Vyhláška č. 362/2018 Z. z.

Vyhláška Národného bezpečnostného úradu, ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení

https://www.zakonypreludi.sk/zz/2018-362

(v znení č. 264/2023 Z. z.)

Platnosť od	**20.12.2018**
Účinnosť od	**01.09.2023 (za 1 mesiac)**

Znenie 01.09.2023

362

VYHLÁŠKA

Národného bezpečnostného úradu

z 11. decembra 2018,

ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení

Národný bezpečnostný úrad podľa § 32 ods. 1 písm. c) zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len „zákon“) ustanovuje:

§ 1

Základné ustanovenia

(1) Táto vyhláška upravuje obsah bezpečnostných opatrení, obsah a štruktúru bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení, ktoré prijíma prevádzkovateľ základnej služby podľa § 3 písm. m) zákona pre informačné systémy a siete, prostredníctvom ktorých zabezpečuje základnú službu podľa § 3 písm. l) zákona a pre informačné systémy a siete, ktorých výpadok alebo poškodenie môže spôsobiť poškodenie alebo znemožnenie poskytovania základnej služby.

(2) Bezpečnostné opatrenia sa prijímajú na základe odporúčaní medzinárodne akceptovaných štandardov kybernetickej bezpečnosti alebo iných vecne obdobných postupov a metód so zreteľom na najnovšie poznatky a pri súčasnom identifikovaní rizík, zraniteľností a požiadaviek regulácie v rámci sektora prevádzkovateľa základnej služby podľa prílohy č. 1 zákona.

(3) Všeobecné bezpečnostné opatrenia sa prijímajú a zadokumentujú v bezpečnostnej dokumentácii pre všetky oblasti podľa § 20 ods. 3 zákona v závislosti od kategorizácie sietí a informačných systémov a v rozsahu podľa § 5 až 17d.

§ 2

Obsah a štruktúra bezpečnostnej dokumentácie

(1) Bezpečnostná dokumentácia obsahuje

a) schválenú stratégiu kybernetickej bezpečnosti a bezpečnostné politiky kybernetickej bezpečnosti,

b) klasifikáciu informácií a kategorizáciu sietí a informačných systémov,

c) zadokumentované vymedzenie rozsahu a spôsobu plnenia všetkých bezpečnostných opatrení; konkrétny obsah môže byť odvodený z princípov niektorého z rámcov riadenia bezpečnostnej architektúry,

d) vykonanú analýzu rizík kybernetickej bezpečnosti,

e) záverečnú správu o výsledkoch auditu kybernetickej bezpečnosti podľa § 29 zákona.

(2) Bezpečnostná dokumentácia sa vypracúva na základe posúdenia poskytovanej základnej služby a s ňou

a) súvisiacej infraštruktúry výrobných a produkčných technológií,

b) súvisiacej infraštruktúry informačno-komunikačných technológií,

c) súvisiacej aplikačnej architektúry,

d) súvisiacej bezpečnostnej architektúry a implementovaných bezpečnostných opatrení,

e) súvisiacich organizačných usporiadaní, pracovných rolí, zodpovednosti a delenia právomocí,

f) súvisiacich zaužívaných rámcov riadenia operačných rizík,

g) súvisiacej organizačnej kultúry a spoločenskej zodpovednosti.

(3) Bezpečnostná dokumentácia kybernetickej bezpečnosti môže zahŕňať aj

a) bezpečnostné štandardy, ktoré interpretujú požiadavky platných bezpečnostných politík v konkrétnych situáciách, určujú aktivity, hlavné pravidlá, zodpovednosti a organizáciu riadenia s cieľom podporiť dodržiavanie bezpečnostných politík a

b) bezpečnostné návody, ktoré predstavujú súhrn predpísaných krokov na vykonanie bezpečnostných politík a bezpečnostných štandardov prostredníctvom konkrétnych akcií a ktoré opisujú bezpečnostné konfigurácie a poskytujú konkrétne, platformovo závislé usmernenia na podporu bezpečnostných politík a bezpečnostných štandardov.

§ 3

Stratégia kybernetickej bezpečnosti

(1) Stratégia kybernetickej bezpečnosti určuje ciele, ktoré je potrebné na základe výsledkov analýzy rizík kybernetickej bezpečnosti dosiahnuť, spolu s uvedením základných princípov na ich dosiahnutie a určením právomocí a zodpovedností za systémy manažérstva,[1)] riadenie rizík kybernetickej bezpečnosti a aktualizáciu bezpečnostnej dokumentácie.

(2) Stratégia môže byť prijatá samostatne alebo aj ako jedna z bezpečnostných politík.

(3) Na základe stratégie sa prijímajú bezpečnostné politiky podľa prílohy č. 1.

§ 4

Klasifikácia informácií a kategorizácia sietí a informačných systémov

(1) Klasifikácia informácií a kategorizácia sietí a informačných systémov podľa § 20 ods. 2 zákona sa vykonáva v klasifikačnej schéme v súlade so štruktúrou klasifikácie informácií a kategorizácie sietí a informačných systémov podľa prílohy 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.

(2) Klasifikácia informácií a kategorizácia sietí a informačných systémov reflektuje požiadavky kybernetickej bezpečnosti počas celého životného cyklu informácií, siete a informačného systému, a to najmä vo fáze

a) špecifikácie, ako definície požiadaviek a potrieb vedúcich k rozhodnutiu o vzniku informačného systému alebo akéhokoľvek spracúvania informácií,

b) návrhu procesu, systému alebo dátovej štruktúry,

c) vývoja systému alebo spôsobu spracúvania informácií,

d) implementácie systému ako inštalácie, nasadenia, zavedenia alebo oživenia systému, alebo začatia procesu spracúvania informácií,

e) prevádzky procesu ako štandardného využívania a údržby systému a údržby informácií,

f) zmeny existujúceho, bežiaceho systému alebo spracúvania informácií, rozvoja a inovácie spracúvania podľa aktuálnych potrieb prevádzkovateľa základnej služby,

g) nahradenia systému alebo procesu spracúvania informácií novým systémom alebo procesom a

h) vyradenia ako ukončenia procesu spracúvania informácií alebo vyňatia systému z prevádzky.

(3) 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.

(4) 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. Informácie sa vytvárajú, spracúvajú a ukladajú tak, že ich kvalita a spoľahlivosť je primeraná ich klasifikačnému stupňu.

(5) Kategorizácia sietí a informačných systémov je založená na klasifikácii informácií.

(6) 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.

(7) 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.

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

(9) 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.

(10) Minimálne požiadavky na bezpečnostné opatrenia v závislosti od kategorizácie sietí a informačných systémov sú uvedené v prílohe č. 3.

§ 5

Bezpečnostné opatrenia podľa § 20 ods. 3 písm. a) zákona

Na organizáciu kybernetickej bezpečnosti sa uplatňuje najmä zásada

a) najnižších privilégií, podľa ktorej sú každému používateľovi obmedzené privilégiá v najväčšom rozsahu potrebnom na splnenie pridelených úloh,

b) oddeľovania zodpovedností, podľa ktorej žiaden používateľ nemá oprávnenie upravovať alebo používať aktíva prevádzkovateľa základnej služby bez autorizácie alebo overenia identity,

c) vymedzenia právomoci, povinnosti a zodpovednosti, ktoré sú súčasťou pracovnej náplne alebo obdobného opisu pracovných činností,

d) sprístupňovania informácií podľa zásady aktuálnej potreby poznať, podľa ktorej prístup k informáciám a ich vlastníctvo je obmedzené len na tie osoby, ktoré z dôvodu plnenia svojich úloh alebo povinností musia byť s takýmito informáciami oboznámené alebo ich spracúvajú.

§ 6

Bezpečnostné opatrenia pre oblasť podľa § 20 ods. 3 písm. b) zákona

(1) Riadenie rizík kybernetickej bezpečnosti a informačnej bezpečnosti je proces spojený s finančnými, zmluvnými a inventarizačnými funkciami na podporu riadenia životného cyklu informačných technológií a konfiguračných položiek. Riadenie rizík kybernetickej bezpečnosti a informačnej bezpečnosti musí zabezpečiť ochranu aktív podľa ich hodnoty.

(2) Všetky aktíva súvisiace so zariadeniami na spracovanie informácií a informačnými prostriedkami sú identifikované a inventár týchto aktív je centrálne zaznamenaný a riadený.

(3) Riadenie aktív pozostáva z identifikácie a evidencie všetkých

a) aktív, od ktorých závisí poskytovanie základnej služby,

b) podporných služieb, prostredníctvom ktorých sa zabezpečuje kontinuita základnej služby a jej poskytovanie,

c) zodpovedných osôb za identifikáciu a evidenciu aktív a

d) vlastníkov aktív.

(4) Rovnaká ochrana sa neuplatňuje pre všetky druhy aktív. Na tento účel sa aktíva klasifikujú a kategorizujú postupom podľa § 4.

(5) Ukončením pracovného pomeru alebo iného obdobného pracovného vzťahu zamestnancov prevádzkovateľa základnej služby a zamestnancov tretích strán sa zadokumentovaným spôsobom vracajú späť všetky zverené aktíva.

(6) Riadenie rizík pozostáva z

a) identifikácie zraniteľností,

b) identifikácie hrozieb,

c) identifikácie a analýzy rizík s ohľadom na aktívum,

d) určenia vlastníka rizika,

e) implementácie organizačných a technických bezpečnostných opatrení v závislosti od identifikovaných rizík vrátane informácie, ktoré bezpečnostné opatrenia sú implementované a ktoré bezpečnostné opatrenia nie sú implementované spolu s odôvodnením,

f) analýzy funkčného dopadu a

g) pravidelného preskúmavania identifikovaných rizík a v závislosti od toho aktualizácie prijatých bezpečnostných opatrení.

(7) Identifikácia rizika sa vykonáva na základe princípu najhoršieho scenára, ktorý môže nastať aj pri nízkej pravdepodobnosti. Na určenie úrovne identifikovaného rizika sa vopred nastaví súbor pravidiel, ktoré umožnia na základe štandardných a opakovateľných postupov určiť merateľné a objektívne úrovne rizika pre najhoršie scenáre.

(8) Analýzou rizík sa určuje pravdepodobnosť vzniku škodlivej udalosti, ktorá môže byť spôsobená zneužitím existujúcej zraniteľnosti aktíva potenciálnou hrozbou v spojitosti s existujúcimi bezpečnostnými opatreniami a identifikáciou dopadov pri narušení dôvernosti, integrity alebo dostupnosti aktíva.

(9) Identifikácia hrozieb je založená na identifikácii aktív a ich vlastníkov a identifikácii zraniteľností potenciálne pôsobiacich na tieto aktíva.

(10) Pre potreby analýzy rizík sa zoznam hrozieb združuje do jednotlivých skupín tak, že je možné tento zoznam použiť univerzálne pre väčšinu aktív. Pre jednotlivé aktíva sú hodnotené len hrozby relevantné pre konkrétne aktívum. Hrozby sa rozdeľujú podľa ich pôvodu do kategórií najmenej ako

a) úmyselné hrozby pre všetky úmyselné aktivity zamerané na aktíva,

b) náhodné hrozby pre všetky ľudské činnosti, ktoré môžu náhodne poškodiť aktíva,

c) hrozby spôsobené vplyvom prostredia pre všetky udalosti, ktoré vznikajú nezávisle od ľudskej činnosti.

(11) Súčasťou riadenia aktív, hrozieb a rizík je aj analýza funkčného dopadu, ktorá pozostáva z hodnotenia dopadu na činnosť prevádzkovateľa základnej služby spôsobeného krízovým scenárom, ktorý môže zasiahnuť zdroje a aktíva podporujúce procesy prevádzkovateľa základnej služby a spôsobiť ohrozenie alebo narušenie kontinuity jeho poskytovanej základnej služby.

§ 7

Bezpečnostné opatrenia pre oblasť podľa § 20 ods. 3 písm. c) zákona

Personálna bezpečnosť pozostáva najmenej

a) z postupov pri zaradení osoby do niektorých z bezpečnostných rolí, presunu práv, povinností a zodpovedností vo vzťahu ku kybernetickej bezpečnosti na inú osobu,

b) zo zavedenia plánu rozvoja bezpečnostného povedomia a vzdelávania spočívajúceho v oboznámení používateľov, administrátorov, osôb zastávajúcich niektorú z bezpečnostných rolí a dodávateľov s bezpečnostnými politikami a v pravidelnom zvyšovaní ich

bezpečnostného povedomia počas trvania pracovnoprávneho vzťahu alebo iného obdobného pracovného alebo zmluvného vzťahu,

c) z kontroly dodržiavania bezpečnostných politík zo strany zamestnancov, administrátorov, osôb zastávajúcich niektorú z bezpečnostných rolí a dodávateľov,

d) z hodnotenia účinnosti plánu rozvoja bezpečnostného povedomia zamestnancov, administrátorov, osôb zastávajúcich niektorú z bezpečnostných rolí a dodávateľov,

e) z určenia pravidiel a postupov na riešenie prípadov porušenia bezpečnostnej politiky zo strany používateľov, administrátorov, osôb zastávajúcich niektorú z bezpečnostných rolí a dodávateľov,

f) z postupov pri skončení pracovnoprávneho vzťahu alebo iného obdobného pracovného alebo zmluvného vzťahu s používateľom, administrátorom, s osobou zastávajúcou niektorú z bezpečnostných rolí umožňujúcich presun práv, povinností a zodpovedností na inú novú osobu,

g) z postupov pri porušení bezpečnostných politík spočívajúcich v oprávnení obmedziť alebo odňať prístupové oprávnenia a privilégiá,

h) z vykonania poučenia o manipulácii s informáciami pre osoby, ktoré vykonávajú činnosť alebo sa oboznamujú s informáciami podľa osobitného predpisu.[1a])

§ 8

Bezpečnostné opatrenia podľa § 20 ods. 3 písm. d) zákona

(1) Riadenie prístupov osôb k sieti a informačnému systému je 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 tento účel sa vypracúvajú zásady riadenia prístupu osôb k sieti a informačnému systému, ktoré definujú spôsob prideľovania a odoberania prístupových práv používateľom, ich evidenciu a vedenie prevádzkových záznamov o každom prístupe do siete a informačného systému.

(2) Riadenie prístupov k sieťam a informačným systémom sa uskutočňuje v závislosti od prevádzkových a bezpečnostných potrieb prevádzkovateľa základnej služby, 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.

(3) Riadenie prístupov osôb k sieti a informačnému systému zahŕňa najmä

a) vypracovanie zásad riadenia prístupu k informáciám,

b) riadenie prístupu používateľov,

c) zodpovednosť používateľov,

d) riadenie prístupu k sieťam,

e) prístup k operačnému systému a jeho službám,

f) prístup k aplikáciám,

g) monitorovanie prístupu a používania informačného systému a

h) riadenie vzdialeného prístupu.

(4) Pri riadení prístupov k sieťam a informačným systémom sa

a) každému používateľovi siete a informačného systému prideľuje jednoznačný identifikátor na autentizáciu na vstup do siete a informačného systému,

b) zabezpečuje riadenie jednoznačných identifikátorov používateľov vrátane prístupových práv a oprávnení používateľských účtov,

c) využíva nástroj 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,

d) v pravidelných intervaloch, najmenej raz ročne, vykonáva kontrola prístupových účtov a prístupových oprávnení na overenie súladu schválených oprávnení so skutočným stavom vykonávania oprávnení, a detekcia a následné trvalé zablokovanie nepoužívaných prístupových účtov, o čom sa vedie záznam preukázateľným spôsobom,

e) určí osoba zodpovedná za riadenie prístupu používateľov do siete a k informačnému systému a za prideľovanie a odoberanie prístupových práv používateľom, ich evidenciu a vedenie prevádzkových záznamov o každom prístupe do siete a informačného systému v zmysle bezpečnostnej politiky.

§ 9

Bezpečnostné opatrenia podľa § 20 ods. 3 písm. e) zákona

(1) Na riadenie kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s tretími stranami sa pri uzatvorení zmluvy s treťou stranou podľa § 19 ods. 2 zákona analyzujú riziká dodávateľských služieb, spôsobom podľa § 6.

(2) Zmluva s treťou stranou obsahuje najmä

a) obdobie trvania zmluvy,

b) ustanovenie záväzku tretej strany dodržiavať bezpečnostné politiky prevádzkovateľa základnej služby a vyjadrenie súhlasu s nimi,

c) ustanovenie o povinnosti tretej strany chrániť informácie poskytnuté prevádzkovateľom základnej služby tretej strane,

d) ustanovenie o povinnosti tretej strany dodržiavať a prijímať bezpečnostné opatrenia,

e) konkrétnu špecifikáciu a rozsah bezpečnostných opatrení, ktoré prijíma tretia strana a vyjadrenie súhlasu s nimi,

f) konkrétny rozsah činnosti tretej strany,

g) zoznam pracovných rolí tretej strany, ktoré majú mať prístup k informáciám a údajom prevádzkovateľa základnej služby, s povinnosťou oznámiť prevádzkovateľovi základnej služby každú zmenu v personálnom obsadení; osoba zúčastnená na predmete plnenia podpisuje vyjadrenie o zachovávaní mlčanlivosti podľa zákona,

h) ustanovenie o rozsahu, spôsobe a možnosti vykonávania kontrolných činností a auditu prevádzkovateľom základnej služby u tretej strany,

i) vymedzenie podmienok a možnosti zapojenia ďalšieho dodávateľa úplne alebo čiastočne zabezpečujúceho plnenie pre prevádzkovateľa základnej služby namiesto dodávateľa,

j) ustanovenia o povinnosti informovať prevádzkovateľa základnej služby o kybernetickom bezpečnostnom incidente a o skutočnostiach majúcich vplyv na zabezpečovanie kybernetickej bezpečnosti a poskytnúť súčinnosť pri jeho riešení,

k) ustanovenia o spôsobe a forme hlásenia ďalších informácií požadovaných prevádzkovateľom základnej služby na plnenie jeho povinností vyplývajúcich zo zákona a ich vymedzenie,

l) ustanovenie o spôsobe a forme hlásenia informácií majúcich vplyv na zmluvu,

m) ustanovenie o sankčných mechanizmoch pri porušení zmluvy,

n) ustanovenia o podmienkach a spôsobe ukončenia zmluvy,

o) záväzok tretej strany po ukončení zmluvného vzťahu vrátiť, previesť alebo zničiť informácie, ku ktorým mala tretia strana počas trvania zmluvného vzťahu prístup u prevádzkovateľa základnej služby,

p) záväzok tretej strany najneskôr ku dňu ukončenia zmluvného vzťahu udeliť, poskytnúť, previesť alebo postúpiť potrebné licencie, práva alebo súhlasy nevyhnutné na zabezpečenie kontinuity prevádzkovanej základnej služby na prevádzkovateľa základnej služby; tento záväzok tretej strany ostáva v platnosti aj po ukončení zmluvného vzťahu po dobu dohodnutú zmluvnými stranami, ktorá nesmie byť kratšia ako päť rokov po ukončení zmluvného vzťahu.

(3) Zmluva s treťou stranou obsahuje bezpečnostné opatrenia najmä pre oblasť podľa § 20 ods. 3 písm. d), g) až i), k) a m) zákona.

(4) Vývoj a akvizícia siete a informačného systému základnej služby sa uskutočňuje s ohľadom na zaistenie kompatibility s existujúcimi sieťami a informačnými systémami a zachovanie úrovne bezpečnosti ustanovenej v stratégii.

(5) Evidencia uzatvorených zmlúv s treťou stranou je súčasťou bezpečnostnej dokumentácie.

§ 10

Bezpečnostné opatrenia podľa § 20 ods. 3 písm. f) zákona

Riadenie bezpečnosti prevádzky sietí a informačných systémov sa zaisťuje prostredníctvom určených pravidiel, zodpovedností a postupov na

a) riadenie zmien,

b) riadenie kapacít,

c) inštaláciu softvéru v sieťach a informačných systémoch,

d) inštaláciu zariadení v sieťach a informačných systémoch,

e) zaznamenávanie bezpečnostných záznamov a

f) zaznamenávanie a vyhodnocovanie prevádzkových záznamov.

§ 11

Bezpečnostné opatrenia podľa § 20 ods. 3 písm. g) zákona

(1) Technické zraniteľnosti informačných systémov ako celku sa identifikujú prostredníctvom

a) nástroja určeného na detegovanie existujúcich zraniteľností programových prostriedkov a ich častí,

b) nástroja určeného na detegovanie existujúcich zraniteľností technických prostriedkov a ich častí,

c) využitia verejných zoznamov a výrobcom poskytovaných zoznamov, ktoré opisujú zraniteľnosti programových a technických prostriedkov.

(2) Cieľom procesu riadenia záplat a aktualizácií je zabezpečiť konzistentné nasadzovanie potrebných softvérových opráv a aktualizácií a plošnú aplikáciu aktualizácií na zariadenia, pre ktoré je softvérová aktualizácia či záplata vydaná.

(3) Úlohami procesu riadenia záplat a aktualizácií sú najmä

a) identifikácia potrieb softvérových záplat a aktualizácií,

b) evidencia softvérových záplat a aktualizácií a informácia o ich nasadení alebo o dôvodoch ich nenasadenia,

c) rozhodnutie o vhodnom prístupe k otestovaniu softvérových záplat a aktualizácií,

d) zabezpečenie implementácie softvérových záplat a aktualizácií,

e) aktualizácia plánu softvérových záplat a aktualizácií.

(4) Neschválené aktualizácie nie sú prípustné.

§ 12

Bezpečnostné opatrenia podľa § 20 ods. 3 písm. h) zákona

(1) Požiadavkami na ochranu proti škodlivému kódu sú najmä

a) určenie zodpovednosti používateľov za prevenciu pred škodlivým kódom,

b) určenie pravidiel pre inštaláciu a používanie systémov prevencie škodlivého kódu,

c) monitorovanie potenciálnych ciest prieniku škodlivého kódu do prostredia sietí a informačných systémov.

(2) Systémy na ochranu proti škodlivému kódu sú nakonfigurované tak, že

a) v reálnom čase vykonávajú kontrolu prístupu k digitálnemu obsahu vrátane sieťovej prevádzky, sťahovania, spúšťania alebo otvárania súborov, priečinkov na vymeniteľnom alebo vzdialenom úložisku a prístupu k webovým sídlam a cloudovým službám,

b) spúšťajú pravidelné kontroly úložísk vrátane cloudových a pripojených vymeniteľných úložísk, najmenej raz ročne,

c) neoprávneným používateľom je zabránené v prístupe k obsahu prostredníctvom funkcie filtrovania obsahu,

d) používateľom je zamedzené v pokusoch odinštalovať alebo zakázať funkcie systému na ochranu proti škodlivému kódu.

§ 13

Bezpečnostné opatrenia podľa § 20 ods. 3 písm. i) zákona

Sieťová a komunikačná bezpečnosť sa zabezpečuje najmä

a) prostredníctvom riadenia bezpečného prístupu medzi vonkajšími a vnútornými sieťami, a to najmä využitím nástrojov na ochranu integrity sietí, ktoré sú zabezpečené segmentáciou sietí, informačné systémy so službami priamo prístupnými z externých sietí sa nachádzajú v samostatných sieťových segmentoch a v rovnakom segmente musia byť len informačné systémy s rovnakými bezpečnostnými požiadavkami, rovnakej kategórie a s podobným účelom,

b) tým, že spojenia medzi segmentmi siete, ktoré sú chránené firewallom sú povoľované na princípe zásady najnižších privilégií,

c) prostredníctvom bezpečnostných opatrení na bezpečné mobilné pripojenie do siete a vzdialený prístup, napríklad s použitím dvojfaktorovej autentizácie alebo použitím kryptografických prostriedkov,

d) tým, že v sieťach sú umožnené len špecifikované služby umiestnené vo vyhradených segmentoch počítačovej siete,

e) tým, že spojenia do externých sietí sú smerované cez sieťový firewall,

f) prostredníctvom serverov dostupných z externých sietí zabezpečovaných podľa odporúčaní výrobcu,

g) udržiavaním zoznamu vstupno-výstupných bodov na hranici siete v aktuálnom stave,

h) použitím automatizačných prostriedkov, ktorými sú identifikované neoprávnené sieťové spojenia na hranici s vonkajšou sieťou,

i) prostredníctvom blokovania neoprávnených spojení zo zdrojov identifikovaných ako škodlivé alebo spôsobujúce hrozby, ak to nastavenie informačného systému umožňuje,

j) neumožnením komunikácie a prevádzky aplikácií cez neautorizované porty,

k) prostredníctvom systému monitorovania bezpečnosti, ktorý je nakonfigurovaný tak, že zaznamenáva a vyhodnocuje aj informácie o sieťových paketoch na hranici siete,

l) v závislosti od prostredia implementovaním systému detekcie prienikov alebo systému prevencie prienikov na identifikáciu nezvyčajných mechanizmov útokov alebo proaktívneho blokovania škodlivej sieťovej prevádzky,

m) prostredníctvom smerovania odchádzajúcej používateľskej sieťovej prevádzky cez autentizovaný server filtrovania obsahu,

n) prostredníctvom vyžiadania použitia dvojfaktorovej autentizácie od každého vzdialeného pripojenia do internej siete,

o) vykonávaním pravidelného alebo nepretržitého posudzovania technických zraniteľností, a posudzovania technických zraniteľností zariadenia, ktoré sa vzdialene pripája do internej siete, alebo zmluvného zaručenia vrátane preukázania plnenia tejto povinnosti.“.

§ 14

Bezpečnostné opatrenia podľa § 20 ods. 3 písm. j) zákona

(1) Požiadavky na akvizíciu, vývoj a údržbu sietí a informačných systémov, ktoré sa uplatňujú na obstarávané, vyvíjané a udržiavané komponenty s digitálnymi prvkami, ktorých zamýšľané a odôvodnene predvídateľné použitie zahŕňa priame alebo nepriame logické alebo fyzické dátové pripojenie k sieťam a informačným systémom sa určujú najmä zavedením pravidiel a postupov

a) pre riadenie systémovej, aplikačnej a bezpečnostnej architektúry, s cieľom prijať už vo fáze návrhu primerané, špecificky navrhnuté technické a organizačné opatrenia,

b) pre riadenie systémovej, aplikačnej a bezpečnostnej architektúry, s cieľom predchádzať zníženiu účinnosti štandardne implementovaných technických a organizačných bezpečnostných opatrení,

c) na zabezpečenie kontroly nad verziami softvéru a zabudovaného softvéru,

d) pre riadenie konfigurácií, ktoré predchádzajú neschváleným a nezdokumentovaným zmenám konfigurácií, s cieľom udržovania sietí a informačných systémov v požadovanom, konzistentnom a očakávanom stave ich funkcií a

e) pre vykonávanie údržby sietí a informačných systémov, ktoré zaručia vymedzenie zodpovedností a pracovných postupov, ktorých cieľom je minimalizácia hrozieb vyplývajúcich z neúmyselných chýb alebo úmyselnej manipulácie pri údržbe sietí a informačných systémov.

(2) Požiadavky na metodiku softvérového vývoja sú určené s cieľom najmä

a) začleniť bezpečnostné požiadavky a kritériá do každej fázy procesu vývoja softvéru, a to vrátane aplikačnej architektúry a koncepcií použiteľnosti softvérového produktu,

b) zaručiť, že sa použijú najnovšie a najbezpečnejšie verzie nástrojov a komponentov na vývoj softvéru,

c) zaručiť, že sa použijú len softvérové knižnice a komponenty, ktoré pochádzajú od dôveryhodných dodávateľov a sú aktívne podporované,

d) zaručiť, že je kód udržateľný, konzistentný, čitateľný, efektívny a bezpečný,

e) zaručiť, že je udržovaný register softvérových komponentov,

f) zaručiť validáciu postupov tak, že softvérový modul neakceptuje nesprávny a neočakávaný vstup,

g) zaručiť, že vo vyvíjanom softvéri je nakonfigurovaný proces logovania, ktorý umožňuje včas zachytiť systémové a bezpečnostné udalosti, s cieľom identifikovať, analyzovať a riešiť neobvyklé udalosti a podozrivé správanie v rámci sietí a informačných systémov.

(3) Ak prevádzkovateľ základnej služby vykonáva softvérový vývoj prostredníctvom tretích strán, požiadavky podľa odseku 2 primerane prenáša na tretiu stranu zmluvou.“.

§ 15

Bezpečnostné opatrenia pre oblasť podľa § 20 ods. 3 písm. k) zákona

(1) Zaznamenávanie udalostí a monitorovanie sietí a informačných systémov sa uskutočňuje implementáciou centrálneho nástroja na zaznamenávanie činnosti sietí a informačných systémov a ich používateľov zabezpečujúceho dohľad nad sieťami a informačnými systémami zaznamenávaním prevádzky týchto sietí a informačných systémov, a to najmenej v rozsahu

a) centrálnych sieťových prvkov a serverov,

b) služieb prístupných do externých sietí a

c) kritických interných serverov a služieb.

(2) Nástroj na zaznamenávanie činnosti sietí a informačných systémov a ich používateľov umožňuje vytvárať prevádzkové záznamy a zaznamenávať najmenej

a) aktivity v podobe vytvorenia, čítania, aktualizácie alebo odstránenia chránených a prísne chránených informácií a údajov alebo ďalších informačných aktív s nimi spojených,

b) iniciáciu pripojenia do siete alebo informačného systému a akceptáciu alebo odmietnutie pripojenia do siete alebo informačného systému zaznamenaním aspoň dátumu a času aktivity, identifikácie technického prostriedku, v rámci ktorého je činnosť zaznamenaná, identifikáciu osoby a zdroja vo forme IP adresy,

c) pridelenie, úpravu alebo zrušenie prístupových práv používateľa vrátane pridania nového používateľa alebo skupiny používateľov, zmenu úrovne oprávnenia používateľa, zmenu pravidiel firewallu alebo zmenu hesla,

d) automatické varovné alebo chybové hlásenia systémov,

e) detegované podozrivé alebo škodlivé aktivity a

f) ďalšie informácie nevyhnutné na posúdenie závažnosti kybernetického bezpečnostného incidentu v spojení s kritickosťou danej služby alebo zariadenia a korektné informácie o dátume, čase a použitej časovej zóne.

(3) Prevádzkové záznamy sú zabezpečené najmenej tak, že

a) sú čitateľné výlučne osobám povereným ich analýzou,

b) zamedzujú možnosti prepísania alebo vymazania záznamu,

c) záznamy prenášané alebo presmerované od pôvodného zdrojového zariadenia do bezpečnostného monitorovacieho systému sú presmerované prostredníctvom zabezpečených kanálov alebo prostredníctvom dedikovanej správcovskej siete,

d) sú uchovávané po dobu zodpovedajúcu kategórii informačného systému.

(4) Za monitorovanie prevádzkových záznamov, ich vyhodnocovanie a vykonanie nahlásenia podozrivej aktivity je zodpovedný na to poverený zamestnanec prevádzkovateľa základnej služby alebo zamestnanec tretej strany, ak je jej táto činnosť zverená.

§ 16

Bezpečnostné opatrenia pre oblasť podľa § 20 ods. 3 písm. l) zákona

(1) Fyzická bezpečnosť sietí a informačných systémov sa realizuje najmenej prostredníctvom

a) umiestnenia siete a informačného systému v takom priestore, že sieť a informačný systém alebo aspoň ich najdôležitejšie komponenty sú chránené pred nepriaznivými prírodnými vplyvmi a vplyvmi prostredia, možnými dôsledkami havárií technickej infraštruktúry a fyzickým prístupom nepovolaných osôb (ďalej len „zabezpečený priestor“),

b) ochrany zabezpečeného priestoru fyzickými prostriedkami, najmä stenami, mechanickými zábrannými prostriedkami, technickými zabezpečovacími prostriedkami, napríklad zariadeniami elektrickej zabezpečovacej signalizácie, systémami na kontrolu vstupu, kamerovými systémami,

c) zaručenia, že sa v okolí zabezpečeného priestoru nevyskytujú zariadenia, ktoré môžu ohroziť sieť a informačný systém umiestnený v tomto zabezpečenom priestore, najmä kanalizácia, vodovod, horľavé alebo iné obdobné materiály,

d) vypracovania, implementácie a kontroly dodržiavania pravidiel na prácu v zabezpečenom priestore,

e) zabezpečenia ochrany pred výpadkom zdroja elektrickej energie tých častí siete a informačného systému, ktoré vyžadujú nepretržitú prevádzku a zabezpečenie, že taký výpadok nenastane,

f) zaručenia, že existujú záložné kapacity siete a informačného systému, zabezpečujúce dostupnosť, funkčnosť alebo náhradu siete a informačného systému, umiestnené v zabezpečenom priestore bezpečne vzdialenom zálohovanému zabezpečenému priestoru,

g) zaručenia, že prevádzka, používanie a manažment siete a informačného systému je v súlade vnútornými predpismi a zmluvnými záväzkami,

h) politiky, ktorá zakazuje nechávanie fyzických dokumentov bez dozoru a prikazuje uzamykanie počítača pred opustením pracoviska.

(2) Organizačné opatrenia vo fyzickej bezpečnosti sietí a informačných systémov sa zabezpečujú najmenej prostredníctvom vypracovania, zavedenia a kontroly dodržiavania pravidiel na

a) údržbu, uchovávanie a evidenciu technických komponentov sietí a informačných systémov a zariadení sietí a informačných systémov,

b) používanie zariadení sietí a informačných systémov na iné účely, ako sú určené,

c) používanie sietí a informačných systémov mimo zabezpečených priestorov,

d) vymazávanie, vyraďovanie a likvidovanie zariadení sietí a informačných systémov a všetkých typov relevantných záloh,

e) fyzický prenos technických komponentov sietí a informačných systémov alebo zariadení sietí a informačných systémov mimo zabezpečených priestorov,

f) narábanie s dokumentáciou systému a pamäťovými médiami tak, že sa zabráni ich neoprávnenému zverejneniu, odstráneniu, poškodeniu alebo modifikácii,

g) dimenzovanie a fyzické parametre sietí a hardvéru, ktoré priamo alebo nepriamo ovplyvňujú najväčšiu prípustnú dobu výpadku siete a informačného systému.

§ 17

Bezpečnostné opatrenia podľa § 20 ods. 3 písm. m) zákona

(1) Riešenie kybernetických bezpečnostných incidentov pozostáva najmä

a) z prípravy a vypracovania štandardov a postupov riešenia kybernetických bezpečnostných incidentov,

b) z monitorovania a analyzovania udalostí v sieťach a informačných systémoch,

c) z detekcie kybernetických bezpečnostných incidentov,

d) zo zberu relevantných informácií o kybernetických bezpečnostných incidentoch,

e) z vyhodnocovania kybernetických bezpečnostných incidentov,

f) z riešenia zistených kybernetických bezpečnostných incidentov a zníženia následkov zistených kybernetických bezpečnostných incidentov a

g) z vyhodnocovania spôsobov riešenia kybernetických bezpečnostných incidentov po ich vyriešení a prijatia opatrení alebo zavedenia nových postupov s cieľom minimalizovať výskyt obdobných kybernetických bezpečnostných incidentov.

(2) Na riešenie kybernetických bezpečnostných incidentov sa vypracúvajú a pravidelne aktualizujú štandardy a postupy riešenia kybernetických bezpečnostných incidentov, ktoré obsahujú najmä

a) postup pri internom nahlasovaní kybernetických bezpečnostných incidentov,

b) postup pri hlásení kybernetických bezpečnostných incidentov podľa § 24 ods. 1 zákona,

c) postup pri riešení jednotlivých typov kybernetických bezpečnostných incidentov a spôsob ich vyhodnocovania a

d) spôsob evidencie kybernetických bezpečnostných incidentov a použitých riešení.

(3) Proces detekcie kybernetických bezpečnostných incidentov sa zabezpečuje 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.

(4) Proces zberu a vyhodnocovania kybernetických bezpečnostných incidentov sa zabezpečuje prostredníctvom nástroja na zber a nepretržité vyhodnocovanie kybernetických bezpečnostných udalostí, ktorý umožňuje

a) zber a vyhodnocovanie informácií o kybernetických bezpečnostných incidentoch,

b) vyhľadávanie a zoskupovanie záznamov súvisiacich s kybernetickým bezpečnostným incidentom,

c) vyhodnocovanie bezpečnostných udalostí na ich identifikáciu ako kybernetických bezpečnostných incidentov,

d) revíziu konfigurácie a monitorovacích pravidiel na vyhodnocovanie bezpečnostných udalostí pri nesprávne identifikovaných kybernetických bezpečnostných incidentoch.

(5) Proces riešenia kybernetických bezpečnostných incidentov sa zabezpečuje prostredníctvom

a) pridelenia zodpovednosti a určenia postupov na zvládanie kybernetických bezpečnostných incidentov,

b) zavedenia procesu získavania a uchovávania podkladov potrebných na analýzu kybernetickej bezpečnostnej udalosti a kybernetického bezpečnostného incidentu,

c) prijímania opatrení na odvrátenie alebo zmiernenie vplyvu kybernetického bezpečnostného incidentu,

d) zavedenia pravidelného testovania, najmenej raz ročne, procesu nahlasovania kybernetických bezpečnostných incidentov, v zmysle štandardov a postupov vypracovaných podľa odseku 2, s vedením záznamov o takomto testovaní,

e) vedenia záznamov o kybernetických bezpečnostných incidentoch vrátane použitých riešení,

f) prešetrovania a určenia príčin vzniku kybernetického bezpečnostného incidentu,

g) aktualizácie bezpečnostnej politiky a prijatia primeraných bezpečnostných opatrení zamedzujúcich opakovanému výskytu kybernetického bezpečnostného incidentu a

h) určenia fyzickej osoby zodpovednej za nahlasovanie a odovzdávanie hlásení o kybernetických bezpečnostných incidentoch.

(6) Súčasťou evidencie kybernetických bezpečnostných incidentov sú na zabezpečenie dôkazu alebo dôkazného prostriedku aj informácie, na základe ktorých sa identifikuje vznik a pôvod kybernetického bezpečnostného incidentu.

§ 17a

Bezpečnostné opatrenia podľa § 20 ods. 3 písm. n) zákona

(1) Dôvernosť, integrita a hodnovernosť údajov v rámci sietí a informačných systémov, prostredníctvom ktorých je poskytovaná základná služba, sa zabezpečuje pomocou kryptografických prostriedkov používajúcich dostatočne odolné kryptografické mechanizmy, pričom sa určujú pravidlá kryptografickej ochrany údajov

a) pri ich prenose v rámci sietí a informačných systémov a

b) pri ich uložení v rámci sietí a informačných systémov.

(2) Systém správy kryptografických kľúčov a certifikátov je zabezpečený počas celého životného cyklu kryptografických kľúčov a certifikátov. Správa kryptografických kľúčov a certifikátov zahŕňa najmä

a) bezpečné nakladanie s kryptografickými kľúčmi a certifikátmi,

b) generovanie pseudonáhodných čísel a kľúčov, zriadenie, distribúciu, vkladanie, zmenu, obmedzenie platnosti, vyberanie, ukladanie a likvidáciu kľúčov a zneplatnenie certifikátov a

c) umožnenie kontroly a auditu systému správy kryptografických kľúčov a certifikátov.

§ 17b

Bezpečnostné opatrenia podľa § 20 ods. 3 písm. o) zákona

(1) Prevádzkovateľ základnej služby určí požiadavky na zabezpečenie kontinuity prevádzky pre prípad vzniku kybernetického bezpečnostného incidentu.

(2) Riadenie kontinuity prevádzky pozostáva najmä z

a) vypracovania stratégie a krízových plánov na zabezpečenie dostupnosti siete a informačného systému po narušení alebo zlyhaní v dôsledku kybernetického bezpečnostného incidentu na základe vykonania analýzy vplyvov kybernetického bezpečnostného incidentu na základnú službu,

b) vyčlenenia adekvátnych finančných, materiálno-technických a personálnych zdrojov na zabezpečenie riadenia kontinuity činností,

c) určenia komunikačného plánu na plnenie havarijných plánov a plánov obnovy spolu s kontaktnými údajmi, určeniami rolí a zodpovednosti za plnenie havarijných plánov a plánov obnovy po kybernetickom bezpečnostnom incidente,

d) určenia cieľovej doby obnovy jednotlivých procesov, siete a informačných systémov a aplikácií, a to najmä určením doby obnovy prevádzky, po ktorej uplynutí je po kybernetickom bezpečnostnom incidente obnovená najnižšia úroveň poskytovania základných služieb,

e) určenia cieľového bodu obnovy jednotlivých procesov, siete a informačných systémov základnej služby a aplikácií, a to najmä určením najnižšej úrovne poskytovania služieb, ktorá je dostatočná na používanie, prevádzku a správu siete a informačného systému a zachovanie kontinuity základnej služby,

f) testovania a vyhodnocovania jednotlivých procesov riadenia kontinuity činností a realizácie opatrení na zvýšenie odolnosti sietí a informačných systémov základnej služby,

g) určenia plánov havarijnej obnovy a postupov zálohovania na obnovu siete a informačného systému po jeho narušení alebo zlyhaní v dôsledku kybernetického bezpečnostného incidentu.

(3) Postupy zálohovania na obnovu siete a informačného systému po jeho narušení alebo zlyhaní v dôsledku kybernetického bezpečnostného incidentu obsahujú najmä

a) frekvenciu a rozsah jej dokumentovania a schvaľovania,

b) určenie osoby zodpovednej za zálohovanie,

c) časový interval, identifikáciu rozsahu údajov, dátového média zálohovania a požiadavku zabezpečenia vedenia dokumentácie o zálohovaní,

d) požiadavku umiestnenia záloh v zabezpečenom prostredí s riadeným prístupom,

e) požiadavku zabezpečenia šifrovania záloh obsahujúcich aktíva klasifikačného stupňa „chránené“ a „prísne chránené“,

f) požiadavku na vykonávanie pravidelného preverenia záloh, testovanie obnovy záloh a precvičovanie zavedených krízových plánov najmenej raz ročne.

§ 17c

Bezpečnostné opatrenia podľa § 20 ods. 3 písm. p) zákona

Požiadavky na audit, riadenie súladu a kontrolné činnosti, s cieľom dodržiavať a vykonávať nezávislé hodnotenie, meranie a preskúmavanie efektivity a účinnosti prijatých opatrení na ošetrenie rizík sa vykonávajú najmä pravidelným a plánovaným výkonom

auditu kybernetickej bezpečnosti podľa osobitného predpisu[1b]) a systémom vnútorného posúdenia bezpečnosti, ktorého cieľom je poskytnutie primeraného uistenia, že stav posudzovaných skutočností je v súlade s požadovanými strategickými cieľmi, politikami, štandardami, zmluvami, predpismi a postupmi organizácie a pri identifikovaní nesúladu sú prijímané opatrenia na ich odstránenie aspoň tak, že je bezpečnostné riziko znížené na prijateľnú úroveň.

§ 17d

Manažér kybernetickej bezpečnosti

Prevádzkovateľom základnej služby určený manažér kybernetickej bezpečnosti

a) predkladá návrhy a oznamuje informácie v oblasti informačnej a kybernetickej bezpečnosti priamo štatutárnemu orgánu prevádzkovateľa základnej služby,

b) riadi aplikáciu bezpečnostných opatrení v rámci systémov manažérstva,

c) je nezávislý od riadenia prevádzky a vývoja služieb informačných technológií a

d) spĺňa znalostné štandardy pre výkon roly manažéra kybernetickej bezpečnosti podľa osobitného predpisu.[1c])

§ 18

Účinnosť

Táto vyhláška nadobúda účinnosť 1. januára 2019.

Jozef Magala v. r.

Príloha č. 1 k vyhláške č. 362/2018 Z. z.

BEZPEČNOSTNÁ STRATÉGIA KYBERNETICKEJ BEZPEČNOSTI

Príloha č. 2 k vyhláške č. 362/2018 Z. z.

KLASIFIKAČNÁ SCHÉMA

A. Kritériá klasifikácie informácií

Klasifikačné stupne

Klasifikačné stupne opisujú citlivosť informácií, údajov alebo ďalších s nimi spojených informačných aktív (ďalej len „informačné aktíva“) z pohľadu narušenia ich dôvernosti, integrity a dostupnosti a odrážajú dôležitosť alebo hodnotu týchto aktív pre procesy prevádzkovateľa základnej služby.

1. Z hľadiska dôvernosti sú klasifikačné stupne informačných aktív definované ako

a) verejné informačné aktíva určené pre verejnosť, ktoré sú získateľné z verejných zdrojov alebo z informácií, ktoré sú pripravené na tento účel alebo sú preklasifikované z inej úrovne prostredníctvom vlastníka a zahŕňajú napríklad informácie z médií, povinne publikované informácie alebo všeobecne dostupné informácie,

b) interné informačné aktíva, ktoré sú používané a prístupné pre všetkých používateľov v rámci organizácie prevádzkovateľa základnej služby bez ohľadu na ich pracovnú rolu; na sprístupnenie týchto aktív tretím stranám je potrebné schválenie zo strany vlastníka informácie,

c) chránené informačné aktíva, ktoré sú používané a prístupné len určeným skupinám oprávnených osôb a ktorých neautorizované odhalenie, prezradenie alebo zničenie môže mať pre prevádzkovateľa základnej služby negatívny vplyv na poskytovanie služby; prístup k údajom klasifikovaným ako „Chránené“ je riadený pomocou zásady „potreby vedieť“ a zásady „najnižších privilégií“ a je vymedzený výhradne vopred definovaným a schváleným útvarom alebo iným jasne vymedzeným skupinám osôb; tretie strany majú k týmto údajom prístup len v nevyhnutných a jednoznačne definovaných prípadoch schválených vlastníkom,

d) prísnechránené informačné aktíva, ktoré sú používané a prístupné len jednotlivým vybraným používateľom prevádzkovateľa základnej služby a ktorých neautorizované odhalenie, prezradenie alebo zničenie môže mať s vysokou pravdepodobnosťou negatívny vplyv na poskytovanie základnej služby; prístup k údajom klasifikovaným ako „Prísne chránené“ je riadený pomocou zásady „potreby vedieť“ a zásady „najnižších privilégií“ a výhradne konkrétnym, vopred definovaným a schváleným osobám; tretie strany majú k týmto údajom prístup len vo výnimočných a jednoznačne definovaných prípadoch schválených vlastníkom alebo na základe ustanovení osobitných predpisov.

Ak nie je informačné aktívum explicitne klasifikované je považované za interné.

2. Z hľadiska integrity sú klasifikačné stupne informačných aktív definované ako

a) nízka zahŕňa informačné aktíva, ktorých chyba alebo nepresnosť výrazne neohrozí poskytovanú základnú službu,

b) stredná zahŕňa informačné aktíva, ktoré sú dôležité pre činnosť prevádzkovateľa základnej služby a ktorých chyba alebo nepresnosť môže spôsobiť dopad na kontinuitu poskytovanej základnej služby, strategickú oblasť, trhové a operačné riziká,

c) vysoká zahŕňa vybrané kľúčové informačné aktíva, ktoré sú kritické pre činnosť prevádzkovateľa základnej služby a ktorých chyba, nepresnosť bezprostredne ohrozuje poskytovanú základnú službu, s ňou spojené aktivity a reputáciu prevádzkovateľa základnej služby.

3. Z hľadiska dostupnosti sú klasifikačné stupne informačných aktív definované ako

a) nízka zahŕňa informačné aktíva prevádzkovateľa základnej služby, ktorých výpadok výrazne neohrozí poskytovanú službu alebo pre ktoré existujú alternatívne postupy,

b) stredná zahŕňa informačné aktíva, ktoré sú dôležité pre činnosť prevádzkovateľa základnej služby a ktorých zlyhanie môže mať dopad na kontinuitu poskytovanej základnej služby, strategickú oblasť, trhové a operačné riziká,

c) vysoká zahŕňa vybrané kľúčové informačné aktíva, ktoré sú kritické pre činnosť prevádzkovateľa základnej služby a ktorých zlyhanie bezprostredne ohrozuje poskytovanú základnú službu, s ňou spojené aktivity a dobrú povesť prevádzkovateľa základnej služby.

Základné pravidlá klasifikácie informácií

1. Každá klasifikovaná informácia má pridelený jeden klasifikačný stupeň dôvernosti, jeden klasifikačný stupeň integrity a jeden klasifikačný stupeň dostupnosti.

2. Bezpečnostné informácie, nastavenia, postupy, smernice a ostatné úkony ohľadom riadenia aktív sa klasifikujú rovnakým alebo vyšším klasifikačným stupňom, akým sú označené informačné aktíva, ktorých riadenie opisujú.

3. Prevádzkovateľ základnej služby môže v rozsahu svojej pôsobnosti jednotlivé informačné aktíva zaradiť do vyššieho stupňa.

4. Prevádzkovateľ základnej služby, ktorý už má vykonanú klasifikáciu informácií podľa inej štandardizačnej metódy, vykonáva na klasifikáciu informácií mapovanie na klasifikačné stupne podľa tejto prílohy.

B. Kritériá kategorizácie sietí a informačných systémov

Kategória I. zahŕňa informačné aktíva v pôsobnosti prevádzkovateľa základnej služby,

a) ktorých ohrozenie nemá žiadny negatívny dopad na poskytovanú základnú službu,

b) ktoré sú klasifikované z hľadiska dôvernosti ako verejné alebo v odôvodnených prípadoch interné,

c) ktoré sú klasifikované z hľadiska dostupnosti klasifikačným stupňom nízka alebo v odôvodnených prípadoch stredná,

d) ktoré sú klasifikované z hľadiska integrity klasifikačným stupňom nízka alebo v odôvodnených prípadoch stredná,

e) pri ktorých nie je predpoklad potreby identifikácie zodpovednosti za aktivity používateľov, alebo

f) pri ktorých nie je potrebné vykonávať kontrolnú činnosť.

Kategória II. zahŕňa informačné aktíva v pôsobnosti prevádzkovateľa základnej služby,

a) ktorých ohrozenie môže spôsobiť kybernetický bezpečnostný incident I. stupňa,

b) ktoré sú klasifikované z hľadiska dôvernosti ako interné, chránené alebo v odôvodnených prípadoch prísne chránené,

c) ktoré sú klasifikované z hľadiska dostupnosti klasifikačným stupňom stredná alebo v odôvodnených prípadoch vysoká,

d) ktoré sú klasifikované z hľadiska integrity klasifikačným stupňom stredná alebo v odôvodnených prípadoch vysoká,

e) pri ktorých je potrebné identifikovať zodpovednosť za kritické aktivity, najmä však aktivity privilegovaných používateľov,

f) pri ktorých je potrebné vykonávať kontrolnú činnosť,

g) tvoriace základné registre a/alebo referenčné registre,

h) zabezpečujúce vytváranie a vedenie agend, ktoré nepatria do I. bezpečnostnej kategórie,

i) ktoré sú agendové informačné systémy,

j) ktorými sú špecializované portály alebo

k) ktoré sú nevyhnutné na rozhodovanie orgánu štátnej moci.

Kategória III. zahŕňa informačné aktíva v pôsobnosti prevádzkovateľa základnej služby,

a) ktorých ohrozenie môže spôsobiť kybernetický bezpečnostný incident II. a III. stupňa,

b) ktoré sú klasifikované z hľadiska dôvernosti ako prísne chránené,

c) ktoré sú klasifikované z hľadiska dostupnosti klasifikačným stupňom vysoká,

d) ktoré sú klasifikované z hľadiska integrity klasifikačným stupňom vysoká,

e) pri ktorých je potrebné auditovať aktivity všetkých používateľov,

f) prostredníctvom ktorých sa poskytuje základná služba a ktorých výpadok alebo poškodenie spôsobí poškodenie alebo znemožnenie poskytovania základnej služby,

g) ktoré sú označené ako utajované skutočnosti alebo ako tajomstvo podľa osobitných predpisov,[2])

h) ktoré sú nevyhnutné a potrebné z hľadiska plnenia úloh týkajúcich sa obrany a bezpečnosti štátu alebo

i) ktorým je ústredný portál verejnej správy.

Príloha č. 3 k vyhláške č. 362/2018 Z. z.

MINIMÁLNE POŽIADAVKY NA BEZPEČNOSTNÉ OPATRENIA V ZÁVISLOSTI OD KATEGORIZÁCIE SIETÍ A INFORMAČNÝCH SYSTÉMOV

Tabuľka zobrazuje minimálne požiadavky na bezpečnostné opatrenia jednotlivých kategórií sietí a informačných systémov, ktoré môže prevádzkovateľ základnej služby pre individuálne aktíva sprísniť.

Bezpečnostné opatrenie pre	Kategória I	Kategória II	Kategória III
Oblasť podľa § 20 ods. 3 písm. a) zákona organizácia kybernetickej a informačnej bezpečnosti	Odporúčané	Povinné	Povinné
Oblasť podľa § 20 ods. 3 písm. b) zákona riadenie rizík kybernetickej a informačnej bezpečnosti	Odporúčané	Povinné	Povinné
Oblasť podľa § 20 ods. 3 písm. c) zákona personálna bezpečnosť	Odporúčané	Povinné	Povinné
Oblasť podľa § 20 ods. 3 písm. d) zákona riadenie prístupov	Odporúčané	Povinné	Povinné
Oblasť podľa § 20 ods. 3 písm. e) zákona riadenie kybernetickej a informačnej bezpečnosti vo vzťahoch s tretími stranami	Povinné	Povinné	Povinné
Oblasť podľa § 20 ods. 3 písm. f) zákona bezpečnosť pri prevádzke informačných systémov a sietí	Odporúčané	Povinné	Povinné
Oblasť podľa § 20 ods. 3 písm. g) zákona hodnotenie zraniteľností a bezpečnostných aktualizácií	Odporúčané	Povinné	Povinné
Oblasť podľa § 20 ods. 3 písm. h) zákona ochrana proti škodlivému kódu	Odporúčané	Povinné	Povinné
Oblasť podľa § 20 ods. 3 písm. i) zákona sieťová a komunikačná bezpečnosť	Odporúčané	Odporúčané	Povinné
Oblasť podľa § 20 ods. 3 písm. j) zákona akvizícia, vývoja a údržba sietí a informačných systémov	Odporúčané	Odporúčané	Povinné
Oblasť podľa § 20 ods. 3 písm. k) zákona zaznamenávanie udalostí a monitorovanie	Povinné	Povinné	Povinné
Oblasť podľa § 20 ods. 3 písm. l) zákona fyzická bezpečnosť a bezpečnosť prostredia	Odporúčané	Odporúčané	Povinné
Oblasť podľa § 20 ods. 3 písm. m) zákona riešenie kybernetických bezpečnostných incidentov	Povinné	Povinné	Povinné
Oblasť podľa § 20 ods. 3 písm. n) zákona kryptografické opatrenia	Odporúčané	Odporúčané	Povinné
Oblasť podľa § 20 ods. 3 písm. o) zákona kontinuita prevádzky	Odporúčané	Odporúčané	Povinné
Oblasť podľa § 20 ods. 3 písm. p) zákona audit, riadenie súladu a kontrolné činnosti	Odporúčané	Povinné	Povinné

Manažér kybernetickej bezpečnosti (§ 20 ods. 4 písm. a) zákona)	Povinné	Povinné	Povinné

Poznámky pod čiarou

1) STN ISO/IEC 27001 Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia. Systémy manažérstva informačnej bezpečnosti. Požiadavky. (36 9789)

1a) § 16 ods. 3 písm. b) zákona č. 500/2022 o Vojenskom spravodajstve.

1b) Vyhláška Národného bezpečnostného úradu č. 493/2022 Z. z. o audite kybernetickej bezpečnosti.

1c) Vyhláška Národného bezpečnostného úradu č. 492/2022 Z. z., ktorou sa ustanovujú znalostné štandardy v oblasti kybernetickej bezpečnosti.

2) Napríklad zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, § 17 až 20 zákona č. 513/1991 Zb. Obchodný zákonník, § 39 zákona Slovenskej národnej rady č. 323/1992 Zb. o notároch a notárskej činnosti (Notársky poriadok) v znení neskorších predpisov, zákon č. 483/2001 Z. z. o bankách a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, § 23 zákona č. 586/2003 Z. z. o advokácii a o zmene a doplnení zákona č. 455/1991 Zb. o živnostenskom podnikaní (živnostenský zákon) v znení neskorších predpisov v znení zákona č. 297/2008 Z. z., zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, § 24 a 25 zákona č. 576/2004 Z. z. o zdravotnej starostlivosti, službách súvisiacich s poskytovaním zdravotnej starostlivosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, § 11 zákona č. 563/2009 Z. z. o správe daní (daňový poriadok) a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, § 10 zákona č. 324/2011 Z. z. o poštových službách a o zmene a doplnení niektorých zákonov.