DataCentrum **Cintorínska č. 5, 814 88 B r a t i s l a v a**

Úloha č.: ***114***

Identifikačný list úlohy na rok 2022

1. Názov úlohy:

Zabezpečenie plnenia bezpečnostných opatrení a notifikačných povinností podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov

1.1. Predmet riešenia

- Vytvorenie formálneho rámca medzi Ministerstvom financií SR (ďalej len „MF SR“) a DataCentrom pre zabezpečenie plnenia bezpečnostných opatrení a notifikačných povinností podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „ZoKB”).
- Definovanie rozsahu bezpečnostných opatrení a činností pre zaistenie kybernetickej bezpečnosti pri zabezpečovaní plnenia úloh DataCentra pre MF SR podporujúcich prevádzku základných služieb MF SR, vyplývajúcich z nasledovných identifikačných listov:
  - IL 122 Podpora používateľov informačného systému CKS,
  - IL 311 Podpora používateľov pri práci s aplikáciami rozpočtového informačného systému (Aplikačná podpora RIS - AP RIS),
  - IL 407 Informačný systém účtovníctva fondov (ISUF),
  - IL 408 Ekonomické informačné systémy (EIS).
- Zabezpečenie zodpovedného riadenia bezpečnosti v rámci celého reťazca dodávateľov technológií a poskytovateľov služieb prenesením primeranej časti zodpovednosti za kybernetickú bezpečnosť na tretie strany a zabezpečenie ich spolupráce pri riešení kybernetických bezpečnostných incidentov.
- Pre účely tohto identifikačného listu sa pojmy uvedené v tomto identifikačnom liste budú vykladať tak, ako ich stanovuje ZoKB a 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 (ďalej len „vyhláška NBÚ“), ako aj ZoITVS.

1.2. Základné povinnosti DataCentra

- V rozsahu zohľadňujúcom charakter a rozsah služieb poskytovaných DataCentrom pri zabezpečovaní plnenia úloh vyplývajúcich z identifikačných listov pre MF SR (ďalej len „poskytovanie služieb“) je Datacentrum povinné:
  - Dodržiavať tie bezpečnostné politiky, štandardy a postupy MF SR v rozsahu nevyhnutne potrebnom pre bezpečné poskytovanie služieb MF SR, s obsahom ktorých bolo DataCentrum preukázateľne oboznámené a s dodržiavaním ktorých DataCentrum vyjadrilo osobitný písomný súhlas.
  - Chrániť všetky informácie ktoré boli DataCentru poskytnuté MF SR v súvislosti so zabezpečovaním služieb MF SR, pri nakladaní s nimi.
  - Prijímať a dodržiavať bezpečnostné opatrenia v oblasti kybernetickej bezpečnosti v rozsahu nevyhnutne potrebnom pre bezpečné poskytovanie služieb MF SR ako sú uvedené v tomto identifikačnom liste (najmä v bode *2. Definícia rozsahu bezpečnostných opatrení*) alebo bezpečnostné opatrenia s porovnateľnými účinkami reflektujúc rozsah opatrení definovaný v ZoKB a vyhláške NBÚ. DataCentrum vyhlasuje, že súhlasí s bezpečnostnými opatreniami stanovenými v tomto identifikačnom liste v rozsahu nevyhnutne potrebnom pre bezpečné poskytovanie služieb MF SR. DataCentrum a MF SR sa dohodli, že pre oblasť technických bezpečnostných opatrení a riadenie záplat sú bezpečnostné opatrenia aplikované iba na:
    - technické prostriedky patriace DataCentru, ktoré Datacentrum priamo využíva pri poskytovaní služieb MF SR,
    - technické prostriedky, ktoré sú umiestnené v priestoroch DataCentra, a to implementovaním opatrení iba v rozsahu zohľadňujúcom rozsah a charakter služieb, ktorý vyplýva z identifikačných listov uvedených v bode 1.1.
  - Informovať MF SR o kybernetickom incidente a o všetkých skutočnostiach majúcich vplyv na zabezpečovanie kybernetickej bezpečnosti, ktoré priamo súvisia s plnením úloh pri poskytovaní služieb MF SR.

- Po ukončení platnosti tohto identifikačného listu vrátiť alebo previesť MF SR informácie, ku ktorým malo DataCentrum prístup počas trvania tohto identifikačného listu, ak osobitný predpis alebo medzinárodná zmluva, ktorou je Slovenská republika viazaná, nepožaduje uchovávanie týchto informácií DataCentrom alebo ak bude tento identifikačný list nahradený iným s obdobným plnením alebo ak MF SR nebude požadovať vrátenie alebo prevedenie týchto informácií.
- Po ukončení platnosti tohto identifikačného listu udeliť, poskytnúť, previesť alebo postúpiť všetky potrebné licencie, práva alebo súhlasy nevyhnutné na zabezpečenie kontinuity činností v rozsahu potrebnom na plnenie úloh súvisiacich s poskytovaním služieb MF SR na MF SR. Tento záväzok ostáva v platnosti aj po ukončení tohto identifikačného listu po dobu piatich rokov. DataCentrum nie je povinné plniť tieto požiadavky iba v prípade, ak bude tento identifikačný list nahradený iným s obdobným plnením alebo ak MF SR nebude požadovať plnenie týchto požiadaviek.

2. Definícia rozsahu bezpečnostných opatrení a činností

Rozsah činností, ktoré DataCentrum vykonáva pre MF SR je definovaný v príslušných identifikačných listoch a v tomto identifikačnom liste:

- ***Pre oblasť personálnej bezpečnosti*** realizuje DataCentrum opatrenia podľa § 7 vyhlášky NBÚ v rozsahu zohľadňujúcom charakter a rozsah služieb poskytovaných DataCentrom organizácii MF SR, prostredníctvom opatrení definovaných v nasledovných bodoch alebo opatrení s porovnateľnými účinkami:
  - monitorovanie zavedených opatrení personálnej bezpečnosti v podmienkach DataCentra,
  - kontrola dodržiavania bezpečnostných politík zo strany zamestnancov DataCentra, administrátorov, osôb zastávajúcich niektorú z bezpečnostných rolí a dodávateľov v zmluvnom vzťahu s DataCentrom participujúcich na poskytovaní služieb MF SR.
- ***Pre oblasť technických zraniteľností systémov a zariadení*** realizuje DataCentrum opatrenia podľa § 9 vyhlášky NBÚ v rozsahu zohľadňujúcom charakter a rozsah služieb poskytovaných MF SR, najmä identifikuje technické zraniteľnosti informačných systémov patriacich Datacentru, ktoré Datacentrum priamo využíva pri poskytovaní služieb MF SR prostredníctvom opatrení definovaných v nasledovných bodoch alebo opatrení s porovnateľnými účinkami:
  - zavedenie a prevádzka nástroja určeného na detegovanie existujúcich zraniteľností programových prostriedkov a ich častí,
  - zavedenie a prevádzka nástroja určeného na detegovanie existujúcich zraniteľností technických prostriedkov a ich častí,
  - využitie verejných a výrobcom poskytovaných zoznamov, ktoré opisujú zraniteľnosti programových a technických prostriedkov.
- ***Pre oblasť riadenia bezpečnosti sietí a informačných systémov*** realizuje DataCentrum opatrenia podľa § 10 vyhlášky NBÚ v rozsahu zohľadňujúcom charakter a rozsah služieb poskytovaných MF SR, prostredníctvom opatrení definovaných v nasledovných bodoch alebo opatrení s porovnateľnými účinkami:
  - riadenie prístupov používateľov k sieťam a informačným systémom v súlade s § 12 vyhlášky NBÚ,
  - riadenie bezpečného prístupu medzi vonkajšími a vnútornými sieťami a informačnými systémami, ktoré DataCentrum využíva pri poskytovaní služieb MF SR, a to najmä využitím nástrojov na ochranu integrity sietí a informačných systémov, ktoré sú zabezpečené segmentáciou sietí a informačných systémov; servery so službami priamo prístupnými z externých sietí sa nachádzajú v samostatných sieťových segmentoch a v rovnakom segmente musia byť len servery s rovnakými bezpečnostnými požiadavkami a rovnakej bezpečnostnej triedy a s podobným účelom,
  - povoľovanie prepojenia medzi segmentmi a externými sieťami, ktoré sú chránené firewallom a všetkých spojení, na princípe zásady najnižších privilégií,
  - zavedenie bezpečnostných opatrení na bezpečné mobilné pripojenie do siete a informačného systému a vzdialený prístup, napríklad bezpečným spôsobom s použitím dvojfaktorovej autentizácie alebo použitím kryptografických prostriedkov,
  - sieťam alebo informačným systémom sú umožnené len špecifikované služby umiestnené vo vyhradených segmentoch siete počítačovej siete,
  - spojenia do externých sietí sú smerované cez sieťový firewall a v závislosti od prostredia

aj cez systém detekcie prienikov,
- servery dostupné z externých sietí sú zabezpečované podľa odporúčaní výrobcu,
- udržiavanie zoznamu všetkých vstupno-výstupných bodov na hranici siete v aktuálnom stave,
- zavedenie a prevádzka automatizačných prostriedkov, ktorými sú identifikované neoprávnené sieťové spojenia na hranici s vonkajšou sieťou,
- blokovanie neoprávnených spojení zo známych adries označených ako škodlivé alebo spôsobujúce známe hrozby, ak to nastavenie informačného systému umožňuje,
- neumožnenie komunikácie a prevádzky aplikácií cez neautorizované porty,
- zavedenie a prevádzka systému monitorovania bezpečnosti, ktorý je nakonfigurovaný tak, že zaznamenáva a vyhodnocuje aj informácie o sieťových paketoch na hranici siete,
- implementácia systému detekcie prienikov alebo systému prevencie prienikov na identifikáciu nezvyčajných mechanizmov útokov alebo proaktívneho blokovania škodlivej sieťovej prevádzky,
- smerovanie odchádzajúcej používateľskej sieťovej prevádzky cez autentizovaný server filtrovania obsahu,
- vyžadované použitie dvojfaktorovej autentizácie od každého vzdialeného pripojenia do internej siete,
- vykonávanie pravidelného alebo nepretržitého posudzovania technických zraniteľností, najmä identifikácie možnej prítomnosti škodlivého kódu zariadenia, ktoré sa vzdialene pripája do internej siete, alebo zmluvného zaručenia vrátane preukázania plnenia tejto povinnosti.

- ***Pre oblasť riadenia prístupov*** realizuje DataCentrum opatrenia podľa § 12 vyhlášky NBÚ v rozsahu zohľadňujúcom charakter a rozsah služieb poskytovaných MF SR, prostredníctvom opatrení definovaných v nasledovných bodoch alebo opatrení s porovnateľnými účinkami:
  - riadenie prístupov osôb k sieti a informačnému systému, založené na zásade, že používateľ má prístup len k tým aktívam a funkcionalitám v rámci siete a informačného systému, ktoré sú nevyhnutné na plnenie zverených úloh používateľa; na to sa vypracúvajú zásady riadenia prístupu osôb k sieti a informačnému systému, ktoré definujú spôsob prideľovania a odoberania prístupových práv používateľom, ich formálnu evidenciu a vedenie úplných prevádzkových záznamov o každom prístupe do siete a informačného systému,
  - riadenie prístupov k sieťam a informačným systémom uskutočnené v závislosti od prevádzkových a bezpečnostných potrieb, pričom sú prijaté bezpečnostné opatrenia, ktoré slúžia na zabezpečenie ochrany údajov, ktoré sú používané pri prihlásení do sietí a informačných systémov a ktoré zabraňujú zneužitiu týchto údajov neoprávnenou osobou,
  - riadenie prístupov osôb k sieti a informačnému systému; to zahŕňa najmenej vypracovanie zásad riadenia prístupu k informáciám, riadenia prístupu používateľov, zodpovednosti používateľov, riadenia prístupu k sieťam, prístupu k operačnému systému a jeho službám, prístupu k aplikáciám, monitorovania prístupu a používania informačného systému a riadenia vzdialeného prístupu,
  - pridelenie jednoznačného identifikátora na autentizáciu na vstup do siete a informačného systému každému používateľovi siete a informačného systému,
  - zabezpečenie riadenia jednoznačných identifikátorov používateľov vrátane prístupových práv a oprávnení používateľských účtov,
  - využitie nástroja na správu a overovanie identity používateľa pred začiatkom jeho aktivity v rámci siete a informačného systému a nástroj na riadenie prístupových oprávnení, prostredníctvom ktorého je riadený prístup k jednotlivým aplikáciám a údajom, prístup na čítanie a zápis údajov a na zmeny oprávnení a prostredníctvom ktorého sa zaznamenávajú použitia prístupových oprávnení (prevádzkové záznamy),
  - výkon kontroly prístupových účtov a prístupových oprávnení na overenie súladu schválených oprávnení so skutočným stavom oprávnení a detekciu a následné zmazanie nepoužívaných prístupových účtov v pravidelných intervaloch,
  - určenie osoby zodpovednej za riadenie prístupu používateľov do siete a k informačnému systému a za prideľovanie a odoberanie prístupových práv používateľom, ich formálnu evidenciu a vedenie úplných prevádzkových záznamov o každom prístupe do siete a informačného systému v zmysle príslušnej bezpečnostnej politiky.
- ***Pre oblasť riešenia kybernetických bezpečnostných incidentov*** realizuje DataCentrum opatrenia podľa § 14 vyhlášky NBÚ v rozsahu zohľadňujúcom charakter a rozsah služieb poskytovaných MF SR, najmä deteguje a rieši kybernetické bezpečnostné incidenty, ktoré

priamo súvisia s plnením úloh pri poskytovaní služieb MF SR. to zahŕňa najmä prijatie opatrení definovaných v nasledovných bodoch alebo opatrení s porovnateľnými účinkami:

- oboznámenie sa so štandardmi a postupmi MF SR pri riešení kybernetických bezpečnostných incidentov a spracovanie interných postupov riešenia kybernetických bezpečnostných incidentov, ktoré zahŕňajú najmä minimálne postupy hlásenia kybernetických bezpečnostných incidentov voči MF SR v súlade s právnymi predpismi, najmä ZoKB a vyhlášky NBÚ tak, aby malo MF SR primeraný čas na splnenie si svojich práv a povinností plynúcich mu z právnych predpisov,
- monitorovanie a analyzovanie udalostí v sieťach a informačných systémoch, ktoré sú využívané na poskytovanie služieb MF SR,
- detegovanie kybernetických bezpečnostných incidentov, najmä prostredníctvom nástroja na detekciu kybernetických bezpečnostných incidentov, ktorý umožňuje v rámci sietí a informačných systémov a medzi sieťami a informačnými systémami overenie a kontrolu prenášaných dát,
- zber relevantných informácií o kybernetických bezpečnostných incidentoch (najmä, avšak nie len: lokalita, hostname, MAC adresy, IP adresy, identifikačné údaje všetkých zariadení a zúčastnených osôb a dátum, čas manipulácie s údajmi a vymedzenie miesta ich uloženia) a vyhodnocovanie kybernetických bezpečnostných incidentov, najmä prostredníctvom nástroja na zber a nepretržité vyhodnocovanie kybernetických bezpečnostných udalostí, ktorý umožňuje zber a vyhodnocovanie informácií o kybernetických bezpečnostných incidentoch, vyhľadávanie a zoskupovanie záznamov súvisiacich s kybernetickým bezpečnostným incidentom, vyhodnocovanie bezpečnostných udalostí na ich identifikáciu ako kybernetických bezpečnostných incidentov, revíziu konfigurácie a monitorovacích pravidiel na vyhodnocovanie bezpečnostných udalostí pri nesprávne identifikovaných kybernetických bezpečnostných incidentoch,
- riešenie zistených kybernetických bezpečnostných incidentov a zníženie následkov zistených kybernetických bezpečnostných incidentov podľa pokynov MF SR,
- vyhodnocovanie spôsobov riešenia kybernetických bezpečnostných incidentov po ich vyriešení a prijatie opatrení alebo zavedenie nových postupov s cieľom minimalizovať výskyt obdobných kybernetických bezpečnostných incidentov v súčinnosti s MF SR.

- ***Pre oblasť monitorovania, testovania bezpečnosti a bezpečnostných auditov*** realizuje DataCentrum opatrenia v rozsahu zohľadňujúcom charakter a rozsah služieb poskytovaných MF SR, najmä:
  - monitoruje a zaznamenáva činnosti sietí a informačných systémov, ktoré zabezpečujú ochranu IS, ktorých správou a prevádzkou bolo DataCentrum poverené prostredníctvom identifikačných listou uvedených v bode 1.1. a to v súlade s požiadavkami § 15 vyhlášky NBÚ.
- ***Pre oblasť fyzickej bezpečnosti*** realizuje DataCentrum opatrenia podľa § 16 vyhlášky NBÚ v rozsahu zohľadňujúcom charakter a rozsah služieb poskytovaných DataCentrom organizácii MF SR.
- ***Pre oblasť riadenia kontinuity procesov*** realizuje DataCentrum opatrenia podľa § 17 vyhlášky NBÚ v rozsahu zohľadňujúcom charakter a rozsah služieb poskytovaných DataCentrom organizácii MF SR a to v rozsahu plánovania a vykonania obnovy prevádzkovaných systémov v súlade s požiadavkami MF SR na obnovu týchto systémov, ktoré sú uvedené v identifikačných listoch vymenovaných v bode 1.1 alebo ktoré určí MF SR pre jednotlivé systémy, ako aj zálohovania prevádzkovaných systémov. Šifrovanie záloh bude DataCentrum zabezpečovať na základe výslovnej požiadavky zo strany MF SR, v rámci ktorej budú identifikované tie zálohy, ktoré obsahujú chránené alebo prísne chránené údaje.

3. Hlásenie kybernetických incidentov

- DataCentrum je povinné bezodkladne informovať MF SR o každom kybernetickom bezpečnostnom incidente, ktorý má dopad na poskytovanie služieb DataCentrom MF SR, ako aj o všetkých skutočnostiach majúcich vplyv na zabezpečovanie kybernetickej bezpečnosti, ktoré priamo súvisia s plnením úloh pri poskytovaní služieb MF SR.
- Pri riešení incidentov je DataCentrum povinné spolupracovať s MF SR, NBÚ a na tento účel im poskytnúť všetku potrebnú súčinnosť a všetky informácie získane z vlastnej činnosti, ktoré by mohli

byť dôležité pre riešenie incidentu v súvislosti poskytovaním služieb MF SR.
- MF SR je povinné informovať v nevyhnutnom rozsahu DataCentrum o kybernetickom bezpečnostnom incidente, o ktorom sa dozvedelo ako prvé a ktorý má vplyv na poskytovanie služieb DataCentrom MF SR alebo na plnenie tohto identifikačného listu alebo identifikačných listov uvedených v časti 1.1.

4. Kontaktné osoby na úseku kybernetickej bezpečnosti

- Akákoľvek komunikácia, hlásenia a ďalšie informácie súvisiace s plnením povinností vyplývajúcich zo ZoKB alebo majúcich vplyv na zabezpečenie kybernetickej bezpečnosti alebo plnenie tohto identifikačného listu, bude realizovaná niektorou z nasledovných foriem: pošta, elektronická pošta, telefón alebo osobne.
- Obsah komunikácie a hlásení informácií, ktoré boli realizované telefonicky alebo osobne si budú strany bezodkladne zasielať aj elektronickou poštou na adresy uvedené v kontaktných údajoch.
- Komunikácia zasielaná elektronická pošta bude zasielaná v chránenej forme (napr. chránená heslom, chránená šifrovaním), v závislosti od dohody komunikujúcich strán a citlivosti informácií, ktoré sú obsahom komunikácie.
- Kontaktné údaje MF SR: odbor informačnej a kybernetickej bezpečnosti MF SR, tel.: +421 2 5958 3211, +421 2 5958 9213, e-mail: *ibezpecnost@mfsr.sk*.
- Kontaktné údaje DataCentrum: útvar bezpečnosti DataCentra, tel.: +421 2 59278 332, +421 2 59278 434, e-mail: *bezpecnost@datacentrum.sk*.

5. Kontrolná činnosť a audit

- DataCentrum a MF SR sa dohodli, že MF SR alebo ním poverená osoba (ďalej len „kontrolór“) je oprávnený vykonať v DataCentre audit a/alebo kontrolu, zameranú na overenie plnenia povinností podľa tohto identifikačného listu, ZoITVS, ZoKB a vyhlášky NBÚ.
- DataCentrum je povinné poskytnúť súčinnosť v potrebnom rozsahu v rámci auditu prijatých bezpečnostných opatrení alebo kontroly zo strany MF SR, Národnej jednotky CSIRT, vládnej jednotky CSIRT alebo kontrolóra.
- DataCentrum je povinné poskytnúť osobe vykonávajúcej audit a/alebo kontrolu na požiadanie všetky informácie potrebné za účelom preukázania splnenia povinností DataCentra vyplývajúcich mu z tohto identifikačného listu, ZoKB a vyhlášky NBÚ s prihliadnutím na informácie dostupné DataCentru.
- DataCentrum je tiež povinné pri audite a/alebo kontrole spolupracovať s osobou vykonávajúcou predmetnú činnosť a bezodkladne jej sprístupniť všetky svoje priestory, ako aj všetku dokumentáciu a programové, technické a technologické vybavenie, ktoré súvisí s plnením úloh na úseku kybernetickej bezpečnosti podľa tohto identifikačného listu.
- MF SR je povinné informovať DataCentrum o termíne vykonania auditu alebo kontroly oznámením zaslaným elektronickou poštou na kontakt podľa bodu 4 tohto identifikačného listu, a to minimálne 7 pracovných dní pred vykonaním auditu alebo kontroly. DataCentrum je povinné bez zbytočného odkladu termín auditu alebo kontroly potvrdiť alebo navrhnúť iný termín tak, aby sa audit alebo kontrola uskutočnili najneskôr do 14 dní odo dňa zaslania oznámenia.
- Prípadné nedostatky zistené auditom a/alebo kontrolou je DataCentrum povinné odstrániť bez zbytočného odkladu, najneskôr však v lehote 90 kalendárnych dní od zistenia toho ktorého nedostatku. O audite ako aj o kontrole bude spísaná zápisnica, ktorej obsah bude potvrdený podpisom DataCentrum a osoby vykonávajúcej predmetnú činnosť, resp. povereným zamestnancom za tú ktorú stranu.
- Náklady, ktoré v súvislosti s auditom alebo kontrolou vzniknú osobe vykonávajúcej predmetnú činnosť, znáša táto osoba. DataCentrum poskytuje súčinnosť pri výkone auditu a kontroly bezodplatne, resp. prípadné náklady znáša bez nároku na ich náhradu.

6. Menný zoznam osôb a pracovných rolí DataCentra

- Zoznam pracovných rolí zamestnancov DataCentra, ktorí sa podieľajú na poskytovaní služieb MF SR a/alebo budú mať prístup k informáciám a údajom MF SR, je nasledovný:
  - manažér kybernetickej bezpečnosti DataCentra,

- manažér bezpečnosti DataCentra,
- zamestnanci odboru prevádzky IS DataCentra.

- Každú zmenu v personálnom obsadení DataCentrum bezodkladne oznámi MF SR; na platnosť takejto zmeny sa nevyžaduje úprava tohto identifikačného listu.
- DataCentrum zabezpečí, aby osoby uvedené v zozname osôb a pracovných rolí DataCentra podpísali vyjadrenie o zachovávaní mlčanlivosti podľa ustanovenia § 12 ZoKB.

7. Subdodávatelia

- DataCentrum je oprávnené zabezpečovať poskytovanie služieb MF SR prostredníctvom zapojenia ďalších dodávateľov (ďalej len „subdodávatelia“) uvedených v tomto zozname:
  - PosAm, spol. s r.o.,
  - Tempest, a.s.,
  - DXC Technology Slovakia s. r. o.,
  - Hewlett Packard Enterprise Slovakia, s.r.o.,
- Každú zmenu v zapojení ďalších subdodávateľov DataCentrum vopred bezodkladne oznámi MF SR, na platnosť takejto zmeny sa nevyžaduje úprava tohto identifikačného listu.
- V prípade, ak DataCentrum plní poskytovanie služieb MF SR prostredníctvom zapojenia subdodávateľa, DataCentrum zabezpečí plnenie povinností v oblasti kybernetickej bezpečnosti vyplývajúcich z tohto identifikačného listu aj u svojich subdodávateľov tak, aby boli naplnené ciele tohto identifikačného listu.

8. Identifikácia vstupov úlohy:

- Identifikačné listy úloh IL 122, IL 311, IL 407 a IL 408.
- Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.
- Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v takej úrovni informačnej bezpečnosti ktorú je ministerstvo zmluvne zaviazané poskytovať používateľom informačných systémov.
- Vyhláška NBÚ č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení.

9. Návrh na riešenie – členenie úlohy, postup riešenia

- ***Zabezpečenie implementácie bezpečnostných opatrení pre oblasť**:*
  - technických zraniteľností systémov a zariadení,
  - riadenia bezpečnosti sietí a informačných systémov,
  - riadenia prístupov,
  - riešenia kybernetických bezpečnostných incidentov,
  - monitorovania, testovania bezpečnosti a bezpečnostných auditov.
- ***Aktualizácia zmlúv s tretími stranami***, podpísanie dodatkov k zmluvám s cieľom zabezpečiť aktívnu účasť tretích strán pri plnení povinností vyplývajúcich zo ZoKB a ZoITVS, na riešení všetkých porušení kybernetickej bezpečnosti a bezpečnostných incidentov v súvislosti s prevádzkovaním informačných systémov MF SR:
  - pre funkčnosť a bezpečnosť prevádzkovaním informačných systémov MF SR budú DataCentrom, resp. treťou stranou so zreteľom na najnovšie poznatky prijaté primerané technické a organizačné opatrenia.
- ***Riadenie poskytovaných služieb tretími stranami:***
  - vykonávanie pravidelného monitoringu a kontroly súladu poskytovaných služieb tretími stranami so ZoKB a ZoITVS.
- ***Auditné zistenia:***
  - náprava nedostatkov a plnenie opatrení vyplývajúcich zo zistení auditov vo vzťahu k poskytovaným službám pre MF SR,
  - informovanie o zisteniach inými auditmi vo vzťahu k poskytovaným službám.

10. Výstupy z riešenia:

- Funkčný systém kybernetickej bezpečnosti a nahlasovania kybernetických bezpečnostných incidentov v zmysle aktuálnej platnej legislatívy aplikovaný na informačné systémy prevádzkované v DataCentre a ktoré podporujú poskytovanie základných služieb MF SR.
- Trvalá súčinnosť medzi MF SR a DC v súvislosti s plnením požiadaviek v oblasti kybernetickej bezpečnosti.
- Bezpečnostná dokumentácia v zmysle aktuálnej platnej legislatívy (minimálne v rozsahu vyhlášky NBÚ č. 362/2018 Z. z.) pre informačné systémy, ktorých správou a prevádzkou bolo DataCentrum poverené prostredníctvom identifikačných listov uvedených v bode 1.1, a to v rozsahu zohľadňujúcom charakter a rozsah služieb poskytovaných DataCentrom organizácii MF SR.

11. Termíny plnenia, spôsob a podmienky ukončenia identifikačného listu:

- Priebežne - rok 2022.
- Tento identifikačný list je ukončený uplynutím obdobia na ktorý bol uzatvorený a prijatím nového identifikačného listu, ktorý ho nahrádza.

12. Odberateľ – užívateľ výsledkov:

Ministerstvo financií SR

13. Kapacita potrebná na riešenie v čl. / hodinách

1 300

14. Riziká riešenia úlohy

- nedostatočná úroveň kybernetickej bezpečnosti,
- nedostatočná spolupráca s prevádzkovateľom IS a riešiteľmi,
- nedostatočná implementácia a dodržiavanie bezpečnostných opatrení,
- nedostatočné finančné prostriedky na realizáciu bezpečnostných opatrení,
- nedostatok odborných a personálnych kapacít.

15. Kritériá hodnotenia:

- počet kybernetických bezpečnostných incidentov v súvislosti s prevádzkou informačných systémov,
- aktualizácia zmlúv s tretími stranami v súvislosti s kybernetickou bezpečnosťou v zmysle platnej legislatívy,
- percento odstránených nedostatkov z auditných správ a úspešné absolvovanie kontrolného auditu.