bezpečnostných incidentov,
- Zabezpečenie kritickej infraštruktúry,
- Zavádzanie európskej stratégie pre kybernetickú bezpečnosť.

C. Ukazovatele:

- Počet informačných systémov verejnej správy s implementovaným nástrojom na rozpoznávanie, monitorovanie a riadenie bezpečnostných incidentov – v prípade, že realizovaný informačný systém bude mať implementované nástroje na centrálne rozpoznávanie, monitorovanie a riadenie bezpečnostných incidentov, ako ich odhaľovanie, zaznamenávanie detailov a mitigovanie a sú zapojené do centrálneho systému monitorovania bezpečnosti.

Doplnenie 1:

V rámci cieľa NKIVS je definovaná počiatočná hodnota 90 percent a cieľová 98 percent štandardných incidentov. V rámci tejto hodnoty sa jedná o počet detegovaných a vyriešených bezpečnostných incidentov prostredníctvom automatizovaných štandardných postupov. Jedná sa napríklad o štandardné phishingy, šírenie štandardného a mierne upraveného škodlivého kódu, detekcia a prevencia štandardných pokusov o kybernetický útok (napríklad SQL injection, command injection, zneužitie známych zapatchovaných zraniteľností).
V rámci štúdie je cieľom systému detegovať a riešiť bezpečnostné incidenty, ktoré sú cielené, sofistikované alebo svojim dopadom spôsobili nejakú škody, alebo kybernetické útoky ktoré sú systematické, dlhodobé alebo vedené na rôzne inštitúcie z rovnakých zdrojov. V súčasnosti je počet takýchto incidentov v reálnej hodnote 5 percent detegovaných a vyriešených a cieľová hodnota po realizovaní projektu je 20 percent detegovaných a vyriešených takýchto bezpečnostných incidentov. Táto hodnota bude ďalej zvyšovaná ďalšími činnosťami úradu, a partnerov projektu ako aj jednotlivými organizáciami verejnej správy prostredníctvom zmien procesov, dodržiavania definovaných štandardov ako aj dopytových výziev na dovybavenie organizácií verejnej správy z hľadiska zabezpečenia

infraštruktúry (nie CSIRT služby, tie budú už pokryté týmto projektom a štátnym rozpočtom z hľadiska prevádzky) .

D. Žiadatelia

- Inštitúcie verejnej správy, ktoré majú v kompetencii kybernetickú bezpečnosť.
- Prevádzkovatelia informačných systémov verejnej správy, ktorí potrebujú zabezpečiť svoje informačné prostredie z pohľadu kybernetickej bezpečnosti (najmä integrácia na centrálny monitoring bezpečnostných incidentov).
- V rámci dopytovo-orientovaných projektov malí a strední podnikatelia, ktorí ponúkajú inovatívne riešenia pre zvýšenie ochrany kybernetického priestoru.

Doplnenie 2:

Dopytovo orienované výzvy nie sú predmetom tohto projektu.

3 Potreba a urgentnosť projektu

Potreba projektu je definovaná z rôznych úrovní postavenia a potrieb Slovenskej republiky. Ide predovšetkým o nasledovné vymedzenie:

- Zabezpečovanie kybernetickej bezpečnosti a spolupráce v rámci SR.
- Zabezpečovanie kybernetickej bezpečnosti a spolupráce v rámci medzinárodného postavenia SR a záväzkov voči EÚ v rámci súvisiacich agiend a interoperabilty.
- Implementácia národnej stratégie a akčného plánu kybernetickej bezpečnosti.
- Zbezpečovanie zákonných povinností a kompetencií jednotiek CSIRT v rámci nového inštitucionálneho vymedzenia.

Urgentnosť projektu vyplýva z naliehavej potreby jednotiek CSIRT na dobudovanie a zvýšenie kapacity svojej infraštruktúry ako aj z potreby na dobudovanie špecializovaných pracovísk pre komplexné riešenie riadenia incidentov v zmysle nových kompetencií a zákonných povinností týchto jednotiek CSIRT.

Nový zákon o kybernetickej bezpečnosti ustanovuje nové zodpovednosti, inštitucionálne vymedzenie a pôsobnosť jednotiek CSIRT ako aj zodpovednosť a povinnosti prevádzkovateľov základných služieb.

Národná jednotka CSIRT, ktorá je v pôsobnosti NBÚ okrem iného zo zákona aj spravuje a prevádzkuje jednotný informačný systém kybernetickej bezpečnosti. Jednotný informačný systém kybernetickej bezpečnosti obsahuje aj komunikačný systém pre hlásenie a riešenie kybernetických bezpečnostných incidentov a centrálny systém včasného varovania. Národná jednotka CSIRT zabezpečuje aj akreditáciu jednotiek CSIRT. Jednotný informačný systém ako aj modul pre akreditáciu sú predmetom tohto národného projektu, preto je nevyhnutné projekt čo najskôr realizovať aby bolo možné tieto aktivity vykonávať v rámci adekvátnej systémovej podpory.

Vládna jednotka CSIRT, ktorá je v pôsobnosti Úradu podpredsedu vlády SR pre investície a informatizáciu zodpovedá za riešenie kybernetických bezpečnostných incidentov a vykonáva preventívne služby a reaktívne služby v rámci podsektora Informačné systémy verejnej správy.

NASES ako prevádzkovateľ základnej služby je zo zákona povinný riešiť a nahlasovať kybernetické bezpečnostné incidenty ako aj spolupracovať s Národnou jednotkou CSIRT a Vládnou jednotkou CSIRT pri riešení hláseného kybernetického bezpečnostného incidentu a na tento účel im poskytnúť potrebnú súčinnosť, ako aj informácie získané z vlastnej činnosti dôležité pre riešenie kybernetického bezpečnostného incidentu.

Žiadateľ v spolupráci s partnermi projektu navrhol vybudovanie národného systému riadenia incidentov kybernetickej bezpečnosti postupne vo viacerých fázach a v zmysle priority - v čo najkratšom čase minimalizovať čo najväčšie množstvo hrozieb a potenciálnych dopadov na ekonomiku SR. Z tohto dôvodu bol do prvej fázy zaradený národný projekt „Národný systém riadenia incidentov kybernetickej bezpečnosti vo verejnej správe“, lebo ISVS predstavujú z hľadiska veľkosti a možnej zraniteľnosti najväčšiu časť v rámci národnej pôsobnosti SR.

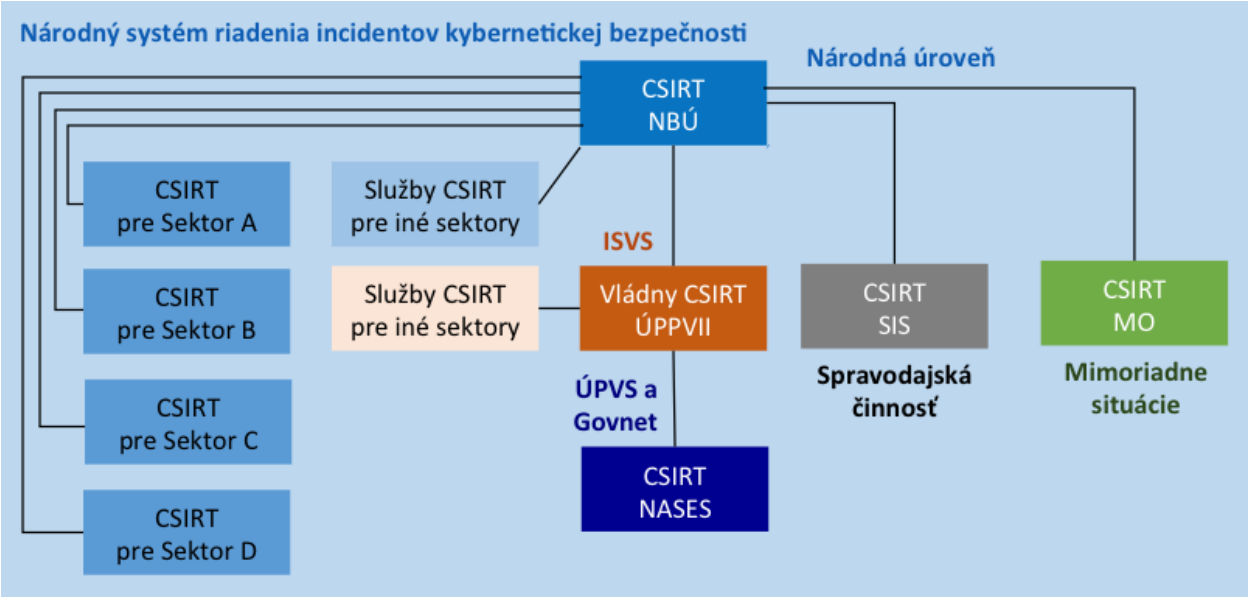
4 Kompetenčný model jednotiek CSIRT

Postavenie partnerov projektu v oblasti kybernetickej bezpečnosti vyplýva zo schválenej legislatívy, operačného pôsobenia jednotlivých partnerov, ako aj systematického prístupu k riešeniu kybernetickej bezpečnosti vo verejnej správe.

Z hľadiska legislatívy sa jedná najmä o :

- Zákon o kybernetickej bezpečnosti
- Zákon o ISVS (výhľadovo ITVS)
- Zákon o E-governemente
- Zákon o kritickej infraštruktúre

Vymedzenie pôsobnosti jednotiek CSIRT znázorňuje nasledovný obrázok:



4.1 Koncept národného systému kybernetickej bezpečnosti

Koncept národného systému je navrhnutý na princípe škáľovateľnosti a umožňuje postupné zapájanie sektorových CSIRT do národného systému ako aj poskytovanie služieb zo strany národnej a vládnej jednotky CSIRT pre tie ústredné orgány, ktoré o to požiadajú pretože sa rozhodli nebudovať si vlastnú sektorovú jednotku CSIRT.

Jednotlivé riešenia partnerov sú navrhnuté tak, že na žiadnom z pracovísk v zmysle ich zamerania v rámci pôsobnosti partnera nedochádza k duplicitám činností ani technologického vybavenia. V rámci analýzy boli vyhodnované aj možnosti zabezpečovať niektoré činnosti pracovísk prostredníctvom nákupu služieb od externých dodávateľov alebo špecializovaných agentúr. Pre výkon svojich zákonných povinností ale partneri takúto možnosť zamietli v záujme zachovania svojej integrity a samostatnosti. To však do budúcnosti nevylučuje zapojiť pre konkrétne účely aj externých poskytovateľov služieb. Na základe výsledov analýzy bola nakoniec zo strany partnerov odsúhlasená alternatíva plnej autonómnosti každej jednotky CSIRT so zapojením do národného systému na báze integrovateľnosti pracovísk do jedného celku. V praxi to znamená, že každá jednotka CSIRT bude vykonávať svoju pôsobnosť prostredníctvom vlastných pracovísk, ktoré budú pripojené do národného systému. V prípade potreby bude preto možné na národnej úrovni spojiť tieto kapacity do jedného celku v rámci spoločného postupu všetkých jednotiek CSIRT.

4.2 Pracoviská národného systému kybernetickej bezpečnosti

Národný systém riadenia incidentov kybernetickej bezpečnosti vo verejnej správe pozostáva z nasledovných pracovísk:

- **Bezpečnostný dohľad** – monitorovanie bezpečnostne relevantných udalostí v zapojených infraštruktúrach, ich korelácia a vyhodnocovanie. Detekcia a riešenie bezpečnostných incidentov. Prevádzka dohľadového centra a monitorovacej infraštruktúry.
- **Manažment a podpora riešenia bezpečnostných incidentov** – podpora procesov riešenia bezpečnostných incidentov, vydávanie varovaní a oznámení o bezpečnostných incidentoch a hrozbách. Notifikácia relevantných subjektov.
- **Dátová analýza** – zber, analýza, vyhodnocovanie a vizualizácia dát z interných, externých, verejných a neverejných zdrojov a ich využitie pre potreby detekcie a prevencie bezpečnostne relevantných udalostí a incidentov.
- **Penetračné testovanie** – interné, externé a hybridné penetračné testy a hodnotenie zraniteľností. Testovanie bezpečnostných vlastností produktov, systémov, sietí a zariadení.
- **Forenzná analýza** – forenzná analýza pracovných staníc, serverov, sieťových prvkov, sieťovej komunikácie, mobilných technológií a ostatných relevantných nosičov digitálnych stôp. Znalecké posudzovanie.
- **Analýza škodlivého kódu** – identifikácia činností a aktivít škodlivého kódu. Statická, behaviorálna, dynamická analýza a reverzné inžinierstvo vzoriek škodlivého kódu. Vytváranie identifikátorov kompromitácie (IOC), detekčných mechanizmov.
- **Testovanie a vývoj** – pracovisko pre testovanie produktov, nových typov útokov, bezpečnostných mechanizmov, nástrojov pre penetračné testovanie, riešenie bezpečnostných incidentov a forenznú analýzu. Testovanie konfigurácií sieťových a bezpečnostných prvkov (Testovacie laboratórium).
- **Certifikácia** – vykonávanie prevádzkových skúšok a testovacej prevádzky ako aj ďalšie úkony spojené s certifikáciou systémov a prostriedkov pre kybernetickú bezpečnosť.

Navrhnutý systém riadenia bezpečnostných incidentov vytvára základnú kostru riešenia bezpečnostných incidentov, bezpečnostného dohľadu a spracovania bezpečnostných udalostí na národnej úrovni.

Uvedený systém je rozdelený na tri časti :

- Vybudovanie infraštruktúry umožňujúcej bezpečnostný dohľad, spracovanie informácií, ich vyhodnotenie, uloženie a diseminácu informácií zapojeným partnerom aj ostatným relevantným subjektom (INFRA).
- Vybavenie pracovísk poskytujúcich preventívne činnosti (PREVE).
- Vybavenie pracovísk poskytujúcich reaktívne činnosti (REAKTI).

Pričom na základe informácií od partnerov, kde je možné informácie zverejniť je pomer medzi jednotlivými časťami :

- INFRA – 60 percent
- PREVE – 20 percent
- REAKTI – 20 percent

Vysoké náklady do prvej časti projektu sú spôsobené prijatím novej legislatívy (Zákon o KB – potreba vybudovania JISKB, Pripravovaný zákon o ITVS – potreba bezpečnostného dohľadu), aktuálnou bezpečnostnou situáciou (dáta v informačných systémoch verejnej správy a komerčného sveta majú kritickú a často krát už nie je možný návrat do papierového sveta –

viď digitalizácia), ale najmä dlhodobého neinvestovania do bezpečnosti vo verejnej správe resp. na národnej úrovni.

Z hľadiska zamerania sa jednotlivé pracoviská rovnako volajú ale systematicky vykonávajú iné činnosti.

Doplnenie 3:

V rámci predpokladaného rozpočtu Vládnej jednotky CSIRT je do sumy hardvéru a softvéru zarátané:

- Investícia do monitorovacieho riešenia a infraštruktúry potrebnej pre vybudovanie monitoringu, vrátane úpravy priestorov, čo predstavuje cca 60 % ceny projektu.
- Štandardný HW a SOFTWARE, ktorý predstavuje cca 15 % ceny projektu.
- Špeciálny HW a SW, vrátene inštalačných prác, konfigurácie a vývoja softvéru, ktorý predstavuje cca 20 % projektu.
- Ostatné položky projektu, ktorý reprezentujú školenia a konzultácie pre zamestnancov CSIRT cca 5 % projektu.

Analogicky sú postavené rozpočty všetkých partnerov, kde vo všeobecnosti platí pravidlo že infraštruktúra predstavuje 60 % ceny projektu a špecializované časti riešenia 40 %. Podiel infraštruktúry zohľadňuje aktuálny stav voči potrebám cieľového riešenia.

4.3 Príklady niektorých pracovísk (primárne tie, ktoré boli rozparované v rámci pripomienok):

Pozn : Pracoviská SIS nie sú uvádzané.

Pracovisko penetračného testovania (napríklad menej ako 5 percent sumy projektu za UPVII):

- NASES : automatizované testy nových buildov prevádzkovaného softvéru a automatizované ohodnocovanie rekonfigurovanej siete primárne z hľadiska dostupnosti poskytovaných služieb.
- UPPVII: testovanie úrovne zabezpečenia IS a infraštruktúr organizácií verejnej správy primárne z Hľadiska možnosti kompromitácie jednotlivých ISVS a infraštruktúr, detekcia bezpečnostných zraniteľností a ich oprava.
- NBÚ : vybudovanie špecifických spôsobilostí, ktoré nemajú ostatní partneri (napr. SCADA lab, žiaden iný parter nepríde do styku zo SCADA systémami)

Pracovisko škodlivého kódu:

- NASES : automatická detekcia škodlivého kódu v prílohách súborov, v sieťovej komunikácií, základné overenie škodlivosti vzorky.
- UPVII : analýza škodlivého kódu ako súčasť reakcie na bezpečnostných incidenty, súčasť threat huntingu
- NBÚ : agregácia a analýza poskytnutých údajov od sektorových CSIRTov, ich obohatenie a identifikácia hrozieb na základe korelácie s ďalšími informáciami.

Pracovisko bezpečnostného dohľadu:

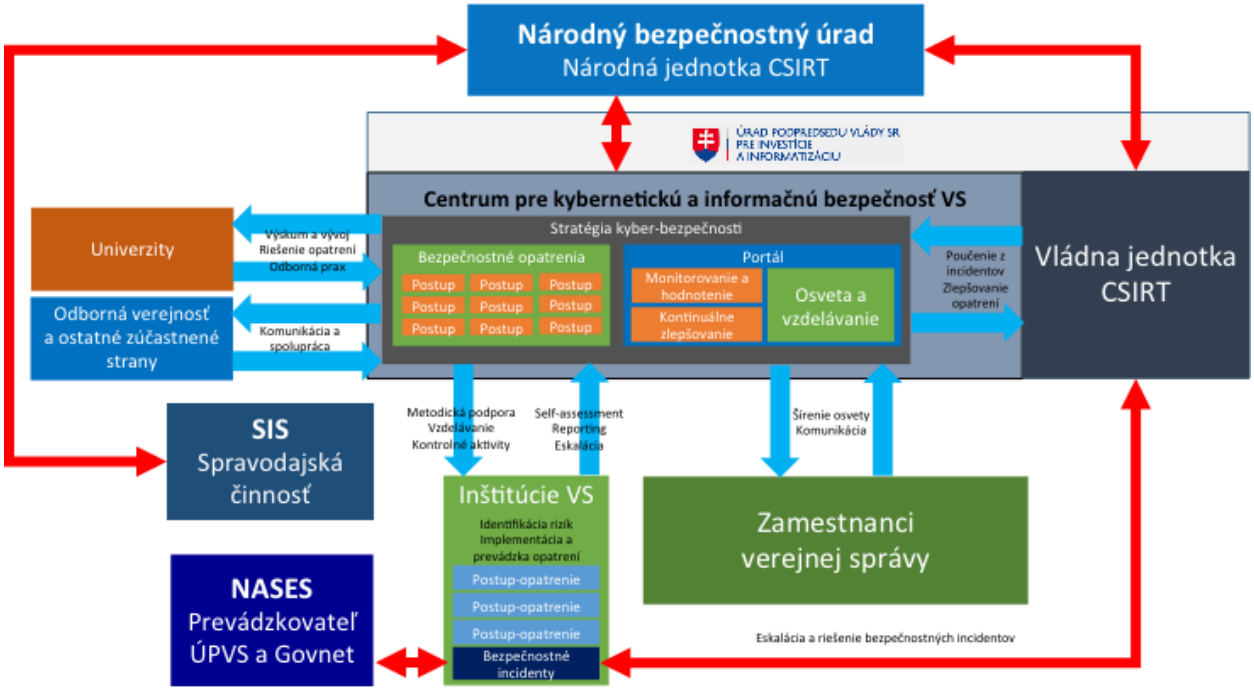
- NASES : monitoring siete Govnet a UPVS
- UPVII: monitoring ostatných OVM nepokrytých NASES (plná integrácia riešenia, systémy budú tvoriť časom jedno riešenie). Vyhodnocovanie poskytnutých dát, korelácia s IOC, ich vyhodnotenie (súčasť pracoviska dátovej analýzy) a ich zdielanie s pracovisko NBU
- NBU: vyhodnocovanie dát na národnej úrovni , detekcia bezpečnostných hrozieb na národnéj úrovni.

Poznámka: Vzhľadom na uvedené rozdelenie rolí a diametrálne odlišné činnosti by vybudovanie pracoviska, ktoré by vykonávalo všetky uvedené činnosti (bez ohľadu na to, že by to legislatívne nebolo možné) by stálo rovnako ako suma všetkých častí. V niektorých prípadoch, vzhľadom na to, že činnosť týchto pracovísk závisí od ďalších kapacít partnera, by bolo potrebné tieto kapacity nahradiť, alebo by bolo potrebné vybudovať interface s týmito kapacitami, čo by si vyžadovalo ďalšie personálne a finančné náklady.

Filozofia, ktorá bola aplikovaná pri jednotlivých partneroch a pracoviskách stála na nasledujúcich pilieroch :

- Monitoring vládnej siete Govnet, zabezpečenie riešenia štandardných bezpečnostných incidentov v sieti Govnet, zabezpečenie proaktívnych bezpečnostných činností pre prevádzkované systémy - NASES
- Monitoring ostatných OVM, systematický analýza bezpečnostných udalostí, proaktívne činnosti vo verejnej správe, reaktívne činnosti vo verejnej správe (forenzná analýza, reakcia na bezpečnostné incidenty – najmä pokročilé a rozsiahle, štandardné, kde nebudú kapacity) - UPVII
- Zabezpečenie JISKB, vyhodnocovanie bezpečnostných udalostí na národnej úrovni, budovanie kapacít, ktoré nemajú ostatné zložky (penetračné testovanie, forenzná analýze a riešenie BI SCADA systémov), vytvorenie last rezort CSIRTu na národnej úrovni (povinnosť zo zákona o KB) - NBU
- Obohacovanie bezpečnostných udalostí o informácie zo spravodajskej činnosti - SIS

Komplexný pohľad na pôsobnosť inštitúcií v oblasti kybernetickej bezpečnosti vo verejnej správe znázorňuje nasledovný obrázok:



4.4 Organizačné zabezpečenie pôsobnosti jednotiek CSIRT

Organizačné zabezpečenie pôsobnosti jednotiek CSIRT bude vzhľadom na prijatý koncept plnej autonómnosti každej jednotky zabezpečovaný zo strany partnerov projektu vlastnými pracovníkmi. Toto si vyžaduje vytvorenie nových pracovných miest a postupné navýšenie personálnych kapacít počas trvania projektu v období 2019 až 2020 v nasleovnom rozsahu:

Žiadateľ UPPVII v rámci projektu ráta s personálnym navýšením vládnej jednotky CSIRT.SK. Personálne navýšenie sa uskutoční vo fázach, tak aby umožnilo zabezpečenie potrebných aktivít a služieb vládnej jednotky CSIRT ako aj bezpečnostného dohľadu (SOC).

Navýšenie personálu je naplánované nasledovne:

- v roku 2018 = 4 špecialisti CSIRT,
- v roku 2019 = 13 špecialistov CSIRT a 8 špecialistov pre bezpečnostný dohľad (SOC),
- v roku 2020 = 6 špecialistov pre bezpečnostný dohľad (SOC).

Vzhľadom na nedostatok špecialistov, ktorí by mohli uvedené role zastávať, ÚPPVII pripravuje v spolupráci s Univerzitami program na systematické vzdelávanie mladých talentov, ktorí dostanú príležitosť pracovať so špecialistami CSIRT.

V rámci vzdelávania ÚPPVII v spolupráci s Univerzitami plánuje spustiť už v roku 2018 projekt **CSIRTie hniezdo**, v rámci ktorého špecialisti s praxe v spolupráci s expertmi z akademického sektora budú systematicky školiť prihlásených študentov v oblasti kybernetickej a informačnej bezpečnosti. V kombinácií s praktickou činnosťou pre ÚPPVII budú absolventi tohto štúdia plne vybavení vykonávať špecializované role v súkromnom alebo štátnom sektore.

Partner NASES má naplánované personálne navýšenie jednotky CSIRT v roku 2019 o 5 nových pracovníkov.

U partnerov NBÚ a SIS sa počet pracovníkov neuvádza nakoľko je predmetom utajovaných skutočností.

5 Návratnosť projektu

5.1 Prístupy pre výpočet návratnosti projektu

Pre výpočet návratnosti projektu môžu byť použité rôzne prístupy a metodiky ako napríklad:

- výpočet na základe vlastných údajov o stave kybernetickej bezpečnosti,
- výpočet na základe dôveryhodných štatistických údajov,
- neposudzovanie návratnosti.

Výpočet na základe vlastných údajov predstavuje modelovanie detailných informácií o aktuálnom stave kybernetickej bezpečnosti, ktoré vyplýva zo skutočného počtu odhalených incidentov, poznania hrozieb a ich výskytu, poznania vlastnej zraniteľnosti, a poznania skutočných dopadov incidentov. Tento prístup predstavuje najpresnejšie východiská pre ocenenie možných dopadov.

Stanovenie dopadov je možné založiť len na expertnom odhade, koľko incidentov sa reálne vyskytne, ktoré dokážeme detekovať, aká je miera detekovaných voči celkovým, koľko z nich bude možné eliminovať a koľko bude takých, čo budú mať skutočný dopad na subjekty a ekonomiku. Ani vyčíslenie dopadov nebude nikdy presné a v mnohých prípadoch je prakticky nemožné. Vyčíslenie celkových dopadov je viaczložkové a pozostáva mnimálne s týchto častí:

1. Náklady na odstránenie chyby a následkov incidentu.
2. Opportunity costs pri nefungujúcich službách.
3. Finančné straty, defraudácia.
4. Finančné manipulácie vďaka zisteným informáciám (insider trading).
5. Strata intelektuálneho vlastníctva, neverejných informácií.
6. Reputačné a právne náklady.

Dôveryhodné štatistické údaje sú publikované prostredníctvom renomovaných spoločností a agentúr. Tie môžu mať tiež rôznu úroveň presnosti nakoľko vznikajú väčšinou v prieskumoch. Z tých prieskumov nie je presne známe, či vybraná vzorka respondentov má dostatočnú vypovedaciu schopnosť o aktuálnom stave kybernetickej bezpečnosti. Taktiež nie je možné potvrdiť mieru dôveryhodnosti údajov lebo nevieme, či respondeti odpovedali pravdivo a v akej miere spoľahlivosti ocenili svoje straty, tzn., ktoré zo šiestich vyššie uvedených nákladov a dopadov ocenili. Samotné ocenenie incidentov má preto veľký cenový rozptyl od tisícov až po milióny pri tých najzávažnejších.

Z uvedeného dôvodu renomované spoločnosti spájajú tieto údaje do metadát, ktoré vychádzajú z množstva štúdií a prieskumov z rôznych krajín a odvodzujú z nich dopady postavené na koeficientoch voči makroekonomickým ukazovateľom. Jedna z najpresnejších metód je dnes uvádzaná ako odvodenie dopadov kybernetických incidentov cez pomerový ukazovateľ voči Hrubému domácemu produktu, ktorý sa aktuálne odporúča nastaviť niekde v intervale od 0,59% do 0,89% HDP. Tu však treba poznamenať, že rádový ročný rast kybernetických dopadov znamená, že bude rásť aj tento koeficient do vyššieho percentuálneho intervalu. V priebehu dvoch rokov môžeme očakávať kľudne jeho dvojnásobok.

5.2 Rôzne argumentačné línie na obhajobu projektu CSIRT

Konzervatívnosť výpočtu

Na základe McAfee štúdie uvažujeme, ze škody z kybernetických incidnetov sú 0.8 percenta HDP. Projekt následne rieši proaktívne a reaktívne služby (cca 1:1), pričom odhadujeme že sa bude riešiť iba 20% všetkých incidentov (zvyšok je priestor napr. pre súkromný sektor - co je jeden z argumentov co pouziva SK.digital, inak povedané, netvrdíme, že tento projekt všetko vyrieši). Z tohto počtu incidentov zase konzervatívne uvažujeme, že projekt zabráni iba cca 40% škodám.

Čize inak povedane, hovoríme, ze projekt z 0.8% HDP ušetrí 8% (v skutočnosti z 0,6HDP, pretože do proaktívne služby sa týkajú iba štátneho rozpočtu).Toto konzervatívny odhad (ale stále dostatočný smerom k obhajobe projektu). Tento konzervatívny odhad sme si mohli dovoliť práve preto, že uvažujeme riešenie najmä závažnejších incidentov, ktoré sa týkajú kritických systémov, kde predpoklad vyšších škôd (cca 100 000 Eur na incident).

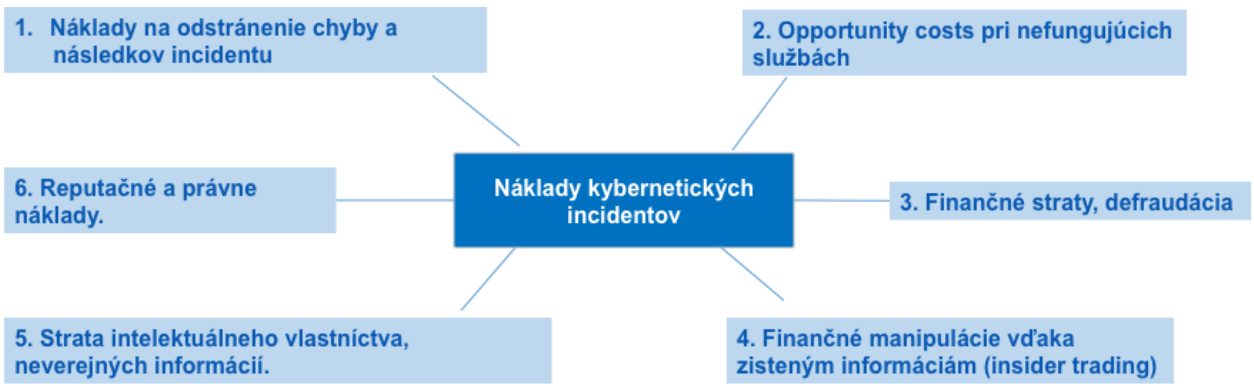
Rekapitulácia = výpočet je 0,6 HDP * 0,8% * 20% incidentov * 40% škôd, t.j. cca 8% * 0.8% HDP. Číslo, ktoré zobralo SK.digital je založené na odhade z UK na veľkom počte incidentov (každý druhý zločin je v UK spojený s kybernetickým priestorom) čo vplýva na nižšiu priemernú cenu. Toto však nie je ďalej zohľadnené. Správne by pri použití nižšej ceny incidentu bolo zvýšenie počtu incidentov (keďže my v súčasnej verzii uvažujeme s nízkym počtom významnejších incidentov – veď CSIRT má v poslednej štatistike iba 347 incidentov, v UK sa bavia o neporovnateľne väčšom počte).

Tento fakt koreluje aj s informáciami uvedenými v štúdii o UK „A senior British official reported, for example, that half of all reported crime in the UK is cyber-related“. Je pravdepodobné, že z tohto faktu vyplýva aj nízka hodnota priemerného UK kybernetického incidentu – pretože ju znižujú početné drobné incidenty zanedbateľnej hodnoty.

Nevieme aké typy škôd berie číslo zvolené SK.digital do úvahy

Čo všetko berie do úvahy štúdia + potenciálne problémy:

- Problém s určovaním cien a nákladov kybernetických incidentov je potrebne brať do úvahy vela faktorov. To vzhľadom na neexistujúce praktiky a štandard spôsobuje veľké variácie v rôznych odhadoch škôd – niektoré štúdie zahŕňajú iba náklady na odstránenie chyby, iné štúdie to berú komplexnejšie. Štúdia McAfee pri určovaní nákladov kybernetických incidentov berie do úvahy nasledovné typy nákladov:



- variáciou je aj aký typ incidentu štúdie rátajú do zoznamu – či sú to jednoduché DoS útoky, alebo až samotné prieniky do infraštruktúry. Štúdia McAfee za incident považuje práve úspešný pienik, resp. získanie prístupu k počítaču/systému obete,
- nereportovanie a nepriznanie incidentov, prípadne priznávanie iba nízkych škôd
- problém distribúcie škôd - ak napr. krajina mala 10 incidentov so sumárnou škodou 100 eur, tak priemerná cena je 10 eur. V skutočnosti však distribúcia bude taká, že dava incidenty stáli 50 a ostatných 8 skoro nič. Navyše, niektoré incidenty (a prípadne škody) ani len neboli odhalené.

Kontrola správnosti odhadu v štúdii McAfee

Autory štúdie spravili aj kontrolu, či ich odhad je reálny porovnaním s výškou škôd iných druhov trestnej činnosti, ako napríklad:

- drobné krádeže (0,5 až 2 percentá HDP),
- medzinárodný zločin (1,2 percenta HDP).

Záver porovnania: škody z kybernetického zločinu sú porovnateľné s inými druhmi trestnej činnosti a nie sú teda „mimo“.

Do úvahy boli brané aj údaje z poisťovní, ktoré poskytujú poistenie proti kybernetickým incidnetom. Vzťah medzi výškou škôd a rozvinutosťou krajiny z hľadiska elektronizácie je nepriamo úmerný, nakoľko elektronizované krajiny poskytujú lepší cieľ. Krajiny s najväčšími stratami sú krajiny s začínajúcou elektronizácou – tie, ktoré sú už elektronizované, ale ešte nemaju rozvinutú ochranu kybernetického priestoru.

Poznámka: pre Európu je odhad od 0,79 do 0,89, čiže zvolené percento je na spodnej úrovni odhadu.

Údaje Slovensko.digital sú menej presné ako údaje z štúdie McAfee

Presnejšie dáta Slovensko.digital nie sú v skutočnosti presnejšie, ale práve naopak nepresnejšie, nakoľko vybrali iba jeden vstup zo štúdie McAfee Economic Impact of Cybercrime.

Aj odhad ÚPPVII aj odhad Slovensko Digital vychádzajú z rovnakého dokumentu – štúdie McAfee Economic Impact of Cybercrime. ÚPPVII však ako vstup použilo výsledok tejto štúdie (t.j., že celkové škody z kybernetických incidentov dosahujú výšku 0.8% HDP), ktorý bol získaný na základe meta-analýzy (teda analýzy analýz) údajov z rôznych krajín sveta.

Jedna z analyzovaných krajín bola Veľká Británia, pri ktorej bolo uvedené, že priemerná cena kybernetického incidentu je 26,700 USD, čo je číslo, ktoré uvádza Slovensko Digital (číslo bolo **zistené na základe telefonického dotazníka** 1523 firiem z UK, čo vytvára otázky o porovnateľnosti tohto výskumu s globálnymi štatistikami) .Rovnako však zo štúdie mohli vziať ľubovolné iné číslo, napríklad že vláda Veľkej Británie plánuje v oblasti kybernetickej bezpečnosti preinvestovať 2.5 miliardy dolárov.

ÚPPVII má tiež v štúdii uskutočniteľnosti uvedený aj prístup na základe výšky škôd z kybernetických incidentov (model aký zvolilo Slovensko Digital). Tento prístup však nebol

zvolený pre vysoký rozptyl medzi odhadmi výšky škôd, ktoré sú v odbornej literatúre uvádzané od spomínaných 26,700 až do rádovo miliónov USD podľa typu incidentu.

ÚPPVII sa dopočítalo k cene kybernetického incidentu presnejším výpočtom na základe:

- odhadu škôd ako podielu HDP (štúdia McAfee, ktora zahŕňa aj údaje Slovensko.digital, avšak aj iné údaje, čo vedie k presnejšiemu odhadu),
- štatistiky českých a slovenských jednotiek pre riešenie kybernetických bezpečnostných incidentov,
- expertného odhadu podielu zachytených incidentov.

Zároveň je však potrebné poznamenať, že odhad škôd z kybernetických incidentov nie je exaktná veda, pretože väčšina firiem nemeria a ani nezverejňuje škody, ktoré nastali. Súčasne je možné odôvodnene predpokladať, že nezanedbateľná časť kybernetických útokov nie je nikdy ani zistená.

Investícia do národného systému, ktorým sa technologicky dovybavia pracoviská CSIRT v štyroch kľúčových inštitúciách je primeraná a porovnateľná s investíciami na národnej úrovni v iných krajinách.

6 Odôvodnenie výberu žiadateľa (prijímateľa) a partnerov projektu

Hlavný cieľ projektu:

Vytvorenie siete adekvátne odborne a technicky vybavených jednotiek CSIRT na celonárodnej úrovni, ktorých úlohou bude vykonávanie preventívnych a reaktívnych opatrení v oblasti svojho pôsobenia a poskytovanie relevantných informácií o kybernetických útokoch Vládnej jednotke CSIRT **s cieľom zaistenia ochrany informačných systémov verejnej správy**.

Hlavné zákonné východiská:

Statusovým predpisom pre oblasť informačných systémov verejnej správy (ďalej len "ISVS") je zákon č. 275/2006 Z.z. v znení neskorších predpisov (ďalej len "zákon o ISVS").

Každý správca ISVS je povinný podľa § 3 ods. 4 písm. b) zákona o ISVS zabezpečovať bezpečnú a spoľahlivú prevádzku ISVS, vrátane organizačného, odborného a technického zabezpečenia.

Statusovým predpisom pre oblasť kybernetickej bezpečnosti a pôsobenie jednotiek CSIRT je zákon č. 69/2018 Z.z. (ďalej len "ZoKB"). ZoKB sa vzťahuje aj na ISVS, keďže podľa § 3 písm. k) je každý ISVS základnou službou.

Podľa § 19 ods. 1 ZoKB je každý prevádzkovateľ základnej služby povinný zaviesť a dodržiavať bezpečnostné opatrenia a podľa § 19 ods. 6 je o.i. povinný každý bezpečnostný incident riešiť, nahlásiť a spolupracovať pri jeho riešení s Národným bezpečnostným úradom (ďalej len "NBÚ") a (v prípade ISVS) aj s ÚPVII.

Jednotka CSIRT podľa ZoKB plní úlohy v oblasti riešenia kybernetických incidentov a je tým útvarom, ktorý pôsobí nielen preventívne, ale aj reaktívne a poskytuje svoje služby primárne pre poskytovateľov základných služieb (teda aj ISVS) pri riešení kybernetických incidentov.

Podľa § 3 písm. k) ZoKB je každý prvok kritickej infraštruktúry základnou službou a vzťahuje sa naň ZoKB so všetkými bezpečnostnými opatreniami. Podľa § 3 písm. c) a prílohy č. 3 zákona č. 45/2011 Z.z. v znení neskorších predpisov (ďalej len "ZoKI") je ÚPVII orgánom, ktorý vykonáva štátnu správu na úseku prvkov kritickej infraštruktúry, ktorými sú informačné systémy a siete, teda aj ISVS.

Prijímateľ a partneri:

Prijímateľom národného projektu je ÚPVII.

ÚPVII je podľa § 34a zákona č. 575/2001 Z.z. v znení neskorších predpisov (ďalej len "kompetenčný zákon") ústredným orgánom štátnej správy (aj) pre oblasť informatizácie spoločnosti, v rámci ktorej o.i. zabezpečuje centrálne riadenie informatizácie spoločnosti.

Táto kompetencia sa v oblasti bezpečnosti ISVS premieta najmä do kompetencií podľa (i) § 4 ods. 1 písm. f) zákona o ISVS, podľa ktorého ÚPVII riadi a koordinuje informačnú bezpečnosť ISVS a (ii) § 6 zákona o ISVS, podľa ktorého ÚPVII vydáva štandardy pre ISVS (aj) v oblasti bezpečnosti ISVS.

Osobitne vo vzťahu ku kybernetickej bezpečnosti je ÚPVII podľa § 4 písm. b) ZoKB ústredným orgánom v sektore verejná správa - ISVS. Okrem toho podľa § 11 ZoKB prevádzkuje ÚPVII zo zákona vládnu jednotku CSIRT, ktorá plní úlohy prevencie a riešenia kybernetických incidentov priamo v sektore verejná správa - ISVS. Vládna jednotky CSIRT má osobitné postavenie z dvoch dôvodov - jednak ide o jednu z troch zákonov priamo zriadených jednotiek CSIRT a tiež je zriadená priamo pre oblasť ISVS.

V sumarizácii teda dôvodmi, prečo je ÚPVII prijímateľom národného projektu platí, že:

- je ústredným orgánom štátnej správy (aj) pre oblasť riadenia bezpečnosti ISVS podľa kompetenčného zákona a zákona o ISVS,
- je ústredným orgánom pre oblasť kybernetickej bezpečnosti v sektore ISVS podľa ZoKB,
- prevádzkuje zo zákona zriadenú vládnu jednotku CSIRT, ktorá poskytuje služby pre ISVS podľa ZoKB,
- v spojení s povinnosťami každého správcu ISVS je ÚPVII svojho druhu regulátorom a celoslovensky pôsobiacim orgánom pre oblasť bezpečnosti a riešenia kybernetických incidentov vo vzťahu k ISVS.

Partnermi národného projektu sú:

- NBÚ,
- Národná agentúra pre sieťové a elektronické služby (ďalej len "NASES"),
- Slovenská informačná služba (ďalej len "SIS") a

NBÚ je podľa § 34 kompetenčného zákona ústredným orgánom štátnej správy (aj) pre kybernetickú bezpečnosť. Táto kompetencia je následne podrobne upravená vo vzťahu k jednotlivým "čiastkovým" kompetenciám v § 5 ZoKB.

Podľa § 5 ods. 1 písm. j) NBÚ spravuje a prevádzkuje jednotný informačný systém kybernetickej bezpečnosti a podľa § 6 ods. 1 ZoKB má NBÚ postavenie Národnej jednotky CSIRT. Okrem toho NBÚ podľa § 13 ZoKB akredituje jednotlivé jednotky CSIRT a spojení s § 28 ZoKB vykonáva kontrolu (aj) dodržiavania podmienok na činnosť vládnej jednotky CSIRT.

NBÚ prostredníctvom jednotného informačného systému kybernetickej bezpečnosti a Národnej jednotky CSIRT zabezpečuje získavanie, sústreďovanie, vyhodnocovanie a informovanosť o kybernetických incidentoch pre celú Slovenskú republiku. Rovnako tak podľa § 26 ZoKB prijíma aj dobrovoľné hlásenia o kybernetických incidentoch (aj) od občanov a užívateľov služieb verejnej správy a ISVS. Zjednodušene povedané, NBÚ je svojho druhu "jednotným kontaktným a koordinačným" bodom pre všetky jednotky CSIRT a pre všetkých poskytovateľov základných služieb, vrátane ISVS a (s použitím jednotného informačného systému kybernetickej bezpečnosti, do ktorého má prístup vládna jednotka CSIRT) získané informácie o kybernetických hrozbách "distribuuje" pre všetkých správcov ISVS, ktorým tak vytvára podmienky na plnenie povinnosti zabezpečiť bezpečnosť a spoľahlivú prevádzku ISVS.

Podľa § 28 NBÚ kontroluje dodržiavanie bezpečnostných opatrení (aj) správcami ISVS a podľa § 27 ZoKB v oblasti riešenia kybernetických incidentov môže vyhlasovať výstrahy a varovania a ukladať povinnosti vo vzťahu k riešeniu incidentov.

V sumarizácii teda dôvodmi, prečo je NBÚ partnerom národného projektu platí, že:

- je ústredným orgánom štátnej správy (aj) pre oblasť kybernetickej bezpečnosti podľa kompetenčného zákona a ZoKB,
- je prevádzkovateľom Národnej jednotky CSIRT a jednotného informačného systému kybernetickej bezpečnosti podľa ZoKB,
- akredituje a kontroluje pôsobenie jednotiek CSIRT v Slovenskej republike a dodržiavanie bezpečnostných opatrení podľa ZoKB (aj) správcami ISVS,
- zabezpečuje informovanosť a vyhlasovanie výstrah a varovaní pred kybernetickými incidentami a ukladá povinnosti vo vzťahu k ich riešeniu.

NASES je príspevková organizácia Úradu vlády Slovenskej republiky (ďalej len „ÚVSR"), ktorá za ÚVSR zabezpečuje vykonávanie správy, prevádzky a rozvoja siete Govnet podľa § 4a ods. 1 zákona o ISVS.

Podľa § 2 ods. 1 písm. u) zákona o ISVS je Govnet vládna dátová sieť orgánov verejnej správy predstavujúca časť integrovanej infraštruktúry a je základným prvkom centrálnej komunikačnej infraštruktúry. Govnet vytvára univerzálnu prepojovaciu sieť pre jednotlivé izolované virtuálne privátne siete subjektov verejnej správy a zabezpečuje bezpečný a spoľahlivý prístup z jednej siete do všetkých ostatných pod kontrolou ostatných zúčastnených subjektov verejnej správy a zabezpečuje komunikáciu medzi subjektami verejnej správy aj v prípade nedostupnosti pripojenia k internetu. Okrem riadeného prepojovania privátnych sietí subjektov verejnej správy umožňuje i pripojenie ďalších sietí, ako Internet, sieť EU TESTA, a pod.

Bez pripojenia na Govnet by jednotlivé subjekty verejnej správy museli pri komunikácii s užívateľmi pristupovať do siete Internet bez zabezpečenia dostatočnej bezpečnosti. Komunikácii prostredníctvom Govnetu a internetom je súčasne poskytovaná zvýšená kybernetická ochrana napr. v podobe antispamu, antivíru a pod.

V sumarizácii teda dôvodmi, prečo je NASES partnerom národného projektu platí, že:

- NASES podľa zákona o ISVS spravuje unikátnu infraštruktúru, ktorá vytvára podmienky (aj) na bezpečné poskytovanie služieb občanom prostredníctvom zabezpečenia prostredia pre ISVS.

SIS je podľa § 1 ods. 2 a § 2 ods. 1 písm. g) zákona NR SR č. 46/1993 Z.z. v znení neskorších predpisov (ďalej len "zákon o SIS") štátnym orgánom, ktorý v oblasti (aj) ochrany vnútorného poriadku a bezpečnosti štátu získava, sústreďuje a vyhodnocuje informácie o aktivitách a ohrozeniach v kybernetickom priestore, ak ohrozujú bezpečnosť štátu.

Podľa § 4 písm. b) ZoKB je SIS ústredným orgánom v sektore verejná správa - spravodajské služby. Podľa § 8 ods. 5 ZoKB a § 15 ods. 2 a § 16 zákona o SIS má SIS prístup k neverejnej časti jednotného informačného systému kybernetickej bezpečnosti a podľa § 9 ods. 1 písm. b) ZoKB poskytuje informácie NBÚ do jednotného informačného systému kybernetickej bezpečnosti, ktoré sa týkajú zabezpečenia kybernetickej bezpečnosti a následne sú, ako uvádzame vyššie, použiteľné pre jednotlivých správcov ISVS.

V sumarizácii teda dôvodmi, prečo je SIS partnerom národného projektu platí, že:

- je štátnym orgánom, ktorý zo zákona o SIS v oblasti spravodajskej činnosti a zabezpečenia bezpečnosti štátu (teda aj ISVS) získava a disponuje informáciami o kybernetických ohrozeniach, ktorými iné orgány nedisponujú a tak vytvára predpoklad pre včasné prijatie opatrení na úseku kybernetickej ochrany,
- je ústredným orgánom podľa ZoKB a je podľa tohto zákona zapojená do činnosti ústredných orgánov na úseku kybernetickej ochrany.

Zhrnutie k prijímateľovi a partnerom:

Keďže

- národný projekt je cielený na zaistenie ochrany ISVS, je výber prijímateľa pochopiteľný, keďže ide o ústredný orgán štátnej správy v danej oblasti, o "hlavného regulátora" pravidiel (aj) bezpečnosti ISVS a o prevádzkovateľa vládnej jednotky CSIRT, zriadenej ZoKB práve pre sektor ISVS,
- zo zákona je na národnej úrovni zriadená Národná jednotka CSIRT v pôsobnosti NBÚ a kontrolu a určovanie pravidiel fungovania jednotiek CSIRT, ako primárnych útvarov pre bezpečnosť ISVS v kybernetickom priestore, má zverenú takisto NBÚ, je NBÚ partnerom projektu,
- všetky ISVS majú z hľadiska bezpečnej infraštruktúry k dispozícii zákonom ustanovenú sieť Govnet, ktorá slúži (aj) na poskytovanie služieb ISVS a na komunikáciu ISVS a je v správe NASES, je partnerom projektu NASES,
- kybernetické hrozby sú vyhodnocované a informácie o nich získavané vo veľkej miere spravodajskou činnosťou a spravodajské služby sú zo zákona zapojené do systému zabezpečenia kybernetickej ochrany (aj) ISVS, sú (najmä z hľadiska prevencie hrozieb) partnerom projektu SIS

7 Príprava projektu na strane štátu

Na príprave projektu sa začalo pracovať na strane štátu v decembri 2017 kedy bola vytvorená úvodná Definícia projektu. Od začiatku januára 2018 sa už stretávala pracovná skupina zložená zo špecialistov partnerov projektu. V tom čase na projekte spolupracovali tímy z ÚPPVII, NBÚ, SIS a NASES.

V rámci úvodnej ageny boli realizované najmä nasledovné úlohy:

- Zistenie súčasného stavu jednotiek CSIRT.
- Identifikácia požiadaviek a zámerov v oblasti kybernetickej ochrany.
- Vymedzenie pôsobnosti a pokrývaných oblastí.
- Definovanie rozhraní pre spoluprácu zúčastnených strán.
- Identifikácia požiadaviek na technické a organizačné vybavenie.

Ďalej pokračovala spolupráca na projekte prostredníctvom nasledovných aktivít:

- Analýza potrieb a projektových zámerov jednotiek CSIRT.
- Analýza legislatívneho rámca.
- Analýza projektového rámca z pohľadu SORO a čerpania EÚ fondov.
- Analýza projektového rámca z pohľadu VO.
- Kvalifikácia jednotiek CSIRT pre 1.fázu projektu.

Na konci januára sa odsúhlasil základný koncept spolupráce jednotiek CSIRT a riešenia národného systému z pohľadu organizácie, kompetencií, procesov, výstupných služieb a príslušnej funkcionality.

V priebehu februára 2018 si partneri projektu v súlade s novou koncepciou prehodnotili aktuálny stav a vydefinovali požiadavky na dobudovanie infraštruktúry ako aj technického dovybavenia v nevyhnutnom rozsahu, aby mohli plniť svoje zákonné povinnosti (variant Must-have). Požiadavky jednotiek CSIRT boli následne konsolidované a posudzované na úrovni potrieb národného systému.

V priebehu marca a apríla 2018 partneri rozpracovali svoje požiadavky až do úrovne položiek technického vybavenia svojich pracovísk a súvisiacich činností. Partneri zabezpečili aj kvalifikovaný odhad nákladov a vypracovali za svoju stranu rozpočet projektu. Jednotlivé rozpočty partnerov boli potom nezávisle posúdené z pohľadu opodstatnenosti položiek v zmysle pôsobnosti partnera ako aj z pohľadu reálnosti stanovených nákladov. V rámci zostavovania rozpočtu bola na strane štátu posúdená aj návratnosť projektu. Výpočet návratnosti vychádzal z informácií o stave kybernetickej bezpečnosti v našej krajine ako aj z poznania kybernetických hrozieb, ich výskytu a dopadov, ktoré vznikli alebo by mohli vzniknúť keby neboli včas eliminované. Tieto informácie ako aj informácie o položkách technického vybavenia partnerov nie sú verejné.

8 Vypracovanie štúdie uskutočniteľnosti

ÚPPVII sa ako žiadateľ národného projektu rozhodol vypracovať verejnú štúdiu uskutočniteľnosti v spolupráci s externým dodávateľom. V rámci vyhláseného verejného obstarávania zo dňa 29.03.2018, zákazky s nízkou hodnotou podľa § 117 zákona č. 343/2015 Z.z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej ako „ZVO“) sa víťazom súťaže stala spoločnosť Ernst & Young, s.r.o. na základe najvýhodnej ponuky za cenu 39.600,- EUR s DPH. Zmluva bola uazvretá 14.5.2018 a účinná od 16.5.2018.

Podmienky účasti boli stanovené požiadavkami na odbornú spôsobilosť uchádzača tak, aby mohlo súťažiť väčšie množstvo firiem. Spôsobilosť sa preukazovala prostredníctvom dvoch 2 expertov: 1. Expert na kybernetickú bezpečnosť s praxou min. 5 rokov a certifikáciou CISSP alebo CISA alebo CISM alebo ich ekvivalentu a 2. Expert na programové/ projektové riadenie s praxou min. 5 rokov a skúsennosťou s min. 3 štúdiami na projekty OPIS alebo OPII.

Dodávateľovi štúdie uskutočniteľnosti boli poskytované len nevyhnutné verejné informácie potrebné na vypracovanie verejnej štúdie uskutočniteľnosti. Utajované skutočnosti boli vytvárané len na strane orgánu verejnej moci.