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

Úloha č.: ***223***

Identifikačný list úlohy na rok 2022

1. Názov úlohy:

Poskytovanie služieb riadenia bezpečnosti vo vzťahu MF SR a DataCentra v súčinnosti s tretími stranami

2. Predmet riešenia:

- vytvorenie formálneho rámca medzi Ministerstvom financií SR a DataCentrom pre zaistenie minimálne takej úrovne informačnej bezpečnosti, ktorú je ministerstvo zmluvne zaviazané poskytovať používateľom informačných systémov a zabezpečenie zodpovedného riadenia bezpečnosti v rámci celého reťazca dodávateľov technológií a poskytovateľov služieb prenesením primeranej časti zodpovednosti za bezpečnosť na tretie strany, rovnako ako zabezpečiť ich spoluprácu pri riešení bezpečnostných incidentov,
- definovanie parametrov, činností, aktivít a procesov pre zaistenie informačnej bezpečnosti, spôsob komunikácie, stanovenie parametrov úrovne dodávanej informačnej bezpečnosti, činností, kontrolných aktivít ako aj jednoznačnej zodpovednosti a vzájomnej informovanosti. V prípade bezpečnostného incidentu je potrebné zo strany DataCentra uplatniť tzv. „chain of custody“ (CoC) informácií, údajov a dôkazov, ktoré by mohli byť dôležité pri vyšetrovaní incidentu a na požiadanie ich poskytnúť MF SR,
- vytvorenie bezpečnostnej SLA, ktorá bude definovať najmä požiadavky na:
  - dôvernosť/nesprístupňovanie informácií;
  - bezpečnostné požiadavky počas celého životného cyklu IT systémov;
  - poskytovanie údajov o aktuálnom stave bezpečnosti;
  - bezpečnostne relevantné aktivity vykonávané treťou stranou;
  - spolupráca pri hodnotení a odstraňovaní bezpečnostných nedostatkov a slabín;
  - spolupráca pri identifikácii a riešeniach bezpečnostných incidentov;
  - oprávnenie vykonávania bezpečnostných previerok a auditov;
  - nastavené zodpovednosti riadenia bezpečnosti v rámci „supply chain“:
    - riadenie bezpečnosti na strane dodávateľa,
    - riadenie bezpečnosti na úrovni podriadenej organizácie,
    - riadenie bezpečnosti poskytovateľa/prevádzkovateľa systémov;
  - zabezpečenie systému riadenia úrovne poskytovaných služieb;
  - vykonávanie pravidelného monitoringu a vyhodnocovanie úrovne poskytovaných služieb;
  - vykonávanie pravidelného monitoringu vyhodnotenie úrovne poskytovaných služieb tretími stranami;

Riešenie je najmä bezpečnostnou nadstavbou úloh, ktoré zároveň tvoria základný rámec bezpečnosti, sú už implementované do systému bezpečnosti a sú neoddeliteľnou súčasťou tejto úlohy. Sú to najmä úlohy vyplývajúce z identifikačných listov (ďalej len IL):

161 *- Centrum monitorovania prevádzky - CMP,*
401 *- Technologická infraštruktúra dátovej sály MF SR,*
406 *- Prevádzka dátovej sály MF SR,*
409*- Riešenie požiadaviek a hlásení pre zamestnancov MF SR,*

Úlohy vyplývajúce s vyššie uvedených IL sú následne jasne identifikované s konkrétnym IL za účelom zamedzenia duplikovaného rozpočtovania.

3. Identifikácia vstupov úlohy:

- aktuálne platná legislatíva SR a EÚ, bezpečnostné štandardy;
- bezpečnostná dokumentácia rezortu MF SR, analýzy rizík;
- úlohy zo zasadnutí Riadiaceho výboru bezpečnosti rezortu MF SR;
- auditné zistenia;
- výsledky penetračného testovania;
- zmeny informačných aktív;
- dohody o výkone správy a údržby informačných systémov medzi MF SR a ÚOŠS;
- identifikačné listy úloh;

4. Návrh na riešenie – členenie úlohy, postup riešenia:

4.1.

- aktualizácia zmlúv s tretími stranami, podpísanie dodatkov k zmluvám (SLA) s cieľom zabezpečiť aktívnu účasť tretích strán na riešení všetkých bezpečnostných incidentov, vrátane kybernetických a GDPR bezpečnostných incidentov;
- pravidelné ročné hodnotenie dosiahnutej úrovne bezpečnosti s dôrazom na hodnotenie:
  - bezpečnej architektúry,
  - posilnenie zabezpečenia systému – hardening,
  - ochrana pred škodlivým kódom,
  - riadenie opráv a nedostatkov,
  - bezpečné riadenie účtov,
  - zapisovanie do denníka (logging) a monitoring,
  - vzdialený prístup,
  - ochrana údajov,
  - aktuálnosti udelených a riadne zadokumentovaných výnimiek,
  - analýza rizík v nadväznosti na vykonané zmeny;
- pre funkčnosť a bezpečnosť IS budú DataCentrom, resp. treťou stranou zabezpečené minimálne nasledovné služby, ktorých konkrétne parametre sú definované v dohodách o výkone správy medzi MF SR a ÚOSS:
  - EPS - elektronickú požiarnu signalizáciu v priestoroch výpočtových systémov,
  - PNS - bezpečnosť vstupov oprávnených osôb k výpočtovým systémom,
  - dostupnosť aplikácií prostredníctvom IKT MF SR,
  - dostupnosť aplikácií prostredníctvom zriadenia a konfigurácie samostatnej virtuálnej privátnej siete (FINNET 2,4,5),
  - monitoring jednotlivých liniek združených vo FINNET 2,4,5,
  - zabezpečenie primeranej a aktuálnej kapacity prenosového pásma jednotlivých liniek FINNET 2,4,5,
  - zabezpečenie kvality poskytovanej komunikačnej služby parametrami Doba opravy (TTR) a dostupnosť služby (Service Availability),
  - garanciu bezpečnosti komunikácie vo FINNET 2,4,5 na CPE smerovačoch,
  - okamžitú aktiváciou trouble ticketov u poskytovateľa IKT prostredníctvom CPU (centrum podpory užívateľov),
  - dostupnosť potrebných procesorových kapacít na prevádzku IS,
  - dostupnosť potrebných pamäťových kapacít na prevádzku IS,
  - dostupnosť potrebných diskových kapacít na prevádzku IS,
  - monitorovanie 24x7 systémového SW za účelom zamedzenia ich neželaných výpadkov s okamžitou aktiváciou servisných kapacít; v zmysle platných zmluvných vzťahov,
  - dostupnosť technickej servisnej podpory pre servis HW platformy výpočtových systémov,
  - monitorovanie a sledovanie incidentov na HW a SW 24 x 7,
  - analýzu systémových logov a protokolov,
  - služby súvisiace s optimalizáciou doby chodu aplikácie;

4.2. Členenie úloh, postupy riešenia identifikované v existujúcich identifikačných listoch:

IL 161 - Centrum monitorovania prevádzky - CMP

- všetky úlohy v bode 3;

IL 401 - Technologická infraštruktúra dátovej sály MF SR

- zásobovanie výpočtových systémov el. energiou z dvoch nezávislých zdrojov (náhradné zdroje el. energie - UPS, motorgenerátor),
- chladenie výpočtovej sály klimatizačnými jednotkami,
- zabezpečenie antivírovej ochrany výpočtových systémov,
- pravidelné zálohovanie a archiváciu údajov;

IL 406 - Prevádzka dátovej sály MF SR

- úlohy v predmete riešenia bod 2 – najmä časť „zabezpečenie“, všetky návrhy na riešenie – aktivity v bode 4 a výstupy v bode 5;

IL 409 - Riešenie požiadaviek a hlásení pre zamestnancov MF SR

- revízia bezpečnostných politík - v ročných intervaloch, t. j. 1x ročne,
- reportovanie incidentov a zásahov na mesačnej báze na oddelenie informačnej a kybernetickej bezpečnosti MF SR,
- školenia o obsahu IRA o LAN a IRA o bezpečnosti podľa potreby - min. 1x mesačne.

5. Výstupy z riešenia:

5.1.

- nové, alebo aktualizované zmluvy o poskytovaní služieb (SLA) tretích strán,
- pravidelné interné a externé penetračné testovanie infraštruktúry MF SR,
- informácia o odstránení nedostatkov z penetračných testovaní,
- aktualizované identifikačné listy úloh;

5.2. Výstupy z riešenia identifikovaných v existujúcich identifikačných listov

- mesačná informácia o množstve a charaktere incidentov a vykonaných konfiguračných zmenách(viď IL 406 a 409),
- úplná segmentácia siete pre zabezpečenie bezpečnosti a dátovej priepustnosti;

6. Termíny plnenia:

6.1.

- informácia o odstránení nedostatkov auditných zistení a penetračných testovaní a návrh na riešenie nevyriešených zistení do 100 pracovných dní od vydania správ,
- nové, alebo aktualizované zmluvy o poskytovaní služieb (SLA) tretích strán,
- raz za dva roky uskutočnené interné a externé penetračné testovanie infraštruktúry MF SR;

6.2. Termíny plnenia identifikovaných v existujúcich identifikačných listov

- mesačná informácia pre zamestnancov oddelenia IBaKB OIT MF SR o množstve a charaktere incidentov do 10 dňa nasledujúceho mesiaca,
- mesačná informácia pre zamestnancov oddelenia IBaKB OIT MF SR o stave a zmenách HW a SW na dátovej sále MF SR,
- aktualizované identifikačné listy úloh.

7. Odberateľ – užívateľ výsledkov:

Ministerstvo financií SR

8. Kapacita potrebná na riešenie v čl. / hodinách

370

9. Riziká riešenia úlohy

- nedostatočné finančné krytie technologicky a organizačne nutných zmien,
- nedostatok odborných kapacít,
- nedostatok personálnych kapacít,
- nedostatočná ochrana IS;

10. Kritériá hodnotenia:

- počet pravidelných mesačných informácií o množstve a charaktere incidentov a o stave a zmenách HW a SW na dátovej sále,
- počet nových, resp. aktualizovaných zmlúv (SLA) s tretími stranami,
- percento odstránených nedostatkov z auditných správ a úspešné absolvovanie kontrolného auditu,
- percento odstránených nedostatkov penetračných testovaní,
- počet odstránených zistení z penetračných testovaní.