

ZBIERKA ZÁKONOV SLOVENSKEJ REPUBLIKY

Ročník 2023

Vyhlásené: 5. 7. 2023

Vyhlásená verzia v Zbierke zákonov Slovenskej republiky

Obsah dokumentu je právne záväzný.

264

VYHLÁŠKA

Národného bezpečnostného úradu

z 19. júna 2023,

**ktorou sa mení a dopĺňa vyhláška Národného bezpečnostného úradu
č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných
opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah
všeobecných bezpečnostných opatrení**

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 v znení zákona č. 287/2021 Z. z. ustanovuje:

Čl. I

Vyhláška Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení sa mení a dopĺňa takto:

1. V § 1 ods. 1 sa slová „§ 3 písm. l) zákona“ nahrádzajú slovami „§ 3 písm. m) zákona“ a slová „§ 3 písm. k) zákona“ sa nahrádzajú slovami „§ 3 písm. l) zákona“.
2. V § 1 ods. 3 sa slová „§ 5 až 17“ nahrádzajú slovami „§ 5 až 17d“.
3. V § 3 ods. 1 sa slová „riadenie kybernetickej bezpečnosti,“ nahrádzajú slovami „systémy manažérstva,¹⁾“.

Poznámka pod čiarou k odkazu 1 znie:

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

4. V § 3 ods. 2 a 3 sa vypúšťajú slová „kybernetickej bezpečnosti“.
5. § 5 vrátane nadpisu znie:

„§ 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. V § 6 odsek 1 znie:

„(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.“.

7. V § 7 písm. h) sa nad slovami „osobitného predpisu“ odkaz¹⁾ nahrádza odkazom^{1a)}.

Poznámka pod čiarou k odkazu 1a znie:

„^{1a)} § 16 ods. 3 písm. b) zákona č. 500/2022 o Vojenskom spravodajstve.“.

8. § 8 až 14 vrátane nadpisov znejú:

„§ 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 pridelovania 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 prideluje 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 pridelenie 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 prevádzkovej 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 tretou 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 tretou 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 povolené 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 udržiavania 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 udržiavaný 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.“.

- 9. V § 15 ods. 1 sa slová „Monitorovanie bezpečnosti sietí“ nahrádzajú slovami „Zaznamenávanie udalostí a monitorovanie sietí“ a vypúšťa sa slovo „bezpečnostný“.
- 10. V § 15 sa vypúšťa odsek 5.
- 11. § 17 vrátane nadpisu znie:

„§ 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 uchovávanía 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.“.

12. Za § 17 sa vkladajú § 17a až 17d, ktoré vrátane nadpisov znejú:

„§ 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 ošetrovanie 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.

Poznámka pod čiarou k odkazu 1b znie:

„^{1b)} Vyhláška Národného bezpečnostného úradu č. 493/2022 Z. z. o audite kybernetickej bezpečnosti.“.

§ 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)} “.

Poznámka pod čiarou k odkazu 1c znie:

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

13. Príloha č. 3 vrátane nadpisu znie:

**„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 zraniteľnosti 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

“.

14. Slová „bezpečnostná stratégia“ vo všetkých tvaroch sa v celom texte vyhlášky nahrádzajú slovom „stratégia“ v príslušnom tvare.

Čl. II

Táto vyhláška nadobúda účinnosť 1. septembra 2023.

Roman Konečný v. r.

