Príloha č. 1: Opis predmetu zákazky: Implementácia organizačných opatrení v súlade so zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti

V rámci implementácie organizačných opatrení v súlade so zákonom č.69/2018 Z.z. o kybernetickej bezpečnosti požaduje Úrad pre reguláciu elektronických komunikácií a poštových služieb zabezpečenie vytvorenia interných smerníc ako i súvisiacej dokumentácie v rámci nižšie uvedeného rozsahu v priebehu 6 mesiacov:

1. **Vypracovanie bezpečnostnej dokumentácie (politiky, štandardy, smernice, pokyny), modelovanie procesov organizácie, analýza dopadov**

   Bezpečnostná dokumentácia upravuje základnú analýzu rizík a analýzu dopadov (AR/BIA), riadi riziká a upravuje základné dokumenty v oblasti bezpečnosti, upravuje zavedenie klientskeho nástroja (modulu) evidencie informačných aktív, ich klasifikácie a kategorizácie a riadenia rizík, z ktorých by vyplývalo aké opatrenia a ktoré je potrebné realizovať na základe zákona č. 69/2018 Z.z.

   a) <u>Bezpečnostná dokumentácia:</u>
      a. Bezpečnostná stratégia kybernetickej bezpečnosti,
      b. Riadenie bezpečnostných rizík,
      c. Riadenie informačných aktív,
      d. Pravidlá správania a dobrej praxe,
      e. Riadenie dodávateľských vzťahov,
      f. Riadenie vývoja a údržby v oblasti informačno-komunikačných technológií,
      g. Riadenie a prevádzka informačno-komunikačných technológií,
      h. Riadenie súladu,
      i. Riadenie kontinuity procesov a činností,
      j. Organizácia bezpečnosti,
      k. Bezpečnostná politika.

   b) <u>Bezpečnosť prevádzky IS a sietí:</u>
      Cieľom smernice je procesne zabezpečiť riadenie bezpečnosti sietí a informačných systémov a naplnenie požiadaviek na základe §11 Vyhlášky č. 362/2018 Z.z. o bezpečnosti prevádzky IT a §10 Vyhlášky č. 362/2018 Z.z. o bezpečnosti komunikačných sietí, zálohe dát, posudzovaní zraniteľností a ďalších ako aj zákona o KB:
      - riadením prevádzky - riadením prístupov používateľov k sieťam a informačným systémom podľa § 12 zákona o KB,
      - prostredníctvom riadenia bezpečného prístupu medzi vonkajšími a vnútornými sieťami a informačnými systémami, 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,

- tým, že prepojenia medzi segmentmi a externými sieťami, ktoré sú chránené firewallom a všetky spojenia sú povoľované na princípe zásady najnižších privilégií,
- prostredníctvom 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,
- tým, že sieťam alebo informačným systémom sú umožnené len špecifikované služby umiestnené vo vyhradených segmentoch siete počítačovej siete,
- tým, že spojenia do externých sietí sú smerované cez sieťový firewall a v závislosti od prostredia aj cez systém detekcie prienikov,
- prostredníctvom serverov dostupných z externých sietí zabezpečovaných podľa odporúčaní výrobcu,
- udržiavaním zoznamu všetkých vstupno-výstupných bodov na hranici siete v aktuálnom stave,
- použitím automatizačných prostriedkov, ktorými sú identifikované neoprávnené sieťové spojenia na hranici s vonkajšou sieťou,
- prostredníctvom blokovania neoprávnených spojení zo známych adries označených ako škodlivé alebo spôsobujúce známe hrozby, ak to nastavenie informačného systému umožňuje,
- neumožnením komunikácie a prevádzky aplikácií cez neautorizované porty,
- prostredníctvom systému monitorovania bezpečnosti, ktorý je nakonfigurovaný tak, že zaznamenáva a vyhodnocuje aj informácie o sieťových paketoch na hranici siete,
- implementovaním systému detekcie prienikov alebo systému prevencie prienikov na identifikáciu nezvyčajných mechanizmov útokov alebo proaktívneho blokovania škodlivej sieťovej prevádzky,
- prostredníctvom smerovania odchádzajúcej používateľskej sieťovej prevádzky cez autentizovaný server filtrovania obsahu,
- prostredníctvom vyžiadania použitia dvojfaktorovej autentizácie od každého vzdialeného pripojenia do internej siete,
- vykonávaním 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.

c) <u>Návrh procesov a postupov pre riadenie prevádzky:</u>

Riadenie bezpečnosti prevádzky siete a informačného systému musí byť zaistené prostredníctvom určených pravidiel a postupov na:

- riadenie zmien,
- riadenie záplat a aktualizácií,

- riadenie kapacít,
- pravidelné zálohovanie a testovanie obnovy informácií zo záloh,
- ochranu pred škodlivým kódom,
- inštaláciu softvéru v sieťach a informačných systémoch,
- inštaláciu zariadení v sieťach a informačných systémoch a
- zaznamenávanie a vyhodnocovanie prevádzkových a bezpečnostných záznamov

d) Kryptografické opatrenia - Návrh procesov a postupov pre kryptografickú ochranu informácií.

e) Riešenie kybernetických incidentov - Návrh procesov a postupov pre riešenie kybernetických incidentov.

Očakávané výstupy časti 1. Vypracovanie bezpečnostnej dokumentácie (politiky, štandardy, smernice, pokyny), modelovanie procesov organizácie, analýza dopadov:

- Politika - Bezpečnostná stratégia kybernetickej bezpečnosti,
- Politika - Riadenie bezpečnostných rizík,
- Politika - Riadenie informačných aktív,
- Politika - Pravidlá správania a dobrej praxe,
- Politika - Riadenie dodávateľských vzťahov,
- Politika - Riadenie vývoja a údržby v oblasti informačno-komunikačných technológií,
- Politika - Riadenie a prevádzka informačno-komunikačných technológií,
- Politika - Riadenie súladu,
- Politika - Riadenie kontinuity procesov a činností,
- Politika - Organizácia bezpečnosti,
- Bezpečnostná politika,
- Smernica - Bezpečnosť prevádzky IS a sietí,
- Smernica - Riadenie prevádzky (change management, zálohovanie, testovanie obnovy, inštalácia zariadení...),
- Smernica/Štandard - Kryptografická ochrana informácií,
- Smernica/Štandard - Riešenie kybernetických incidentov.

2. Inventarizácia, klasifikácia a kategorizácia informačných aktív

Smernica pre klasifikáciu informácií a kategorizácia sietí a informačných systémov podľa § 20 ods. 2 zákona č. 69/2018 Z.z. sa vykonáva v klasifikačnej schéme v súlade so štruktúrou klasifikácie informácií a kategorizácie sietí a informačných systémov podľa prílohy č. 2 vyhlášky 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 „príloha č.2“) . Ak prevádzkovateľ základnej služby disponuje vlastnou klasifikáciou informácií a kategorizáciou sietí a informačných systémov, vykoná sa mapovanie na klasifikáciu v klasifikačnej schéme v súlade so štruktúrou klasifikácie informácií a kategorizácie sietí a informačných systémov podľa prílohy č. 2.

Klasifikácia informácií a kategorizácia sietí a informačných systémov reflektuje požiadavky kybernetickej bezpečnosti počas celého životného cyklu informácií, siete a informačného systému. Predpokladom na úspešnú klasifikáciu informácií a kategorizáciu sietí a informačných systémov je pozostáva najmä z nižšie uvedených aktivít:

- špecifikácie, ako definície požiadaviek a potrieb vedúcich k rozhodnutiu o vzniku informačného systému alebo akéhokoľvek spracúvania informácií,
- návrhu procesu, systému alebo dátovej štruktúry,
- vývoja systému alebo spôsobu spracúvania informácií,
- implementácie systému ako inštalácie, nasadenia, zavedenia alebo oživenia systému, alebo začatia procesu spracúvania informácií,
- prevádzky procesu ako štandardného využívania a údržby systému a údržby informácií,
- zmeny existujúceho, bežiaceho systému alebo spracúvania informácií, rozvoja a inovácie spracúvania podľa aktuálnych potrieb prevádzkovateľa základnej služby,
- nahradenia systému alebo procesu spracúvania informácií novým systémom alebo procesom,
- vyradenia ako ukončenia procesu spracúvania informácií alebo vyňatia systému z prevádzky.

Informácia sa klasifikuje bez ohľadu na jej formát, spôsob uloženia, systémy, aplikácie alebo nástroje, v ktorých sa nachádza alebo prostredníctvom ktorých sa informácia spracúva alebo prostredníctvom ktorých je prenášaná.

Pri klasifikácii informácií sa uplatňuje odstupňovaný prístup tak, že do nižších úrovní sú zahrnuté také informácie, pri ktorých sú najnižšie nároky na dôvernosť, integritu, dostupnosť a zodpovednosť vrátane zabezpečovania kvality služby. Informácie sa vytvárajú, spracúvajú a ukladajú tak, že ich kvalita a spoľahlivosť je primeraná ich klasifikačnému stupňu.

Kategorizácia sietí a informačných systémov je založená na klasifikácii informácií.

Kategorizácia sietí a informačných systémov sa vykonáva pre každú sieť a informačný systém vytvorením zoznamu vybraných komponentov sietí a informačných systémov, ktorý identifikuje jednotlivé siete a informačné systémy, ich podporné systémy a podsystémy s uvedením ich bezpečnostnej funkcie a zaradenia do príslušných bezpečnostných kategórií.

Zoznam komponentov sietí a informačných systémov identifikujúci jednotlivé siete a informačné systémy sa môže skladať z textovej, tabuľkovej alebo grafickej časti tak, že sú jednoznačne definované hranice vybranej siete a informačného systému, rozhrania medzi definovanými hranicami, bezpečnostné funkcie komponentov, ktoré majú byť zahrnuté v posudzovaní úrovne bezpečnosti a požiadavky príslušných regulačných požiadaviek a technických noriem alebo iných vecne obdobných postupov a metód na ich projektovanie, vytváranie, implementáciu a kontrolu.

Siete a informačné systémy tvoriace hranicu medzi rôznymi bezpečnostnými kategóriami v bezpečnostnom systéme sa zaradia do vyššej bezpečnostnej kategórie.

Kategorizácia sietí a informačných systémov zohľadňuje, že zlyhanie siete alebo informačného systému v ľubovoľnej bezpečnostnej úrovni nespôsobí zlyhanie vybranej siete a informačného systému zaradeného do bezpečnostnej úrovne s vyššou kategóriou. Pomocné siete a informačné systémy a podsystémy, ktoré pomáhajú funkciám vybraných informačných systémov, musia byť zaradené do príslušnej bezpečnostnej kategórie s ohľadom na zaradenie nadradeného systému.

Minimálne požiadavky na bezpečnostné opatrenia v závislosti od kategorizácie sietí a informačných systémov sú uvedené v *prílohe č. 3*. k vyhláške č. 362/2018 Z. z.

Táto kapitola by mala pokryť vypracovanie dokumentov, ktoré budú pokrývať vypracovanie dokumentácie, ktorá bude pokrývať nižšie uvedenú problematiku:

a. Spracovanie metodiky pre klasifikáciu informácií a kategorizáciu sietí a informačných systémov,
b. Vypracovanie klasifikačnej schémy,
c. Spracovanie klasifikácie informácií a kategorizácie sietí.

3. Vzdelávanie a príprava vzdelávacích materiálov pre IT aj neIT zamestnancov

Táto aktivita pozostáva z dvoch častí.

Prvá časť sa týka prípravy smernice, ktorá bude obsahovať informácie pre zodpovedných zamestnancov odboru informačných a komunikačných technológií, ktorá bude slúžiť ako nástroj na minimalizáciu, prevenciu a riešenie vzniknutých hrozieb a následných postupov spojených s neoprávneným prístupom do informačných systémov organizácie, siete organizácie a údajov, ktorými organizácia disponuje. Predmetná dokumentácia bude obsahovať postupy spojené s minimalizáciou rizík spojených s neoprávneným prístupom do informačných systémov, nástrojmi, ktoré by riešili prevenciu voči takémuto konaniu a spôsobmi riešenia už vzniknutých incidentov. Smernica bude slúžiť ako nástroj IT zamestnancov, podľa ktorého budú zodpovední IT zamestnanci riešiť vzniknuté incidenty a usmerňovať ostatných zamestnancov v predchádzaní takýmto incidentom.

Druhá časť bude pozostávať zo spracovania plánu rozvoja bezpečnostného povedomia a vzdelávania zamestnancov a dodávateľov, vrátane hodnotenia účinnosti. Plán rozvoja bezpečnostného povedomia bude obsahovať školiace materiály pre zamestnancov z pohľadu zvýšenia povedomia o kybernetickej bezpečnosti a hrozieb, ktoré zamestnancom hrozia, vzdelávanie zamestnancov o súčasných hrozbách a spôsoboch ako majú tieto hrozby reportovať zodpovedným IT zamestnancom.

Organizačná a personálna bezpečnosť bude pozostávať z nasledujúcich dokumentov:

a. Návrh procesov a postupov v oblasti personálnej bezpečnosti,
b. Spracovanie plánu rozvoja bezpečnostného povedomia a vzdelávania zamestnancov a dodávateľov, vrátane hodnotenia účinnosti

4. Vykonanie analýzy rizík kybernetickej bezpečnosti a návrh na riadenie rizík

Smernica upravuje základnú analýzu rizík a analýzu dopadov (AR/BIA), riadi riziká a upravuje základné dokumenty v oblasti bezpečnosti, upravuje zavedenie klientskeho nástroja (modulu) evidencie informačných aktív, ich klasifikácie a kategorizácie a riadenia rizík, z ktorých by vyplývalo aké opatrenia a ktoré je potrebné realizovať na základe zákona č. 69/2018 Z.z.

Smernica výkonu analýzy rizík a analýzy dopadov musí definovať proces riadenia rizika pozostávajúci z cyklických a na seba nadväzujúcich procesov:

1. stanovenie kontextu rizík
2. posúdenie rizík
3. ošetrovanie rizík
4. komunikácia o rizikách
5. monitorovanie a preskúmanie rizika

Postup posudzovania rizík ako musí byť popísaný ako komplexný proces, ktorý pozostáva z:

1. identifikácie rizík,
2. analýzy rizík a
3. ohodnotenia rizík.

V rámci predmetnej smernice musí byť zabezpečené procesné nastavenie výkonu analýzy rizík a analýzy dopadov (AR/BIA) organizáciou vrátane:

- identifikácie aktív a ohodnotenia ich kritickosti,
- klasifikácie aktív a kategorizácie IS a sietí,
- identifikácie hrozieb a vektorov útokov,
- analýzy potenciálnych dopadov,
- identifikácie rizík na základe pravdepodobností výskytu hrozieb a možných dopadov,
- identifikácie existujúcich opatrení a reziduálnych rizík,
- návrhu opatrení.

Návrh katalógu rizík a spôsobov ich riadenia:

Katalóg rizík definuje všetky možné ohrozenia, ktoré môžu pôsobiť na aktíva alebo chránené osobné údaje. Cieľom popisu rizika je zachytiť identifikované riziko do štruktúrovaného prehľadného formátu. V zozname rizík je potrebné uviesť najmä základné informácie o riziku, informácie pre analýzu rizík, informácie o odozve na vyhodnotenie rizika.
Návrh katalógu rizík a spôsobu ich udržiavania, aktualizácie a riadenia (mitigácie), bude obsahovať identifikované riziká z AR/BIA a spôsoby (možnosti) ich riadenia (mitigácie), vrátane zavedenia formalizovaného a opakovaného procesu riadenia rizík a ich schválenia Bezpečnostným výborom Úradu pre reguláciu elektronických komunikácií a poštových služieb.

Predmetná kapitola bude popisovať nasledovné oblasti problematiky:

a. Návrh procesov a postupov spojených s riadením rizík kybernetickej bezpečnosti a informačnej bezpečnosti,
b. Spracovanie inventarizácie aktív spolu s určením vlastníkov aktív kybernetickej bezpečnosti a informačnej bezpečnosti,
c. Spracovanie analýzy rizík kybernetickej bezpečnosti.

5. Analýza zmluvných vzťahov s tretími stranami z pohľadu KB, adaptácia odporúčaní do zmlúv

Riadenie dodávateľov - Návrh procesov a postupov pre riadenie kybernetickej bezpečnosti a informačnej bezpečnosti dodávateľských služieb, akvizícií a údržby IS. Smernica upravuje koncept životného cyklu vývoja systémov, ktorý sa vzťahuje na celý rad hardverových a softvérových konfigurácií, pretože systém sa môže skladať iba z hardvérových, iba zo softvérových alebo kombinácie oboch.

Bude pokrývať všetky fázy SSDLC z pohľadu bezpečnosti a bezpečnostných požiadaviek: - od fázy zámeru projektu a návrhu požiadaviek (okrem funkčných požiadaviek je potrebné zadefinovať aj bezp. požiadavky) - cez fázy samotného vývoja (zabezpečenie vývojového prostredia a pod.) - testovania (otestovania nie len funkčných ale aj bezp. požiadaviek, vrátane zabezpečenia anonymizácie

testovacích dát a pod.) - implementácie, nasadenia a riadenia zmien - až po bezpečné vyradenie IS z prevádzky - checklist bezpečného/kontrol vývoja webových aplikácií Návrh bezpečnostných požiadaviek pre aplikácie bude obsahovať základnú množinu (base line) týchto požiadaviek rozdelenú podľa klasifikačných stupňov.

6. **Plán kontrol, interných auditov, compliance management**
   Návrh procesov a postupov pre riešenie kybernetických incidentov:
   a) Zaznamenávanie udalostí a monitorovanie - Návrh procesov a postupov pre zaznamenávanie udalostí a monitorovanie,
   b) Riadenie súladu a kontrolné činnosti - Návrh procesov a postupov overovania účinnosti bezpečnostných opatrení, vyhodnocovania aktuálnosti bezpečnostnej dokumentácie

Príloha č. 1: Opis predmetu zákazky: Implementácia organizačných opatrení v súlade so zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti

V rámci implementácie organizačných opatrení v súlade so zákonom č.69/2018 Z.z. o kybernetickej bezpečnosti požaduje Úrad pre reguláciu elektronických komunikácií a poštových služieb zabezpečenie vytvorenia interných smerníc ako i súvisiacej dokumentácie v rámci nižšie uvedeného rozsahu v priebehu 6 mesiacov:

7. **Vypracovanie bezpečnostnej dokumentácie (politiky, štandardy, smernice, pokyny), modelovanie procesov organizácie, analýza dopadov**

   Bezpečnostná dokumentácia upravuje základnú analýzu rizík a analýzu dopadov (AR/BIA), riadi riziká a upravuje základné dokumenty v oblasti bezpečnosti, upravuje zavedenie klientskeho nástroja (modulu) evidencie informačných aktív, ich klasifikácie a kategorizácie a riadenia rizík, z ktorých by vyplývalo aké opatrenia a ktoré je potrebné realizovať na základe zákona č. 69/2018 Z.z.

   f) <u>Bezpečnostná dokumentácia:</u>
      a. Bezpečnostná stratégia kybernetickej bezpečnosti,
      b. Riadenie bezpečnostných rizík,
      c. Riadenie informačných aktív,
      d. Pravidlá správania a dobrej praxe,
      e. Riadenie dodávateľských vzťahov,
      f. Riadenie vývoja a údržby v oblasti informačno-komunikačných technológií,
      g. Riadenie a prevádzka informačno-komunikačných technológií,
      h. Riadenie súladu,
      i. Riadenie kontinuity procesov a činností,
      j. Organizácia bezpečnosti,
      k. Bezpečnostná politika.

   g) <u>Bezpečnosť prevádzky IS a sietí:</u>
      Cieľom smernice je procesne zabezpečiť riadenie bezpečnosti sietí a informačných systémov a naplnenie požiadaviek na základe §11 Vyhlášky č. 362/2018 Z.z. o bezpečnosti prevádzky IT a

§10 Vyhlášky č. 362/2018 Z.z. o bezpečnosti komunikačných sietí, zálohe dát, posudzovaní zraniteľností a ďalších ako aj zákona o KB:

- riadením prevádzky - riadením prístupov používateľov k sieťam a informačným systémom podľa § 12 zákona o KB,
- prostredníctvom riadenia bezpečného prístupu medzi vonkajšími a vnútornými sieťami a informačnými systémami, 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,
- tým, že prepojenia medzi segmentmi a externými sieťami, ktoré sú chránené firewallom a všetky spojenia sú povoľované na princípe zásady najnižších privilégií,
- prostredníctvom 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,
- tým, že sieťam alebo informačným systémom sú umožnené len špecifikované služby umiestnené vo vyhradených segmentoch siete počítačovej siete,
- tým, že spojenia do externých sietí sú smerované cez sieťový firewall a v závislosti od prostredia aj cez systém detekcie prienikov,
- prostredníctvom serverov dostupných z externých sietí zabezpečovaných podľa odporúčaní výrobcu,
- udržiavaním zoznamu všetkých vstupno-výstupných bodov na hranici siete v aktuálnom stave,
- použitím automatizačných prostriedkov, ktorými sú identifikované neoprávnené sieťové spojenia na hranici s vonkajšou sieťou,
- prostredníctvom blokovania neoprávnených spojení zo známych adries označených ako škodlivé alebo spôsobujúce známe hrozby, ak to nastavenie informačného systému umožňuje,
- neumožnením komunikácie a prevádzky aplikácií cez neautorizované porty,
- prostredníctvom systému monitorovania bezpečnosti, ktorý je nakonfigurovaný tak, že zaznamenáva a vyhodnocuje aj informácie o sieťových paketoch na hranici siete,
- implementovaním systému detekcie prienikov alebo systému prevencie prienikov na identifikáciu nezvyčajných mechanizmov útokov alebo proaktívneho blokovania škodlivej sieťovej prevádzky,
- prostredníctvom smerovania odchádzajúcej používateľskej sieťovej prevádzky cez autentizovaný server filtrovania obsahu,
- prostredníctvom vyžiadania použitia dvojfaktorovej autentizácie od každého vzdialeného pripojenia do internej siete,

- vykonávaním 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.

h) Návrh procesov a postupov pre riadenie prevádzky:

Riadenie bezpečnosti prevádzky siete a informačného systému musí byť zaistené prostredníctvom určených pravidiel a postupov na:

- riadenie zmien,
- riadenie záplat a aktualizácií,
- riadenie kapacít,
- pravidelné zálohovanie a testovanie obnovy informácií zo záloh,
- ochranu pred škodlivým kódom,
- inštaláciu softvéru v sieťach a informačných systémoch,
- inštaláciu zariadení v sieťach a informačných systémoch a
- zaznamenávanie a vyhodnocovanie prevádzkových a bezpečnostných záznamov

i) Kryptografické opatrenia - Návrh procesov a postupov pre kryptografickú ochranu informácií.

j) Riešenie kybernetických incidentov - Návrh procesov a postupov pre riešenie kybernetických incidentov.

Očakávané výstupy časti 1. Vypracovanie bezpečnostnej dokumentácie (politiky, štandardy, smernice, pokyny), modelovanie procesov organizácie, analýza dopadov:

- Politika - Bezpečnostná stratégia kybernetickej bezpečnosti,
- Politika - Riadenie bezpečnostných rizík,
- Politika - Riadenie informačných aktív,
- Politika - Pravidlá správania a dobrej praxe,
- Politika - Riadenie dodávateľských vzťahov,
- Politika - Riadenie vývoja a údržby v oblasti informačno-komunikačných technológií,
- Politika - Riadenie a prevádzka informačno-komunikačných technológií,
- Politika - Riadenie súladu,
- Politika - Riadenie kontinuity procesov a činností,
- Politika - Organizácia bezpečnosti,
- Bezpečnostná politika,
- Smernica - Bezpečnosť prevádzky IS a sietí,
- Smernica - Riadenie prevádzky (change management, zálohovanie, testovanie obnovy, inštalácia zariadení...),
- Smernica/Štandard - Kryptografická ochrana informácií,
- Smernica/Štandard - Riešenie kybernetických incidentov.

8. Inventarizácia, klasifikácia a kategorizácia informačných aktív

Smernica pre klasifikáciu informácií a kategorizácia sietí a informačných systémov podľa § 20 ods. 2 zákona č. 69/2018 Z.z. sa vykonáva v klasifikačnej schéme v súlade so štruktúrou klasifikácie informácií a kategorizácie sietí a informačných systémov podľa prílohy č. 2 vyhlášky 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 „príloha č.2“) . Ak prevádzkovateľ základnej služby disponuje vlastnou klasifikáciou informácií a kategorizáciou sietí a informačných systémov, vykoná sa mapovanie na klasifikáciu v klasifikačnej schéme v súlade so štruktúrou klasifikácie informácií a kategorizácie sietí a informačných systémov podľa prílohy č. 2.

Klasifikácia informácií a kategorizácia sietí a informačných systémov reflektuje požiadavky kybernetickej bezpečnosti počas celého životného cyklu informácií, siete a informačného systému. Predpokladom na úspešnú klasifikáciu informácií a kategorizáciu sietí a informačných systémov je pozostáva najmä z nižšie uvedených aktivít:

- špecifikácie, ako definície požiadaviek a potrieb vedúcich k rozhodnutiu o vzniku informačného systému alebo akéhokoľvek spracúvania informácií,
- návrhu procesu, systému alebo dátovej štruktúry,
- vývoja systému alebo spôsobu spracúvania informácií,
- implementácie systému ako inštalácie, nasadenia, zavedenia alebo oživenia systému, alebo začatia procesu spracúvania informácií,
- prevádzky procesu ako štandardného využívania a údržby systému a údržby informácií,
- zmeny existujúceho, bežiaceho systému alebo spracúvania informácií, rozvoja a inovácie spracúvania podľa aktuálnych potrieb prevádzkovateľa základnej služby,
- nahradenia systému alebo procesu spracúvania informácií novým systémom alebo procesom,
- vyradenia ako ukončenia procesu spracúvania informácií alebo vyňatia systému z prevádzky.

Informácia sa klasifikuje bez ohľadu na jej formát, spôsob uloženia, systémy, aplikácie alebo nástroje, v ktorých sa nachádza alebo prostredníctvom ktorých sa informácia spracúva alebo prostredníctvom ktorých je prenášaná.

Pri klasifikácii informácií sa uplatňuje odstupňovaný prístup tak, že do nižších úrovní sú zahrnuté také informácie, pri ktorých sú najnižšie nároky na dôvernosť, integritu, dostupnosť a zodpovednosť vrátane zabezpečovania kvality služby. Informácie sa vytvárajú, spracúvajú a ukladajú tak, že ich kvalita a spoľahlivosť je primeraná ich klasifikačnému stupňu.

Kategorizácia sietí a informačných systémov je založená na klasifikácii informácií.

Kategorizácia sietí a informačných systémov sa vykonáva pre každú sieť a informačný systém vytvorením zoznamu vybraných komponentov sietí a informačných systémov, ktorý identifikuje jednotlivé siete a informačné systémy, ich podporné systémy a podsystémy s uvedením ich bezpečnostnej funkcie a zaradenia do príslušných bezpečnostných kategórií.

Zoznam komponentov sietí a informačných systémov identifikujúci jednotlivé siete a informačné systémy sa môže skladať z textovej, tabuľkovej alebo grafickej časti tak, že sú jednoznačne definované hranice vybranej siete a informačného systému, rozhrania medzi definovanými hranicami, bezpečnostné funkcie komponentov, ktoré majú byť zahrnuté v posudzovaní úrovne

bezpečnosti a požiadavky príslušných regulačných požiadaviek a technických noriem alebo iných vecne obdobných postupov a metód na ich projektovanie, vytváranie, implementáciu a kontrolu.

Siete a informačné systémy tvoriace hranicu medzi rôznymi bezpečnostnými kategóriami v bezpečnostnom systéme sa zaradia do vyššej bezpečnostnej kategórie.

Kategorizácia sietí a informačných systémov zohľadňuje, že zlyhanie siete alebo informačného systému v ľubovoľnej bezpečnostnej úrovni nespôsobí zlyhanie vybranej siete a informačného systému zaradeného do bezpečnostnej úrovne s vyššou kategóriou. Pomocné siete a informačné systémy a podsystémy, ktoré pomáhajú funkciám vybraných informačných systémov, musia byť zaradené do príslušnej bezpečnostnej kategórie s ohľadom na zaradenie nadradeného systému.

Minimálne požiadavky na bezpečnostné opatrenia v závislosti od kategorizácie sietí a informačných systémov sú uvedené v *prílohe č. 3*. k vyhláške č. 362/2018 Z. z.

Táto kapitola by mala pokryť vypracovanie dokumentov, ktoré budú pokrývať vypracovanie dokumentácie, ktorá bude pokrývať nižšie uvedenú problematiku:

d. Spracovanie metodiky pre klasifikáciu informácií a kategorizáciu sietí a informačných systémov,
e. Vypracovanie klasifikačnej schémy,
f. Spracovanie klasifikácie informácií a kategorizácie sietí.

9. Vzdelávanie a príprava vzdelávacích materiálov pre IT aj neIT zamestnancov

Táto aktivita pozostáva z dvoch častí.

Prvá časť sa týka prípravy smernice, ktorá bude obsahovať informácie pre zodpovedných zamestnancov odboru informačných a komunikačných technológií, ktorá bude slúžiť ako nástroj na minimalizáciu, prevenciu a riešenie vzniknutých hrozieb a následných postupov spojených s neoprávneným prístupom do informačných systémov organizácie, siete organizácie a údajov, ktorými organizácia disponuje. Predmetná dokumentácia bude obsahovať postupy spojené s minimalizáciou rizík spojených s neoprávneným prístupom do informačných systémov, nástrojmi, ktoré by riešili prevenciu voči takémuto konaniu a spôsobmi riešenia už vzniknutých incidentov. Smernica bude slúžiť ako nástroj IT zamestnancov, podľa ktorého budú zodpovední IT zamestnanci riešiť vzniknuté incidenty a usmerňovať ostatných zamestnancov v predchádzaní takýmto incidentom.

Druhá časť bude pozostávať zo spracovania plánu rozvoja bezpečnostného povedomia a vzdelávania zamestnancov a dodávateľov, vrátane hodnotenia účinnosti. Plán rozvoja bezpečnostného povedomia bude obsahovať školiace materiály pre zamestnancov z pohľadu zvýšenia povedomia o kybernetickej bezpečnosti a hrozieb, ktoré zamestnancom hrozia, vzdelávanie zamestnancov o súčasných hrozbách a spôsoboch ako majú tieto hrozby reportovať zodpovedným IT zamestnancom.

Organizačná a personálna bezpečnosť bude pozostávať z nasledujúcich dokumentov:

c. Návrh procesov a postupov v oblasti personálnej bezpečnosti,
d. Spracovanie plánu rozvoja bezpečnostného povedomia a vzdelávania zamestnancov a dodávateľov, vrátane hodnotenia účinnosti

10. Vykonanie analýzy rizík kybernetickej bezpečnosti a návrh na riadenie rizík

Smernica upravuje základnú analýzu rizík a analýzu dopadov (AR/BIA), riadi riziká a upravuje základné dokumenty v oblasti bezpečnosti, upravuje zavedenie klientskeho nástroja (modulu) evidencie informačných aktív, ich klasifikácie a kategorizácie a riadenia rizík, z ktorých by vyplývalo aké opatrenia a ktoré je potrebné realizovať na základe zákona č. 69/2018 Z.z.

Smernica výkonu analýzy rizík a analýzy dopadov musí definovať proces riadenia rizika pozostávajúci z cyklických a na seba nadväzujúcich procesov:

6. stanovenie kontextu rizík
7. posúdenie rizík
8. ošetrovanie rizík
9. komunikácia o rizikách
10. monitorovanie a preskúmanie rizika

Postup posudzovania rizík ako musí byť popísaný ako komplexný proces, ktorý pozostáva z:

4. identifikácie rizík,
5. analýzy rizík a
6. ohodnotenia rizík.

V rámci predmetnej smernice musí byť zabezpečené procesné nastavenie výkonu analýzy rizík a analýzy dopadov (AR/BIA) organizáciou vrátane:

- identifikácie aktív a ohodnotenia ich kritickosti,
- klasifikácie aktív a kategorizácie IS a sietí,
- identifikácie hrozieb a vektorov útokov,
- analýzy potenciálnych dopadov,
- identifikácie rizík na základe pravdepodobností výskytu hrozieb a možných dopadov,
- identifikácie existujúcich opatrení a reziduálnych rizík,
- návrhu opatrení.

Návrh katalógu rizík a spôsobov ich riadenia:

Katalóg rizík definuje všetky možné ohrozenia, ktoré môžu pôsobiť na aktíva alebo chránené osobné údaje. Cieľom popisu rizika je zachytiť identifikované riziko do štruktúrovaného prehľadného formátu. V zozname rizík je potrebné uviesť najmä základné informácie o riziku, informácie pre analýzu rizík, informácie o odozve na vyhodnotenie rizika.
Návrh katalógu rizík a spôsobu ich udržiavania, aktualizácie a riadenia (mitigácie), bude obsahovať identifikované riziká z AR/BIA a spôsoby (možnosti) ich riadenia (mitigácie), vrátane zavedenia formalizovaného a opakovaného procesu riadenia rizík a ich schválenia Bezpečnostným výborom Úradu pre reguláciu elektronických komunikácií a poštových služieb.

Predmetná kapitola bude popisovať nasledovné oblasti problematiky:

d. Návrh procesov a postupov spojených s riadením rizík kybernetickej bezpečnosti a informačnej bezpečnosti,
e. Spracovanie inventarizácie aktív spolu s určením vlastníkov aktív kybernetickej bezpečnosti a informačnej bezpečnosti,
f. Spracovanie analýzy rizík kybernetickej bezpečnosti.

11. Analýza zmluvných vzťahov s tretími stranami z pohľadu KB, adaptácia odporúčaní do zmlúv

Riadenie dodávateľov - Návrh procesov a postupov pre riadenie kybernetickej bezpečnosti a informačnej bezpečnosti dodávateľských služieb, akvizícií a údržby IS. Smernica upravuje koncept životného cyklu vývoja systémov, ktorý sa vzťahuje na celý rad hardverových a softvérových konfigurácií, pretože systém sa môže skladať iba z hardvérových, iba zo softvérových alebo kombinácie oboch.

Bude pokrývať všetky fázy SSDLC z pohľadu bezpečnosti a bezpečnostných požiadaviek: - od fázy zámeru projektu a návrhu požiadaviek (okrem funkčných požiadaviek je potrebné zadefinovať aj bezp. požiadavky) - cez fázy samotného vývoja (zabezpečenie vývojového prostredia a pod.) - testovania (otestovania nie len funkčných ale aj bezp. požiadaviek, vrátane zabezpečenia anonymizácie testovacích dát a pod.) - implementácie, nasadenia a riadenia zmien - až po bezpečné vyradenie IS z prevádzky - checklist bezpečného/kontrol vývoja webových aplikácií Návrh bezpečnostných požiadaviek pre aplikácie bude obsahovať základnú množinu (base line) týchto požiadaviek rozdelenú podľa klasifikačných stupňov.

12. Plán kontrol, interných auditov, compliance management

Návrh procesov a postupov pre riešenie kybernetických incidentov:

c) Zaznamenávanie udalostí a monitorovanie - Návrh procesov a postupov pre zaznamenávanie udalostí a monitorovanie,
d) Riadenie súladu a kontrolné činnosti - Návrh procesov a postupov overovania účinnosti bezpečnostných opatrení, vyhodnocovania aktuálnosti bezpečnostnej dokumentácie