**Dôvodová správa**

**A. Všeobecná časť**

Národný bezpečnostný úrad ako ústredný orgán štátnej správy pre kybernetickú bezpečnosť na základe úlohy B.1. z uznesenia vlády Slovenskej republiky č. 55 z 1. februára 2024 k návrhu Plánu legislatívnych úloh vlády Slovenskej republiky na rok 2024, pripravil v súlade so schváleným Programovým vyhlásením vlády Slovenskej republiky na roky 2023-2027 a v súlade so schválenou Národnou stratégiou kybernetickej bezpečnosti na roky 2021-2025 a Akčným plánom realizácie Národnej stratégie kybernetickej bezpečnosti na roky 2021-2025 návrh zákona, ktorým sa mení a dopĺňa zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a o zmene a doplnení niektorých zákonov (ďalej len „návrh zákona“).

Zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len „zákon č. 69/2018 Z. z.“) bola do právneho poriadku Slovenskej republiky transponovaná smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (smernica NIS 1). Siete a informačné systémy, rýchla digitálna transformácia a ich prepojenosť na spoločnosť sa premietajú do celého spektra činností verejného aj súkromného sektora a vytvárajú nové výzvy pre oblasť kybernetickej bezpečnosti. Tento vývoj odhalil prirodzené nedostatky smernice NIS 1 a potrebu reakcie na tento vývoj.

Návrhom zákona sa do právneho poriadku Slovenskej republiky transponuje smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (smernica NIS 2) (Ú. v. EÚ L 333, 27.12.2022) (ďalej len „smernica NIS 2“) a zároveň návrh zákona reaguje na potreby a požiadavky aplikačnej praxe. Návrh zákona modernizuje existujúcu právnu úpravu, čím sa zvýši celková úroveň kybernetickej bezpečnosti na národnej úrovni a znižujú sa riziká, ktoré prichádzajú s rýchlym technologickým vývojom a digitalizáciou.

Najvýraznejšou zmenou v návrhu zákona je zmena prístupu k identifikácii povinných subjektov, tzv. prevádzkovateľov základnej služby. Mechanizmus identifikácie prevádzkovateľa základnej služby sa smernicou NIS 2 mení oproti právnej úprave vyplývajúcej zo smernice NIS 1 tak, že pôvodný mechanizmus kombinovanej identifikácie podľa prílohy zákona č. 69/2018 Z. z. v spojení s prekročením identifikačných kritérií sa nahrádza taxatívnym vymenovaním subjektov priamo v návrhu zákona. Návrhom zákona nedochádza k výraznému nárastu regulovaných odvetví, ale dochádza k rozšíreniu pôsobnosti na ďalšie subjekty. Upravuje sa a precizuje hlásenie kybernetického bezpečnostného incidentu, významnej kybernetickej hrozby, udalosti odvrátenej v poslednej chvíli, zraniteľnosti a riešenie kybernetického bezpečnostného incidentu a podporuje sa dobrovoľné hlásenie. Smernicou NIS 2 sa odstraňuje rozdiel medzi prevádzkovateľom základnej služby a poskytovateľom digitálnej služby, a samotné regulované subjekty – prevádzkovatelia základných služieb, sa de facto rozdeľujú na základe ich dôležitosti do dvoch kategórií, na kľúčové subjekty – prevádzkujúce kritickú základnú službu a dôležité subjekty – ostatní prevádzkovatelia základných služieb. Návrh zákona tak zavádza podľa pravidiel smernice NIS 2 prahovú hodnotu veľkosti subjektu (stredné podniky podľa článku 2 prílohy k odporúčaniu 2003/361/ES alebo presahujúce limity pre stredné podniky), ale do regulácie budú spadať aj subjekty kritického významu bez hodnotenia ich veľkosti. V návrhu zákona sa upravujú a precizujú bezpečnostné opatrenia tak, aby reflektovali nové bezpečnostné štandardy, vrátane kladenia dôrazu na riešenie rizík vyplývajúcich z dodávateľského reťazca. Taktiež sa posilňuje využívanie nástroja analýzy rizík pre aplikáciu bezpečnostných opatrení. Zavádza sa minimálna úroveň bezpečnostných opatrení. Taktiež sa posilňuje dohľadová činnosť zavedením foriem dohľadu, podporuje sa vzdelávanie, dopĺňa sa zodpovednosť a posilňuje sa funkcia manažéra kybernetickej bezpečnosti. Natrvalo sa zavádza inštitút samohodnotenia. Návrh zákona opatreniami zvyšuje odolnosť a kapacity reakcie na kybernetické bezpečnostné incidenty príslušných subjektov.

Návrh zákona je v súlade s Ústavou Slovenskej republiky, s ústavnými zákonmi a nálezmi Ústavného súdu Slovenskej republiky, so zákonmi a ostatnými všeobecne záväznými právnymi predpismi platnými v Slovenskej republike, s medzinárodnými zmluvami, ktorými je Slovenská republika viazaná, ako aj s právom Európskej únie.

Návrh zákona má pozitívne a negatívne vplyvy na rozpočet verejnej správy a pozitívne a negatívne vplyvy na podnikateľské prostredie. Návrh zákona nemá vplyvy na limit verejných výdavkov, sociálne vplyvy, vplyvy na životné prostredie, vplyvy na služby verejnej správy pre občana, vplyvy na informatizáciu spoločnosti a ani vplyvy na manželstvo, rodičovstvo a rodinu.

##### **B. Osobitná časť**

**Čl. I**

**K bodu 1**

Ide o spresnenie predmetu návrhu zákona podľa požiadaviek, ktoré vyplynuli zo smernice NIS 2 a praxe. Predmet návrhu zákona zodpovedá požiadavkám transpozície a predstavuje nevyhnutný súbor nástrojov zabezpečenia kybernetickej bezpečnosti. Návrh zákona upravuje podmienky pre riadenie a zabezpečenie kybernetickej bezpečnosti, správu v oblasti kybernetickej bezpečnosti a organizáciu a pôsobnosť jednotiek CSIRT, úlohy a pôsobnosť národnej autority pre certifikáciu kybernetickej bezpečnosti a kontrolu nad dodržiavaním ustanovení tohto zákona vrátane auditu a dohľadu.

**K bodu 2**

Pôsobnosť návrhu zákona bola upravená na základe požiadaviek vyplývajúcich zo smernice NIS 2 a taktiež na základe požiadavky Úradu jadrového dozoru Slovenskej republiky a Ministerstva obrany. Výnimky, ktoré sa v praxi neosvedčili, boli upravené a zaradené do kategórie sektorových úprav, kedy sa na bezpečnostné opatrenia aplikujú osobitné právne predpisy. Ide napríklad aj o atómový zákon alebo zákon o informačných technológiách verejnej správy.

Návrh zákona sa primerane vzťahuje aj na tie informačné systémy, ktoré sú v pôsobnosti Ministerstva obrany Slovenskej republiky, o ktorých to ustanoví v zmysle spoločných ustanovení ústredný orgán. Ide o primeranú reguláciu tých informačných systémov, ktoré majú dosah na verejný sektor, vrátane civilného (mimo spravodajskej služby).

V prípade osobitnej kategórie konkrétne vymedzených osôb a poskytovaných činností, resp. služieb, sú doplnené podmienky, za ktorých sa ustanovenia návrhu zákona vzťahujú aj na osobu, ktorá nemá sídlo, trvalý pobyt alebo miesto podnikania na území Slovenskej republiky. Uvedené podmienky vyplynuli priamo zo smernice NIS 2. Podmienkami na to, aby mohli byť konkrétne osoby zapísané do registra prevádzkovateľov základnej služby sú, že osoba na území Slovenskej republiky:

* najčastejšie prijíma rozhodnutia týkajúce sa bezpečnostných opatrení na riadenie kybernetických rizík,
* vykonáva opatrenia s cieľom zachovať kybernetickú bezpečnosť a zároveň nie je možné určiť miesto podľa predchádzajúcej odrážky alebo ak osoba neprijíma rozhodnutia podľa prvej odrážky na území členského štátu Európskej únie alebo v štáte, ktorý je zmluvnou stranou zmluvnej strane Dohody o Európskom hospodárskom priestore (ďalej len „členský štát Európskej únie“),
* má prevádzkareň s najvyšším počtom zamestnancov spomedzi prevádzkarní umiestnených v iných členských štátoch Európskej únie,
* má sídlo, trvalý pobyt alebo miesto podnikania zástupca podľa § 21 ods. 1 zákona a zároveň ide o osobu, ktorá nemá sídlo, trvalý pobyt alebo miesto podnikania v členskom štáte Európskej únie.

V návrhu zákona sa precizuje negatívna výnimka zákona č. 69/2018 Z. z., a to že zákon sa nevzťahuje na dohľad a kontrolu plnenia požiadaviek podľa § 2 ods. 1 písm. d) návrhu zákona. Ide o doplnenie výnimky v nadväznosti na prijatie nariadenia Európskeho parlamentu a Rady (EÚ) 2022/2554 zo 14. decembra 2022 o digitálnej prevádzkovej odolnosti finančného sektora a o zmene nariadení (ES) č. 1060/2009, (EÚ) č. 648/2012, (EÚ) č. 600/2014, (EÚ) č. 909/2014 a (EÚ) 2016/1011 (Ú. v. EÚ L 333, 27.12.2022) (ďalej len „nariadenie (EÚ) 2022/2554“).

**K bodom 3 až 7**

Preberajú sa pojmy definované v smernici NIS 2 alebo na ktoré smernica NIS 2 odkazuje, najmä pojmy vyplývajúce z nariadenia Európskeho parlamentu a Rady (EÚ) 2019/881 zo 17. apríla 2019 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013 (akt o kybernetickej bezpečnosti) (Ú. v. EÚ L 151, 7.6.2019) (ďalej len „nariadenie (EÚ) 2019/881“). Ide o vymedzenie základných pojmov na účely zákona č. 69/2018 Z. z. a transpozíciu smernice NIS 2.

**K bodu 8**

Ustanovenie definuje prevádzkovateľa základnej služby zápisom v registri prevádzkovateľov základnej služby, ktorý je vedený Národným bezpečnostným úradom.

**K bodu 9**

Legislatívnotechnická úprava. Ide o precizovanie textu.

**K bodu 10**

Legislatívnotechnická úprava. Ide o zosúladenie názvu Ministerstva dopravy Slovenskej republiky so zmenou vykonanou zákonom č. 172/2022 Z. z.

Návrhom zákona sa dopĺňa Správa štátnych hmotných rezerv Slovenskej republiky medzi orgány verejnej moci, ktoré majú na účel zákona č. 69/2018 Z. z. zavedenú legislatívnu skratku „ústredný orgán“ z dôvodu, že Správa štátnych hmotných rezerv Slovenskej republiky bola identifikovaná v sektore energetika, v podsektore ropa ako ústredný orgán pre subjekt správy zásob ropy, teda pre Agentúru pre núdzové zásoby ropy a ropných výrobkov.

**K bodu 11**

Z čl. 9 smernice NIS 2 vyplynula požiadavka, aby každý členský štát prijal národný plán reakcie na rozsiahle kybernetické incidenty a krízy. V Slovenskej republike bude tento strategický dokument vypracovávať Národný bezpečnostný úrad v spolupráci s príslušnými štátnymi orgánmi. Národný bezpečnostný úrad je zároveň určený ako orgán pre riadenie kybernetických kríz, ktorý plní úlohy národného koordinátora rozsiahlych kybernetických bezpečnostných incidentov a kybernetických kríz.

**K bodu 12**

Národný bezpečnostný úrad je nielen kontaktným miestom pre kybernetickú bezpečnosť pre zahraničie vrátane orgánov Európskej únie, ale aj pre vnútroštátnu spoluprácu. Zároveň sa však vypúšťajú orgány Organizácie Severoatlantickej zmluvy, pretože to nie je požiadavka smernice NIS 2 a komunikáciu a notifikačné povinnosti ohľadom kybernetickej obrany, vo vzťahu k Organizácii Severoatlantickej zmluvy, plní Ministerstvo obrany Slovenskej republiky.

**K bodu 13**

Organizácia Severoatlantickej zmluvy je vojensko-politickou medzinárodnou organizáciou, ktorá plní úlohy kolektívnej obrany. Keďže ide o úlohy vojenskej povahy, v podmienkach kybernetickej domény sú jej aktivity zadefinované ako kybernetická obrana (CYBER DEFENCE). Podľa príslušných ustanovení zákona č. 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy v znení neskorších predpisov, zákona č. 319/2002 Z. z. o obrane Slovenskej republiky  znení neskorších predpisov a zákona č. 500/2022 Z. z. o Vojenskom spravodajstve spadá problematika obrany, vrátane spolupráce v oblasti kybernetickej obrany s Organizáciou Severoatlantickej zmluvy, do kompetencie rezortu Ministerstva obrany Slovenskej republiky, resp. Vojenského spravodajstva, ktoré vystupuje ako národná autorita pre kybernetickú obranu Slovenskej republiky a zároveň ako hlavná národná autorita na úseku medzinárodnej spolupráce pre oblasť kybernetickej obrany.

**K bodu 14**

Pojem „poskytovateľ digitálnych služieb“ sa vypustil a namiesto neho sa doplnili medzi subjekty, s ktorými Národný bezpečnostný úrad spolupracuje pri plnení úloh podľa tohto zákona, „vedecké a akademické inštitúcie“ ako dôležitý článok zabezpečujúci pokrok vo vývoji kybernetickej bezpečnosti. Smernicou NIS2 sa upustilo od delenia medzi poskytovateľom digitálnej služby a prevádzkovateľom základnej služby a tak ako smernica NIS2, aj návrh zákona operuje už len s pojmom prevádzkovateľ základnej služby.

**K bodu 15**

Vzhľadom na to, že návrh zákona už neobsahuje základnú službu, ktorá by mala indikovať zápis jej prevádzkovateľa do registra prevádzkovateľov základnej služby, dochádza k úprave konať vo veci určenia prevádzkovateľa základnej služby. Národný bezpečnostný úrad nielen zapisuje do registra prevádzkovateľov základnej služby, ale zabezpečuje aj výmaz prevádzkovateľa základnej služby z registra prevádzkovateľov základnej služby.

Ku kompetencii Národného bezpečnostného úradu viesť a spravovať register prevádzkovateľov základnej služby a zoznam akreditovaných jednotiek CSIRT pribudla kompetencia viesť a spravovať zoznam autorizovaných orgánov posudzovania zhody, zoznam vydaných európskych certifikátov kybernetickej bezpečnosti a zoznam notifikovaných osôb akreditovaných v rozsahu schémy certifikácie kybernetickej bezpečnosti podľa čl. 49 nariadenia (EÚ) 2019/881.

**K bodu 16**

Ide o kompetenciu Národného bezpečnostného úradu určiť ústredný orgán podľa § 4 písm. b) zákona č. 69/2018 Z. z. v súlade s oblasťami jeho pôsobnosti podľa zákona č. 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy v znení neskorších predpisov a plní úlohy ústredného orgánu pre typ subjektu podľa prílohy č. 1 a  prílohy č. 2. Ide o úpravu, ak by nastala situácia, že pre subjekt nie je možné identifikovať ústredný orgán, napr. vznik nového subjektu.

**K bodom 17 a 18**

Precizovanie textu v súvislosti so skutočnosťou, že Národný bezpečnostný úrad je určený ako orgán pre riadenie kybernetických kríz, ktorý plní úlohy národného koordinátora rozsiahlych kybernetických bezpečnostných incidentov a kybernetických kríz. Ide o rozšírenie kompetencie Národného bezpečnostného úradu v oblasti kybernetickej bezpečnosti na účely plnenia úloh z národného rámca pre riadenie kybernetických kríz. Vzhľadom na skutočnosť, že Národný bezpečnostný úrad systematicky získava, sústreďuje, analyzuje a vyhodnocuje informácie o stave kybernetickej bezpečnosti v Slovenskej republike, ďalej spolupracuje s ústrednými orgánmi podľa § 4 písm. b) zákona č. 69/2018 Z. z., s inými orgánmi štátnej správy podľa § 4 písm. c) zákona č. 69/2018 Z. z., s jednotkami CSIRT a prevádzkovateľmi základných služieb pri plnení úloh podľa zákona č. 69/2018 Z. z., a taktiež prijíma vnútroštátne hlásenia o kybernetických bezpečnostných incidentoch, o kybernetických hrozbách, o udalostiach odvrátených v poslednej chvíli a o zraniteľnostiach, má Národný bezpečnostný úrad spôsobilosť na určenie a vyhlásenie výstrah alebo stavu kybernetickej krízy.

**K bodu 19**

Precizovanie textu v súvislosti so zmenou terminológie vyplývajúcou zo smernice NIS 2.

**K bodu 20**

Ide o precizovanie textu, Národný bezpečnostný úrad doteraz dohľad ako taký nevykonával, pričom smernica NIS 2 nabáda na efektívnejší spôsob dohliadania a kontroly plnenia povinností.. Dohľadom je dohľad nad plnením povinností prevádzkovateľa základnej služby podľa tohto zákona alebo povinností uložených na základe tohto zákona (ďalej len „dohľad“).“

**K bodu 21**

Zosúladenie názvu dotknutého ministerstva so zmenou vykonanou zákonom č. 7/2024 Z. z., ktorým sa mení a dopĺňa zákon č. 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony.

**K bodu 22**

Legislatívnotechnická úprava.

**K bodu 23**

Precizuje sa pôsobnosť Národného bezpečnostného úradu v súvislosti s plnením jeho úlohy ako vnútroštátneho orgánu pre certifikáciu kybernetickej bezpečnosti podľa nariadenia (EÚ) 2019/881. Právomoc vykonávať kontrolu a dozor vyplýva priamo z čl. 58 ods. 7 písm. a) a b) nariadenia (EÚ) 2019/881. Súčasne sa ustanovuje kompetencia prijímať opatrenia podľa čl. 58 ods. 8 písm. c) nariadenia (EÚ) 2019/881. Ide o nevyhnutné vykonanie predmetného nariadenia v oblasti určenia a stanovenia kompetencií vnútroštátneho orgánu pre certifikáciu kybernetickej bezpečnosti.

**K bodu 24**

Návrh zákona v súlade so smernicou NIS 2 ustanovuje ústredné orgány v prílohe č. 1 a v prílohe č. 2. Z tohto dôvodu sa vypúšťa ustanovenie § 5 ods. 1 písm. ac) zákona č. 69/2018 Z. z.

**K bodu 25**

Ide o zosúladenie systému certifikácie kybernetickej bezpečnosti s nariadením (EÚ) 2019/881, v ktorom sa upravil rámec, spôsob prijímania európskych schém certifikácie kybernetickej bezpečnosti a proces certifikácie kybernetickej bezpečnosti informačných a komunikačných technológií. V období prijímania zákona č. 69/2018 Z. z. (január 2018) ešte nebolo prijaté nariadenie (EÚ) 2019/881 (apríl 2019). Na účely certifikácie kybernetickej bezpečnosti návrh zákona ustanovuje, že systémom certifikácie je súbor pravidiel a postupov na riadenie jednotlivých schém certifikácie kybernetickej bezpečnosti. Ďalej sa definuje schéma certifikácie kybernetickej bezpečnosti s tým, že predkladateľ zámerne v súlade s technickou normou ISO/IEC 17000: 2020 (definičná norma) definuje systém a schému a nepoužíva pojem „rámec“ ako sa uvádza v oficiálnom preklade nariadenia (EÚ) 2019/881, ktorý nie je súladný s vyššie uvedenou normou. Ustanovuje sa podmienka, že certifikáciu kybernetickej bezpečnosti pre úrovne záruky základná, významná a vysoká vykonáva len akreditovaná osoba, teda osoba podľa čl. 60 nariadenia (EÚ) 2019/881 a § 19 ods. 2 zákona č. 53/2023 Z. z. o akreditácii orgánov posudzovania zhody. Zároveň sa v súlade s článkom 56 ods. 6 nariadenia (EÚ) 2019/881ustanovuje, že akreditovanou osobou pre certifikáciu kybernetickej bezpečnosti pre úroveň záruky vysoká, môže byť len Národný bezpečnostný úrad ako národná autorita pre certifikáciu kybernetickej bezpečnosti zriadená podľa článku 58 ods. 1 nariadenia (EÚ) 2019/881.

**K bodu 26**

Legislatívnotechnická úprava súvisiaca s vypustením pojmu „digitálna služba“.

**K bodu 27**

Na účely koordinovaného zverejňovania zraniteľností sa Národným bezpečnostným úradom zriadená národná jednotka CSIRT – Národné centrum kybernetickej bezpečnosti, určuje ako koordinátor vo veciach komunikácie o zistených alebo nahlásených zraniteľnostiach medzi prevádzkovateľom základnej služby, výrobcom alebo dodávateľom produktu IKT alebo služby IKT a inými dotknutými osobami. Zo smernice NIS 2 vyplynula pre koordinátora povinnosť zabezpečiť, aby oznamovateľ mohol oznamovať zraniteľnosti aj anonymne (ak o to požiada oznamovateľ). Koordinátor zabezpečuje aj postupovanie informácií o zraniteľnostiach základných služieb, ku ktorým vykonáva služby jednotka CSIRT iného členského štátu Európskej únie, tzn. oznámi zraniteľnosť jednotke CSIRT iného členského štátu Európskej únie a informuje o tom oznamovateľa tejto zraniteľnosti.

**K bodu 28**

Podľa smernice NIS 2 každý členský štát prijme národnú stratégiu kybernetickej bezpečnosti, v ktorej stanoví strategické ciele, zdroje potrebné na dosiahnutie týchto cieľov a vhodné politické a regulačné opatrenia na dosiahnutie a zachovanie vysokej úrovne kybernetickej bezpečnosti. Súčasťou národnej stratégie kybernetickej bezpečnosti sú politiky a akčný plán, ako konkrétny plán čiastkových úloh a zdrojov.

V druhom odseku sa vymedzujú obsahové náležitosti národnej stratégie kybernetickej bezpečnosti.

V treťom odseku sa upravuje zameranie politík, ktoré sa prijímajú v rámci národnej stratégie kybernetickej bezpečnosti. V rámci národnej stratégie kybernetickej bezpečnosti sa prijímajú politiky okrem iného aj podpory aktívnej kybernetickej ochrany za ktoré sa považuje. Podľa bodu 57 recitálu smernice NIS2 členské štáty by mali v rámci svojich národných stratégií kybernetickej bezpečnosti prijať politiky na podporu aktívnej kybernetickej ochrany ako súčasti širšej obrannej stratégie. Aktívna kybernetická ochrana je aktívna prevencia, odhaľovanie, monitorovanie, analýza a zmierňovanie narušení bezpečnosti siete v spojení s využitím spôsobilostí nasadených v zasiahnutej sieti a mimo nej, a nie reaktívne reagovanie. Mohla by zahŕňať poskytovanie bezplatných služieb alebo nástrojov určitým subjektom zo strany členských štátov, a to vrátane samoobslužných kontrol, detekčných nástrojov a služieb odstraňovania. Schopnosť rýchlo a automaticky si vymieňať a pochopiť informácie a analýzy týkajúce sa hrozieb, varovaní pred kybernetickou činnosťou a opatrení reakcie je zásadne dôležitá pre umožnenie jednotného úsilia o úspešnú prevenciu, odhaľovanie, riešenie a blokovanie útokov proti sieťam a informačným systémom. Aktívna kybernetická ochrana je založená na obrannej stratégii, ktorá vylučuje ofenzívne opatrenia.

Vo štvrtom odseku sa vymedzuje spolupráca ústredných orgánov podľa § 4 písm. b) a iných orgánov štátnej správy podľa § 4 písm. c) s Národným bezpečnostným úradom pri vypracovávaní národnej stratégie kybernetickej bezpečnosti. Uvedené orgány sú povinné poskytnúť súčinnosť Národnému bezpečnostnému úradu v podobe poskytovania informácií v potrebnom rozsahu.

Podľa piateho odseku národnú stratégiu kybernetickej bezpečnosti na návrh Národného bezpečnostného úradu schvaľuje vláda Slovenskej republiky, na obdobie piatich rokov.

Podľa smernice NIS 2 každý členský štát prijme národný plán reakcie na rozsiahle kybernetické incidenty a krízy, v ktorom sa stanovia ciele a spôsoby riadenia rozsiahlych kybernetických incidentov a kríz.

V šiestom odseku sa vymedzujú obsahové náležitosti národného plánu reakcie na rozsiahle kybernetické bezpečnostné incidenty a kybernetické krízy.

Podľa siedmeho odseku národný plán reakcie na rozsiahle kybernetické bezpečnostné incidenty a kybernetické krízy na návrh Národného bezpečnostného úradu schvaľuje vláda Slovenskej republiky a aktualizuje sa podľa potreby. Tomuto procesu predchádza riadne pripomienkové konanie v rámci Slov-Lexu, keďže ide o nelegislatívne materiály, ktoré sa predkladajú na rokovanie vlády Slovenskej republiky.

V ôsmom odseku sa vymedzuje spolupráca ústredných orgánov podľa § 4 písm. b) a iných orgánov štátnej správy podľa § 4 písm. c) s Národným bezpečnostným úradom pri vypracovávaní národného plánu reakcie na rozsiahle kybernetické bezpečnostné incidenty a kybernetické krízy. Uvedené orgány sú povinné poskytnúť súčinnosť Národnému bezpečnostnému úradu v podobe poskytovania informácií v potrebnom rozsahu.

**K bodu 29**

V súlade so zmenami sa upravuje aj obsah verejnej časti jednotného informačného systému kybernetickej bezpečnosti. Keďže sa upúšťa od pojmu „základná služba“ a aj „poskytovateľ digitálnych služieb“, jednotný informačný systém kybernetickej bezpečnosti už takéto registre neobsahuje. K obsahu vyplývajúcemu zo smernice NIS 1 [písmená a) až g)], sa doplnil nástroj na registráciu zmien, hlásenie zmien a ostatné súvisiace nástroje. Ide o nástroje, ktoré sú primárne určené prevádzkovateľom základnej služby na účely ich registrácie do registra prevádzkovateľov základnej služby a s tým súvisiacich hlásení zmien, ako aj nástroje na vykonanie samohodnotenia, pomôcky a návody. Komunikačný systém pre hlásenie a riešenie kybernetických bezpečnostných incidentov je komunikačný systém, ktorý zaisťuje systematický zber a vyhodnocovanie informácií o kybernetických bezpečnostných incidentoch a ich analýzu. Dopĺňa sa jeho funkcia zabezpečovať komunikáciu medzi národnou jednotkou CSIRT, vládnou jednotkou CSIRT a akreditovanými jednotkami CSIRT v Slovenskej republike a takýmito jednotkami CSIRT v iných členských štátoch Európskej únie.

**K bodu 30**

Legislatívnotechnická úprava súvisiaca s prebratím terminológie z čl. 6 bodu 10 smernice NIS 2.

**K bodu 31**

Legislatívnotechnická úprava súvisiaca s vypustením pojmu „poskytovateľ digitálnej služby“.

**K bodu 32**

Legislatívnotechnická úprava v súvislosti s novým obsahom prílohy č. 1 a prílohy č. 2.

**K bodu 33**

Ustanovenia o kritériách základnej služby sa vypúšťajú, keďže návrh zákona na základe ustanovení smernice NIS 2, kde je podstatný subjekt, nie jeho služba, už tento pojem nepozná.

**K bodu 34**

Legislatívnotechnická úprava v súvislosti so zmenou prístupu k identifikácii povinných subjektov, tzv. prevádzkovateľov základnej služby.

**K bodu 35**

Legislatívnotechnická úprava. Ide o precizovanie textu v súvislosti s vypustením pojmu „základná služba“.

**K bodom 36, 38 a 41**

Legislatívnotechnická úprava súvisiaca s vypustením pojmu „poskytovateľ digitálnej služby“.

**K bodu 37**

Legislatívnotechnická úprava. Ide o precizovanie textu. Nie je porušením povinnosti zachovávať mlčanlivosť v prípadoch vyhlasovania kybernetickej krízy ako novej kompetencie úradu v zmysle smernice NIS 2.

**K bodu 39**

Precizovanie textu v súvislosti so zmenou terminológie vyplývajúcou zo smernice NIS 2.

**K bodu 40**

Preventívne služby poskytované jednotnou CSIRT sa zameriavajú na prevenciu, predchádzanie vzniku kybernetických bezpečnostných incidentov. Do preventívnych služieb sa dopĺňajú ďalšie úlohy jednotiek CSIRT podľa požiadaviek smernice NIS 2.

**K bodu 42**

Jednotky CSIRT môžu pri výkone svojich úloh podľa § 15 ods. 2 a 3 zákona uprednostňovať konkrétne úlohy na základe prístupu založeného na rizikách.

**K bodu 43**

Pre toho, kto plní úlohy jednotky CSIRT, sa dopĺňa povinnosť zabezpečovať vnútroštátnu spoluprácu (medzi ním, Národným bezpečnostným úradom, ústrednými orgánmi podľa zákona, ostatnými jednotkami CSIRT). Okrem toho ten, kto plní úlohy jednotky CSIRT, zabezpečuje účasť na partnerských preskúmaniach organizovaných v rámci spolupráce medzi členskými štátmi Európskej únie, Európskou komisiou a Agentúrou Európskej únie pre kybernetickú bezpečnosť (ENISA).

**K bodu 44**

Mechanizmus identifikácie prevádzkovateľa základnej služby sa smernicou NIS 2 mení oproti právnej úprave vyplývajúcej zo smernice NIS 1. Pôvodný mechanizmus identifikácie podľa prílohy č. 1 v spojení s prekročením identifikačných kritérií uvedených v § 18 zákona sa nahrádza taxatívnym vymenovaním subjektov v § 17 ods. 1 zákona, teda podniky, ktoré možno zapísať do registra prevádzkovateľov základnej služby sú priamo identifikovateľné zo zákona bez potreby vydania ďalšieho usmerňujúceho vykonávacieho predpisu. Pri identifikovaní prevádzkovateľa základnej služby Národný bezpečnostný úrad nevylučuje, že môžu vnikať anomálie z dôvodu, že zákon musí byť všeobecný, aby v príslušnej oblasti upravoval všetky základné spoločenské vzťahy. Základná služba (a teda ani jej rozsah) sa nedefinuje, upustila od toho smernica NIS 2, definuje sa iba prevádzkovateľ základnej služby a kritická základná služba. Pri posudzovaní, či subjekt spadá pod reguláciu zákona č. 69/2018 Z. z. sa bude brať do úvahy aj to, či podniky spadajú do niektorého sektora iba okrajovo (ako napríklad pri elektroenergetike, ak si podnik vyrába elektrickú energiu iba pre seba a príležitostne predáva iba prebytky, ktoré nespotreboval).

Ak pôjde o prepojený podnik, pričom jeden podnik nespadá pod reguláciu smernice NIS 2, ale je prepojený k podniku, ktorý spadá pod reguláciu smernice NIS 2, tak sa bude prihliadať na každý podnik samostatne.

Do registra prevádzkovateľov základnej služby sa zapisuje okrem iných taxatívne vymedzených subjektov aj subjekt hospodárskej mobilizácie, ktorému bolo uložené opatrenie podľa osobitného predpisu, tzn. Nemá ísť o každý subjekt hospodárskej mobilizácie ale ten, ktorému bola uložená povinnosť napr. počas krízovej situácie alebo mimoriadnej situácie niečo plniť. Cieľom tejto úpravy je aby sa za prevádzkovateľa základnej služby nepovažovali napr. domovy sociálnych služieb, ktoré sú síce subjektom hospodárskej mobilizácie ale neplnia opatrenia uložené podľa osobitného predpisu.

V § 17 ods. 2 zákona sa ustanovuje oznamovacia povinnosť pre toho, kto vykonáva činnosti v sektoroch podľa prílohy č. 1 alebo prílohy č. 2 zákona a pre toho, kto poskytuje službu registrácie názvu domény. Oznámenie sú povinní adresovať Národnému bezpečnostnému úradu do 60 dní odo dňa, kedy začali vykonávať relevantnú činnosť. Na realizáciu oznámenia sa využíva jednotný informačný systém kybernetickej bezpečnosti (§ 8 ods. 2 písm. i) zákona). Toto ustanovenie upravuje aj obsahové náležitosti oznámenia.

Podľa § 17 ods. 3 zákona Národný bezpečnostný úrad zapisuje do registra prevádzkovateľov základnej služby osobu uvedenú v odseku 1 aj na základe vlastnej iniciatívy, a to bez ohľadu na splnenie podmienok veľkosti po predchádzajúcej konzultácii s príslušným ústredným orgánom, pričom sa vždy postupuje tak, aby bol každý takýto zápis odôvodený a primeraný a ďalej na návrh ústredného orgánu (§ 4 písm. b) zákona) alebo na základe oznámenia osoby, ktorá vykonáva činnosti podľa prílohy č. 1 alebo prílohy č. 2.

Ustanovenia § 17 ods. 4 až 6 sa prijímajú za účelom transpozície článku 3 ods. 3 a 4 smernice NIS 2, pričom sa má zabezpečiť jasný prehľad o subjektoch, ktoré patria do rozsahu pôsobnosti tejto smernice, kde členské štáty majú zostaviť zoznam kľúčových a dôležitých subjektov (prevádzkovateľov základných služieb) ako aj subjektov poskytujúcich služby registrácie názvov domén. Na tento účel by členské štáty mali od subjektov vyžadovať, aby príslušným orgánom predložili aspoň tieto informácie, t. j. názov, adresu a aktuálne kontaktné údaje vrátane e-mailových adries, rozsahov IP adries a telefónnych čísel subjektu, a podľa potreby príslušné odvetvie a pododvetvie uvedené v prílohách smernice NIS 2, ako aj prípadne zoznam členských štátov, v ktorých poskytujú služby patriace do rozsahu jej pôsobnosti.

Zároveň je potrebné zabezpečiť jednoznačný prehľad poskytovateľov služieb DNS, správcov TLD, subjektov poskytujúcich služby registrácie domén pre TLD, poskytovateľov služieb cloud computingu, poskytovateľov služieb dátových centier, poskytovateľov sietí na sprístupňovanie obsahu, poskytovateľov riadených služieb, poskytovateľova riadených bezpečnostných služieb, ako aj o poskytovateľov online trhov, internetových vyhľadávačov a platforiem služieb sociálnych sietí, ktorí poskytujú služby v celej Únii a patria do pôsobnosti smernice, tak aby agentúra ENISA mohla zriadiť a viesť register takýchto subjektov na základe informácií poskytnutých členským štátom.

Vykonanie zápisu do registra prevádzkovateľov základnej služby oznamuje Národný bezpečnostný úrad prostredníctvom jednotného informačného systému kybernetickej bezpečnosti a zároveň toto oznámenie o zápise doručuje do elektronickej schránky podľa osobitného predpisu, ktorým je zákon o e-Governmente. Osobitné rozhodnutie o vykonaní zápisu sa nevyhotovuje. Práva a povinnosti prevádzkovateľa základnej služby vznikajú konkrétnemu prevádzkovateľovi základnej služby dňom uvedeným v oznámení o zápise do registra prevádzkovateľov základnej služby. Tento deň nemôže byť určený skôr ako tridsiaty deň nasledujúci po dni zápisu.

Národný bezpečnostný úrad vykonáva zmeny v zapísaných skutočnostiach v registri prevádzkovateľov základnej služby aj bez návrhu. Na tento účel má prevádzkovateľ základnej služby povinnosť najneskôr do 14 dní písomne oznamovať zmeny zapísaných údajov (okrem referenčných údajov) prostredníctvom jednotného informačného systému kybernetickej bezpečnosti Národnému bezpečnostnému úradu.

V § 17 ods. 7 zákona sa dopĺňa kompetencia Národného bezpečnostného úradu vymazať prevádzkovateľa základnej služby z registra prevádzkovateľov základnej služby,

* na základe odôvodnenej žiadosti prevádzkovateľa základnej služby, po predchádzajúcej konzultácií s príslušným ústredným orgánom, najneskôr do 60 dní odo dňa doručenia odôvodnenej žiadosti,
* na základe oznámenia ústredného orgánu (§ 4 písm. b) zákona), alebo
* z vlastnej iniciatívy.

V § 17 ods. 8 zákona sa dopĺňa povinnosť Národného bezpečnostného úradu informovať prevádzkovateľa základnej služby o tom, že bol vymazaný z registra prevádzkovateľov základnej služby.

V § 18 sa identifikuje kritická základná služba taxatívnym vymenovaním základných služieb, ktoré sú kritickými základnými službami. Ak prevádzkovateľ základnej služby vykonáva aspoň jednu z kritických základných služieb, vzniká mu povinnosť túto skutočnosť oznámiť Národnému bezpečnostnému úradu. Národný bezpečnostný úrad zapisuje do registra prevádzkovateľov základných služieb informácie o kritických základných službách, o zmenách v týchto skutočnostiach a o ich prevádzkovateľoch.

**K bodu 45**

Ide o precizovanie textu pôvodného § 19 ods. 1. Ide o odstránenie duplicity pri prijímaní bezpečnostných opatrení (§ 20 zákona). Aby prevádzkovateľ základnej služby nemusel prijímať všeobecné bezpečnostné opatrenia a ešte následne aj duplicitne sektorové bezpečnostné opatrenia, pristúpilo sa k právnej úprave, že ak sú osobitným predpisom ustanovené sektorové bezpečnostné opatrenia, prevádzkovateľ základnej služby má povinnosť ich (sektorové bezpečnostné opatrenia) prijať, dodržiavať a vykonávať. Prevádzkovateľ základne služby v takom prípade nemá povinnosť prijať, dodržiavať a vykonávať všeobecné bezpečnostné opatrenia; povinnosť prijímať opatrenia podľa § 20 ods. 4 tým nie je dotknutá*.* Ako príklady osobitných predpisov, ktoré upravujú sektorové bezpečnostné opatrenia sú uvedené nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554 zo 14. decembra 2022 o digitálnej prevádzkovej odolnosti finančného sektora a o zmene nariadení (ES) č. 1060/2009, (EÚ) č. 648/2012, (EÚ) č. 600/2014, (EÚ) č. 909/2014 a (EÚ) 2016/1011 (Ú. v. EÚ L 333, 27.12.2022) (ďalej len „nariadenie (EÚ) 2022/2554“), zákon č. 95/2019 Z. z., zákon č. 541/2004 Z. z., vyhláška Úradu jadrového dozoru Slovenskej republiky č. 430/2011 Z. z. o požiadavkách na jadrovú bezpečnosť v znení vyhlášky č. 103/2016 Z. z. Uvedené platí a sa vzťahuje aj na prevádzkovateľa kritickej základnej služby, keďže systematika celého zákona je navrhnutá tak, že všade, kde sa hovorí o „prevádzkovateľovi základnej služby“ myslí sa tým aj prevádzkovateľ kritickej základnej služby“ ak zákon neustanovuje výnimku, že nejde o prevádzkovateľa základnej služby, ktorý prevádzkuje kritickú základnú službu.

**K bodu 46**

V súlade so smernicou NIS2 sa posilňuje bezpečnosť a kontrola celého dodávateľského reťazca. V praxi totiž dochádzalo k neželaným situáciám, kedy dodávateľ nebol prevádzkovateľom základnej služby nijako kontrolovaný a prevádzkovateľ základnej služby si nemohol plnenie bezpečnostných opatrení prostredníctvom dodávateľa overiť. Tretia strana - dodávateľ, je počas trvania zmluvného vzťahu povinná vykonávať a realizovať bezpečnostné opatrenia v súlade s písomnou zmluvou a týmto zákonom a je povinná podrobiť sa kontrole plnenia týchto opatrení zo strany prevádzkovateľa základnej služby ako aj úradu, ak ide o prevádzkovateľa kritickej základnej služby.

**K bodu 47**

Legislatívnotechnická úprava súvisiaca s vypustením pojmu „poskytovateľ digitálnej služby“. Výnimka pre tretiu stranu, ak nejde o prevádzkovateľa základnej služby, ktorý prevádzkuje kritickú základnú službu je už obsiahnutá v zákone č. 69/2018 Z. z., a to povinnosť uzatvoriť zmluvu podľa odseku 2 neplatí, ak je tretia strana prevádzkovateľom základnej služby. Pod pojmom „prevádzkovateľ základnej služby“ sa rozumie aj prevádzkovateľ základnej služby, ktorý prevádzkuje kritickú základnú službu.

**K bodom 48 a 49**

Ustanovujú sa ďalšie povinnosti prevádzkovateľovi základnej služby vyplývajúce zo smernice NIS 2 ako aj bezpečnostných štandardov v oblasti kybernetickej bezpečnosti s cieľom vytvoriť efektívny systém riadenia kybernetickej bezpečnosti, pri ktorej nechýba efektívna výmena informácii a podpora analýzy rizík a závislostí v rámci dodávateľského reťazca. Ide o doplnenie elementárnych a nevyhnutných povinností prevádzkovateľa základnej služby v zmysle požiadaviek smernice NIS 2.

**K bodu 50**

Legislatívnotechnická úprava.

**K bodu 51**

V návrhu zákona sa upravujú a precizujú bezpečnostné opatrenia tak, aby reflektovali nové bezpečnostné štandardy, vrátane kladenia dôrazu na riešenie rizík vyplývajúcich z dodávateľského reťazca subjektu a jeho vzťahu s dodávateľmi, pretože sa vyskytli incidenty, keď sa subjekty stali obeťami kybernetických útokov spôsobom, že páchatelia dokázali ohroziť bezpečnosť sietí a informačných systémov subjektu využitím zraniteľností v produktoch a službách tretích strán.

V § 20 ods. 1 zákona sa precizuje definícia bezpečnostných opatrení. V § 20 ods. 2 zákona sú vymenované minimálne požadované oblasti, ktoré by sa mali prijímať v bezpečnostných opatreniach a rovnako tak toto ustanovenie reflektuje požiadavky ustanovené v článku 20 smernice NIS 2. Bezpečnostné opatrenia by sa mali zaoberať aj fyzickou a environmentálnou bezpečnosťou sietí a informačných systémov tým, že budú zahŕňať opatrenia na ochranu takýchto systémov pred systémovými zlyhaniami, ľudskými chybami, zlomyseľným konaním alebo prírodnými javmi v súlade s európskymi a medzinárodnými normami, ako sú normy uvedené v sérii ISO/IEC 27000. V tejto súvislosti by sa prevádzkovatelia základných služieb mali v rámci svojich opatrení na riadenie kybernetických rizík zaoberať aj bezpečnosťou ľudských zdrojov a mali by mať zavedené vhodné postupy kontroly prístupu. Predpokladá sa, že bezpečnostné opatrenia budú v súlade aj so smernicou (EÚ) 2022/2557.

V § 20 ods. 3 zákona sa konštatuje, že bezpečnostné opatrenia sa prijímajú a realizujú v rozsahu a spôsobom podľa vyhlášky č. 362/2018 Z. z. alebo podľa osobitného predpisu, ak je vydaný. Týmto ustanovením má zákonodarca za cieľ pokryť sektorovú úpravu, ktorá môže byť prijatá a vtedy platí, že sa prijímajú a realizujú bezpečnostné opatrenia záväzné pre daný sektor.

**K bodu 52**

Rozširuje sa minimálne požadovaný obsah bezpečnostných opatrení. Každý prevádzkovateľ základnej služby si má určiť a prideliť úlohy, role a ich zodpovednosť podľa svojich podmienok a zároveň má pre tieto u neho zavedené role zabezpečiť primerané vzdelávanie a preškoľovanie. Prevádzkovateľ základnej služby si má určiť osobu, ktorá mu bude zodpovedať za schvaľovanie bezpečnostných opatrení, za dohľad, za kontrolu, za audit, za zabezpečenie primeranosti zdrojov na riadenie kybernetickej bezpečnosti a za vzdelávanie. Ako minimálny požadovaný štandard z pohľadu bezpečnostných opatrení sa určuje aspoň dodržiavanie základnej kybernetickej hygieny. Z pohľadu bezpečnosti sa odporúča prevádzkovateľom základnej služby využívať, a teda aj obstarávať certifikované produkty IKT, služby IKT a procesy IKT. V súvislosti s bezpečnostnými opatreniami je potrebné klásť dôraz aj na riešenie rizík vyplývajúcich z dodávateľského reťazca subjektu a jeho vzťahu s dodávateľmi, ako sú poskytovatelia služieb ukladania a spracúvania údajov alebo poskytovatelia riadených bezpečnostných služieb a vydavatelia softvéru. Toto je obzvlášť dôležité vzhľadom na výskyt incidentov, keď sa subjekty stali obeťami kybernetických útokov, pri ktorých páchatelia dokázali ohroziť bezpečnosť sietí a informačných systémov subjektu využitím zraniteľností v produktoch a službách tretích strán. Aj malé a stredné podniky sa čoraz viac stávajú terčom útokov na dodávateľské reťazce z dôvodu ich menej prísnych opatrení na riadenie kybernetických rizík a zvládanie útokov a skutočnosti, že majú obmedzené bezpečnostné zdroje. Takéto útoky na dodávateľské reťazce majú vplyv nielen na samotné malé a stredné podniky a ich izolovanú činnosť, ale môžu mať aj kaskádový účinok na väčšie útoky na subjekty, ktorým poskytli dodávky. Kľúčové subjekty a dôležité subjekty by preto mali posúdiť a zohľadniť celkovú kvalitu a odolnosť produktov a služieb, opatrenia na riadenie kybernetických rizík, ktoré zahŕňajú, a tiež postupy svojich dodávateľov a poskytovateľov služieb v oblasti kybernetickej bezpečnosti vrátane ich bezpečných vývojových postupov.

**K bodu 53**

Legislatívnotechnická úprava.

**K bodu 54**

Ustanovenia upravujú pôsobnosť tohto zákona na niektoré subjekty, u ktorých dochádza k cezhraničnému poskytovaniu niektorých služieb. V § 21 ods. 1 zákona sa ustanovuje osobitná povinnosť pre osobu, ktorá poskytuje niektorú zo služieb alebo vykonávajúcu niektorú z činností podľa § 2 ods. 2 zákona, alebo pre osobu, ktorá je treťou stranou, a ktorá nemá sídlo, trvalý pobyt alebo miesto podnikania na území členského štátu Európskej únie a poskytuje tieto služby alebo vykonáva tieto činnosti na území Slovenskej republiky určiť si zástupcu na území Slovenskej republiky alebo na území členského štátu Európskej únie, v ktorom tiež poskytuje služby alebo vykonáva činnosti. Taktiež sa upravuje spolupráca Národného bezpečnostného úradu s príslušnými orgánmi členských štátov Európskej únie vo vzťahu ku subjektom, u ktorých dochádza k cezhraničnému poskytovaniu niektorých služieb. Takéto subjekty majú povinnosť hlásiť prostredníctvom jednotného informačného systému kybernetickej bezpečnosti určité požadované údaje a taktiež hlásiť zmeny týchto údajov. Národný bezpečnostný úrad následne oznamuje vybrané údaje Agentúre Európskej únie pre kybernetickú bezpečnosť na účely vedenia registra poskytovateľov služieb DNS, správcov TLD, subjektov poskytujúcich služby registrácie názvov domén, poskytovateľov služieb cloud computingu, poskytovateľov služieb dátového centra, poskytovateľov sietí na sprístupňovanie obsahu, poskytovateľov riadených služieb, poskytovateľov riadených bezpečnostných služieb, ako aj poskytovateľov online trhov, internetových vyhľadávačov a platforiem služieb sociálnych sietí.

V § 22 zákona sa ustanovuje pre osoby, ktoré zabezpečujú správu TLD a pre osoby, ktoré poskytujú služby registrácie názvov domén povinnosť viesť osobitnú evidenciu registračných údajov názvu domény, povinnosť prijať vnútorné predpisy a zaviesť osobitné postupy na zabezpečenie overovania údajov predkladaných pri registrácii názvov domén, povinnosť vybrané údaje zverejňovať a povinnosti v súvislosti s poskytovaním vybraných údajov orgánom verejnej moci

**K bodu 55**

Legislatívnotechnická úprava súvisiaca s vypustením poskytovateľa digitálnej služby.

**K bodu 56**

Povinnosť prevádzkovateľa základnej služby hlásiť všetky závažné kybernetické incidenty zostáva nezmenená oproti predchádzajúcej právnej úprave. V § 24 ods. 2 zákona sa však mení definícia závažného kybernetického incidentu. Zrušilo sa delenie závažných kybernetických incidentov na kategórie. V § 24 ods. 3 sa ustanovuje spôsob hlásenia kybernetického bezpečnostného incidentu, prostredníctvom jednotného informačného systému kybernetickej bezpečnosti, pričom sa určujú lehoty na hlásenie kybernetického bezpečnostného incidentu v súlade so smernicou NIS2. Dopĺňa sa prevádzkovateľovi základnej služby povinnosť hlásiť okrem závažných kybernetických incidentov aj povinnosť hlásiť významnú kybernetickú hrozbu, udalosť odvrátenú na poslednú chvíľu, ktorá mohla spôsobiť závažný kybernetický incident a zraniteľnosť ním prevádzkovaných verejne dostupných sietí a informačných systémov, ktorá podľa dostupných informácií a technických znalostí by mohla byť zneužitá na spôsobenie závažného kybernetického incidentu a prevádzkovateľ základnej služby nemohol v primeranom čase prijať opatrenia na jej odstránenie alebo zníženie rizika. Prevádzkovateľovi základnej služby a iným osobám, a to aj nad rozsah povinného hlásenia, sa umožňuje dobrovoľne hlásiť kybernetické bezpečnostné incidenty, kybernetické hrozby a udalosti odvrátené na poslednú chvíľu.

Navrhovaná povinnosť podľa odseku 8 prevádzkovateľa základnej služby, na ktorého sa vzťahuje nariadenie (EÚ) 2022/2554, plní povinnosť podľa odseku 1, prostredníctvom príslušného orgánu, za ktorý sa považuje Národná banka Slovenska, úradu v rozsahu a v lehotách ustanovených v nariadení (EÚ) 2022/2554. Cieľom tohto ustanovenia je akceptovať, že nariadenie (EÚ) 2022/2554 je lex specialis voči smernici NIS 2 a ak si prevádzkovateľ základnej služby plní povinnosť podľa tohto nariadenia, plní si túto povinnosť len raz prostredníctvom Národnej banky Slovenska, ktorej skutočnosti prevádzkovateľ základnej služby hlási. Cieľom navrhovanej úpravy je, aby si prevádzkovateľ plnil túto povinnosť len raz, ale zároveň, aby Národný bezpečnostný úrad, ako regulátor v oblasti kybernetickej bezpečnosti, mal relevantné informácie v danej oblasti nevyyhnutné pre riešenie kybernetického bezpečnostného incidentu.. Cieľom návrhu zákona je odstránenie duplicity podľa nariadenia (EÚ) 2022/2554 a smernice NIS 2.

**K bodom 57 a 58**

Legislatívnotechnická úprava.

**K bodu 59**

Vypustenie ustanovení § 25 a 26 vyplýva z dôvodu transpozície smernice NIS 2.

**K bodom 60 až 64**

Úprava problematiky reakcie na kybernetické bezpečnostné incidenty a kybernetické hrozby a ich riešenie v súlade so smernicou NIS 2.

**K bodom 65 a 66**

Keďže došlo k zrušeniu jednotlivých kategórií závažného kybernetického bezpečnostného incidentu, je potrebné upraviť aj príslušné ustanovenia týkajúce sa spolupráce s orgánmi, ktoré majú v regulácii obranu kybernetického priestoru, konkrétne s Ministerstvom obrany Slovenskej republiky, resp. Vojenským spravodajstvom. V texte dochádza k vypusteniu kybernetického bezpečnostného incidentu kategórie tretieho (III) stupňa a poskytovateľa digitálnej služby.

V rámci novej kompetencie úradu v oblasti vyhlasovania stavu kybernetickej krízy je nutné upraviť celý proces tak, aby nedochádzalo k zamieňaniu tohto stavu s vyhlasovaním ústavného stavu. Ustanovujú sa postupy pred samotným vyhlásením stavu kybernetickej krízy, informačná povinnosť zo strany úradu voči zainteresovaným subjektom ako aj postupy jeho odvolania. Všetky opatrenia a činnosti vykonávané v stave kybernetickej krízy vychádzajú z dokumentu, ktorý schvaľuje vláda Slovenskej republiky – Národný plán reakcie na kybernetické bezpečnostné incidenty a krízy.

**K bodu 67**

Vypustenie ustanovenia z dôvodu aplikačnej praxe.

**K bodu 68**

Legislatívnotechnická úprava súvisiaca so zmenou návrhu zákona spočívajúca v skutočnosti, že kontrola je upravená v rámci dohľadu.

**K bodu 69**

Samohodnotenie, ako spôsob preverenia účinnosti prijatých bezpečnostných opatrení pre určené siete a informačné systémy sa počas prechodného obdobia, do konca roka 2023, osvedčilo a tento inštitút sa tak zavádza natrvalo. Podmienkou je, aby išlo o prevádzkovateľa základnej služby, ktorý neprevádzkuje kritickú základnú službu.

**K bodu 70**

Legislatívnotechnická úprava, z dôvodu vypustenia klasifikácie informácií a kategorizácie sietí a informačného systému zo zákona. Uvedené je plnohodnotne nahradené povinnosťou vykonať analýzu rizík.

**K bodu 71**

Ustanovuje sa podmienka, že certifikačný orgán certifikujúci audítora kybernetickej bezpečnosti je výlučne subjekt verejnej správy akreditovaný spôsobom ako doteraz, teda akreditovaný podľa zákona č. 505/2009 Z. z. ako orgán certifikujúci osoby v oblasti kybernetickej bezpečnosti. Zmena vyplýva z aplikačnej praxi a z nutnosti podporiť a vytvoriť dôveryhodný systém.

**K bodu 72**

Prevádzkovateľovi základnej služby (okrem prevádzkovateľa kritickej základnej služby) sa umožňuje zabezpečiť splnenie povinnosti vykonať audit kybernetickej bezpečnosti v lehote do dvoch rokov odo dňa zaradenia prevádzkovateľa základnej služby do registra prevádzkovateľov základných služieb vykonaním preverenia účinnosti prijatých bezpečnostných opatrení a plnenia požiadaviek ustanovených týmto zákonom funkcionalitou jednotného informačného systému kybernetickej bezpečnosti spôsobom podľa odseku 8, t. j. preverenie účinnosti podľa predchádzajúcej vety vykonáva audítor kybernetickej bezpečnosti (tzv. samohodnotenie). Ďalej sa navrhuje sa, aby subjekt, ktorý sa podrobí samohodnoteniu bol povinný vykonať audit minimálne raz za šesť rokov (teda každé tretie samohodnotenie bude musieť byť nahradené auditom v zmysle zákona). Pravidlá samohodnotenia a periodicita samohodnotenia budú upravené vo vyhláške č. 493/2022 Z. z. v súlade s navrhovanou zmenou splnomocňovacieho ustanovenia § 32 návrhu zákona.

V § 29 ods. 9 sa ustanovuje, že prevádzkovateľ základnej služby, na ktorého sa vzťahuje nariadenie (EÚ) 2022/2554, vykonáva preverenie účinnosti prijatých bezpečnostných opatrení podľa nariadenia (EÚ) 2022/2554 osobou podľa odseku 3. Osoba podľa odseku 3 je subjekt verejnej správy akreditovaný ako orgán certifikujúci osoby v oblasti kybernetickej bezpečnosti. Znalostné štandardy sú ustanovené vo vyhláške č. 492/2022 Z. z. a pravidlá auditu kybernetickej bezpečnosti vo vyhláške č. 493/2022 Z. z. Na úrovni týchto vykonávacích právnych predpisov sa bude riešiť situácia, keď napr. nariadenie (EÚ) 2022/2554 alebo iné predpisy ustanovia nové štandardy na osobu audítora v sektorovej oblasti, tak sa upraví resp. rozšíri subjekt, kto sa považuje za certifikovaného audítora na účely auditu kybernetickej bezpečnosti. Táto formulácia opäť priznáva, že nariadenie (EÚ) 2022/2554 je lex specialis vo vzťahu k NIS 2 a potvrdzuje systematiku návrhu zákona, že ak existuje sektorová regulácia, prevádzkovateľ základnej služby postupuje v zmysle tejto regulatívy.

**K bodu 73**

Smernica NIS 2 určila pre členské štáty povinnosť zabezpečiť dohľad nad kybernetickou bezpečnosťou a nad plnením povinností z nej vyplývajúcich.

V § 29a zákona sa ustanovujú pre Národný bezpečnostný úrad formy dohľadu, konkrétne ide o dohľad v podobe vybavovania sťažností, dohľad v podobe vykonávania kontrol, dohľad v podobe ukladania opatrení na zastavenie porušovania povinností a na nápravu nezákonného stavu, dohľad v podobe schvaľovania dohody o náprave a dohľad v podobe ukladania sankcií za porušenie tohto zákona. Zároveň sa tu vymedzuje pôsobnosť dohľadu Národného bezpečnostného úradu, t. j. že sa vykonáva dohľad vo vzťahu k prevádzkovateľom základnej služby, ktorí majú sídlo na území Slovenskej republiky alebo na ktorého sa vzťahuje tento zákon podľa § 2 ods. 2 tohto zákona. Ustanovenie definuje základné princípy výkonu dohľadu nad prevádzkovateľmi základnej služby a taktiež negatívnym vymedzením určuje úlohu dohľadu. Dohľad je neverejný, s cieľom zabezpečiť, aby informácie získané pri dohľade Národným bezpečnostným úradom, nemohli byť nijakým spôsobom zneužité a nemohli spôsobiť zníženie úrovne kybernetickej bezpečnosti dohliadaného u prevádzkovateľa základnej služby.

V § 29b zákona je upravený dohľad v podobe vybavovania sťažností, pri ktorom sa aplikuje zákon č. 9/2010 Z. z. o sťažnostiach v znení neskorších predpisov. Národný bezpečnostný úrad rieši sťažnosti týkajúce sa porušenia povinností prevádzkovateľa základnej služby, ak ich podá odberateľ základnej služby alebo osoba, ktorej hlavným predmetom činnosti je ochrana a presadzovanie práv a právom chránených záujmov odberateľov základnej služby alebo oblasť kybernetickej bezpečnosti. Národný bezpečnostný úrad nebude vybavovať sťažnosti, ktoré vyplynuli zo sporov medzi dvoma alebo viacerými prevádzkovateľmi základnej služby alebo ich dodávateľmi, pokiaľ títo nie sú v postavení odberateľa služby a nesúvisia s odberaním tejto služby. V prípade ak prevádzkovateľ základnej služby, proti ktorému je sťažnosť podaná nespadá do jurisdikcie Slovenskej republiky, Národný bezpečnostný úrad nie je oprávnený proti takémuto prevádzkovateľovi základnej služby konať ale je povinný sťažnosť odstúpiť príslušnému orgánu iného členského štátu Európskej únie.

V § 29c až §29h zákona sa upravuje kontrola. Na rozdiel od predchádzajúcej právnej úpravy sa už neaplikuje zákon NR SR č. 10/1996 Z. z. o kontrole v štátnej správe v znení neskorších predpisov, v jednotlivých ustanoveniach je upravený celý proces kontrol. Vykonávať kontrolu plnenia povinností prevádzkovateľa základnej služby podľa tohto zákona alebo povinností uložených prevádzkovateľovi základnej služby na základe tohto zákona je príslušný Národný bezpečnostný úrad. Zákonnou úpravou sa zefektívňuje a modernizuje výkon kontrolnej činnosti v oblasti kybernetickej bezpečnosti na základe poznatkov z praxe.

V § 29c zákona sa vymedzuje predmet kontroly a rozsah subjektov, nad ktorými je Národný bezpečnostný úrad oprávnený vykonať kontrolu. Národný bezpečnostný úrad je oprávnený vykonať kontrolu nielen u prevádzkovateľa základnej služby, ale aj nad skupinou osôb alebo účelových združení majetku, ktorých súčasťou je prevádzkovateľ základnej služby. Kontrolu na konsolidovanom základe nad skupinou osôb alebo účelových združení majetku, ktorých súčasťou je prevádzkovateľ základnej služby možno vykonať iba v rozsahu, v ktorom tieto subjekty majú vplyv alebo spôsobilosť mať vplyv na kybernetickú bezpečnosť u prevádzkovateľa základnej služby. Požiadavka rozšíriť možnosť na výkon kontroly na konsolidovanom základe vychádza z aplikačnej praxe, kedy doterajšia právna úprava neumožňovala vykonať kontrolu v inom subjekte ako u prevádzkovateľa základnej služby alebo jeho dodávateľa ani v prípade, ak by tento subjekt mal priamy vplyv nad úrovňou kybernetickej bezpečnosti u prevádzkovateľa základnej služby, čo spôsobovalo neúplný dohľad a skresľovalo získanie informácií o komplexnej úrovní kybernetickej bezpečnosti. Kontrolu je možno vykonať na mieste, čím sa zabezpečuje objektívny hodnoverné zistenie skutkového stavu kontrolovaného subjektu.

V § 29d zákona sa upravuje proces kontroly, akým úkonom sa kontrola začína, obsahové náležitosti poverenia na vykonanie kontroly, ustanovujú sa oprávnenia a povinnosti Národného bezpečnostného úradu v súvislosti s výkonom kontroly. Národný bezpečnostný úrad je pri kontrole oprávnený vyžadovať a odoberať informácie, doklady a iné podklady, čím však nemôže byť ohrozená alebo obmedzená poskytovaná služba prevádzkovateľa základnej služby, ani tým nemôže byť znížená úroveň kybernetickej bezpečnosti u prevádzkovateľa základnej služby. Zároveň je Národný bezpečnostný úrad oprávnený odoberať záznamy dát na pamäťových médiách prostriedkov výpočtovej techniky alebo prenášaných v sieti a ich výpisy a výstupy, vyjadrenia, informácie, dokumenty a iné podklady súvisiace s kontrolou, vyhotovovať si ich kópie a nakladať s nimi v rozsahu, ktorým nebude zasiahnuté do poskytovanej služby, a ktoré majú priamy súvis s predmetom kontrolnej činnosti. V prípade, ak dôjde k odobratiu techniky alebo originálov či úradne overených dokumentov, sú osoby vykonávajúce kontroly ich odobratie písomne potvrdiť prevádzkovateľovi základnej služby. Po ukončení potrebnosti je Národný bezpečnostný úrad povinný vrátiť všetky odobraté originály alebo úradne osvedčené kópie dokumentov alebo dát. Na základe zistených nedostatkov v priebehu kontroly Národný bezpečnostný úrad bude vyžadovať od prevádzkovateľa základnej služby písomný zoznam opatrení, ktoré sa rozhodol prijať, aby napravil nedostatky, ktoré boli pri kontrole zistené rovnako aj opatrenia, ktoré prijal aby sa do tieto nedostatky opätovne nenastali. V prípade ak Národný bezpečnostný úrad vyhodnotí, že opatrenia, ktoré sa prevádzkovateľ základnej služby rozhodol implementovať sú nedostatočné na zabezpečenie potrebnej úrovne kybernetickej bezpečnosti, môže vyžadovať prepracovanie zoznamu prijatých opatrení, aby bol naplnený ich účel. Zároveň aby bol naplnený účel dohľadu, je Národný bezpečnostný úrad oprávnený overiť splnenie prijatých opatrení a teda preveriť deklarovaný stav s reálnym a či si prevádzkovateľ základnej služby plní svoje zákonné povinnosti. Ustanovenie odseku 6 priamo súvisí s možnosťou vykonávať kontrolu na mieste a je nevyhnutné pre naplnenie účelu kontroly. Pri výkone kontroly sa nemôže vstupovať do objektov tretej osoby, ktoré nesúvisia s výkonom činností poskytovania služby prevádzkovateľom základnej služby. Národný bezpečnostný úrad je povinný oboznámiť prevádzkovateľa základnej služby s návrhmi výstupných materiálov z kontroly a umožniť mu voči ním podať písomné námietky, ktorými je povinný sa zaoberať. V prípade akceptovania námietky, zohľadniť túto skutočnosť vo výstupnom materiály z kontroly a v prípade ich neakceptovania sa vyžaduje riadne odôvodnenie, pre ktoré nie je možné námietku akceptovať.

V § 29e zákona sa upravujú oprávnenia a povinnosti kontrolovaného subjektu, ktorým je prevádzkovateľ základnej služby, ktoré vyplývajú z práv a povinností Národného bezpečnostného úradu pri výkone kontroly.

V § 29f zákona sa upravujú výsledné materiály z kontroly, ktorými môžu byť návrh čiastkovej správy, návrh správy, čiastková správa a správa, ich náležitosti a procesy súvisiace s nimi. Zároveň sa v tomto ustanovení upravuje aj spôsob ukončenia kontroly. Kontrola je ukončená dňom zaslania správy prevádzkovateľovi základnej služby. Zaslaním čiastkovej správy je skončená tá časť kontroly, ktorej sa čiastková správa týka. Ak je kontrola alebo jej časť zastavená z dôvodov hodných osobitného zreteľa, kontrola alebo jej časť je ukončená vyhotovením záznamu s uvedením dôvodu jej zastavenia. Národný bezpečnostný úrad takýto záznam bezodkladne zašle prevádzkovateľovi základnej služby.

V § 29g zákona sa upravuje inštitút tzv. prizvanej osoby, kedy je potrebné, vzhľadom na povahu kontroly, rozšíriť spôsobilosť kontrolnej skupiny o osoby so špecifikami znalosťami alebo zručnosťami. Zároveň sa do kontrolnej skupiny prizve osoba určená CSRITom iného členského štátu Európskej únie, ak o to požiada, z dôvodu presahu poskytovanej služby prevádzkovateľa základnej služby do jeho pôsobnosti alebo ak je to v záujme toho členského štátu Európskej únie.

V § 29h zákona sa upravuje nezaujatosť osôb vykonávajúcich kontrolu (zamestnanec alebo príslušník Národného bezpečnostného úradu alebo prizvaná osoba), hlásenie prípadnej zaujatosti zo strany osôb vykonávajúcich kontrolu aj zo strany kontrolovaného subjektu. O ich zaujatosti, resp. nezaujatosti rozhoduje riaditeľ Národného bezpečnostného úradu. Zároveň sa v tomto ustanovení ustanovuje povinnosť zachovávať mlčanlivosť o skutočnostiach, o ktorých sa dozvedeli v súvislosti s výkonom kontroly. Oslobodiť od tejto povinnosti ich môže iba riaditeľ Národného bezpečnostného úradu.

V § 29i zákona sa upravuje možnosť Národného bezpečnostného úradu pred uložením opatrenia na zastavenie porušovania povinností a na nápravu nezákonného stavu vydať predbežné opatrenie, ktorým v rozsahu nevyhnutne potrebnom na predídenie vzniku vážnej škody alebo inej ujmy uloží prevádzkovateľovi základnej služby, aby niečo vykonal, niečoho sa zdržal alebo niečo strpel alebo nariadi zabezpečenie vecí, ktoré sú potrebné na vykonanie dôkazov. Cieľom tohto ustanovenia je zamedziť škodám alebo potencionálnym škodám, ktoré by mohli nastať v prípade ak by prevádzkovateľ základnej služby sám nekonal. Pokiaľ prevádzkovateľ základnej služby príjme vhodné opatrenia na zamedzenie škodlivej udalosti, Národný bezpečnostný úrad je povinný predbežné opatrenie zrušiť, čo platí aj v prípade, ak sa už javia ako neúčelné.

V § 29j zákona sa upravuje konanie o uložení opatrenia, t. j. právomoc Národného bezpečnostného úradu ukladať prevádzkovateľovi základnej služby taxatívne vymenované povinnosti, ak zistí nedostatky v činnosti prevádzkovateľa základnej služby spočívajúce v plnení povinností prevádzkovateľa základnej služby podľa tohto zákona alebo iných všeobecne záväzných právnych predpisov, ktoré ukladajú povinnosti prevádzkovateľovi základnej služby, ako aj povinností uložených na ich základe, podľa závažnosti, rozsahu, dĺžky trvania, následkov a povahy zistených nedostatkov. Národný bezpečnostný úrad môže uložiť povinnosť vykonať audit kybernetickej bezpečnosti a vykonať odporúčania podľa výsledkov tohto auditu v určenej lehote, povinnosť prijať opatrenia na nápravu, povinnosť informovať dotknuté osoby alebo verejnosť o rizikách alebo následkoch porušenia povinnosti, alebo povinnosť zakázať poskytovať základnú službu do času nápravy nezákonného stavu, ak nejde o prevádzkovateľa základnej služby, ktorý je orgánom verejnej moci alebo ktorý poskytuje základnú službu na základe povinnosti uloženej zákonom alebo na jeho základe. Zároveň môže Národný bezpečnostný úrad spolu s uložením opatrenia na nápravu uložiť aj pokutu za správny delikt, prípadne môže uložiť penále za každý deň omeškania so splnením povinnosti.

Národný bezpečnostný úrad ako orgán zabezpečujúci dohľad nad kybernetickou bezpečnosťou musí mať k dispozícií právomoci a inštitúty na dosiahnutie plnenia zákonných požiadaviek, ktorými sa má zabezpečiť kybernetická bezpečnosť tak, aby sa znížila miera rizika pre poskytovanú službu. Ustanovenia § 29 umožňujú Národnému bezpečnostnému úradu docieliť plnenie povinností prevádzkovateľa základnej služby efektívnejším spôsobom čim aj ochrániť odberateľov poskytovanej služby ako aj samotného prevádzkovateľ základnej služby pred incidentmi. Národný bezpečnostný úrad pri ukladaní povinností podľa odseku 1 musí vždy zvážiť závažnosti, rozsahu, dĺžky trvania, následkov a povahy zistených nedostatkov a primerane k tomu uložiť povinnosť. Národný bezpečnostný úrad k ukladaniu povinností pristúpi až vtedy, keď prevádzkovateľ základnej služby si neplní svoje zákonom alebo na jeho základe uložené povinnosti. Ustanovenia odseku 4 sú terminálny inštitútom, ak si prevádzkovateľ základnej služby neplní uloženú povinnosť vykonať audit kybernetickej bezpečnosti alebo prijať patrenia, ktoré vplývajú priamo z bodu 133 recitálu a čl. 32 ods. 5 písm. b) smernice NIS 2.

V § 29k zákona sa upravuje možnosť Národného bezpečnostného úradu navrhovať súdu, aby svojím rozhodnutím dočasne obmedzil prístup odberateľov dotknutých nezákonným stavom k základnej službe, alebo obmedzil prístup k online rozhraniu, prostredníctvom ktorého dochádza k porušeniu spôsobujúcemu nezákonný stav v prípade, že prevádzkovateľ základnej služby neplní povinnosti uložené podľa § 29j ods. 1 zákona riadne a včas, nezákonný stav pretrváva a spôsobuje vážnu škodu alebo inú ujmu a obsahuje znaky trestného činu proti životu, zdraviu alebo bezpečnosti osôb. Pre zabránenie pokračovania stavu spôsobujúceho vážnej škody alebo inej ujmy, ktorý nesie znaky trestného činu je nevyhnutné dať možnosť Národnému bezpečnostnému úradu takémuto stavu zabrániť alebo ho prerušiť. Rozhodovanie o uložení povinnosti dočasne obmedziť prístup sa ustanovuje súdu so zreteľom na závažnosť možného dopadu. Národný bezpečnostný úrad vypracuje odôvodnený návrh na uloženie povinnosti dočasne obmedziť prístup, ktorý bude obsahovať argumentáciu, prečo sú podľa Národného bezpečnostného úradu splnené zákonné predpoklady na uloženie danej povinnosti o ktorom bude rozhodovať nezávislí a nestranný súd, čím sa zabezpečí objektivizácia v rozhodovacom procese a zabráni sa svojvôli Národného bezpečnostného úradu. Ak takéto obmedzenie prístupu nie je v dispozícii prevádzkovateľa základnej služby, povinnosť obmedziť prístup možno v druhom rade uložiť osobe, ktorá je objektívne spôsobilá takéto obmedzenie vykonať. Ustanovujú sa náležitosti žiadosti Národného bezpečnostného úradu, ktorou súdu navrhujú uložiť obmedzenie prístupu. Stanovuje sa možnosť súdu v rámci svojho rozhodnutia oprávniť Národný bezpečnostný úrad rozhodnúť na opakované predĺženie doby obmedzenia prístupu. Samotné rozhodnutie súdu doručuje Národný bezpečnostný úrad.

V § 29l zákona sa upravuje inštitút tzv. rozkazného konania. Ide o oprávnenie Národného bezpečnostného úradu v prípade, ak bolo pri výkone dohľadu podľa § 29a ods. 1 písm. a) až c) zákona spoľahlivo zistené, že prevádzkovateľ základnej služby v jednotlivom prípade porušil povinnosť, bez ďalšieho konania vydať rozkaz o uložení sankcie prevádzkovateľovi základnej služby za zistené porušenie. Tento inštitút sleduje zásadu hospodárnosti a efektívnosti. Pokiaľ sa v priebehu dohľadu preukáže jednoznačné porušenie povinnosti prevádzkovateľa základnej služby, ktorý so zisteniami dohľadu súhlasí a nemá voči nim námietky, je na nápravu postačujúce rozkázané konanie bez potreby ďalšieho konania.

V § 29m zákona sa upravuje inštitút tzv. dohody o náprave. Ide o nový procesný inštitút, ktorý umožňuje Národnému bezpečnostnému úradu kedykoľvek navrhnúť prevádzkovateľovi základnej služby uzatvoriť dohodu o náprave. Národný bezpečnostný úrad môže uzatvoriť dohodu o náprave s prevádzkovateľom základnej služby, ak opatrenia a náhrada, ktoré sú obsahom dohody, sú spôsobilé odstrániť nezákonný stav a primerane nahradiť vzniknutú škodu alebo inú ujmu a ak neexistuje iný záujem na pokračovaní vo výkone dohľadu. Ak je uzatvorená dohoda o náprave, Národný bezpečnostný úrad zastaví výkon dohľadu v rozsahu porušení povinností, ktoré sú obsahom dohody o náprave. Zároveň sa ponecháva Národnému bezpečnostnému úradu právo opätovne začať dohľad vo veci porušenia povinností, ktoré sú obsahom dohody o náprave v taxatívne uvedených prípadoch. Dohoda o náprave sa javí ako efektívny nástroj na nápravu zistených nedostatkov u prevádzkovateľa základnej služby tam, kde nie je vysoká závažnosť porušenia povinností a najmä, keď je prevádzkovateľ základnej služby súčinný pri odstránení nedostatkov zistených dohľadom a je schopný tieto nedostatky napraviť tak, aby nedochádzalo k ďalšiemu porušovaniu povinností prevádzkovateľa základnej služby ani nebola ohrozená poskytovaná služba. Dohoda o náprave vzniká ako konsenzus medzi návrhom Národného bezpečnostného úradu a možnosťami prevádzkovateľa základnej služby. Nikoho nemožno do takejto dohody nútiť, rovnako nemôže byť nikomu na škodu, že odmietol uzatvoriť dohodu o náprave.

V § 29n sa upravuje inštitút poriadkovej pokuty, ktorá umožňuje Národnému bezpečnostnému úradu ukladať poriadkovú pokutu kontrolovanému subjektu, ktorý neplní povinnosti podľa tohto zákona a tým znemožňuje priebeh kontroly podľa § 29c až § 29h zákona.

**K bodom 74 až 76**

Dopĺňajú sa nové skutkové podstaty priestupkov súvisiacich s auditom a preverovaním účinnosti prijatých bezpečnostných opatrení a vykonávajú sa legislatívnotechnické úpravy súvisiace so skutkovými podstatami priestupkov.

**K bodu 77**

Ustanovenie o správnych deliktoch upravené podľa zmien vyplývajúcich zo smernice NIS 2 a z aplikačnej praxe.

**K bodom 78 a 81**

Dochádza k vypusteniu splnomocňovacích ustanovení a zrušení vyhlášky č. 164/2018 Z. z. a vyhlášky č. 165/2018 Z. z. z dôvodov vyplývajúcich zo smernice NIS 2.

**K bodu 79**

Ide o precizovanie splnomocňovacieho ustanovenia v oblasti bezpečnostných opatrení.

**K bodu 80**

Ide o precizovanie splnomocňovacieho ustanovenia v oblasti bezpečnostných štandardov a znalostných štandardov.

**K bodu 82**

Splnomocňovacie ustanovenie v oblasti auditu sa rozširuje o samohodnotenie, periodicitu vykonávania auditu samohodnotením a dochádza k precizovaniu splnomocňovacieho ustanovenia.

**K bodu 83**

Dopĺňajú sa dve nové splnomocňovacie ustanovenia, ktoré vyplynuli ako potreba z návrhu zákona.

**K bodu 84**

Dopĺňajú sa vybrané ustanovenia v súvislosti s dohľadom, na ktoré sa nevzťahuje správny poriadok.

**K bodu 85**

Ustanovuje sa kompetencia Národného bezpečnostného úradu rozhodnúť, do ktorého sektoru a pod ktorý ústredný orgán bude prevádzkovať základnej služby zaradený s tým, tomuto rozhodnutiu predchádza povinnosť Národného bezpečnostného úradu konzultovať toto zaradenie s príslušnými ústrednými orgánmi.

**K bodu 86**

Legislatívnotechnická úprava súvisiaca s plnením úloh Ministerstva obrany Slovenskej republiky na úseku kybernetickej bezpečnosti, ktoré sa realizuje prostredníctvom Vojenského spravodajstva.

**K bodu 87**

Ide o úpravu v oblasti finančného sektora a postavenia Národnej banky Slovenska na úseku kybernetickej bezpečnosti, ktorá je výsledkom vzťahu NIS2 a nariadenia EÚ 2022/2554. Národná banka Slovenska nie je prevádzkovateľom základnej služby podľa tohto zákona avšak z dôvodu zabezpečenia vysokej úrovne kybernetickej bezpečnosti na území Slovenskej republiky sa ustanovuje povinnosť Národnej banky Slovenska a úradu uzatvoriť písomnú dohodu o spolupráci predmetom ktorej, budú základné rámce hlásenia kybernetických bezpečnostných incidentov a riešenia kybernetických bezpečnostných incidentov a stavu zabezpečovania kybernetickej bezpečnosti v Národnej banke Slovenska. Cieľom tejto dohody je zabezpečenie spolupráce medzi Národným bezpečnostným úradom ako regulátorom v oblasti kybernetickej bezpečnosti a Národnou bankou Slovenska, ktorá je z pohľadu oboch subjektov veľmi podstatná.

Uvedenou zmluvou o spolupráci, ktorou sa dohodnú podrobnosti hlásenia incidentov medzi Národným bezpečnostným úradom a Národnou bankou Slovenska, sa zabezpečí nahlasovanie kybernetických bezpečnostných incidentov prevádzkovateľmi základnej služby, ktorí sú regulovaní nariadením (EÚ) 2022/2554 aj Národnému bezpečnostnému úradu prostredníctvom Národnej banky Slovenska ako orgán príslušný podľa nariadenia (EÚ) 2022/2554.

**K bodu 88**

Dopĺňajú sa prechodné ustanovenia v súvislosti so zmenami, ktoré vyplynuli zo smernice NIS 2, najmä v súvislosti so zmenami pri identifikácii prevádzkovateľa základnej služby a s vypustením pojmu „poskytovateľ digitálnych služieb“.

Ten, kto bol prevádzkovateľom základnej služby 31. decembra 2024, bude automaticky od 1. januára 2025 prevádzkovateľom kritickej základnej služby podľa tohto zákona. Zároveň sa určuje lehota pre Národný bezpečnostný úrad, aby mohol rozhodnúť, ktorý z takýchto prevádzkovateľov kritickej základnej služby nebude prevádzkovateľom kritickej základnej služby z dôvodu, že nespĺňa podmienky podľa § 18 ods. 1 tohto zákona v znení účinnom od 1. januára 2025.

Obdobne ten, kto bol poskytovateľom digitálnej služby 31. decembra 2024, bude od 1. januára 2025 automaticky prevádzkovateľom základnej služby podľa tohto zákona. Taktiež sa určuje lehota pre Národný bezpečnostný úrad, aby mohol rozhodnúť, ktorý z takýchto prevádzkovateľov základnej služby nebude prevádzkovateľom základnej služby z dôvodu, že nespĺňa podmienky podľa § 17 ods. 1 tohto zákona v znení účinnom od 1. januára 2025.

Prevádzkovateľovi základnej služby sa umožňuje, aby v prechodnom období, t. j. od 1. januára 2025 do 31. decembra 2026 mohol splniť podmienku zavedenia bezpečnostných opatrení požadovaných podľa tohto zákona v znení účinnom od 1. januára 2025 tak, že bude mať v tomto prechodnom období zavedené bezpečnostné opatrenia podľa tohto zákona v znení účinnom do 31. decembra 2024.

Určuje sa lehota, dokedy je Národný bezpečnostný úrad povinný najneskôr vyzvať na plnenie povinnosti podľa § 21 ods. 3 zákona.

Prevádzkovateľovi základnej služby sa umožňuje, aby v prechodnom období, t. j. od 1. januára 2025 do 31. decembra 2026, mohol vykonávať audit podľa právnej úpravy účinnej do 31. decembra 2024. Rovnako tak sa ustanovuje možnosť určitým prevádzkovateľom základnej služby plniť povinnosť vykonať audit kybernetickej bezpečnosti, ktorý bol povinný vykonať v roku 2024, spôsobom podľa odseku 9, teda samohodnotením, do 30. septembra 2025. Táto možnosť vyplynula ako potreba z aplikačnej praxe.

**K bodu 89**

Zrušovacie ustanovenia, ktorým sa zrušuje vyhláška Národného bezpečnostného úradu č. 164/2018 Z. z., ktorou sa určujú identifikačné kritéria prevádzkovanej služby (kritériá základnej služby) a vyhláška Národného bezpečnostného úradu č. 165/2018 Z. z., ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov.

**K bodu 90**

Legislatívnotechnická úprava súvisiaca s pojmom „prevádzkovateľ základnej služb“.

**K bodu 91**

Pôvodné prílohy č. 1 a č. 2 sa nahrádzajú novými prílohami podľa požiadaviek smernice NIS 2. Prílohy č. 1 a č. 2 slúžia na identifikáciu prevádzkovateľov základnej služby podľa § 17 ods. 1 zákona.

V prílohe č. 1 sú uvedené sektory s vysokou úrovňou kritickosti, podsektory, typy subjektov a ústredný orgán, ktorý tieto subjekty zastrešuje. V poznámke sú uvedené právne predpisy Slovenskej republiky upravujúce problematiku sektorov, podsektorov, prípadne typov subjektov. Pri tvorbe prílohy č. 1 sa vychádzalo primárne z prílohy č. 1 smernice NIS 2. Väčšina sektorov, podsektorov a typov subjektov s vysokou úrovňou kritickosti bola identifikovaná už v prílohe č. 1 zákona v znení účinnom do 31. decembra 2024. Príloha č. 1 slúži aj na identifikáciu kritickej základnej služby, pretože činnosti uvedené v prílohe č. 1, okrem sektoru verejná správa, sa považujú za kritickú základnú službu, ak ju vykonáva osoba, ktorá presahuje podmienky veľkosti pre stredný podnik.

V prílohe č. 2 sú uvedené iné kritické sektory, vrátane ich podsektorov, typov subjektov a ústredných orgánov, ktoré tieto typy subjektov zastrešujú. V poznámke sú uvedené právne predpisy Slovenskej republiky upravujúce problematiku sektorov, podsektorov, prípadne typov subjektov.

V prípade prílohy č. 3 ide iba o legislatívnotechnickú úpravu.

**Čl. II (Zákon č. 455/1991 Zb.)**

Medzi viazané živnosti sa do skupiny 214 - Ostatné dopĺňa živnosť s poradovým číslom 95. „Certifikovaný audítor kybernetickej bezpečnosti“. Odborná spôsobilosť sa preukazuje Certifikátom audítora kybernetickej bezpečnosti, ktorý je vydaný v súlade s § 29 ods. 3 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

**Čl. III (Zákon Národnej rady Slovenskej republiky č. 145/1995 Z. z.)**

Vzhľadom na to, že zákon č. 452/2021 Z. z. o elektronických komunikáciách v znení neskorších predpisov (viď čl. VI) v novom § 52a ustanovuje pre fyzickú osobu, ktorá bude obsluhovať vybrané rádiové zariadenie vybavené zariadeniami GMDSS na lodiach, ktoré nie sú povinne týmito zariadeniami vybavené, povinnosť pred vykonaním skúšky absolvovať praktický výcvik v školiacom stredisku uznanom Úradom pre reguláciu elektronických komunikácií a poštových služieb, je potrebné upraviť nový druh správneho poplatku za podanie žiadosti o uznanie školiaceho strediska.

**Čl. IV (Zákon č. 143/1998 Z. z.)**

Školenia o kybernetickej bezpečnosti sa týmto upravujú v zákone o civilnom letectve. Vykonávacie Nariadenie Komisie (EÚ) 2015/1998 požaduje, aby osoby ním definované absolvovali odbornú prípravu v oblasti kybernetickej bezpečnosti. Legislatívno-technická úprava v nadväznosti na novú úpravu. Dopĺňajú sa nové sankcie v nadväznosti na novú úpravu. V súvislosti s číslovaním poznámok dávame do pozornosti vládny návrh zákona, ktorým sa mení a dopĺňa zákon č. 143/1998 Z. z. o civilnom letectve (letecký zákon) a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony (tlač 214).

**Čl. V (Zákon č. 541/2004 Z. z.)**

**K bodu 1**

Ustanovuje sa kompetencia štátneho dozoru v oblasti využívania jadrovej energie, pri fyzickej ochrane, kybernetickej bezpečnosti a pri havarijnom plánovaní.

**K bodu 2**

Doplnenie nového dokladu v rámci inšpekcie je dôležité z dôvodu analýzy aktuálneho stavu kybernetickej bezpečnosti počítačových systémov dôležitých predovšetkým z hľadiska jadrovej bezpečnosti, fyzickej ochrany, havarijnej pripravenosti a evidencie a kontroly jadrových materiálov. Výsledky záverečnej správy z auditu budú použité ako podklad pravidelných inšpekcií kybernetickej bezpečnosti vykonávaných Úradom jadrového dozoru Slovenskej republiky a zároveň poskytnú inšpektorom Úradu jadrového dozoru Slovenskej republiky prehľad bezpečnostných opatrení, ktoré by mal držiteľ povolenia vykonať pre zabezpečenie požadovanej úrovne kybernetickej bezpečnosti.

**Čl. VI (Zákon č. 452/2021 Z. z.)**

**K bodu 1**

Navrhuje sa ustanovenie kompetencie Úradu pre reguláciu elektronických komunikácií a poštových služieb uznávať školiace stredisko pre fyzické osoby, ktoré budú obsluhovať vybrané rádiové zariadenie na lodiach povinne vybavených zariadeniami globálneho námorného tiesňového a bezpečnostného systému (GMDSS).

**K bodu 2**

Navrhuje sa rozdelenie odseku § 52 tak, že právna úprava uznávania školiaceho strediska bude upravená v samostatnom § 52a.

**K bodu 3**

Navrhuje sa úprava, ktorá ustanovuje, že fyzická osoba, ktorá bude obsluhovať vybrané rádiové zariadenie podľa návrhu, je povinná pred vykonaním skúšky podľa § 52 absolvovať praktický výcvik v školiacom stredisku uznanom Úradom pre reguláciu elektronických komunikácií a poštových služieb. Upravujú sa náležitosti a proces uznávania školiaceho strediska, pričom sa súčasne ustanovujú náležitosti žiadosti a požiadavky na žiadateľa o uznanie školiaceho strediska. Ďalej sa ustanovuje proces udeľovania rozhodnutia o uznaní školiaceho strediska resp. dôvody jeho zrušenia. Na proces uznávania resp. zrušenia rozhodnutia o uznaní školiaceho strediska sa vzťahuje všeobecný predpis o správnom konaní. Taktiež sa ustanovujú povinnosti pri výkone činnosti školiaceho strediska s ohľadom na potrebu zabezpečiť požadovanú úroveň vedomostí absolventov a ich evidenciu.

V nadväznosti na prijatie novely zákona č. 452/2021 Z. z. o elektronických komunikáciách v týchto bodoch bude môcť Úrad pre reguláciu elektronických komunikácií a poštových služieb vydať všeobecne záväzný právny predpis, ktorý stanoví podrobnosti o postupe a spôsobe uznávania školiaceho strediska podľa prvej vety, rozsah povinného technického vybavenia školiaceho strediska, a náležitosti plánu praktického výcviku a podrobnosti o požiadavkách, ktoré musí školiace stredisko spĺňať.

**K bodu 4**

Ide o legislatívnotechnické úpravy súvisiace so zmenami vyplývajúcimi z transpozície smernice NIS 2. Ide o odstránenie duplicity vo vzťahu k zabezpečovaniu kybernetickej bezpečnosti podľa tohto zákona a podľa zákona č. 452/2021 Z. z. o elektronických komunikáciách v znení neskorších predpisov. Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov má v tomto prípade postavenie tzv. lex generalis.

**Čl. VII**

Účinnosť zákona sa navrhuje 1. januára 2025 vzhľadom na dĺžku legislatívneho procesu.