1.

# Vybudovanie Centra simulácie, výskumu a výuky kybernetických hrozieb a kybernetickej bezpečnosti

dátum 30.03.2019 Tento dokument obsahuje 55 strán

Obsah

Zoznam tabuliek



## 2. Základné informácie

## 2.1. Prehľad

Štúdiu uskutočniteľnosti národného projektu „Vybudovanie Centra simulácie, výskumu a výuky kybernetických hrozieb a kybernetickej bezpečnosti" (ďalej aj „Centrum" alebo „národný projekt") vypracoval Úrad podpredsedu vlády SR pre investície a informatizáciu (ďalej aj „ÚPPVN").
Hlavnou motiváciou národného projektu je vybudovanie Centra simulácie, výskumu a výuky kybernetických hrozieb a kybernetickej bezpečnosti, ktoré by slúžilo pre potreby zvyšovania povedomia, zručností, metodickej pripravenosti a praktickej pripravenosti na kybernetické hrozby a útoky v kontexte celej verejnej správy. Tento cieľ bude možné naplniť prostredníctvom nosných služieb Centra, ktorými sú výuka a simulácia.
Kybernetická bezpečnosť je dynamicky sa vyvíjajúcim odvetvím, ktoré musí neustále reagovať na nové výzvy. Z tohto dôvodu je nutné zaviesť procesy pre zvládnutie situácie prelomenia bezpečnosti tak, aby bola do čo možno najvyššej možnej miery zabezpečená biznis kontinuita informačných systémov a aby bol minimalizovaný dopad kybernetických bezpečnostných incidentov. Na účely zabezpečenia kybernetickej bezpečnosti a účinného reagovania na kybernetické bezpečnostné incidenty je nevyhnutné zabezpečiť neustále vzdelávanie a tréning nielen bežných používateľov, ale rovnako tak i rôznych skupín odborníkov medzi ktorých patria bezpečnostní manažéri, bezpečnostní architekti, administrátori bezpečnostných systémov, špecialisti manažmentu IT rizík, audítori bezpečnosti informačných systémov, bezpečnostní analytici, kryptológovia či vyšetrovatelia bezpečnostných incidentov. To všetko sú špecialisti, ktorí sa v každodennej praxi zaoberajú otázkami ochrany informačných aktív, manažmentu IT rizík, forenznou informatikou, testovaním bezpečnostných systémov, auditom bezpečnosti, architektonickým návrhom informačných systémov z pohľadu informačnej a kybernetickej bezpečnosti a implementáciou bezpečnostnej infraštruktúry.
Národný projekt Centra simulácie, výskumu a výuky kybernetických hrozieb a kybernetickej bezpečnosti má za cieľ vytvoriť unikátne virtuálne prostredie pre overovanie nových bezpečnostných metód a nástrojov určených na zabezpečenie kybernetickej bezpečnosti, analýzu závažných kybernetických bezpečnostných incidentov, realizáciu školení používateľov a interaktívnych školení a cvičení odborníkov na kybernetickú bezpečnosť. V tomto prostredí bude tiež možné vytvárať rôzne scenáre, ktoré môžu obsahovať rozsiahle siete a informačné systémy, vrátane v nich bežiacich služieb a aplikácií.
Centrum bude poskytovať nasledovné okruhy služieb (ďalej aj „nosné služby"):

- výuka (ďalej aj „Vzdelávanie"), ktorá predstavuje vzdelávanie bežných používateľov (ďalej aj „používatelia", alebo "L1"), vytváranie povedomia bežných IT zamestnancov v oblasti kybernetickej bezpečnosti (ďalej aj ako "L2") a tréning bezpečnostných tímov a používateľov (ďalej aj ako "L4") v nastavení kybernetickej arény (ďalej aj „tímový arénový kybernetický výcvik"),
- simulácia, ktorá zahŕňa realizáciu obranných i útočných techník zahŕňajúcich penetračné testovanie, identifikovanie zraniteľností či forenznú analýzu nad sieťami a informačnými systémami pre IT a rovnako tak i OT prostredie, a využívanie tejto simulácie pre účely výuky.

Odborné vzdelávanie študentov stredných a vysokých škôl na bezpečnosť na úrovni napríklad CCNA (alebo školení ekvivalentnej úrovne) L3 bude riešené samostatným projektom v gescii ministerstva školstva. Tento projekt bude zahŕňať rekonštrukciu existujúcich učební na stredných a vysokých školách.
Miera detailu informácií uvedených v tejto štúdii uskutočniteľnosti je podmienená skutočnosťou, že národné centrum (vrátane technického vybavenia, organizačného a personálneho usporiadania) bude podriadené prísnym bezpečnostným opatreniam. Tieto opatrenia sa vzťahujú na nakladanie s „citlivými a rizikovými" aktívami a informáciami v určitom druhu režimu, ktorý vyžaduje riadený prístup a obmedzenie verejného sprístupňovania informácií. V štúdii uskutočniteľnosti sú uvedené len tie informácie, ktoré je možné zverejniť, a ktoré schválila komisia špeciálne zriadená za účelom riadenia procesu spracovania štúdie (ďalej aj „steering committee").
Členmi steering committee boli poverení zástupcovia prijímateľa národného projektu (ÚPPVII), spracovateľa štúdie a poverení zástupcovia partnerov národného projektu. Hlavnými úlohami steering committee boli:

- vytvoriť projektový plán tvorby štúdie uskutočniteľnosti,
- analyzovať potreby jednotlivých subjektov verejnej správy SR vo vzťahu ku kybernetickej bezpečnosti a stanoviť okruh partnerov národného projektu,
- zadefinovať hlavné logické celky Centra a okruh poskytovaných služieb,
- zabezpečiť pracovné stretnutia s vedúcimi predstaviteľmi partnerov národného projektu,
- zabezpečiť dôvernosť informácií spracúvaných počas tvorby štúdie uskutočniteľnosti,
- stanoviť celkovú mieru detailu textu štúdie uskutočniteľnosti tak, aby v nej boli uvedené výhradne informácie určené na zverejnenie,
- stanoviť mieru detailu jednotlivých typov architektonických modelov tak, aby boli vyobrazené len modely, ktoré je možné zverejniť,
- stanoviť granularitu typov nákladov, ktoré budú súčasťou CBA (príloha štúdie uskutočniteľnosti),
- preskúmať možnosti využitia vládneho cloudu,
- rozhodnúť o variantných riešeniach, ktoré budú súčasťou štúdie uskutočniteľnosti.

Centrum simulácie, výskumu a výuky kybernetických hrozieb a kybernetickej bezpečnosti bude na základe rozhodnutia steering committee tvorené z týchto partnerov:

- Ústredné tréningové centrum kybernetickej bezpečnosti SR v gescii Národného bezpečnostného úradu (ďalej aj „NBÚ") V Bratislave,
- Regionálne spoločné tréningové pracoviská ÚPPVII a NBÚ,
- Tréningové pracovisko Slovenskej informačnej služby (ďalej aj „SIS").

Tabuľka 1 Základné informácie - zhrnutie

Zdôvodnenie využitia národného projektu a vylúčenia výberu projektu prostredníctvom výzvy

Tento projekt v kontexte Národnej koncepcie informatizácie verejnej správy (ďalej aj „NKIVS") prispieva k realizácii priority informatizácie verejnej správy „Formovanie infraštruktúry" a je plne v súlade so všetkými tromi strategickými cieľmi „prevencia", „pripravenosť" a „udržateľnosť" Národnej stratégie pre informačnú bezpečnosť v Slovenskej republike, ktorú odkazuje NKIVS. Projekt je taktiež plne v súlade i so zásadným dokumentom kybernetickej bezpečnosti Slovenskej republiky Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020 schváleným vládou SR.
Realizáciou projektu sa celkovo zvýši dôvera v kybernetický priestor a povedomie o spôsobe riešenia kybernetických útokov, čo prispeje ku zabezpečeniu komplexnej kybernetickej bezpečnosti v spoločnosti v súlade s nasledovnými strategickými cieľmi:
V rámci OPII projekt prispieva k naplneniu výsledkov špecifického cieľa 7.9 „Zvýšenie kybernetickej bezpečnosti v spoločnosti", ktorými sú:

- 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.

Národný projekt si berie za cieľ napĺňať investičnú prioritu 2c) prostredníctvom zabezpečenia komplexnej kybernetickej bezpečnosti v spoločnosti:

- vytvorenie nástrojov na rozpoznanie, monitorovanie a riadenie kybernetických bezpečnostných incidentov,
- zabezpečenie kritickej infraštruktúry,
- zavádzanie európskej stratégie pre kybernetickú bezpečnosť.

Táto štúdia uskutočniteľnosti bude súčasťou národného projektu.

Zdôvodnenie prijímateľa/partnerov národného projektu a dôvod ich určenia ÚPPVII

Národný projekt je cielený na zvýšenie vzdelanostnej úrovne používateľov a špecialistov pre kybernetickú bezpečnosť vo verejnej správe, takže výber ÚPPVII ako prijímateľa národného projektu je pochopiteľný. Hlavnými dôvodmi, na základe ktorých je ako prijímateľ národného projektu určený ÚPPVII sú:

- ÚPPVII je ústredným orgánom štátnej správy pre oblasť riadenia bezpečnosti ISVS podľa kompetenčného zákona a zákona č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisoch (ďalej aj „zákon o ISVS"),
- ÚPPVII je ústredným orgánom pre oblasť kybernetickej bezpečnosti v podsektore ISVS podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej aj „zákon o kybernetickej bezpečnosti"),
- prevádzkuje zo zákona zriadenú vládnu jednotku CSIRT (CSIRT.SK), ktorá poskytuje služby pre ISVS podľa zákona o kybernetickej bezpečnosti,
- v spojení s povinnosťami každého správcu ISVS je ÚPPVII svojho druhu regulátorom a celoslovensky pôsobiacim orgánom pre oblasť bezpečnosti a riešenia kybernetických incidentov vo vzťahu k ISVS.

V rámci Centra simulácie, výskumu a výuky kybernetických hrozieb a kybernetickej bezpečnosti bude ÚPPVII zriaďovateľom a prevádzkovateľom funkčného celku tréningového pracoviska.

Partneri národného projektu Partnermi národného projektu sú:

- NBÚ,
- SIS.

Odôvodnenie partnerov národného projektu:

NBÚ

Zo zákona o kybernetickej bezpečnosti je na národnej úrovni hlavnou autoritou NBÚ, ktorý plní množstvo úloh súvisiacich s kybernetickou bezpečnosťou. NBÚ zriadil a prevádzkuje národnú jednotku pre riešenie kybernetických incidentov (SK-CERT), v rámci ktorej pôsobí množina špecialistov na kybernetickú bezpečnosť. Vzhľadom na skutočnosť, že NBÚ je vrcholovým ústredným orgánom pre kybernetickú bezpečnosť, je tak prirodzeným partnerom projektu. V rámci Centra simulácie, výskumu a výuky kybernetických hrozieb a kybernetickej bezpečnosti bude NBÚ zriaďovateľom a prevádzkovateľom funkčného celku Ústredné tréningové centrum kybernetickej bezpečnosti SR.

SIS

Kybernetické hrozby vzťahujúce sa (nielen) na ISVS sú vyhodnocované a informácie o nich získavané vo veľkej miere spravodajskou činnosťou a spravodajské služby sú zo zákona zapojené do systému zabezpečenia kybernetickej ochrany, je - najmä z hľadiska prevencie kybernetických hrozieb - partnerom projektu aj SIS.

V rámci Centra simulácie, výskumu a výuky kybernetických hrozieb a kybernetickej bezpečnosti bude SIS zriaďovateľom a prevádzkovateľom funkčného celku tréningového pracoviska.

V súlade s Operačným programom Integrovaná infraštruktúra 2014 - 2020 si bude ÚPPVII uplatňovať maximálne 3 % oprávnených výdavkov projektu pre implementáciu štandardov riadenia informačno-technologických projektov, ktoré zabezpečia aktívnu participáciu na riadení projektu a komplexné riadenie budovania informačnej spoločnosti.

| | |
|---|---|
| Príslušnosť národného projektu k relevantnej časti PO7 OPII | PRIORITNÁ OS Operačného programu Integrovaná infraštruktúra PO7: Informačná spoločnosť TEMATICKÝ CIEĽ 2: Zlepšenie prístupu k IKT a zlepšenie ich využívania a kvality INVESTIČNÁ PRIORITA 2c): Posilnenie aplikácií IKT v rámci elektronickej štátnej správy, elektronického vzdelávania, elektronickej inklúzie, elektronickej kultúry a elektronického zdravotníctva ŠPECIFICKÝ CIEĽ 7.9: Zvýšenie kybernetickej bezpečnosti v spoločnosti |
| Indikatívna výška finančných prostriedkov určených na realizáciu národného projektu | 19 953 885,00 € |

## 2.2. Dôvod

Základným strategickým cieľom Koncepcie kybernetickej bezpečnosti Slovenskej republiky na roky 2015 - 2020 schválenej v roku 2015 vládou SR je otvorený, bezpečný a chránený národný kybernetický priestor, t. j. vybudovanie dôvery v spoľahlivosť a bezpečnosť najmä kritickej informačnej a komunikačnej infraštruktúry, ako aj istoty, že táto bude plniť svoje funkcie a slúžiť národným záujmom aj v prípade kybernetického útoku.
V súvislosti s elektronizáciou služieb verejnej správy (e-Government) dochádza k veľmi významnému zvýšeniu závislosti výkonu verejnej správy na informačno-komunikačných technológiách t. j. informačných systémoch verejnej správy. Z uvedeného dôvodu je nevyhnutné zaistiť vysokú úroveň kybernetickej bezpečnosti týchto systémov a zabezpečiť dôvernosť, dostupnosť a integritu spracúvaných informácií a údajov. Prevencia, včasná a adekvátna reakcia na kybernetické útoky je jedným zo základných pilierov pre zabezpečenie tohto strategického cieľa ako aj pre zachovanie dôvery občanov v e-Goverment služby.
Pre zaistenie včasnej a efektívnej reakcie na kybernetické útoky vo verejnej správe je potrebné disponovať špecialistami, riadiacimi kádrami a výkonnými zamestnancami, ktorí budú schopní správne, rýchlo a odborne reagovať v momente kybernetického ohrozenia a útoku. Nedostatok odborníkov v tejto oblasti konštatuje viacero pracovných skupín zriadených na úrovni orgánov štátnej správy, ako aj iné medzinárodné inštitúcie.
Potreba riešenia programov odbornej prípravy v oblasti bezpečnosti sietí a informačných systémov je aj predmetom smernice Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (ďalej aj „smernica NIS").

Nedostatok odborníkov na oblasť kybernetickej bezpečnosti je potrebné riešiť koncepčne na úrovni prípravy nových študentov, ale aj na úrovni vzdelávania súčasných zamestnancov VS - čo je predmetom práve tohto projektu. Výsledky tohto projektu však budú sprístupnené aj školám na voľné využitie, prípadne môžu školy participovať aj na organizovaných cvičeniach.
Vybudovanie Centra simulácie, výskumu a výuky kybernetických hrozieb a kybernetickej bezpečnosti, ktorého projektová príprava je základným obsahom tohto projektu, je reakcia na aktuálny nárast potreby prehlbovania kvalifikácie a vzdelávania v oblasti kybernetickej bezpečnosti a nutnosť zvyšovania kvalifikácie odborníkov VS na naplnenie požiadaviek vyplývajúcich zo zákona o kybernetickej bezpečnosti, ktorým sa implementuje smernica NIS. Prostredie Centra bude možné aktívne využívať na realizáciu vzdelávania v oblasti informačnej a kybernetickej bezpečnosti a nadobúdanie zručností bezpečnostných špecialistov a tímov v štátnych organizáciách. Centrum bude okrem vzdelávania zamerané i na vývoj scenárov na nové zraniteľnosti, vývoj a tvorbu unikátnych IT prostredí pre analýzu bezpečnostných hrozieb smerujúcich na informačné systémy a simuláciu podmienok v čase kybernetického ohrozenia štátu. Taktiež bude slúžiť i na simuláciu rozsiahlych počítačových sietí, služieb a aplikácií takým spôsobom, aby bolo možné skúmať šírenie kybernetických hrozieb a ich dopady.
Absenciu takéhoto Centra konštatuje aj Koncepcia kybernetickej bezpečnosti SR na roky 2015 - 2020 a prostredníctvom opatrenia 4 - "Podpora, vypracovanie a zavedenie systému vzdelávania v oblasti kybernetickej bezpečnosti." priamo hovorí o potrebe odborného vzdelávacieho systému na troch úrovniach.

Keďže jedným z cieľov Operačného programu integrovaná infraštruktúra v Prioritnej osi č. 7 je aj zvýšenie kybernetickej bezpečnosti v spoločnosti (špecifický cieľ č. 7.9), ÚPPVII považuje za potrebné preskúmať možnosť zabezpečenia financovania Centra z vyššie uvedeného operačného programu prostredníctvom tejto štúdie uskutočniteľnosti, ktorá detailne popíše možné riešenie prostredníctvom národného projektu.

Dôvodom realizácie je aj naplnenie legislatívnych požiadaviek, nakoľko podľa § 6 zákona 69/2018 Z.z. o KyB NBÚ prostredníctvom národnej jednotky CSIRT s pôsobnosťou pre Slovenskú republiku a pre všetky sektory musí riešiť preventívne a reaktívne služby (§ 15). Medzi tieto služby patria aj:

- vytváranie bezpečnostného povedomia,
- výcvik,
- reaktívne služby priamo u poskytovateľa základnej služby v jednotlivých sektoroch.

Aj aktuálna správa"Kybernetická pripravenosť v kocke" hovorí, že Slovensko už teraz patrí medzi najzraniteľnejšie krajiny v Európe z hľadiska kybernetickej kriminality. Navyše, vďaka svojmu členstvu v EÚ aj NATO sa stáva cieľom štátmi financovanej špionáže, ktorá z historického hľadiska spôsobuje najväčšie škody. Sofistikované útoky prebiehajú roky a útočníci môžu byť pripravený kedykoľvek na povel aktivovať škodlivý kód. Takéto útoky sa spravidla veľmi ťažko odhaľujú a treba na to dobre vyškolených ľudí.Tento projekt má za cieľ pomôcť národnému hospodárstvu najmä s prvým aktérom (štátom financovaný) prostredníctvom tréningu štátnych expertov, ktorí môžu pomôcť v reakcii na tieto incidenty, a to konkrétne v nasledovných oblastiach:

- efektívnejšie predchádzanie a detekcia kybernetických incidentov v prostredí verejnej správy,
- efektívnejšia reakcia na kybernetické incidenty v prostredí celého hospodárstva.

## 2.3. Rozsah

Predložená štúdia uskutočniteľnosti vychádza zo súčasného stavu kybernetickej bezpečnosti v SR. Cieľom tejto štúdie uskutočniteľnosti je poskytnúť strategický rámec, plánovaný rozsah, očakávaný časový harmonogram a prípadné odporúčania ďalších aktivít, z ktorých je potrebné pri realizácii národného projektu vychádzať.
Štúdia rieši aktuálny problém súčasného stavu, ktorým je nízka úroveň vzdelanostnej úrovne a úrovne zručností bezpečnostných špecialistov v oblasti kybernetickej bezpečnosti vo verejnej správe.
V rámci jednotlivých nosných služieb Centra výuka a simulácia je rozsah národného projektu možné rozdeliť nasledovne:
Výuka:
• zabezpečenie technického vybavenia na prevádzkovanie jednotných e-learningových školení používateľov pre oblasť informačnej a

kybernetickej bezpečnosti v sektore verejnej správy (vrátane vytvorenia iniciálneho súboru teoretických školení),
- vytvorenie tréningových pracovísk a zabezpečenie technického vybavenia pre teoretický aj praktický tréning špecialistov v oblasti kybernetickej bezpečnosti (vrátane vytvorenia iniciálneho súboru teoretických školení a praktických scenárov),
- vytvorenie tréningových pracovísk a zabezpečenie tréningovej IT/OT infraštruktúry pre arénový kybernetický výcvik (vrátane vytvorenia iniciálneho súboru špecializovaných arénových tréningových scenárov).

Simulácia:
- vytvorenie simulačných pracovísk a zabezpečenie simulačnej IT/OT infraštruktúry pre simulačné tréningy v oblasti kybernetickej bezpečnosti,
- návrh a vytvorenie riadiaceho a simulačného SW pre celkové riadenie, správu, návrh a vyhodnocovanie simulačných tréningov v oblasti kybernetickej bezpečnosti pre IT/OT prostredie.

V súčasnej dobe je viacero typov aktérov, ktorí sú aktívni na poli kybernetickej kriminality. Zvyčajne sa rozdeľujú do nasledovných kategórii:
- štátom financovaný aktéri,
- organizovaný zločin,
- aktivisti,
- vnútorný nepriateľ,
- chyba interného používateľa.

Tento projekt svojím rozsahom reaguje predovšetkým na prvé dva typy aktéra, ktorí aj historicky spôsobujú najväčšie škody hospodárstvu krajiny, a to prostredníctvom tréningu a školenia štátnych expertov na KyB.

V rámci projektu budú vytvorené:
- tréningová platforma,
- školiaci obsah, t.j. tréningové scenáre a školiace materiály,
- HW a SW infraštruktúra pre samotné tréningové scenáre,
- učebne.

Národný projekt je navrhnutý ako národný projekt, ktorého cieľovou skupinou sú tieto zainteresované strany:
- prijímateľ národného projektu (ÚPPVII) a partneri národného projektu (NBÚ, SIS),
- všetky subjekty verejnej správy,
- subjekty regulované zákonom o KyB, t.j. prvky kritickej infraštruktúry, prevádzkovatelia základnej služby a poskytovatelia digitálnej služby.

| Oblasť/situácia | Aktér | ISVS |
|---|---|---|
| Zvyšovanie povedomia o kybernetickej bezpečnosti - školenia bežných zamestnancov L1 | verejný správa | n/a |
| Zvyšovanie úrovne vedomostí zamestnancov IT verejnej správy v oblasty KyB L2 | verejný správa | n/a |
| Zvyšovanie vedomostí a praktických skúseností špecialistov na bezpečnosť vo verejnej správe L4 | verejný správa | n/a |

Miera detailu informácií uvedených v tejto štúdii uskutočniteľnosti je podmienená skutočnosťou, že národné centrum (vrátane technického vybavenia, organizačného a personálneho usporiadania) bude podriadené prísnym bezpečnostným opatreniam. Tieto opatrenia sa vzťahujú na nakladanie s „citlivými a rizikovými" aktívami a informáciami v určitom druhu režimu, ktorý vyžaduje riadený prístup a obmedzenie verejného sprístupňovania informácií. V štúdii uskutočniteľnosti sú uvedené len tie informácie, ktoré je možné zverejniť, a ktoré schválila komisia špeciálne zriadená za účelom riadenia procesu spracovania štúdie.
V nasledujúcej tabuľke je uvedené, ktoré údaje je možné v rámci štúdie uskutočniteľnosti uviesť bez obmedzení a ktoré informácie musia byť z bezpečnostných dôvodov uvedené v obmedzenom režime.

| Údaje uvedené v štúdii štúdie | Neobmedzená miera detailu | Obmedzený režim |
|---|---|---|
| Prehľad | X | |
| Dôvod | X | |
| Rozsah | X | |
| Motivácia | X | |
| Manažérske zhrnutie | X | |
| Legislatíva | X | |
| Biznis architektúra | X | |

| | | |
|---|---|---|
| Architektúra IS | X | |
| Technologická architektúra | X | |
| Bezpečnostná architektúra | X | |
| Prevádzka | X | |
| Alternatívne riešenia | X | |
| Agregovaný rozpočet | X | |
| Detailný rozpočet na úrovni jednotlivých komponentov | | X |

Rovnako je potrebné uviesť, že štúdia neobsahuje klasické elementy iných agendových štúdii ako sú ISVS, aplikačné a koncové služby. Dôvodom je, že Centrum nebude poskytovať agendové, resp. typické koncové alebo aplikačné služby a ani sa týmto projektom nebude budovať informačný systém verejnej správy. Realizáciou projektu sa zabezpečí vybudovanie Centra a jeho vybavenia, ktoré bude umožňovať simuláciu, tréning a výuku kybernetických hrozieb a kybernetickej bezpečnosti, čo sa prejaví najmä vo zvýšení schopností bezpečnostných špecialistov a tímov takýchto špecialistov predchádzať a reagovať na kybernetické bezpečnostné incidenty vo verejnej správe.

## 2.4. Použité skratky a značky

Tabuľka 2 Skratky a značky

| Skratka / Značka | Vysvetlenie |
|---|---|
| API | Application Programming Interface |
| CBA | Analýza nákladov a prínosov (Cost-Benefit Analysis) |
| CERT | Jednotka pre riešenie počítačového nebezpečenstva (Computer Emergency Response Team) |
| CSIRT | Jednotka pre riešenie kybernetických bezpečnostných incidentov (Computer Security Incident Response Team) |
| ENPV | Čistá súčasná ekonomická hodnota (Economic Net Present Value) |
| EÚ | Európska únia |
| HSM | Kryptografické zariadenie hardvérovej ochrany kľúča (Hardware Security Module) |
| HTTPS | Zabezpečený hypertextový prenosový protokol (Hypertext Transfer Protocol Secure) |
| HW | Hardvér (Hardware) |
| IAM | Správa identít a prístupových práv (Identity and Access Management) |
| IKT | Informačné a komunikačné technológie |
| IoT | Internet vecí (Internet of Things) |
| ISVS | Informačný systém verejnej správy |
| IT | Informačné technológie (Information Technology) |
| KPI | Kľúčový ukazovateľ výkonnosti (Key Performance Indicator) |
| LED | Light-Emitting Diode |
| NBÚ | Národný bezpečnostný úrad |
| NIS | Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii |

| | |
|---|---|
| NKIVS | Národná koncepcia informatizácie verejnej správy |
| OPII | Operačný program Integrovaná infraštruktúra |
| OS | Operačný systém (Operating System) |
| OT | Operačné technológie (Operational Technology) |
| PBP | Rok návratu investície (Payback Period) |
| PO7 | Prioritná os 7 |
| SCADA | Dispečerské riadenie a zber dát (Supervisory Control and Data Acquisition) |
| SIEM | Manažment bezpečnostných informácií a udalostí (Security Information and Event Management) |
| SIS | Slovenská informačná služba |
| SK | Slovensko |
| SLA | Dohoda o úrovni poskytovaných služieb (Service Level Agreement) |
| SR | Slovenská republika |
| SSL | Secure Sockets Layer |
| SW | Softvér (Software) |
| ÚPPVII | Úrad podpredsedu vlády SR pre investície a informatizáciu |

# 3. Manažérske zhrnutie

Štúdia uskutočniteľnosti pre národný projekt „Vybudovanie Centra simulácie, výskumu a výuky kybernetických hrozieb a kybernetickej bezpečnosti" je vypracovaná na základe požiadavky ÚPPVN.
Predložená štúdia vychádza zo súčasného stavu kybernetickej bezpečnosti v SR. Cieľom tejto štúdie uskutočniteľnosti je poskytnúť strategický rámec, plánovaný rozsah, očakávaný časový harmonogram a prípadné odporúčania ďalších aktivít, z ktorých je potrebné pri realizácii implementácie národného projektu vychádzať.
Hlavným cieľom národného projektu je vybudovanie Centra simulácie, výskumu a výuky kybernetických hrozieb a kybernetickej bezpečnosti, ktoré by prostredníctvom nosných služieb výuka a simulácia umožnilo:

- realizáciu bezpečnostných školení, tréningov a arénových kybernetických výcvikov, ktorých hlavnou výhodou je vysoká miera interaktivity s užívateľmi a realistickosť cvičení daná možnosťou presne modelovať infraštruktúru IT/OT,
- vytvárať komplexné scenáre, ktoré je možné neobmedzene opakovať a upravovať,
- modelovať reálne sieťové topológie, stroje a zapojené systémy, ktoré sú následne vystavené najnovším kybernetickým hrozbám,
- realizovať vo virtuálnom prostredí a na rozličných operačných systémoch experimenty súvisiace s kybernetickými bezpečnostnými hrozbami (napr. útok na siete a informačné systémy),
- opakované prevádzanie experimentov zahrňujúce zmeny konfigurácií sietí, operačných systémov a aplikácií,
- vytvorenie jedinečného prostredia pre výskum a vývoj metód a proprietárneho SW na ochranu proti kybernetickým hrozbám a kybernetickým útokom na siete a informačné systémy.

Okruh ústredných orgánov štátnej správy, ktoré budú priamo zapojené do Centra:

- ÚPPVII (prijímateľ národného projektu), ako zriaďovateľ a prevádzkovateľ funkčného celku tréningového pracoviska,
- NBÚ (partner národného projektu), ako zriaďovateľ a prevádzkovateľ funkčného celku Ústredné tréningové centrum kybernetickej bezpečnosti SR,
- SIS (partner národného projektu). ako zriaďovateľ a prevádzkovateľ funkčného celku tréningového pracoviska.

Oblasť pôsobenia národného systému je vymedzená na sektormi podľa prílohy č. 1 k zákonu č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov.
Štúdia uskutočniteľnosti popisuje súčasný a budúci stavu legislatívneho prostredia a obsahuje popis týchto typov architektúry:

- biznis architektúra,
- architektúra informačných systémov,
- technologická architektúra,
- bezpečnostná architektúra.

Popis biznis architektúry zahŕňa vysokoúrovňový popis nosných služieb, ktoré bude Centrum poskytovať. Týmito službami sú najmä:

- výuka,
- simulácia.

Uvedené nosné služby budú poskytované prostredníctvom jednotlivých funkčných celkov Centra. Architektúra informačných systémov a technologickej architektúry pokrýva architektonický pohľad na jednotlivé pracoviská, ktoré je potrebné vybudovať a vybaviť technickým (hardvérovým a softvérovým) vybavením. Ide o tieto logické celky:

- Ústredné tréningové centrum kybernetickej bezpečnosti SR v gescii NBÚ,
- Tréningové pracoviská partnerov národného projektu:
- Regionálne tréningové pracoviská ÚPPVII a NBÚ,
- Tréningové pracovisko SIS.

Štúdia uskutočniteľnosti analyzuje aj tri alternatívne riešenia, akými je možné pristupovať k národnému projektu:

- prvou alternatívou je ponechať súčasný nevyhovujúci stav,
- druhou alternatívou, ktorá sa javí ako najvýhodnejšia, je vybudovanie Centra simulácie, výskumu a výuky kybernetických hrozieb a kybernetickej bezpečnosti konzervatívnym spôsobom zachyteným v popise budúceho stavu,
- tretia alternatíva uvažuje s možnosťou finančne enormne nákladného Centra simulácie, výskumu a výuky kybernetických hrozieb a kybernetickej bezpečnosti, ktoré by bolo zabezpečované plne outsourcovaným spôsobom.

Porovnanie všetkých alternatívnych riešení a odôvodnenie najvýhodnejšej alternatívy (vrátane multikriteriálnej analýzy) je súčasťou kapitoly 2.3 „Alternatívne riešenia".

Náklady národného projektu uvedené v ekonomickej analýze sú zostavené v nasledovnej štruktúre:

- nevyhnutné stavebné úpravy jednotlivých funkčných celkov Centra,
- obstarávacie náklady na hardvér a prevádzkové náklady na hardvér počas trvania projektu,
- obstarávacie náklady na softvér, softvérové licencie a prevádzkové náklady na softvér počas trvania projektu,
- obstarávacie náklady na zaškolenie personálu Centra.

Čo sa týka možností využitia kapacít vládneho cloudu možno konštatovať, že vzhľadom na povahu Centra nie je možné z prevádzkového a bezpečnostného hľadiska využiť túto možnosť a bude potrebné obstarať samostatné hardvérové vybavenie, ktoré nepresiahne 30 % z celkového objemu oprávnených výdavkov projektu. Avšak pri dodržaní bezpečnostných pravidiel je možné časť centrálnej infraštruktúry Centra umiestniť v priestoroch štátneho datacentra na Kopčianskej ulici.

## 3.1. Motivácia

Tabuľka 3 Motivácia - budúci stav

Súhrnný popis

V Slovenskej republike sa aktuálne na národnej úrovni rieši viacero projektov z oblasti kybernetickej bezpečnosti:

- projekt Národný systém riadenia incidentov kybernetickej bezpečnosti vo verejnej správe (budovanie bezpečnostného povedomia),
- projekt Vybudovanie nosnej infraštruktúry bezpečného informačno-komunikačného systému FS SR,
- sektorové projekty na zvýšenie úrovne bezpečnosti na jednotlivých ústredných orgánoch štátnej správy.

Tieto projekty riešia predovšetkým procesné, technické a softvérové aspekty bezpečnosti. Nemenej dôležitou súčasťou však je aj organizačný aspekt bezpečnosti - bez kvalitne trénovaných ľudí je aj ten najlepší mix technického zabezpečenia časom neúčinný.

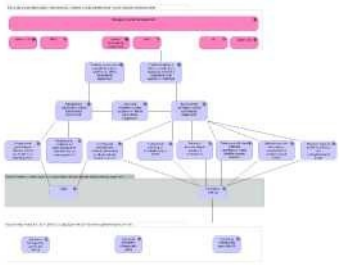
Hlavnou motiváciou tohto národného projektu je teda zvýšenie povedomia, zručností, metodickej pripravenosti a praktickej pripravenosti na kybernetické hrozby a útoky pracovníkov v kontexte celej verejnej správy a to prostredníctvom vybudovania Centra simulácie a výuky kybernetických hrozieb a kybernetickej bezpečnosti. Tento cieľ bude možné naplniť prostredníctvom dvoch nosných služieb Centra, ktorými sú výuka a simulácia.

Výuka:

- poskytovanie prostredia pre školenia bežných používateľov vo verejnej správe L1,
- poskytovanie prostredia pre tréning zamestnancov IT oddelení na kybernetickú bezpečnosť vo verejnej správe L2,
- poskytovanie prostredia pre arénový kybernetický výcvik pre špecialistov zo subjektov verejnej správy L4.

Simulácia:

- poskytovanie meniacej sa infraštruktúry typu IT/OT s preddefinovanou množinou meraných veličín a s možnosťami jej rozšírenia,
- realizácia bezpečnostných simulácií a experimentov spoločne s maximálnou mierou konfigurovateľnosti technických zariadení, topológií sietí, komunikačnej infraštruktúry a inej IT/OT infraštruktúry,
- virtualizácie dejov a udalostí prebiehajúcich v sieťach a systémoch typu IT/OT,
- poskytovanie výstupov národného projektu v rámci nosnej služby simulácia ako službu pre verejnú správu (vrátane bezpečnostných zložiek štátu a prípadne škôl).



| Aktér | Cieľ | Požiadavka | Obmedzenie |
|---|---|---|---|
| UPVII | Zvýšenie úrovne bezpečnostného povedomia zamestnancov VS | Vytvorenie tréningového pracoviska | Potrebné zabezpečiť dostatočnú úroveň (počet a schopnosti) zamestnancov kybernetickej arény. |
| | Zvýšenie praktických skúseností odborníkov v oblasti KyB | Realizácia školení zamestnancov v oblasti KyB | |
| NBÚ | Zvýšenie úrovne bezpečnostného povedomia zamestnancov VS Zvýšenie praktických skúseností odborníkov v oblasti KyB | Vytvorenie tréningového pracoviska Realizácia školení zamestnancov v oblasti KyB | Potrebné zabezpečiť dostatočnú úroveň (počet a schopnosti) zamestnancov kybernetickej arény. |
| SIS | Zvýšenie úrovne bezpečnostného povedomia zamestnancov VS Zvýšenie praktických skúseností odborníkov v oblasti KyB | Vytvorenie tréningového pracoviska Realizácia školení zamestnancov v oblasti KyB | Potrebné zabezpečiť dostatočnú úroveň (počet a schopnosti) zamestnancov kybernetickej arény. |
| ústredné orgány štátnej správy | Zvýšenie úrovne bezpečnostného povedomia zamestnancov VS Zvýšenie praktických skúseností odborníkov v oblasti KyB | Vytvorenie tréningového pracoviska Realizácia školení zamestnancov v oblasti KyB | Je potrebné implementovať motivačný mechanizmus pre zamestnancov VS, aby sa zúčastňovali školení. |
| ostatné OVM | Zvýšenie úrovne bezpečnostného povedomia zamestnancov VS | Realizácia školení zamestnancov v oblasti KyB | Je potrebné implementovať motivačný mechanizmus pre zamestnancov VS, aby sa zúčastňovali školení. |

V projekte sú navrhované nasledovné KPI:

| Parameter | AS hodnota | ISTO hodnota | BEO cieľov | Obmedzenia |
|---|---|---|---|---|
| Počet vyškolených používateľov v Centre (bežní IT používatelia subjektov verejnej správy) - úroveň 1 | 0 | | | Školenie na dvojročnej báze |
| Počet vyškolených štandardných IT zamestnancov - úroveň 2 | 0 | | | Školenie na ročnej báze |
| Počet trénovaných špecialistov na kybernetickú bezpečnosť v Centre - úroveň 4 | 0 | 200 | | Tréning na ročnej báze |
| Počet vytvorených scenárov pre účely arénového kybernetického výcviku | 0 | 6/rok | | |
| Počet zrealizovaných arénových kybernetických výcvikov v Centre | 0 | 12/rok | | |
| Počet zriadených učební na školenie a tréning v oblasti kybernetickej bezpečnosti | 0 | 8 | | |

| | |
|---|---|
| Riziká | Spresnenie identifikovaných rizík: Odkazy na relevantné identifikátory rizík v prílohe Riziká. |
| R1 Splnenie KPI definovaných v rámci tejto štúdie | |
| Prílohy | Diagramy, modely, obrázky v plnom rozlíšení |

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

## 3.2. Popis aktuálneho stavu

### 3.2.1. Legislatíva

Tabuľka 4 Legislatíva - aktuálny stav

Súhrnný popis

Legislatívny rámec pre vybudovanie Centra simulácie, výskumu a výuky kybernetických hrozieb a kybernetickej bezpečnosti rámcovo ustanovuje nasledovný základný európsky a národný legislatívny rámec:

- smernica Európskeho parlamentu a rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii,
- vykonávacie nariadenie Komisie (EÚ) 2018/151 z 30. januára 2018, ktorým sa stanovujú pravidlá uplatňovania smernice Európskeho parlamentu a Rady (EÚ) 2016/1148, pokiaľ ide o bližšiu špecifikáciu prvkov, ktoré musia poskytovatelia digitálnych služieb zohľadňovať pri riadení rizík v oblasti bezpečnosti sietí a informačných systémov, a parametrov na posudzovanie toho, či má incident závažný vplyv,
- zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov,
- súvisiace vykonávacie predpisy k zákonu o kybernetickej bezpečnosti:
- vyhláška Národného bezpečnostného úradu č. 164/2018 Z. z., ktorou sa určujú identifikačné kritériá prevádzkovanej služby (kritériá základnej služby),
- vyhláška Národného bezpečnostného úradu č. 165/2018 Z. z., ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov,
- vyhláška Národného bezpečnostného úradu č. 166/2018 Z. z. o podrobnostiach o technickom, technologickom a personálnom vybavení jednotky pre riešenie kybernetických bezpečnostných incidentov,
- vyhláška Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení,
- zákon č. 95/2019 Z. z. o informačných technológiach vo verejnej správe,
- zákon č. 45/2011 Z. z. o kritickej infraštruktúre v znení neskorších predpisov.

Podľa recitálu (34) smernice NIS by členské štáty mali mať primerané vybavenie, pokiaľ ide o technické a organizačné spôsobilosti, aby mohli predchádzať incidentom a rizikám v oblasti sietí a informačných systémov, odhaľovať ich, reagovať na ne a zmierňovať ich. V článku 7 smernica NIS ukladá členským štátom:

- určenie vzdelávacích programov, programov na zvyšovanie informovanosti a programov odbornej prípravy súvisiacich s národnou stratégiou v oblasti bezpečnosti sietí a informačných systémov,
- určenie plánov výskumu a vývoja súvisiacich s národnou stratégiou v oblasti bezpečnosti sietí a informačných systémov.

Základnou národnou legislatívnou úpravou pre kybernetickú bezpečnosť je zákon o kybernetickej bezpečnosti, ktorý implementoval smernicu NIS do slovenského právneho systému. Zákon o kybernetickej bezpečnosti možno súčasne považovať aj za legislatívny základ pre vytvorenie Centra, nakoľko v § 7 ods. 2 písm. f) a g) zakladá právny základ pre strategické riešenie vzdelávacích programov, programov na budovanie bezpečnostného povedomia, zvyšovanie informovanosti a odbornej prípravy, výskumu a vývoja.

V zmysle § 5 ods. 1 NBÚ riadi a koordinuje výkon štátnej správy v oblasti kybernetickej bezpečnosti, vydáva znalostné štandardy, zabezpečuje budovanie bezpečnostného povedomia a koordinuje výskum a vývoj. Okrem toho určuje štandardy a operačné postupy, vydáva metodiku a politiku správania sa v kybernetickom priestore a určuje zásady predchádzania kybernetickým bezpečnostným incidentom a zásady ich riešenia.

Zákon o kybernetickej bezpečnosti v § 9 ústredným orgánom podľa tohto zákona ukladá budovať bezpečnostné povedomie, koordinovanú spoluprácu na všetkých stupňoch riadenia kybernetickej bezpečnosti a aplikovať bezpečnostné opatrenia a politiku správania sa v kybernetickom priestore.

Zákon č. 45/2011 Z. z. o kritickej infraštruktúre v znení neskorších predpisov pojednáva o odbornej príprave osôb, ktoré zabezpečujú ochranu prvku v prílohe 2.

Najdôležitejšími koncepčnými dokumentmi, ktoré sa priamo týkajú národného projektu sú:

- koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015 - 2020 (ďalej aj „koncepcia kybernetickej bezpečnosti" alebo „koncepcia"),
- akčný plán realizácie Koncepcie kybernetickej bezpečnosti Slovenskej republiky na roky 2015 - 2020 (ďalej aj „akčný plán").

Základným strategickým cieľom uvedeným v úvodnom slove ku koncepcii kybernetickej bezpečnosti schválenej v roku 2015 vládou SR je otvorený, bezpečný a chránený národný kybernetický priestor, t. j. vybudovanie dôvery v spoľahlivosť a bezpečnosť najmä kritickej informačnej a komunikačnej infraštruktúry, ako aj istoty, že táto bude plniť svoje funkcie a slúžiť národným záujmom aj v prípade kybernetického útoku. Koncepcia v bode 2.3 konštatuje, že zvyšovanie povedomia

a vzdelávania v oblasti kybernetickej, či informačnej bezpečnosti nie je všeobecne obsahovou súčasťou systému vzdelávania v Slovenskej republike (základné, stredné a vysoké školy), ani systému formovania spoločenského povedomia. Vzdelávanie nie je riešené na úrovni špecializovaných odborov, ale nanajvýš na úrovni špecializovaných predmetov v rámci vybraných vzdelávacích inštitúcií. Pretrváva rôzna úroveň spôsobilosti a pripravenosti na kybernetické hrozby. Chýba centrum výnimočnosti, ktoré by sa sústredilo na otázky týkajúce sa kybernetickej bezpečnosti.

Koncepcia kybernetickej bezpečnosti v kapitole 3 predstavuje základné prostriedky realizácie cieľov stanovených koncepciou, medzi ktoré patria aj:

- systematická osveta a komplexný systém vzdelávania v oblasti kybernetickej bezpečnosti,
- rozvoj vnútorného trhu s produktmi a službami kybernetickej bezpečnosti, najmä s využitím grantov, fondov EÚ a podporou novovznikajúcich projektov či začínajúcich firiem, ako aj podporu výskumu, vývoja a inovácií priemyselných a technologických zdrojov kybernetickej bezpečnosti.

Koncepcia v kapitole 3 taktiež navrhuje sedem kľúčových opatrení, z ktorých národný projekt priamo adresuje dve:

- Opatrenie 4: Podpora, vypracovanie a zavedenie systému vzdelávania v oblasti kybernetickej bezpečnosti,
- Opatrenie 7: Podpora vedy a výskumu v oblasti kybernetickej bezpečnosti.

Vyššie uvedené opatrenia potom detailne rozpracúva akčný plán, ktorý v tabuľke úloh definuje tieto hlavné úlohy (boldom sú označené tie, ktoré bude projekt riešiť):

- Pre opatrenie 4: Podpora, vypracovanie a zavedenie systému vzdelávania v oblasti kybernetickej bezpečnosti:
- zmapovať súčasný stav vzdelávania v oblasti kybernetickej bezpečnosti,
- zabezpečiť vzdelávanie v oblasti kybernetickej bezpečnosti,
- zaviesť inovovaný systém vzdelávania v oblasti kybernetickej bezpečnosti,
- vytvoriť Národné centrum vzdelávania v oblasti kybernetickej bezpečnosti,
- systematicky zvyšovať povedomie o aspektoch kybernetickej bezpečnosti,
- zabezpečiť školenie o kybernetickej bezpečnosti,
- vytvoriť študijné programy v rámci celoživotného vzdelávania profesionálnych vojakov,
- zabezpečiť vzdelávanie v oblasti informačnej a kybernetickej bezpečnosti vrámcijustičných orgánov,
- zabezpečiť vzdelávanie v oblasti kybernetickej bezpečnosti v rámci vyšetrovacích orgánov,
- zabezpečiť vytvorenie popisu kvalifikácie pre oblasť informačnej a kybernetickej bezpečnosti v rámci národnej sústavy kvalifikácií v SR.
- Pre opatrenie 7: Podpora vedy a výskumu v oblasti kybernetickej bezpečnosti:
- podporovať výskumnú činnosť v oblasti kybernetickej bezpečnosti,
- podporovať budovanie forenzných pracovísk (podporovať budovanie nových špecializovaných pracovísk za účelom posilnenia ochrany významných informačných aktív štátu, s následným využitím ich poznatkov pre podporu rozvoja vedy a výskumu v oblasti kybernetickej bezpečnosti).

Poznámka: Hrubým písmom sú zvýraznené tie úlohy akčného plánu, k plneniu ktorých národný projekt priamo prispieva. Akčný plán okrem zadefinovania jednotlivých úloh nevyhnutných na implementáciu koncepcie kybernetickej bezpečnosti v kapitole Záver priamo uvádza predpokladané zdroje financovania v ňom uvedených aktivít, pričom

Riziká

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

Prílohy

Diagramy, modely, obrázky v plnom rozlíšení

### 3.2.2. Architektúra

#### 3.2.2.1. Biznis architektúra

Tabuľka 5 Biznis architektúra - aktuálny stav

Súhrnný popis

V súčasnosti nie sú úlohy súvisiace so vzdelávaním, výskumom a vývojom v oblasti kybernetickej bezpečnosti vykonávané na dostačujúcej úrovni.
V nasledujúcom texte je popísaný stav týkajúcich sa jednotlivých nosných služieb, ktoré sa plánujú v rámci národného projektu zaviesť.

Výuka:

Pre súčasný stav vzdelávania vo verejnej správe v oblasti informačnej a kybernetickej bezpečnosti vo všeobecnosti platí:

- školenia kybernetickej bezpečnosti bežných používateľov sú teoreticky zabezpečované v réžii subjektov verejnej správy, bez strategickej koordinácie,
- úroveň školení v sektore verejnej správy nie je na rovnakej úrovni, alebo vôbec neexistujú,
- významná množina používateľov verejnej správy školenie kybernetickej bezpečnosti neabsolvovalo,
- tréningy špecialistov na kybernetickú bezpečnosť musia byť obstarávané dodávateľsky, čo je istou záťažou pre štátny rozpočet,
- absentuje strategické plánovanie tréningov špecialistov na kybernetickú bezpečnosť,
- nie je zabezpečené kontinuálne vzdelávanie špecialistov na kybernetickú bezpečnosť,
- špecialisti na kybernetickú bezpečnosť získavajú zručnosti prevažne samoštúdiom, resp. až počas riešenia skutočného kybernetického incidentu,
- arén pre kybernetické výcviky je nedostatok, na Slovensku sa nenachádza žiadna,
- arénové kybernetické výcviky pre subjekty verejnej správy musia byť obstarávané dodávateľsky v zahraničí, čo je významnou záťažou pre štátny rozpočet.

Ministerstvo financií SR má vypracované a zverejnené školiace materiály pre verejnú správu v oblasti bezpečnosti. Zbežná analýza týchto materiálov však ukazuje, že nie sú priamo použiteľné pre potreby projektu bez prepracovania. Existujúce platformy sa viac hodia na použitie v prostredí vysokých škôl.

Simulácia:

Pre súčasné možnosti simulovania aktivít v kybernetickej bezpečnosti vo verejnej správe vo všeobecnosti platí, že:

- prakticky neexistuje kvalitná infraštruktúra typu IT/OT, na ktorej by bolo možné realizovať simulácie a experimenty v oblasti kybernetickej bezpečnosti,
- potenciálne vhodné existujúce infraštruktúry neumožňujú finančne a časovo akceptovateľné možnosti konfigurovateľnosti, resp. rozšírenia, neumožňujú simulácie prostredí používaných o prvkov KI,
- potenciálne vhodné existujúce infraštruktúry neumožňujú virtualizácie dejov a udalostí prebiehajúcich v sieťach a systémoch typu IT/OT na požadovanej úrovni,
- okrem jednotiek pre riešenie kybernetických incidentov (ďalej aj „CSIRT") simulácia v oblasti kybernetickej bezpečnosti nie je vo verejnej správe realizovaná.

Výskum:

- v súčasnosti neexistuje kvalitné prostredie pre výskum a vývoj metód a proprietárneho SW na ochranu proti útokom na siete a informačné systémy,
- okrem jednotiek CSIRT výskum a vývoj v oblasti kybernetickej bezpečnosti nie je vo verejnej správe realizovaný.

Centrum simulácie, výskumu a výuky kybernetických hrozieb a kybernetickej bezpečnosti, ktoré je predmetom národného projektu nie je vybudované a z tohto dôvodu nie je možné popísať biznis architektúru súčasného stavu.
Aktuálny stav biznis architektúry súčasného stavu bude upresnený na workshopoch s prijímateľom a partnermi národného projektu.

Riziká

Spresnenie identifikovaných rizík: Odkazy na relevantné identifikátory rizík v prílohe Riziká.
R2 Pri zachovaní súčasného stavu nie je možné efektívne plniť ciele súvisiace so vzdelávaním, výskumom a vývojom definované v koncepcii kybernetickej bezpečnosti Slovenskej republiky na roky 2015 - 2020.
R3 Nedostatočné technické vybavenie pre zabezpečenie nosných služieb Centra.
R4 Nedostatočná vzdelanostná úroveň v oblasti kybernetickej bezpečnosti.

Prílohy

Diagramy, modely, obrázky v plnom rozlíšení

### 3.2.2.2. Architektúra informačných systémov

Tabuľka 6 Architektúra informačných systémov - aktuálny stav

Súhrnný popis

V súčasnosti neexistuje relevantná architektúra informačných systémov. Systém by bol budovaný od nuly na zelenej lúke.

Riziká

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

R5 Pri zachovaní súčasného stavu sa nepokryjú všetky činnosti definované v legislatívnych požiadavkách.
R6 Nie všetky informačné systémy a moduly budú vybudované systematickým spôsobom.

Prílohy

Diagramy, modely, obrázky v plnom rozlíšení

### 3.2.2.3. Technologická architektúra

Tabuľka 7 Technologická architektúra - aktuálny stav

Súhrnný popis
V súčasnosti nie sú úlohy súvisiace so vzdelávaním, výskumom a vývojom v oblasti kybernetickej bezpečnosti vykonávané na dostačujúcej úrovni a teda nie je k nemu ani relevantná technologická architektúra.

Rôzne školenia sú k dispozícii na webových stránkach (MFSR, CSIRT.sk). V komerčnej sfére existujú rôzni dodávatelia školení, ktorí ich poskytujú na svojich platformách.

Riziká

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

R5 Pri zachovaní súčasného stavu technologických komponentov sa nepokryjú všetky činnosti definované v legislatívnych požiadavkách.

Prílohy

Diagramy, modely, obrázky v plnom rozlíšení

Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.

Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.

### 3.2.2.4. Bezpečnostná architektúra

Tabuľka 8 Bezpečnostná architektúra - aktuálny stav

Súhrnný popis

V súčasnosti nie sú úlohy súvisiace so vzdelávaním, výskumom a vývojom v oblasti kybernetickej bezpečnosti vykonávané na dostačujúcej úrovni. Bezpečnostná architektúra teda nie je z dôvodu súča sného stavu relevantná.

Riziká

Spresnenie identifikovaných rizík: Odkaz y na relevantné identifikátory rizík v prílohe Riziká.

R2 Pri zachovaní súčasného stavu nie je možné efektívne plniť ciele súvisiace so vzdelávaním, výskumom a vývojom definované v koncepcii kybernetickej bezpečnosti Slovenskej republiky na roky 2015 - 2020.
R3 Nedostatočné technické vybavenie pre zabezpečenie nosných služieb Centra.
R4 Nedostatočná vzdelanostná úroveň v oblasti kybernetickej bezpečnosti.

Prílohy

Diagramy, modely, obrázky v plnom rozlíšení

### 3.2.3. Prevádzka

Tabuľka 9 Prevádzka - aktuálny stav

Súhrnný popis

V súčasnosti sa úlohy súvisiace s výukou, simuláciou a výskumom realizujú v obmedzenej miere na úrovni jednotiek CSIRT, ktoré majú prijímateľ národného projektu (CSIRT.SK) a partneri národného projektu (SK-CERT, CSIRT SIS) zabezpečujú prevádzku špecializovaných pracovísk, ktoré majú aktuálne zriadené. Prevádzka je v prevažnej miere pokrývaná vlastným personálnym vybavením doplnená o externú hardvérovú a softvérovú podporu. Napriek tomu, že prevádzkovatelia jednotiek CSIRT, ktoré budú súčasťou budúceho národného systému realizujú prevádzku s maximálnou odbornou starostlivosťou, sú limitované najmä nedostatočným priestorovým, personálnym, znalostným a technickým (hardvérovým a softvérovým) vybavením.

Riziká

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

R7 Prevádzka súčasného riešenia je obmedzovaná nedostatočným personálnym, znalostným a technickým (hardvérovým a softvérovým) vybavením

Prílohy

Diagramy, modely, obrázky v plnom rozlíšení

Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.

Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.

## 3.3. Alternatívne riešenia

Štúdia uskutočniteľnosti analyzuje aj tri alternatívne riešenia, akými je možné pristupovať k národnému projektu:

- prvou alternatívou je ponechať súčasný nevyhovujúci stav,
- druhou alternatívou, ktorá sa javí ako najvýhodnejšia, je vybudovanie Centra simulácie, výskumu a výuky kybernetických hrozieb a kybernetickej bezpečnosti konzervatívnym spôsobom zachyteným v popise budúceho stavu,
- tretia alternatíva uvažuje s možnosťou finančne enormne nákladného Centra simulácie, výskumu a výuky kybernetických hrozieb a kybernetickej bezpečnosti, ktoré by bolo zabezpečované plne outsourcovaným spôsobom.

Všetky alternatívy sú detailnejšie popísane nižšie v texte. Ďalej je zhodnotená ich reálnosť, uskutočniteľnosť, dostupnosť, efektívnosť a efektivita z hľadiska legislatívy, prevádzky, vývoja situácie v kybernetickej bezpečnosti, existujúceho stavu, nákladov a udržateľnosti.

### 3.3.1. Alternatíva A - „Ponechanie súčasného stavu"

Súhrnný popis

V rámci tejto alternatívy by bol ponechaný súčasný stav, t. j. Centrum simulácie, výskumu a výuky kybernetických hrozieb a kybernetickej bezpečnosti by sa nevybudovalo. Súčasný stav, rozsah a fungovanie je popísané vyššie v tejto štúdii (kapitola 2.2 „Popis aktuálneho stavu"). Táto alternatíva nepredpokladá realizáciu žiadnych investícií do stavebných úprav či rozšírenia hardvérových, softvérových a ľudských kapacít oproti aktuálnemu stavu.
Výhody tejto alternatívy sú zrejmé: žiadne ďalšie investície, žiadne zmeny a známe súčasné prevádzkové náklady.
Nevýhodou je jednoznačne neudržateľnosť tohto stavu. Počet kybernetických útokov, ich sofistikovanosť a riziko značných škôd narastá. Je pravdepodobné, že bez možností výuky, simulácia a výskumu o množstve útokov a bezpečnostných incidentov sa vôbec nedozvieme a tiež, že niektoré systémy sú dlhodobo kompromitované bez akejkoľvek detekcie a nápravy havarijného stavu.
Súčasný stav tiež nevyhovuje požiadavkám Koncepcie kybernetickej bezpečnosti Slovenskej republiky na roky 2015 - 2020, nakoľko nie sú realizované opatrenia 4 a 7 ustanovené koncepciou.
Vzhľadom k vyššie uvedenému túto alternatívu vylučujeme a bola by vážnym a stále rastúcim ohrozením kybernetickej bezpečnosti v SR.

### 3.3.2. Alternatíva B - „Nákladovo efektívne vybudovanie Centra - preferovaný variant"

Súhrnný popis

Táto alternatíva uvažuje s nákladovo efektívnym vybudovaním Centra simulácie, výskumu a výuky kybernetických hrozieb a kybernetickej bezpečnosti. Vybudovanie Centra vychádza z požiadaviek bližšie popísaných v kapitole 2.1 „Motivácia".
Jednotlivé funkcie pracovísk boli vybrané na základe strategických, legislatívnych, organizačných, funkčných a technických požiadaviek prijímateľa a partnerov národného projektu a následne posúdením nezávislým expertom na kybernetickú bezpečnosť. Rozloženie jednotlivých funkcií predstavuje nákladovo efektívny variant naplnenia všetkých vyššie uvedených požiadaviek.
Táto alternatíva predstavuje z pohľadu dosiahnutia cieľov budúceho národného projektu najlepšie riešenie. Vybudovanie Centra spôsobom popísaným v rámci tejto alternatívy je najrozumnejším spôsobom, ako dosiahnuť strategické ciele sledované týmto národným projektom pri zachovaní akceptovanej miery nákladov na kybernetickú bezpečnosť. Táto alternatíva je podrobne rozpracovaná v kapitole 2.4 „Popis budúceho stavu".

Centrum môže byť budované vytvorením novej platformy, nákupom existujúceho riešenia, alebo nákupom hotových tréningov(toto je popísané v alt. C). Súčasné možnosti na trhu sú nasledovné:

- CyberG Europe Fyzický polygón, Česká republika
- Kybernetický polygon MU Fyzický polygón, Česká republika CRYSTAL, Softvér
- CDeX (Cyber Defence eXercise Platform), Fyzický polygón, Poľsko Facebook CTF Softvér
- CybExer Range Platform Softvér

Tieto platformy sú popísané v tabuľke nižšie. Na základe analýzy jednotlivých možností je možné konštatovať:

- platformy, ktoré spĺňajú väčšinu kritérii sú dostupné iba ako služba a sú veľmi nákladné,
- hotové riešenia (open source alebo komerčné) nemajú požadované spektrum cvičení (sú orientované iba na jeden typ cvičenia),
- ako vhodné sa teda javí implementovať vlastnú platformu, ktorej efektivita bude preukázaná pomocou CBA.

Preferovanou alternatívou je implementácia platformy, obsahu a súvisiaceho HW/SW v plnom rozsahu, t.j. implementácia nasledovných komponentov:

- tréningová platforma,
- školiaci obsah, t.j. tréningové scenáre a školiace materiály,
- HW a SW infraštruktúra pre samotné tréningové scenáre,
- učebne na NBÚ, ÚPVII, SIS a na vybraných školách.

### 3.3.3. Alternatíva C - „Outsourcing"

Súhrnný popis

Alternatívnym riešením súvisiacim s Centrom simulácie, výskumu a výuky kybernetických hrozieb a kybernetickej bezpečnosti, ktoré sa prirodzene ponúka je outsourcing celej služby vzdelávania, výuky a simulácie, resp. vysielanie pracovníkov na školenia a na arénové tréningy. Realizácia tejto alternatívy by zabezpečila:

- uistenie o dostatočnom zabezpečení cieľov Centra, avšak za cenu vynaloženia enormných finančných prostriedkov,
- vysokú dostupnosť všetkých funkcií Centra.

Nevýhodou a hlavnými rizikami, ktoré so sebou táto alternatíva prináša sú:

- vysoká finančná náročnosť riešenia,
- tréningové scenáre nebudú môcť byť prispôsobené na všetky typy požadovaných infraštruktúr a typov zraniteľností (čo je výsledok analýzy na trhu dostupných riešení uvedenej v tab. nižšie),
- negatívne vnímanie outsourcovania kľúčových vzdelávacích, simulačných a výskumných služieb pre verejnú správu.

Túto alternatívu analyzujeme aj v CBA, kde porovnávame náklady alt. B s alt. C, nakoľko prínosy alternatívy B sú počítané ako náklady na realizáciu alternatívy C.

### 3.3.4. Alternatíva D - „Vybudovanie centra - maximalistický variant"

Súhrnný popis

Maximalistickou alternatívou je vybudovanie Centra simulácie, výskumu a výuky kybernetických hrozieb a kybernetickej bezpečnosti väčšieho rozsahu, na ktorom bude možné paralelne vycvičiť veľké skupiny (nad 10 ľudí) a ktoré bude zároveň schopné organizovať aj medzinárodné cvičenia typu NATO Locked shields. Za účelom zabezpečenia väčšieho rozsahu cvičenia bude potrebné zväčšiť HW a SW inventár ako aj infraštruktúru na ktorej beží softvér centra. Rozdiel maximalistického variantu oproti preferovanému variantu je teda nasledovný:

- zvačšenie rozsahu HW inventáru o 30% (vo finančnom aj výkonnostnom vyjadrení),
- zväčšenie rozsahu SW inventáru o 40% (keďže bude potrebných viac licencií na spustenie väčšieho množstva virtuálnych strojov),
- zvýšenie kapacity hardvéru na beh samotnej platformy (o 40% vo finančnom aj výkonnostnom vyjadrení),
- zvýšenie počtu učební na dvojnásobok kapacity.

Z hľadiska prínosov by hlavným rozdielom oproti alternatíve C bola prestíž a kvalita spojená s prípadným organizovaním medzinárodných tréningov a cvičení. Tento benefit je značný, nakoľko by mal okrem iného vplyv aj na kvalitu celého projektu, nie je však priamo vyčísliteľný. Zároveň v prípade úspechu platformy aj v preferovanom variante C nie je vylúčené jeho neskoršie rozšírenie v prípade potreby alebo ambícii. Práve z tohto dôvodu nie je tento maximalistický variant, ktorý by síce Slovensko posadil pevne na mapu boja proti kybernetickému zločinu, preferovaným variantom.

| Názov a formát | Popis | Výhody | Nevýhody |
|---|---|---|---|
| CyberG Europe<br>Fyzický polygón<br>Česká republika<br>https://www.cybergeurope.com/ | Vzdelávacia platforma, založená na trénovaní organizácií v tzv. Aréne. Aréna je nakonfigurovaná podľa požiadaviek organizácie, ktorá trénuje. Dôraz kladený na tímovú spoluprácu a na široké spektrum rolí, ktoré možno trénovať. | + komplexita<br>+ Možnosť nakonfigurovať cvičenie podľa požiadaviek zákazníka | - komerčná platforma<br>- cena<br>vytvorenie scenára vyžaduje dlhší čas<br>- pre zaistenie idenálnej kontinuity nutnosť cvičiť v rámci infraštruktúry spoločnosti |
| Kybernetický polygon MU<br>Fyzický polygón<br>Česká republika https://www.kypo.cz/ | Kybernetický polygón Masarykovej univerzity. Poskytujú dvojdenné kybernetické cvičenia, ako zvládať kybernetické bezpečnostné incidenty. | + rôznorodé scenáre<br>+ rôzne typy cvičení | - nutnosť cvičiť fyzicky iba v rámci polygónu (priestory MU) |

| | | | |
|---|---|---|---|
| CRYSTAL<br>Softvér<br>http://crystalproject.ch/ | Platforma pre technické a C&C cvičenia | + open source<br>+ možnosť integrovať na vlastnej infraštruktúre | - obmedzené typy cvičení |
| CDeX (Cyber Defence eXercise Platform)<br>Fyzický polygón<br>Poľsko<br>https://www.vectorsynergy.com/vector-synergy-cdex-cyber-defence-exercise-platform | Platforma založená na Blue/Red team princípe, prebiehajúca v reálnom čase | + rôznorodé scenáre<br>+ možnosť Blue teamu hardenovať infraštruktúru pred začatím cvičenia<br>+ simulácia APT útokov | komerčné riešenie<br>obmedzené typy cvičení |
| Facebook CTF<br>Softvér<br>https://github.com/facebook/fbctf | Platforma určená na vytváranie Capture The Flag (CTF) cvičení | + opensource<br>+ možnosť inštalácie na vlastnej infraštruktúre | - len Capture The Flag cvičenie |
| CTF365<br>Webová platxforma<br>https://ctf365.com/ | Platforma určená na vytváranie CTF cvičení | + rôzne možnosti financovania | - len Capture The Flag cvičenie<br>komerčné riešenie<br>- scenár je pevne daný developerom<br>- len na systéme developera (cloud) |
| CybExer Range Platform<br>Softvér<br>https://cybexer.com/#range | Platforma zameraná na technické cvičenia | + scenár vytvorený na mieru zákazníka<br>+ cvičenie môže prebiehať na infraštruktúre zákazníka | komerčné riešenie<br>- len možnosť technických cvičení |

### 3.3.5. Porovnanie alternatív riešenia

Tabuľka 10 Porovnanie alternatív riešenia

| Kritérium | Alternatíva A | Alternatíva B | Alternatíva C | Alternatíva D |
|---|---|---|---|---|
| Školenie požadovaného počtu používateľov L1 | - | + | + | + |
| Školenie požadovaného počtu používateľov L2 | - | + | + | + |
| Tréning požadovaného počtu používateľov L4 | - | + | + | + |
| Tréningová a školiaca platforma umožňujúca hranie širokého rozsahu scenárov | - | + | + | + |
| Možnosť realizácie technických, manažérských a kombinovaných školení | - | + | - | + |
| Možnosť realizácie praktických (hands on) architektonických školení | - | + | - | + |
| Jednoduchosť riešenia | ++ | - | -+ | - |

Legenda a vysvetlivky:

| Znak | Vysvetlenie |
|---|---|
| ++ | Tento symbol vyjadruje, že dané alternatívne riešenie je vzhľadom na stanovené kritérium veľmi výhodné. |
| + | Tento symbol vyjadruje, že dané alternatívne riešenie je vzhľadom na stanovené kritérium výhodné. |
| - | Tento symbol vyjadruje, že dané alternatívne riešenie je vzhľadom na stanovené kritérium nevýhodné. |
| -+ | Tento symbol vyjadruje, že dané alternatívne riešenie je vzhľadom na stanovené kritérium ambivalentné. |

Výber alternatívy: Ako najefektívnejší variant sa javí alternatíva B „Nákladovo efektívne vybudovanie Centra", ktorý zabezpečí všetky požiadavky vyplývajúce z legislatívy a je aj víťazom multikriteriálnej analýzy spolu s maximalistickým variantom - alternatívou D. Z hľadiska minimalizácie rizika je síce možné zvažovať aj alternatívu C, avšak veľkou nevýhodou tejto alternatívy je vysoká finančná náročnosť riešenia, pričom je otázne, či by sa podarilo dosiahnuť lepšie výsledky ako pri alternatíve B. V prospech alternatívy B hovoria aj kvalitatívne prínosy, napríklad dostupnosť riešenia aj pre školy, prípadne dostupnosť vytvoreného zdrojového kódu a prípadne aj časti obsahu pre komunitu. V neprospech alternatívy D hovorí fakt, že prínosy sú totožné s alternatívou B, ale náklady sú vyššie. Celkovým víťazom multikriteriálnej analýzy aj ekonomického porovnania je teda alternatíva B.

## 3.4. Popis budúceho stavu

### 3.4.1. Legislatíva

Tabuľka 11 Legislatíva - budúci stav

Súhrnný popis

Budúce riešenie Centra simulácie, výskumu a výuky kybernetických hrozieb a kybernetickej bezpečnosti musí zabezpečiť úplný súlad s nasledujúcimi existujúcimi právnymi predpismi:

- smernica Európskeho parlamentu a rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii,
- vykonávacie nariadenie Komisie (EÚ) 2018/151 z 30. januára 2018, ktorým sa stanovujú pravidlá uplatňovania smernice Európskeho parlamentu a Rady (EÚ) 2016/1148, pokiaľ ide o bližšiu špecifikáciu prvkov, ktoré musia poskytovatelia digitálnych služieb zohľadňovať pri riadení rizík v oblasti bezpečnosti sietí a informačných systémov, a parametrov na posudzovanie toho, či má incident závažný vplyv,
- zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov,
- súvisiace vykonávacie predpisy k zákonu o kybernetickej bezpečnosti:
- vyhláška Národného bezpečnostného úradu č. 164/2018 Z. z., ktorou sa určujú identifikačné kritériá prevádzkovanej služby (kritériá základnej služby),
- vyhláška Národného bezpečnostného úradu č. 165/2018 Z. z., ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov,
- vyhláška Národného bezpečnostného úradu č. 166/2018 Z. z. o podrobnostiach o technickom, technologickom a personálnom vybavení jednotky pre riešenie kybernetických bezpečnostných incidentov,
- vyhláška Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení,
- zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
- zákon č. 45/2011 Z. z. o kritickej infraštruktúre v znení neskorších predpisov.

Budúce riešenie ďalej musí byť v súlade s týmito platnými koncepčnými dokumentmi:

- Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015 - 2020,
- Akčný plán realizácie Koncepcie kybernetickej bezpečnosti Slovenskej republiky na roky 2015 - 2020.

V rámci budúceho legislatívneho stavu sa predpokladá s prijatím zákona o výkone správy v oblasti informačných technológií verejnej správy a o zmene a doplnení niektorých zákonov, ktorý by však nemal mať zásadný vplyv na národný projekt.

Kritéria kvality

Spresnenie kritérií kvality: Odkazy na relevantné identifikátory kritérií kvality v prílohe Kritéria kvality.

P1 Súlad s legislatívou

Riziká

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

R8 Legislatívna príprava bude meškať, respektíve výsledné znenia nových právnych predpisov budú obsahovať ustanovenia, ktoré môžu mať vplyv na národný projekt R9 Politické riziko pri zmene vlády

Prílohy

Diagramy, modely, obrázky v plnom rozlíšení

## 3.4.2. Architektúra 3.4.2.1.

### Biznis architektúra

Tabuľka 12 Biznis architektúra - budúci stav

Súhrnný popis

Biznis architektúru budúceho riešenia možno popísať nasledovne:
Biznis aktérmi Centra sú:
- NBÚ,
- ÚPPVII,
- SIS,
- subjekty verejnej správy.

Z pohľadu biznis rolí sú aktéri zaradení nasledovne:
- NBÚ - zriaďovateľ a prevádzkovateľ funkčného celku ústredného tréningového centra,
- ÚPPVII - zriaďovateľ a prevádzkovateľ tréningového pracoviska,
- SIS - zriaďovateľ a prevádzkovateľ tréningového pracoviska,
- subjekty verejnej správy:
- využívatelia výstupov národného projektu v rámci nosnej služby Výuka:
- účastníci školení bežných používateľov na zvyšovanie bezpečnostného povedomia L1,
- účastníci tréningov IT zamestnancov L2,
- účastníci tímových arénových kybernetických výcvikov L4,

Centrum bude poskytovať nasledovné nosné biznis služby:
- výuka,
- simulácie.

Tieto služby budú poskytované pomocou nasledovných biznis komponentov:
- tréningová platforma,
  HW a SW infraštruktúra,
- samotné školenia - obsah a školiace scenáre,
- fyzické pracoviská - učebne:
  - Ústredné tréningové centrum kybernetickej bezpečnosti SR (NBÚ)
  - Tréningové pracoviská UPVII (pripadne SIS)

Projekt bude obsahovať nasledovné biznis funkcie:
- vzdelávacie funkcie:
- školenie bežných používateľov na zvyšovanie bezpečnostného povedomia,
- tréning špecialistov nakybernetickú bezpečnosť,
- funkcie simulácie:
- tímový arénový kybernetický výcvik,
- realizácia bezpečnostných simulácií a experimentov:
- simulačné cvičenie na fyzickej IT infraštruktúre,
- simulačné cvičenie na fyzickej OT infraštruktúre,

Tieto funkcie umožnia realizovať nasledovné typy cvičení a ich kombinácií:
- Testovanie vedomostí a spôsobilostí
- Technické cvičenia: blue team, red team na rôznych typoch IT infraštruktúry
- Technické cvičenia nad priemyselnými riadiacimi systémami (SCADA, ICS)
- CTF cvičenia,
- Tabletop cvičenia,
- Procesné cvičenia a cvičenia bezpečnostných politík,
- Cvičenia zamerané na návrh bezpečnej infraštruktúry a bezpečnostnej

architektúry. Z hľadiska obsahu sa výučba bude zameriavať najmä na nasledovné

oblasti:

L1

- Terminológia
- Základné povedomie
- Schopnosť používania stanovených bezpečnostných mechanizmov
- Znalosť a uplatnenie interných procesov (smerníc) v rôznych situáciách
- Schopnosť správne analyzovať a zhodnotiť situáciu

L2

- Znalosť bezpečnostných zásad, postupov a techník
- Znalosť zásad fyzickej a objektovej bezpečnosti, personálnej bezpečnosti
- Znalosť princípov testovania a zásad auditu kybernetickej a informačnej bezpečnosti
- Znalosť základných (príslušných) právnych predpisov, politík, požiadaviek na súlad a noriem (KB, GDPR)
- Znalosť metodík a procesov riadenia rizika, postupov na analýzu rizík

- Znalosť typických hrozieb, postupov pre identifikáciu hrozieb a zraniteľností
- Schopnosť analýzy a hodnotenia bezpečnostných mechanizmov
- Znalosť metodík podnikovej architektúry
- Znalosť procesov incident handlingu, princípov Disaster Recovery, Business Continuity
- Znalosť princípov logovania a bezpečnostného monitorovania
- Znalosť konceptov počítačových sietí, zásad architektúry sietí a základných bezpečnostných princípov
- Znalosti riadenia IT služieb

L4

- Znalosti na úrovni CCNA Routing/Switching, SecOps a pod.
- Znalosti typových techník útokov a princípov obrany

- Znalosti malware analýzy a forenzie (rôzne technológie, rôzne prostredia)

- Tréning obrany prostredia

ICS/SCADA Výučba prostredníctvom SaaS

Služby výučby, t.j. vzdelávanie používateľov L1 a L2 by malo prebiehať platforme SaaS od firmy Cisco. Je uzatvorená predbežná dohoda o tom, že Cisco poskytne:

- SaaS platformu na realizáciu školení, testov, a reportingu - vyhodnotenia,
- obsah školení pre relevantných používateľov v anglickom jazyku,
- rozhranie pre preklad.

V rámci projektu sa zabezpečí preklad všetkého relevantného obsahu pre používateľov úrovní L1 a L2 do slovenského jazyka.
V rámci prevádzky bude zabezpečený preklad anglických aktualizácii.

Tréningy a cvičenia v kybernetickej aréne

Služby simulácie v kybernetickej aréne na platforme slúžia predovšetkým pre používateľov L4 na praktické "hands on" tréningy rôznych druhov (blue/red team, CTF, Tabletop, procesné a architektonické cvičenia). Takéto cvičenie je možné demoštrovať na príklade cvičení NATO Locked Shields.

Cvičenie bude podporovať nasledovné skupiny používateľov:

- Študenti / cvičené osoby

o blue team - obrancovia (študenti alebo automaty/ľudia) o

správcovia systémov a sietí o manažéri

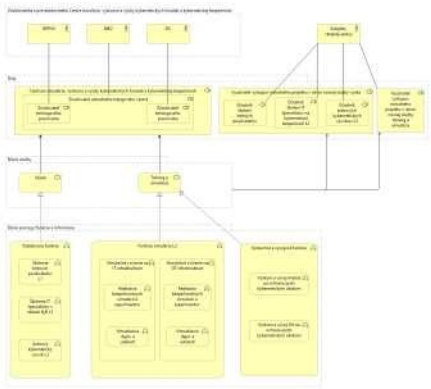
o red team - útočníci (študenti alebo automaty/ľudia)

- Učitelia / tréneri
- White team - simulovaní používatelia (automaty/ľudia)
- Pozorovatelia
- Tím dizajnu, prípravy a obsluhy infraštruktúry - administrátori / green team
- Tím dizajnu tréningových scenárov - autori študijného materiálu, plánovači scenárov
- Manažment

### 3.4.3. Scenáre

Účastníkom arénových tréningov budú pridelované scenáre podľa obtiažnosti na základe ich schopností a skúseností. Jednoduché scenáre budú pozostávať z jednej jednoduchšej, alebo známejšej zraniteľnosti. Sofistikovanejšie cvičenia budú pozostávať viacerých scenárov, prípadne z storylines, ktoré budú simulovať komplexnú spoločnosť z daného sektora, ktorá bola napadnutá sofistikovaným útorokom, kde na prienik bola použitá jedna zraniteľnosť a na preniknutie do celej infraštruktúry iná. Budú budované aj cvičenia, ktoré budú simulovať známe uskutočnené útoky. Takéto cvičenia budú budované pre rôzne sektory, pričom do infraštruktúry bude možné nasadiť aj priamo aplikácie používané v konkrétnej spoločnosti.
Základnou jednotkou je scenár, ktorý bude zameraný na jednu vrstvu a jeden typ útoku. Takýto scenár sa skladá z:
programovej implementácie konkrétnej zraniteľnosti, alebo útoku, táto typicky môže pozostávať z docker image s špecifickým programom
hodnotenia splnenia úlohy pri zachovaní funkčnosti, priradenia HW a SW komponentov k scenáru, definícii monitorovacích bodov pre monitoring,

Príklady útokov, ktoré je možné zreplikovať do storylines, ktoré budú tvoriť základ sofistikovanejších arénových tréningov: https://www.wired.com/story/xbox-underground-videogame-hackers/ https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ https://www.wired.com/story/mirai-botnet-minecraft-scam-brought-down-the-internet/



Poznámka: Zobrazené služby predstavujú všeobecné služby pre subjekty verejnej správy poskytované Centrom. Nepredstavujú koncové služby.

Kritéria kvality

Spresnenie kritérií kvality: Odkazy na relevantné identifikátory kritérií kvality v prílohe Kritéria kvality.

P1 Miera splnenia legislatívnych požiadaviek.
P2 Miera úplnosti a optimalizácie procesov v rámci Centra.

Riziká

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

R10 Riešenie bude náročne na biznis (kapacitne a vedomostne)

Prílohy

Diagramy, modely, obrázky v.

### 3.4.3.2. Architektúra informačných systémov

Tabuľka 13 Architektúra informačných systémov - budúci stav

Súhrnný popis
Budúce riešenie bude pozostávať z nasledovných aplikačných modulov/funkcií:

- platforma pre elektronické školenia (formou SaaS), ktorá bude poskytovať služby pre používateľov L1 a L2,
- arénová platforma pre beh scenárov a cvičení pre používateľov L4 (pozostáva z HW a SW), repozitár HW a SW (sklad infraštruktúry),
- podporné komponenty,
- vybavenie učební.

## 3.5. Elektronické školenia

Elektronické školenia budú poskytované prostredníctvom SaaS služby od firmy Cisco, s ktorou je uzatvorená predbežná dohoda na základe ktorej poskytne svoju vzdelávaciu platformu pre školenia zamestnancov VS. Tento projekt zabezpečí:

- preklady materiálov,
- vydávanie anonymizovaných prístupových údajov k SaaS službe,
- reporting a štatistiky,
- notifikačný systém.

## 3.6. Arénová platforma

Systém bude okrem iného obsahovať

- engine pre podporu vytvárania a behu scenárov,
- rozhranie pre vytváranie nových scenárov, komponentov a aktivít,
- detailný monitoring a reporting prevádzky počas cvičenia aj naprieč všetkými cvičeniami,
- simulačnú platformu a virtuálnu a fyzickú infraštruktúru, ktorá bude prideľovaná zo skladu infraštruktúry pre konkrétne cvičenia.
- Postaviť tréningovú SW platformu pre on-line tréning zručností v oblasti kybernetickej bezpečnosti a kybernetickej obrany
- Možnosť kolaboračného / skupinového tréningu (cvičenia), zapojiť ďalšie skupiny na diaľku so vzdialeným prístupom rôznymi formami

### 3.6.1. Riadiaci a simulačný SW

o Voliteľne SCADA (ICS) pracovisko pre tréningy zručností v tejto oblasti

- Riadiaci a simulačný SW musí umožňovať alebo obsahovať najmenej

o Vytváranie tréningovej infraštruktúry podľa potrieb tréningových skupín (od jednoduchej po náročnú infraštruktúru pozostávajúcu z rôznych HW a SW komponentov prepojených do sietí s rôznou architektúrou),

o Simulátor internetu pre potreby cvičení,

o Využitie rôznych typov a platforiem pre aplikačné prostredie, malo by umožňovať ad-hoc inštaláciu SW nástrojov pre potreby tréningových skupín (špecifických tréningov) a pod.

o Vytváranie nových / užívateľských tréningových scenárov

o Vytváranie (definovanie) tréningových úloh (typy a prevedenie útočných resp. obranných aktivít, ich monitorovacie a hodnotiace body a pod.)

o Automatizované a poloautomatizované vykonávanie tréningových scenárov

o Vykonávať administratívu tréningov, evidenciu študentov a pod.

o Priebežný dohľad nad prebiehajúcim tréningom, priebežný scoring (platforma trénera)

o Po skončení každého tréningu automatizovane vytvoriť rôzne reporty pre učiteľa, management a prípadne pre študentov

### 3.6.2. Scenáre

Základná jednotka každého cvičenia na platforme je scenár (napr. zraniteľnosť aplikačného sekera, zle zabezpečený notebook, nesprávne nastavené aktualizácie na severoch, chýbajúce zálohy, aktívne sa šíriaci vírus atď). Scenár sa skladá z komponentov scenára (konkrétne vlastnosti HW a SW z repozitára, ktoré sú do scenára zapojené a na ktorých scenár de fakto beží), ktoré v prípade zložitejších a viacvrstvových scenárov môžu byť zoskupené v príbehoch (story line, napr. Virtuálna spoločnosť X je napadnutá externým útočníkom na viacerých rozhraniach a využíva konkrétne zraniteľnosti).

Cvičenia sú vykonávané online na prostriedkoch tréningovej platformy. Každá aktivita sa zaznamenáva a vyhodnocuje. Na jednom tréningovom pracovisku je možné vykonávať súbežne viacero na sebe nezávislých cvičení.

Popis blue vs red team cvičení je napríklad tu.

V nasledovnej tabuľke sa nachádzajú typy útokov, ktoré je potrebné implementovať pre jednotlivé vrstvy infraštruktúry, resp. aplikácii v scenároch. Tieto scenáre budú implementované pre jednotlivé sektory podľa zákona o KyB, resp. podľa zákona o kritickej infraštruktúre.V rámci týchto oblastí bude vytvorených priemerne 15 scenárov, predpokladá sa však 80% prepoužiteľnosť scenárov v rámci jednotlivých sektorov (keďže základná infraštruktúra je podobná).

| Typy útokov / cielená IT vrstva | Vrstva HW infraštruktúry (firmware, zraniteľnosti HW) | Virtualizačná vrstva | Databázová vrstva | Aplikačná vrstva | Sieťová vrstva (1-6 ISO/OSI layer) |
|---|---|---|---|---|---|
| Malware | x | | | | |
| Webové útoky a zraniteľnosti | | | | | |
| Útoky zameraného odmietnutie služby (DoS/DDoS) | x | | | | |
| Phishing a sociálne inžinierstvo | | | | | |
| Ransomware | | | | | |
| Botnety | x | | | | |
| Cieľené / zero day útoky | x | | | | |

## 3.6.3. Monitoring a vyhodnocovanie

Platforma musí podporovať viacero typov monitoringu

- Monitoring priebehu cvičenia a dosahovaných cieľov, ako ich definuje scenár a jeho komponenty
- Detailný monitoring naprieč všetkými cvičeniami
- Technický monitoring priebehu cvičenia a aktivity hráčov formami

o keylogger

o ukladanie záberov obrazovky

o tento monitoring umožní spätne prehrávať a analyzovať akcie hráčov a ich reakcie na scenár za účelom vzdelávania počas záverečnej fázy cvičenia alebo ako ukážkový materiál pri ďalších cvičeniach

- Technický monitoring softvérových a hardvérových platforiem a ich komponentov

Nad týmto monitoringom platforma umožní vyhodnocovanie formami

- Real-time dashboardov a skórovania
- Manažérskych prehľadov a zhrnutí

## 3.6.4. Inštalácia, manažment zmien a konfigurácií

Open-source softvér platformy by mal podporovať dnes bežné vývojové paradigmy, architektúry a mechanizmy inštalácie, napríklad:

- zdrojový kód v SCM (napr. GIT repozitári)
- Inštalačné skripty pre celú platformu v automatizačnom nástroji ako napr. Ansible
- Inštalačné skripty na riadenie cvičenia (napr. Integračné komponenty infraštruktúry) v automatizačnom nástroji ako napr. Ansible
- členenie frontend-backend

## 3.6.5. Technické komponenty infraštruktúry

Pre potreby rôznorodých tréningov je nevyhnutné mať možnosť postaviť rôznu tréningovú (simulovanú) infraštruktúru kombinovanú zo zariadení a softvérových platforiem rôznych výrobcov / dodávateľov. V rámci prípravy dizajnu, prípravy a obsluhy infraštruktúry spolu s červeným tímom navrhne a postaví simulovanú infraštruktúru pre potreby konkrétnej tréningovej skupiny z komponentov, ktoré sú k dispozícii na pracovisku alebo špeciálnych komponentov.

- Sieťová tréningová platforma (Routers, LAN switches etc, najmenej traja až štyria najpoužívanejší výrobcovia sieťových zariadení) - navrhujeme CISCO, Juniper, DELL, HP, IBM, Lenovo, Huawei, ZTE a pod
- Wifi technológie (rôzne zariadenia - Cisco, Ubiquiti, TP-Link, ASUS, Huawei ... )
- Bezpečnostné produkty typu FW, IDS/IPS senzory, WAF a pod. - navrhujeme CISCO, Checkpoint, Palo Alto, Fortinet, F5, Snort/Suricata ...
- Iné HW zariadenia - VOIP telefóny a ústredne, inteligentné tlačiarne, a pod. Každá technológia od viacerých výrobcov vrárane open source riešení ako Asterisk
- Servery a virtualizácie - VMware, XEN, KVM, MS HyperView
- Server OS - Windows Server (rôzne verzie), OS Linux (rôzne verzie, rôzne server distribúcie)
- Mail (rôzne aj aplikácie, Windows, Mac aj Linux SW, vrátane MS Exchange)
- DB (rôzne free aj licencované DB Linux aj MS vrátane Oracle, NoSQL ESK, Hadoop)
- Rôzny software (DNS/DNSSEC servery, AV - ESET, Kaspersky, Trend Micro a pod.) klient aj server side
- Desktopy/NB (Windows rôzne verzie, Linux - rôzne distribúcie a Apple Mac OS X)
- Mobilné platformy (rôzne Android a IOS zariadenia)
- IOT zariadenia - najmä kamery, led žiarovky, senzory (rôzni výrobcovia - Grandstream, HiWatch,
- HSM zariadenia, dvojfaktorová autentifikácia,
- zariadenia eZdravie.

## 3.6.6. Podporné komponenty

Medzi podporné komponenty patria:

- komponent, ktorý bude vydávať anonymizované prístupy k SaaS platforme,
- reporting a štatistiky školení na SaaS platforme,
- jednoduchý notifikačný komponent,

jednoduchý portálový komponent slúžiaci na prezentáciu výsledkov projektu a ako štartovací bod.

Kritéria kvality:
P1 Miera splnenia legislatívnych požiadaviek a strategických dokumentov P3
Interná integrácia tréningových pracovísk na ústredné tréningové centrum.

R11 Riešenie nebude dostatočne flexibilné.

R12 Interná integrácia tréningových pracovísk na ústredné tréningové centrum.

Prílohy

Diagramy, modely, obrázky v plnom rozlíšení

Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.

Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.

### 3.6.3.3. Technologická architektúra

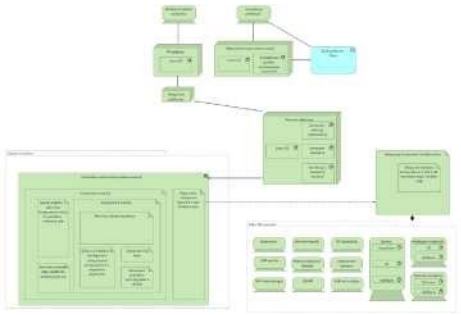
Tabuľka 14 Technologická architektúra - budúci stav

Súhrnný popis
Technologická architektúra Centra bude pozostávať z nasledovných hlavných technologických komponentov:

- platforma pre elektronické školenia (formou SaaS), ktorá bude poskytovať služby pre používateľov L1 a L2,
- arénová platforma pre beh scenárov a cvičení pre používateľov L4 (pozostáva z HW a SW),
- repozitár HW a SW (sklad infraštruktúry),
- podporné komponenty,
- vybavenie učební.

Medzi repozitár HW a SW patria napríklad nasledovné položky:

- smerovače,
- LAN switche,
- Wi-Fi technológie,
- sieťové firewally,
- webové aplikačné firewally,
- IDS/IPS,
- servery,
- mobilné zariadenia,
- VoIP ústredne,
- VoIP telefóny,
- inteligentné tlačiarne,
- IoT Kamery,
- IoT LED žiarovky,
- IoT senzory,
- SCADA (ICS) zariadenia,
- rôzny komerčný SW ako databázy,
- HSM servery a technológie dvojfaktorovej autentifikácie,
- virtualizačné technológie a samotné hypervisory,
- medicínske zariadenia a komponenty z eZdravie.



Technologická architektúrura bude nasadená paralelne u partnerov SIS a NBÚ, pričom modul kooperácia umožní prepojenie oboch platforiem za účelom realizácie kooperatívnych scenárov. Používatelia pristupujú k architektúre prostredníctvom tréningových učební. Technologický pohľad vzhľadom na partnerov je nasledovný:

- u partnera NBÚ sú nasadené všetky komponenty,
- u partnera UPVII sa nachádzajú iba učebne,
- u partnera SIS sa nachádzajú učebne a arénová platforma, ktorá pristupuje na HW/SW repozitár nasadený u partnera NBÚ.

## 3.7. Školiace pracoviská / tréningové učebne

- Vytvoriť pracovisko (minimálne 2 učebne) s možnosťou súčasného teoretického tréningu 2 skupín študentov automatizovanou formou tréningu alebo jednej skupiny študentov spolu s vlastnou skupinou trénerov v rozsahu do 10 študentov na učebňu
- učebne musia byť vybavené

minimálne: o Študentskými pracoviskami

- Pracovný stôl,
- stolička,
- prívod elektrickej energie,
- Zásuvky do štrukturovanej kabeláže (min

2ks/študent) o terminálmi na prístup do platformy

o modernou audiovizuálnou technikou

- Prezentačná technika
- wallboardy/dashboardy
- Jednoduché telekonferenčné riešenie

o RGB náladové osvetlenie miestnosti (red team, blue team, časový stres, indikácia úspechu prienikov a pod.) o

Kontrolovaným prístupom do učebne (bezpečnostné dvere)

- Pozorovacia/oddychová miestnosť
- Technická miestnosť (umiestnenie serverov a fyzickej infraštruktúry, štruktúrovaná kabeláž, klimatizácia, zabezpečovacie zariadenie a pod.)
- Možnosť vzdialeného tréningu - učebňa umiestnená na vzdialenej lokalite
- Pracoviská (učebne) musia umožňovať zároveň tréning SW analytických vedomostí - forenziu pri dodržaní vysokej miery bezpečnosti pracoviska a ostatnej infraštruktúry

| Prílohy | Diagramy, modely, obrázky v plnom rozlíšení |
|---|---|

### 3.7.3.4. Implementácia a migrácia

Tabuľka 15 Implementácia a migrácia

Súhrnný popis

V projekte sa predpokladá dodanie projektových výstupov popísaných nižšie, vrátane stavených úprav. Samotný projekt bude rozdelený do viacerých fáz, resp. aktivít:

- Analýza a dizajn

  Výstupom aktivity Analýza a dizajn bude vypracovanie detailnej funkčnej špecifikácie, najmä pre predpokladanú softvérovú platformu, potrebný je však holistický pohľad zahŕňajúci aj ostatné výstupy . DFŠ prejde po častiach akceptačným konaním. Paralene s touto aktivitou začína aj implementácia, kde budú dodávané už v DFŠ odsúhlasené časti riešenia. V rámci analýzy budú dodané aj rámcové návrhy obrazoviek, ktoré budú priebežne odsúhlasované s biznis vlastníkmi konkrétnej časti.

- Nákup HW a krabicového softvéru

  V rámci tejto aktivity sa zabezpečí nákup nevyhnutného hardvérového vybavenia pre realizáciu projektu ako aj krabicového softvéru pre potreby repozitára platformy.

- Implementácia riešenia predstavuje customizáciu a integráciu riešenia agilným sposobom s min. mesačnou frekvenciou dodávania funkcionality. Požiadavkou je transparentný vývoj open source platformy, pričom výsledná platforma má byť vo forme frameworku, do ktorého sa budú už počas prevádzky pridávať ďalšie komponenty.

  Implementácia zabezpečí:
  - prípravu technologických prostredí, vrátane inštalácie požadovaných SW produktov,
  - implementáciu funkcionality jednotlivých výstupov implementačného projektu,
  - dodanie sady školení, politík a procesov,
  - akceptáciu produktov,
  - dodanie dokumentácie (používateľskej, administrátorskej a pod.),
  - prípravu školiacich pracovísk / učební vrátane stavebných úprav.
- Testovanie - výstupom aktivity Testovanie bude realizované funkčné aj nefunkčné testovanie, vrátane:
  - Integračného testovania,
  - Regresného testovania,
  - Akceptačného testovania,
  - Výkonnostného a penetračného testovania (týka sa iba platformy)
    Testovanie bude prebiehať paralelne s implementáciou na strane dodávateľa, pričom sa však predpokladá aj testovanie na strane zákazníka (min. za výsledky agilného dodávania funkcionality ako výsledok jednotlivých "sprintov", pričom sa predpokladá 1x test a 1x retest).
- Nasadenie - v rámci aktivity prebehne nasadenie a spustenie riešenia na produkčnom prostredí, ako aj dodávka ostatných prostredí (testovacie, vývojové). V rámci nasadenia bude:

- po dokončení a vyladení jednotlivých komponentov Centra prechod na plnú prevádzku už plne v gescii prijímateľa a partnerov národného projektu,
- dokončenie všetkých školení,
- knowledge transfer.

Je potrebné klásť dôraz na:

- podľa možností agilný prístup k nasadzovaniu technických komponentov a vývoju,
- zabezpečenie dostatočného projektového tímu na strane zákazníka minimálne na úrovni garantov, ktorí sa vedia projektu venovať na dennej báze,
- dodržiavanie princípov projektového riadenia PRINCE2 (definované produkty s akceptačnými kritériami, zmenový rozpočet, tolerancie jednotlivých míľnikov, etáp a aj samotných produktov),
- knowledge transfer - transfer vedomostí od dodávateľa členom prevádzkových tímov jednotlivých funkčných celkov Centra.

Podporné aktivity sú:

Publicita a informovanosť

Aktivita začne 4 mesiace pred začatím realizácie hlavných aktivít činnosťami v zmysle pravidiel definovaných v Manuáli pre informovanie a komunikáciu (vzhľadom na predpokladaný termín podpisu Zmluvy o poskytnutí NFP) a bude trvať počas celej doby realizácie hlavných aktivít projektu. Pokrýva oblasť výdavkov na zabezpečenie aktivít informovania a publicity definovaných v Manuáli pre informovanie a komunikáciu. UPVII bude priebežne informovať o stave projektu na svojej webstránke a taktiež osadí na hlavnom mieste realizácie projektu veľkoplošný pútač k projektu, ktorý nahradí po jeho ukončení stálou tabuľou. V neposlednom rade budú súčasťou aktivity aj činnosti zabezpečované v zmysle Metodiky riadenia kvality a projektového riadenia ÚPPVII a to najmä v oblasti nákupu priestoru nadlinkovej komunikácie a produkcie a výroby mediálnej kampane.

Riadenie projektu

Aktivita začne 6 mesiacov pred začatím realizácie hlavných aktivít činnosťami partnera a následne bude trvať počas celej doby realizácie hlavných aktivít projektu. V rámci tejto aktivity budú stanovené základne role a vytvorený riadiaci výbor projektu, menovaný projektový manažér za stranu UPVII, ako aj za stranu dodávateľa, projektové tímy so stanovenými úlohami a zodpovednosťami. V neposlednom rade bude aktivita pokrývať zaistenie dohľadu nad kvalitou riešenia (quality assurance) a projektovým riadením v zmysle Metodiky riadenia kvality a metodiky projektového riadenia UPPVII.

Plán VO

Verejné obstarávanie je plánované realizovať ako jeden celok, pričom jeho realizácia je plánovaná hneď po uzatvorení zmluvy o NFP. Podpis NFP je plánovaný na 09/2019, ukončenie VO je plánované v 12/2019.

Projektové výstupy

Projekt musí poskytnúť komplexné riešenie problematiky vzdelávania a tréningov v oblasti kybernetickej bezpečnosti, vrátane týchto oblastí:

- Holistický návrh celého riešenia, vrátane priestorov, hardvéru a softvéru, politík a procesov
- Obstaranie potrebných hardvérových komponentov
- Obstaranie alebo vývoj potrebných softvérových komponentov

o Navrhnúť a vytvoriť potrebný riadiaci a simulačný SW pre celkové riadenie, správu, návrh, vykonávanie a vyhodnocovanie simulačných tréningov, školení a cvičení v oblasti kybernetickej bezpečnosti

- Vytvoriť prvú sadu základných školení (tréningových scenárov) pre potreby jednotlivých pracovísk, pričom tieto scenáre budú zahŕňať:
  - základné všeobecné scenáre,
  - špecializované scenáre na jednotlivé sektory, pričom scenáre budú jednoducho konfigurovateľné aj na iné sektory.
- Návrh politík a procesov
- Zabezpečiť vytvorenie tréningových pracovísk pre rôzne cieľové skupiny pre teoretický aj praktický tréning špecialistov v oblasti kybernetickej bezpečnosti

o Pre každé pracovisko

- Vykonať príslušné stavebné úpravy pre vytvorenie priestoru pre tréning špecialistov
- Dodať a implementovať tréningovú infraštruktúru
- Implementovať riadiaci a simulačný SW

- Implementovať prvú sadu základných školení (tréningových scenárov)

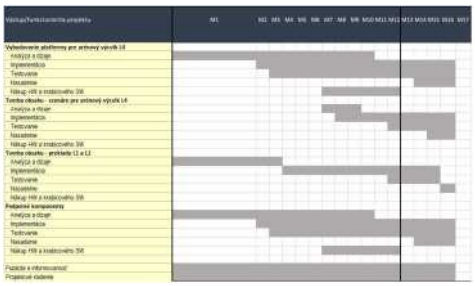
Míľnik

| | Harmonogram dokončenia od času začiatku (t=ukončenie verejného obstarávania, predbežne Q4/2019) |
|---|---|
| Analýza a dizajn | t+6 |
| Nákup HW a krabicového SW | t+10 |
| Implementácia | t+14 |
| Testovanie | t+15 |
| Nákup technického vybavenia | t+10 |
| Nasadenie | t+16 |
| Projektové riadenie | t+16 |

Publicita a informovanosť t+16

Kritéria kvality:
P4 Dodržiavanie plánu národného projektu
P5 Funkčné projektové registre a manažment zmien
P6 Definované produkty s konkrétnymi a merateľnými kritériami

Riziká:
R13 Spolupráca zúčastnených strán nebude na dostatočnej úrovni
R14 Centrum nebude plne vyladené do času uvedenia do produkčnej prevádzky



### 3.7.3.5. Bezpečnostná architektúra

Tabuľka 16 Bezpečnostná architektúra - budúci stav

Súhrnný popis

Vzhľadom na skutočnosť, že prijímateľ a partneri národného projektu už majú vybudovanú bezpečnostnú infraštruktúru, nepredpokladá sa významné hardvérové ani softvérové zosilňovanie bezpečnostnej infraštruktúry, do ktorej bude Centrum zasadené.
V každom prípade bude nevyhnutné uistiť sa, že budúce riešenie Centra bude spĺňať nižšie uvedené základné bezpečnostné požiadavky. V prípade, že si to povaha budúceho riešenia vyžiada, bude nutné zabezpečiť dodatočné technické vybavenie a nastavenie prevádzkových postupov tak, aby bola zabezpečená bezpečnostná architektúra riešenia. Súčasťou bude:

- správa a riadenie bezpečnostných funkcií,
- bezpečná sieťová infraštruktúra (routre, firewally, aplikačné firewally),
- generovanie auditných a log záznamov (SIEM),
- riadenie prístupov.

Ak súčasťou riešenia bude aj zosilňovanie bezpečnostnej architektúry, bude ju potrebné realizovať podľa odporúčaní výrobcu príslušného hardvéru a softvéru ako aj odporúčaných a bežných postupov v odbore, prípadne pravidelného externého auditu. Minimálne požiadavky sú však nasledovné:

- oddelenie sietí pomocou segmentov, správneho nastavenia routra a firewallových pravidiel,
- organizačné nastavenia segregácie právomocí,
- používanie HTTPS a SSL certifikátov,
- zvážiť ukladanie eventov a logov aj do oddelenej aplikácie a napojenie na prípadné existujúce SIEM riešenie,
- hardening operačných systémov, databáz, platformových riešení a poskytovaných softvérových riešení,
- kontrola prístupov a IAM, ktorý predstavuje centrálne riadenie prístupov.

Kritériá kvality:
P7 Akceptovateľný výsledok bezpečnostného auditu

Riziká:
R15 Nedodržiavanie organizačných bezpečnostných opatrení a procesov

Prílohy

Diagramy, modely, obrázky v plnom rozlíšení

Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.

Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.

### 3.7.4. Prevádzka

Tabuľka 17 Prevádzka - budúci stav

Súhrnný popis

Prevádzkové a bezpečnostné dopady na budúci stav riešenia sú determinované predovšetkým vyspelosťou obslužného personálu na strane prijímateľa a partnerov národného projektu.
Predpokladá sa, že prevažnú väčšinu bežných prevádzkových požiadaviek na úrovni Level 1 a Level 2 budú prijímateľ a partneri národného projektu schopné pokryť vlastným personálnym vybavením. Prevádzkový support na úrovni Level 3 však bude musieť byť zabezpečený prostredníctvom nákladovo efektívnej zmluvy typu SLA.
Vzhľadom na množstvo špecifického hardvérového a softvérového vybavenia jednotlivých funkčných celkov Centra však možno s určitosťou predpokladať, že bude nutné počítať i s externou hardvérovou a softvérovou podporou, ktorú bude potrebné zmluvne upraviť.
Zvýšené prevádzkové nároky si vyžiada aj zintenzívnená komunikácia medzi prijímateľom a partnermi národného projektu.
Ako vhodnými opatreniami na zníženie prevádzkových nákladov sa javia:

- zaškolenie obslužného personálu, aby sa znížila závislosť na tretích stranách,
- optimalizácia prevádzkových procesov a vytvorenie smerníc upravujúcich prevádzkové procesy za účelom celkového zefektívnenia prevádzky,
- zdieľanie prevádzkových kapacít medzi jednotlivými funkčnými jednotkami Centra,
- implementácia účinného monitoringu technických komponentov nasadených v funkčných celkoch Centra,
- vykonávanie pravidelnej profylaktiky na zabránenie prevádzkových incidentov.

Kritéria kvality:
P8 Zníženie počtu prevádzkových incidentov v procese prevádzky Centra

Riziká:
R16 Nedostatok finančných prostriedkov na pokrytie prevádzky

Prílohy

Diagramy, modely, obrázky v plnom rozlíšení

Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.

Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.

### 3.7.5. Ekonomická analýza

Tabuľka 18 Ekonomická analýza - budúci stav

Súhrnný popis

Čísla do ekonomickej analýzy budú doplnené po stanovení a pripomienkovaní rozpočtu a prínosov zo strany partnerov a UHP. Pracovným materiálom je do toho času CBA v XLS.

Prehľad ukazovateľov efektivity Náklady projektu 19 953 885 €
Čistá súčasná ekonomická hodnota (ENPV) = 31 279 991€
Rok návratu investície (PBP) = 4
BCR - pomer prínosov a nákladov = 2,63
EIRR - ekonomická vnútorná výnosová miera (%) = 43,5

- Rozdelenie nákladov medzi partnerov:
- cca 20% nákladov predstavuje partner SIS,
- cca 80% nákladov patrí medzi partnerom NBÚ (kde je dislokovaný HW a SW) a ÚPVII, pričom obaja partneri pristupujú k riešeniu uloženému na NBÚ prostredníctvom tréningových učební, ktoré sa nachádzajú na oboch úradoch.

Prehľad úspor a benefitov
Ekonomické parametre projektu je sú definované jeho nákladmi a prínosmi.
Prínosy projektu sú postavené na fakte, že vybudovanie Centra významnou mierou zníži náklady na výuku a simuláciu v oblasti kybernetickej bezpečnosti. Prínosy je možné rozdeliť na:

- prínosy zo zníženia nákladov na školenia bežných používateľov vo verejnej správe prostredníctvom zjednotenia a centralizácie e-learningových školení týkajúcich sa kybernetickej bezpečnosti L1,
- prínosy zo zníženia nákladov na školenia zamestnancov IT vo verejnej správe v oblasti KyB (L2),
- prínosy zo zníženia nákladov na arénové kybernetické výcviky tímov zložených zo špecialistov venujúcich sa kybernetickej bezpečnosti z radov verejnej správy (L4),
- prínosy zo zníženia z cvičení simulujúcich kybernetickú obranu a kybernetické útoky na infraštruktúru typu IT/OT (súčasť cvičení kyber arény).

Prehľad kľúčových parametrov použitých pre výpočet prínosov je uvedený v nasledovnej tabuľke:

| Parameter | Hodnota |
|---|---|
| Priemerná cena e-learningového školenia kybernetickej bezpečnosti pre jedného bežného používateľa | 20 EUR |
| Počet školení bežných používateľov vo verejnej správe ročne (L1) | 300 000 |
| Priemerná cena školenia/tréningu IT zamestnanca v oblasti KyB | 1000 EUR |
| Počet školení IT zamestnancov vo verejnej správe na kybernetickú bezpečnosť ročne (L2) | 3 500 |
| Priemerná cena arénového kybernetického výcviku | 100 000 EUR |
| Počet arénových kybernetických výcvikov za kalendárny rok (L4) | 12 |

Poznámka: Uvedený prístup výpočtu benefitov je pomerne konzervatívny v tom, že Centrum bude zrejme generovať aj viac benefitov, avšak pre účely tejto CBA sme sa snažili konzervatívne identifikovať predovšetkým benefity postačujúce pre obhajobu projektu. Medzi prínosy, ktoré neboli kvantifikované patria napríklad:

- 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.

Prehľad výdavkov CAPEX a OPEX
Náklady projektu pozostávajú z:

- nevyhnutných stavebných úprav jednotlivých funkčných celkov Centra,
- obstarávacích nákladov na hardvér a prevádzkových nákladov na hardvér počas trvania projektu,

- obstarávacích nákladov na softvér, softvérové licencie a prevádzkových nákladov na softvér počas trvania projektu,
- obstarávacích nákladov na zaškolenie personálu Centra.

Potrebné inštalačné práce sú súčasťou obstarávacej ceny jednotlivých komponentov. Súčasťou projektu sú aj prevádzkové náklady počas doby trvania projektu ako aj školenia spojené s dodávaným HW a SW a stavebné úpravy uvedené v rámci položky nákladov na priestory. Prevádzkové náklady predstavujú nevyhnutné výdavky na údržbu a najmä na aktualizácie produktov. V rámci rozpočtu sa uvažuje aj s položkami projektové riadenie vo výške 4 percent.
V rámci modelovania budúcich nákladov sú dôležité nasledovné parametre:

| Parameter | CAPEX (EUR) |
|---|---|
| SW produkty - sumár obstaranie | 558 245 |
| SW produkty - sumár prevádzka | 2 601 113 |
| Aplikácie - sumár obstaranie | 13 005 563 |
| Aplikácie - sumár prevádzka | 800 000 |
| HW sumár obstaranie | 5 448 500 |
| HW sumár prevádzka | 989 700 |
| Riadenie projektu | 941 577 |
| Spolu | 19 953 885 |

Prehľad TCO projektu sa nachádza v nasledovnej tabuľke:

| TO BE | Spolu | t1 | t2 | t3 | t4 | t5 | t6 | t7 | t8 | t9 | t10 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| SW produkty - sumár obstaranie | 558 245 | 558 245 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| SW produkty - sumár prevádzka | 2601 113 | 0 | 0 | 325 139 | 325 139 | 325 139 | 325 139 | 325 139 | 325 139 | 325 139 | 325 139 |
| Aplikácie - sumár obstaranie | 13 005 563 | 6 502 781 | 6 502 781 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Aplikácie - sumár prevádzka | 800 000 | 0 | 0 | 100 000 | 100 000 | 100 000 | 100 000 | 100 000 | 100 000 | 100 000 | 100 000 |
| SW a Aplikácie - výstupné náklady | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| HW sumár obstaranie | 5 448 500 | 5 448 500 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| HW sumár prevádzka | 989 700 | 0 | 0 | 123 713 | 123 713 | 123 713 | 123 713 | 123 713 | 123 713 | 123 713 | 123 713 |
| Riadenie projektu, publicita a informovanosť | 941 577 | 941 577 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

Čísla sú v EUR s DPH.|

Riziká:
R17 Nepodarí sa dosiahnuť preukázateľné úspory podľa plánu

R18 Náklady na vybudovanie alebo prevádzku sa vymknú kontrole / presiahnu plánovanou hodnotu

Prílohy

CBA projektu vo formáte XLS