Dôvodová správa

B. Osobitná časť

K čl. I

K bodu 1
V tomto novelizačnom bode ide o negatívne vymedzenie pôsobnosti zákona. Ide o precizovanie výnimky pre sektor bankovníctva, financií, finančných trhov, platobných systémov a systémov zúčtovania cenných papierov, ktorý je harmonizovaný a striktne regulovaný právom EÚ. Takto nastavené pravidlá v oblasti kybernetickej bezpečnosti tak prevyšujú rámec stanovený smernicou 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 (ďalej len „smernica NIS“).

K bodu 2
Úprava poznámky pod čiarou z dôvodu neaktuálnosti predpisu a navrhovanej zmeny v normatívnej časti zákona.

K bodu 3
Úprava poznámky pod čiarou z dôvodu navrhovanej zmeny v normatívnej časti zákona.

K bodom 4 a 5
Súčasne navrhované zmeny pojmov odrážajú požiadavky vyplývajúce z aplikačnej praxe kvôli ich jasnejšiemu a zrozumiteľnejšiemu uchopeniu v návrhu zákona.

K bodu 6
Legislatívno-technická úprava.

K bodu 7 a 8
Zo zákona sa vypúšťa základná služba, ktorá je informačným systémom verejnej správy. Na tieto služby sa vzťahujú identifikační kritéria podľa vyhlášky Národného bezpečnostného úradu č. 164/2018 Z. z.

K bodu 9
Ustanovenie sa upravuje v súvislosti s vypustením podsektoru Spravodajské služby, a to Slovenskej informačnej služby a Vojenského spravodajstva z okruhu ústredných orgánov. Predmetná zmena odzrkadľuje ustanovenie článku 1 ods. 6 smernice NIS a súčasne vyplýva z aplikačnej praxe, pretože súčasná úprava sa ukázala ako neefektívna. Tak ako Slovenská informačná služba, ani Vojenské spravodajstvo nedisponuje v rámci svojej regulácie inými subjektami a spravujú len vlastné systémy. Z toho dôvodu nevykonávajú pôsobnosť ústredného orgánu v zmysle zákona. Vypúšťa sa Ministerstvo vnútra SR ako ústredný orgán.

K bodu 10
Zmena navrhovaná v § 5 ods. 1 písm. v) reaguje na požiadavky aplikačnej praxe z dôvodu vyššej miery zrozumiteľnosti a špecifikácie konkrétneho subjektu vykonávajúceho audit.

K bodu 11

Úrad vydané štandardy zverejňuje na svojom webovom sídle.

K bodu 12
Doplnením ustanovenia § 5 ods. 1 dochádza k úprave právomocí úradu. Zavádza sa legislatívne vymedzenie inštitútu „blokovania“. Rovnako bolo potrebné špecifikovať pôsobnosť úradu v súvislosti s plnením úloh vnútroštátneho orgánu pre certifikáciu kybernetickej bezpečnosti s odkazom na nariadenie (EÚ) č. 2019/881. Ďalej úprava reaguje na potrebu vzniku zoznamu audítorov kybernetickej bezpečnosti a zoznamu právnických osôb, prostredníctvom ktorých je možné realizovať audity kybernetickej bezpečnosti. V zmysle § 29 ods. 6 zákona náklady na audit kybernetickej bezpečnosti znáša prevádzkovateľ základnej služby. Keďže náklady hradia prevádzkovatelia základnej služby, je potrebné zabezpečiť, aby mali k dispozícii dôveryhodný zoznam audítorov, resp. zoznam právnických osôb, prostredníctvom ktorých je možné realizovať audity kybernetickej bezpečnosti. Ďalej ustanovenie predstavuje implementáciu Európskeho toolboxu kybernetickej bezpečnosti 5G sietí (EU Toolbox) (https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_127). EU Toolbox obsahuje tri typy opatrení -strategické, technické a podporné opatrenia. Samotné strategické opatrenia sa ďalej členia v kontexte adresátov týchto opatrení, a to: právomoci regulačných orgánov, dodávatelia - tretie strany, diverzifikácia dodávateľov – tretích strán a udržateľnosť a rozmanitosť dodávateľského a hodnotového reťazca. Súčasťou strategických opatrení je aj časť posilnenie regulačných právomocí orgánov, konkrétne oprávnenia týchto orgánov v podobe uloženia povinností týkajúcich sa bezpečnosti poskytovateľom 5G, zákaz alebo uloženie konkrétnych požiadaviek, a to na základe prístupu založenom na hodnotení rizika v určitých parametroch (politické, geografické, právne). Ide teda o osobitnú bezpečnostnú reguláciu. Úrad zvolil všeobecnú úpravu namiesto definovania konkrétnej 5G („internet piatej generácie“) pre účely ďalšej praxe. Úrad sa ďalej zaväzuje vypracovávať každoročnú správu o ochrane osobných údajov v spojitosti s kybernetickými bezpečnostnými incidentami a ich riešením.

K bodu 13
V tomto novelizačnom bode sa stanovuje v súlade s nariadením (EÚ) č. 2019/881, že vnútroštátnym orgánom pre certifikáciu kybernetickej bezpečnosti na území Slovenskej republiky je úrad. Zároveň sa stanovuje, že certifikačný orgán úradu bude spĺňať požiadavky na orgán posudzovania zhody podľa nariadenia Európskeho parlamentu a Rady (ES) č. 765/2008 z 9. júla 2008 , ktorým sa stanovujú požiadavky akreditácie a dohľadu nad trhom v súvislosti s uvádzaním výrobkov na trh a ktorým sa zrušuje nariadenie (EHS) č. 339/93 a postavenie certifikačného orgánu, ktorý je verejným subjektom.
Úrad sa tak v zmysle nariadenia konštituuje ako nezávislý a akreditovaný subjekt zodpovedný za certifikáciu kybernetickej bezpečnosti, na základe čoho bude plniť dôležitú úlohu pri zvyšovaní dôvery v produkty a služby a ich bezpečnosti. Certifikácia slúži na informovanie a uistenie kupujúcich a používateľov o bezpečnostných vlastnostiach produktov a služieb IKT, ktoré nakupujú alebo používajú. V súčasnosti je situácia v oblasti certifikácie kybernetickej bezpečnosti produktov a služieb IKT v EÚ pomerne nevyrovnaná. V prípade neexistencie jednotného systému certifikácie kybernetickej bezpečnosti v celej EÚ musia byť spoločnosti za mnohých okolností certifikované jednotlivo v každom členskom štáte, čo vedie k fragmentácii trhu. Podľa nariadenia zavedenie jedeného alebo viacerých vnútroštátnych orgánov (prípad veľkých štátov) pre certifikáciu kybernetickej bezpečnosti na svojom území prispeje k zvyšovaniu miery harmonizácie práva EÚ pre produkty a služby IKT. Rozdiely medzi normami a postupmi certifikácie kybernetickej bezpečnosti v členských štátoch sa tak v praxi budú potierať a dôjde k zamedzeniu vzniku 28 rôznych bezpečnostných trhov v EÚ, kde by každý z nich mal svoje vlastné technické požiadavky, testovacie metódy a postupy

certifikácie kybernetickej bezpečnosti. Určením jednotlivých certifikačných orgánov v členských štátoch zároveň dôjde, a to nielen na úrovni EÚ, k posilneniu oblasti kybernetickej bezpečnosti, kde spoločný postup týchto orgánov môže viesť k efektívnejšiemu vytváraniu a prijímaniu konkrétnych opatrení v danej oblasti. Rozdielne prístupy na národnej úrovni sa tak výrazne eliminujú a prispeje sa tak významnou mierou k prekonávaniu prekážok pri dosahovaní jednotného digitálneho trhu a spomaľovaní pozitívnych účinkov z hľadiska rastu a pracovných miest.
S ohľadom na potreby aplikačnej praxe nie je vylúčené, aby v rámci členského štátu v riadne odôvodnených prípadoch certifikáciu kybernetickej bezpečnosti podľa nariadenia vykonával iný verejný subjekt, ktorý však musí napĺňať požiadavku uvedenú v článku 58 ods. 5 nariadenia a podmienky ustanovené zákonom č. 505/2009 Z. z. o akreditácii orgánov posudzovania zhody a o zmene a doplnení niektorých zákonov. Takýto verejný subjekt musí hodnoverným spôsobom preukázať spôsobilosti pre splnenia akreditačných požiadaviek, tak aby vnútroštátny akreditačný orgán mohol o tom vydať potvrdenie, že orgán posudzovania zhody spĺňa požiadavky vykonávať špecifické činnosti posudzovania zhody v oblasti kybernetickej bezpečnosti stanovené harmonizovanými normami a v prípade potreby akékoľvek dodatočné požiadavky vrátane tých, ktoré sú stanovené v príslušných sektorových systémoch.
Ustanovenie identifikuje konania, ktoré predstavujú porušenie tohto zákona v súvislosti s certifikáciou produktov, služieb alebo procesov v rámci Európskeho systému certifikácie kybernetickej bezpečnosti, čo je reakciou na implementačnú povinnosť podľa nariadenie (EÚ) č. 2019/881. Pri jednotlivých skutkových podstatách sa uvádza konkrétna sadzba pokuty, ktorá je určená ako rozpätie sumy. Pokuty sa realizujú vo vzťahu k výrobcovi alebo poskytovateľovi za nesplnenie zákonnej povinnosti alebo k opomenutiu takého konania alebo ktorý sa dopustí správneho deliktu podľa zákona. Priestupky a správne delikty prejednáva úrad a príjmy z nich sú príjmom štátneho rozpočtu

K bodu 14
Úrad zriadil Národné centrum kybernetickej bezpečnosti SK-CERT transformáciou Národnej jednotky SK CERT. Vytvorením Národného centra kybernetickej bezpečnosti SK-CERT úrad plní úlohu Akčného plánu realizácie Koncepcie kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020. Budovanie spôsobilostí Slovenskej republiky v oblasti kybernetickej bezpečnosti je pre úrad najvyššou prioritou. Cieľom Národného centra kybernetickej bezpečnosti SK-CERT bude nielen rozvíjanie spôsobilostí pri riešení kybernetických bezpečnostných incidentov na celonárodnej úrovni, ale aj rozšírenie a zdieľanie vedomostí a skúseností v tejto oblasti a aktívna spolupráca s verejnosťou, profesijnými organizáciami a akademickým sektorom. Národné centrum kybernetickej bezpečnosti SK-CERT zabezpečuje nielen služby spojené s riadením kybernetických bezpečnostných incidentov, odstraňovaním ich následkov a následnou obnovou činnosti informačných systémov v spolupráci s vlastníkmi a prevádzkovateľmi týchto systémov, ale aj výkon analytických činností, výskumu, rozširovania bezpečnostného povedomia a vzdelávania v oblasti kybernetickej bezpečnosti.

K bodu 15
Precizovanie textu.

K bodom 16 a 17
Navrhované zmeny v § 9 reagujú na požiadavky aplikačnej praxe s ohľadom na rigidnosť a neúmerné administratívne a personálne zaťaženie ústredných orgánov v súčasnom znení. Na základe navrhovanej zmeny sa upúšťa od povinnosti zriadiť a prevádzkovať vlastnú

akreditovanú jednotku CSIRT, naproti tomu na zabezpečenie plnenia úloh súvisiacich s kybernetickou bezpečnosťou ústredný orgán v navrhovanom znení využíva Národnú jednotku CSIRT. Predmetná zmena tak predstavuje ucelenejší a efektívnejší výkon činností v súvislosti s kybernetickou bezpečnosťou na úseku ústredného orgánu, pričom možnosť zriaďovať vlastnú jednotku CSIRT zostáva zachovaná.

K bodom 18 a 19
Legislatívno-technická úprava súvisiaca s novým § 10a.

K bodu 20
Navrhovaným ustanovením sa zavádza všeobecná povinnosť poskytovať úradu súčinnosť v rámci kybernetickej bezpečnosti. Prax ukázala, že bez adekvátnych praktických vstupov nie je možné realizovať výstupné činnosti úradu s požadovanou kvalitou tak, aby odzrkadľovali reálny stav. Úrad na zabezpečenie svojej riadnej činnosti potrebuje nevyhnutnú súčinnosť pri získavaní informácií na účely zabezpečovania kybernetickej bezpečnosti. Ide o také informácie, ktoré si úrad nevie zabezpečiť vlastnými prostriedkami a majú slúžiť na účely zákona. Zároveň sa ustanovuje, že subjekt poskytuje informácie na základe odôvodnenej žiadosti.

K bodu 21 a 22
Uvedená zmena reaguje na požiadavky aplikačnej praxe s odôvodnením potreby extenzívneho účinku vo vzťahu k subjektu, ktorý môže podať žiadosť o akreditáciu jednotky CSIRT.

K bodu 23
Ide o požiadavku vyplývajúcu z aplikačnej praxe z dôvodu jasného a nespochybniteľné vymedzenia relevantných právnych skutočností.

K bodu 24 až 27
Ide o úpravu vo vzťahu k novej definícii základnej služby. Z definície základnej služby sa vypúšťa základná služba, ktorá je informačným systémom verejnej správy. V uvedenom kontexte je potrebné vykonať príslušné legislatívno-technické úpravy.

K bodu 28
Podľa § 19 ods. 1 sa upravuje predĺženie lehoty z pôvodných šesť na dvanásť mesiacov na prijatie a dodržiavanie bezpečnostných opatrení v spravovaných a prevádzkovaných sieťach a informačných systémoch a vedenie príslušnej dokumentácie o uvedenom, pričom lehota plynie prevádzkovateľovi základnej služby od doručenia oznámenia o jeho zaradení do registra prevádzkovateľov základných služieb. Navrhovaná zmena vyplynula z požiadaviek aplikačnej praxe.

K bodu 29
Upravuje sa povinnosť prevádzkovateľov základných služieb požadovať od dodávateľa služieb na výkon činností, ktoré priamo súvisia s prevádzkou sietí a informačných systémov pre prevádzkovateľa základnej služby, dodatočné bezpečnostné opatrenia v súlade s požiadavkami tohto zákona. Táto povinnosť má byť vykonaná prostredníctvom zmluvných záväzkov, dohôd o zabezpečení plnenia povinností podľa tohto zákona.
Pri uzatvorení zmluvy s treťou stranou podľa § 19 ods. 2 sa analyzujú riziká, zmyslom ktorých je koordinovať využívanie zdrojov a monitorovať, kontrolovať a minimalizovať pravdepodobnosť a dopad kybernetických incidentov, ktoré by mohli ohroziť samotné hodnotenie rizika. Hodnotenia rizika môže poskytnúť cenné informácie na vypracovanie,

vykonanie a vyhodnotenie stratégie. Vyhodnotenie rizika sa tak týka určenia a porozumenia významu úrovne rizika.
Uvedené ustanovenie odseku 3 zároveň reaguje na možné prípady duplicity, kedy v situácii, ak by bol zmluvnou stranou samotný prevádzkovateľ základnej služby alebo poskytovateľ digitálnej služby, by došlo k neprimeranej požiadavke v súvislosti so zabezpečením plnenia bezpečnostných opatrení a notifikačných povinností, ktoré sú tieto subjekty už povinné plniť podľa tohto zákona.

K bodu 30
Legislatívno-technická úprava vyplývajúca z aplikačnej praxe.

K bodu 31
Úprava textu vyplýva z aplikačnej praxe a potreby jasnejšej a zrozumiteľnejšej špecifikácie oblastí pre prijímanie bezpečnostných opatrení, ktoré sú vymedzené všeobecne a ich splnenie je možné dosiahnuť rôznymi technologickými prostriedkami. Subjekty, ktoré majú povinnosť aplikovať tieto bezpečnostné opatrenia si môžu zvoliť vlastný konkrétny spôsob realizácie týchto bezpečnostných opatrení. Táto premisa zodpovedá princípu technickej neutrality zákona o kybernetickej bezpečnosti. Ďalej sa zavádzajú oblasti ako komunikačná bezpečnosť, šifrovanie a riadenie súladu a súčasne dochádza k jasnejšiemu vymedzeniu názvu niektorých oblastí oproti súčasnej úprave v zákone.

K bodu 32
Bezpečnostnou úlohou manažéra kybernetickej bezpečnosti je zodpovednosť za organizovanie systému riadenia kybernetickej bezpečnosti. Cieľom tohto prístupu je obmedziť škody, ktoré by mohli vzniknúť v dôsledku chýb, omylov alebo neoprávneného použitia sietí a informačných systémov. Táto úloha je úplne kľúčová pre správne nastavenie fungovania systému riadenia kybernetickej bezpečnosti. Manažér kybernetickej bezpečnosti má povinnosť informovať vrcholový manažment o činnostiach vyplývajúcich z výkonu úlohy, teda najmä o stave systému riadenia kybernetickej bezpečnosti. Ide o požiadavku, ktorá má viesť k uľahčeniu presadzovania konceptu riadenia kybernetickej bezpečnosti a vedie k dobrej informovanosti vrcholového manažmentu. Na výkon činnosti manažéra kybernetickej bezpečnosti sa predpokladá preukázanie odbornej spôsobilosti v súlade s osobitným predpisom vydaným úradom. Doteraz postavenie manažéra kybernetickej bezpečnosti upravovala 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.

K bodu 33
Ustanovenie výslovne zavádza povinnosť realizovať bezpečnostné opatrenia na základe analýzy rizík. Analýza rizík je postavená na predpovedi pravdepodobnosti vzniku škodlivej udalosti a je základným východiskom pri realizovaní a nastavovaní bezpečnosti ako takej. V rámci ustanovenia dochádza k zosúladeniu odporúčaní a aktov EÚ v oblasti bezpečnosti sietí s národnou úpravou, ktorá momentálne absentuje vo vzťahu najmä k diskutovaným „5G sieťam“.

K bodu 34
Z dôvodu postupnej harmonizácie bezpečnostných opatrení pre prevádzkovateľov základných služieb, ktorí sú regulovaní v rámci iných zákonov, ako aj pri absencii bezpečnostných opatrení v niektorých segmentoch, úrad zvolil legislatívnu oporu pre aplikovanie týchto bezpečnostných opatrení bez potreby novelizácie zákona o kybernetickej bezpečnosti.

K bodu 35
Z dôvodu harmonizácie so smernicou NIS sa vypúšťajú povinnosti poskytovateľa digitálnej služby, ktoré spôsobovali aplikačné nejasnosti. Vo vzťahu k poskytovateľovi digitálnej služby platí, že sa naň v plnej miere aplikujú ustanovenia smernice NIS.

K bodu 36
Upravuje sa spôsob hlásenia kybernetického bezpečnostného incidentu. Uvedená potreba zmeny ustanovenia vyplynula z aplikačnej praxe.

K bodu 37
Úrad na základe získaných poznatkov a z dôvodu dopytu jednotlivých prevádzkovateľov základnej služby zavádza inštitút automatizovaného zasielania systémových informácie zo sietí a informačných systémov. Ide o zasielanie takých údajov, ktoré sú potrebné pri riešení kybernetického bezpečnostného incidentu. Automatizované hlásenie sa realizuje na rozhraní siete Internet a siete prevádzkovateľa základnej služby, nezasahuje ani nezaznamenáva obsah správ alebo prenášaných údajov, ale vytvára bezpečnostný perimeter., ktorý svojim účinkom napomáha prevádzkovateľovi základnej služby úspešne zaznamenať a riešiť kybernetický bezpečnostný incident. Na tento účel ustanovenie jasne vymedzuje, že nedotknuteľnosť tajomstva a osobných údajov zostáva zachovaná. Národný bezpečnostný úrad z tohto dôvodu pridal do svojich úloh aj povinnosť vypracovávať ročnú správu o dodržiavaní ochrany osobných údajov, ako jeden z nástrojov verejnej kontroly, aby nevznikali pochybnosti o účele a transparentnosti výkonu činností. Zavedením tejto povinnosti sa zabezpečuje prenos všetkých relevantných informácií nevyhnutných pre rýchle, efektívne riešenie kybernetických bezpečnostných incidentov alebo ich hrozby.

K bodu 38
K § 27a)
Ustanovenie zavádza oprávnenie úradu zakázať alebo obmedziť prevádzkovateľovi základnej služby využívať konkrétny produkt, proces alebo službu z dôvodu bezpečnostných záujmov štátu a z dôvodu závažných okolností predpokladaných zákonom. Ide o krajné riešenie v prípadoch, kedy absentujú iné zákonné možnosti zabezpečenia a realizácie kybernetickej bezpečnosti. Ustanovenie je pokračovaním implementácie EÚ Toolbox. Platí, že obmedzenie alebo zákaz možno realizovať len na základe podrobnej analýzy rizík a len na základe vyjadrenia Bezpečnostnej rady Slovenskej republiky. Dvojstupňovosť sa zvádza z dôvodu predchádzania pochybnostiam o výkone takéhoto zásahu. Pre účely dodržania záväznosti takéhoto aktu sa konkrétne rozhodnutie zverejní v Zbierke zákonov Slovenskej republiky, pričom sa musí určiť aj primeraná doba na odstránenie nežiaduceho produktu a jeho nahradenie novým. Pred vydaním rozhodnutia na účely transparentnosti úrad zverejní začatie konania na svojom webovom sídle ako aj v jednotnom informačnom systéme kybernetickej bezpečnosti. Po zverejnení rozhodnutia je prevádzkovateľ základnej služby povinný zdržať sa používania konkrétneho produktu, procesu alebo služby alebo ich používať obmedzeným spôsobom v zmysle rozhodnutia.

K § 27b)
V záujme zabezpečenia dôveryhodnosti služieb a aktivít poskytovaných prostredníctvom internetu a ochrany práv osôb zúčastňujúcich sa na týchto aktivitách, ako aj ochrany konečného užívateľa týchto služieb bola vznesená spoločenská požiadavka efektívneho zamedzovania škodlivých aktivít alebo škodlivého obsahu na internete. Škodlivých aktivít na internete z roka na rok pribúda. Zároveň rastie sofistikovanosť útokov a s neustále

prebiehajúcou informatizáciou spoločnosti aj riziká spojené s úspešne vykonanými útokmi. Reakcie na rôzne typy škodlivých aktivít spadajú do kompetencie rôznych štátnych orgánov. Množstvo útokov je vykonávaných buď plošne (napr. phishingové kampane lákajúce veľké množstvo používateľov kliknúť na rozoslaný link), alebo na svoju činnosť využíva identifikovateľný škodlivý obsah alebo sieťovú infraštruktúru (napr. riadiace servery botnet sietí, DNS servery k nim smerujúce, zariadenia vykonávajúce DDOS útoky a pod.). Z tohto dôvodu mnohé krajiny zavádzajú legislatívne podmienky a technické prostriedky na blokovanie nežiadúceho obsahu, IP adries, domén, URL, súborov a podobne. Úrad na túto potrebu adekvátne reaguje a svoje odborné schopnosti a kompetencie, ktoré využíva pri riešení kybernetických bezpečnostných incidentov primerane aplikuje aj na iné škodlivé aktivity na internete. Blokovanie infikovaných domén a IP adries je nutné považovať za reaktívne opatrenie vedúce k zamedzeniu prístupu k škodlivému obsahu. Dôvody, prečo využiť tento prostriedok, je možné zhrnúť do niekoľkých bodov:

1. Ochrana používateľov napadnutých služieb a nevedomých používateľov podvodných služieb - ak je na šírenie škodlivého obsahu, vylákanie údajov alebo na ilegálne aktivity zneužitá legitímna doména alebo služba; zablokovanie obsahu alebo konkrétneho URL zabezpečí ochranu používateľov, ktorí túto službu alebo doménu využívajú.
2. Zmiernenie alebo zamedzenie škodlivých následkov - blokovaním domén a IP adries so škodlivým obsahom či phishingom je takisto možné dosiahnuť zmiernenie následkov v podobe menšieho dopadu na potenciálne obete, resp. zasiahnutých používateľov. Rovnako aj včasným blokovaním možno zabezpečiť úplné zamedzenie škodlivých následkov, pretože nemusí dôjsť napríklad k stiahnutiu škodlivého obsahu alebo k dokončeniu všetkých fáz phishingovej kampane.
3. Zastavenie šírenia škodlivého obsahu - v tomto bode ide najmä o šírenie malvéru, existenciu riadiacich serverov pre botnety, phishingové stránky a pod. Domény a IP adresy s takýmto obsahom sú využívané útočníkmi na nelegitímne ciele a ich blokovanie bráni ďalšiemu šíreniu takéhoto škodlivého obsahu.

Navrhované ustanovenie upravuje, že úrad vykonáva blokovanie v rámci riešenia kybernetického bezpečnostného incidentu. V rámci riešenia kybernetického bezpečnostného incidentu vydá úrad rozhodnutie o blokovaní, v ktorom určí metódu (spôsob) blokovania a blokovanie vykoná. Spôsob blokovania musí vychádzať z metód uvedených vo všeobecne záväznom právnom predpise, ktorý vydá úrad.
Samozrejme, ide o krajný prostriedok, nástroj, ktorý predstavuje zásah do práv subjektov, ale zároveň predstavuje aj riešenie kybernetického bezpečnostného incidentu v prípade, kedy sú iné nástroje neúčinné a protiprávna, resp. škodlivá aktivita naďalej pokračuje a ohrozuje konečného užívateľa. Zodpovednosť za prípadnú škodu znáša úrad.

Účelom ustanovenie je teda v konečnom dôsledku výšenie obranyschopnosti Slovenskej republiky voči kybernetickým útokom na významné informačné systémy z externého prostredia (internetu), najmä voči šíreniu škodlivého kódu zo sietí infikovaných počítačov a šíreniu škodlivej aktivity z IP adresného rozsahu SR.

Rozhodnutiu úradu o blokovaní sa musí každý povinný subjekt podriadiť. Keďže ide o zásahy na rôznych úrovniach regulácie, úrad pri takomto zásahu môže požadovať súčinnosť rôznych zainteresovaných subjektov. Zmyslom je, aby blokovanie bolo vykonané s ohľadom na spojené riziká, aby bolo účelné, efektívne a zmysluplné.

K § 27c)

V nadväznosti na predchádzajúci paragraf sa ustanovuje možnosť vykonať blokovanie aj na základe žiadosti iného subjektu. Takouto žiadosťou sa rozumie vykonateľné rozhodnutie konkrétneho oprávneného subjektu podľa osobitných predpisov. Úrad v tomto prípade toto rozhodnutie vykoná s náležitou odbornosťou. Zákon dáva každému takémuto subjektu možnosť požiadať úrad o spoluprácu ešte pred vydaním svojho rozhodnutia, čím je možné predchádzať technicky nerealizovateľným rozhodnutiam či neprimeraným zásahom.

K bodu 39
V predmetnom ustanovení § 28 ods. 1 pri výkone kontrolnej činnosti je žiadúce uplatňovať všetky príslušné ustanovenia podľa zákona Národnej rady Slovenskej republiky č. 10/1996 Z. z. o kontrole v štátnej správe v znení neskorších predpisov, ako napr. uloženie poriadkovej pokuty.

K bodu 40 a 41
Certifikovať (t. j. posudzovať zhodu) v súvislosti s formálne stanovenými požiadavkami na znalosti je logicky možné iba pre fyzickú osobu, nie však pre právnickú osobu. Ak by sa mali certifikovať spôsobilosti právnickej osoby, táto by v konečnom dôsledku musela preukázať pred vykonaním každého auditu, že disponuje audítormi, ktorí spĺňajú príslušné znalostné štandardy. Preto certifikačná schéma pre audit v súlade so zákonom č. 69/2018 Z. z. v znení neskorších predpisov je navrhnutá podľa normy STN EN ISO/IEC 17024:2013 Posudzovanie zhody - Všeobecné požiadavky na orgány vykonávajúce certifikáciu osôb. Z uvedených skutočností vyplýva, že audítorom kybernetickej bezpečnosti môže byť len fyzická osoba, spôsobilosti ktorej boli certifikované akreditovaným orgánom posudzovania zhody. Pritom spôsobilosti audítora kybernetickej bezpečnosti sú stanovené v prílohe č. 1 vyhláške č. 436/2019 Z. z. Znalostný štandard audítora sa overuje skúškou. Nie je vylúčené, aby prevádzkovateľ základnej služby zabezpečil vykonanie auditu u niektorej právnickej osoby, ak budú kumulatívne splnené podmienky, že audit kybernetickej bezpečnosti vykoná audítor certifikovaný akreditovaným certifikačným orgánom certifikujúcim osoby príslušným pre certifikáciu personálu v oblasti kybernetickej bezpečnosti podľa ISO/IEC 17024 Personnel Certification - Documents and Resources a zároveň tento audítor spĺňa podmienky uvedené v znalostnom štandarde audítora.

K bodu 42
V § 29 ods. 4 sa navrhuje zabezpečenie auditu kybernetickej bezpečnosti právnickou osobou označiť ako podnikanie podľa Obchodného zákonníka. Uvedená úprava má za cieľ spresniť, že ide o zárobkovú činnosť a zároveň umožní audítorom (vystupujúcim v mene právnickej osoby) zrealizovať zápis činnosti do predmetu podnikateľskej činnosti, resp. získanie identifikačného čísla Štatistickým úradom Slovenskej republiky. Ustanovenie upravuje zodpovednosť právnickej osoby za škodu spôsobenú pri výkone auditu kybernetickej bezpečnosti.

K bodu 43
Zmena navrhovaná v § 29 ods. 6 reaguje na požiadavky aplikačnej praxe s odôvodnením potreby zmeny názvoslovia „orgán posudzovania zhody“ z dôvodu vyššej miery zrozumiteľnosti a špecifikácie konkrétneho subjektu vykonávajúceho audit.

K bodu 44 a 46
Legislatívno-technická úprava.

K bodom 45, 47 až 49

Ide o doplnenie sankcií v súvislosti s povinnosťami.

K bodu 50
Legislatívno-technická úprava. Oprava chyby.

K bodu 51 a 52
Precizuje sa splnomocňovacie ustanovenie, ktorým sa upravujú podrobnosti auditu kybernetickej bezpečnosti v súvislosti s implementáciou nariadenia (EÚ) č. 2019/881 a z dôvodu ďalších normatívnych zmien v zákone.

K bodu 53
Precizuje sa úprava z dôvodu normatívnych zmien.

K bodu 54
V spoločnom ustanovení sa ďalej uvádza, že Ministerstvo obrany Slovenskej republiky vykonáva svoje úlohy prostredníctvom Vojenského spravodajstva. Ide o úpravu v súvislosti s vypustením Vojenského spravodajstva ako ústredného orgánu.

K bodu 55
Prechodné ustanovenie určuje pre prevádzkovateľov základných služieb, ktorí prevádzkujú sieť alebo informačný systém kategórie I a II prechodné obdobie, počas ktorého vykonanie auditu možno nahradiť vykonaním posúdenia účinnosti prijatých bezpečnostných opatrení a plnenia požiadaviek manažérom kybernetickej bezpečnosti.
Ďalej sa uvádza, že zmluvy, ktoré boli uzatvorené v zmysle § 9 ods. 2, resp. odsek 3 zostávajú v platnosti.

K bodom 56 až 63
Ide o úpravu príloh, týkajúcich sa jednotlivých sektorov, vyplývajúcu z aplikačnej praxe. Modifikujú a dopĺňajú sa jednotliví prevádzkovatelia služieb pre niektoré sektory. V časti podsektor „Letecká doprava“ sa mení názov prevádzkovateľa „riadiace orgány letiska“ na „prevádzkovateľ letiska“, pretože letiská poskytujú služby, ktoré je nutné považovať za základné, preto bolo nevyhnutné zrozumiteľnejšie identifikovať prevádzkovateľa týchto služieb. V sektore „Digitálna infraštruktúra“ boli doplnení noví prevádzkovatelia ako „poskytovateľ dátových, hlasových a internetových služieb – služieb pripojenia do internetu“, „prevádzkovateľ obchodu na internete s možnosťou vyhľadávania, objednávania a nákupu tovarov a služieb“ a „poskytovateľ služieb webhostingu, DNS hostingu alebo mailhostingu“ s ohľadom na vzniknutú potrebu regulovať aj uvedené subjekty s podstatným vplyvom na zabezpečenie ochrany kybernetickej bezpečnosti. V sektore „Zdravotníctvo“ boli doplnení uvedení prevádzkovatelia ako Úrady verejného zdravotníctva Slovenskej republiky, správca národných zdravotných registrov, národných zdravotných administratívnych registrov a národného zdravotníckeho informačného systému, s ohľadom na špecifickosť každého z uvádzaných subjektov. V sektore „Verejná správa“ sa vypúšťa podsektor „Spravodajské služby“ a v stĺpci „Prevádzkovateľ služieb“ sa vypúšťajú slová „Správcovia a prevádzkovatelia sietí a informačných systémov prevádzkovaných spravodajskou službou“ a v stĺpci „Ústredný orgán“ sa vypúšťajú slová „Slovenská informačná služba“ a „Vojenské spravodajstvo“. K predmetnému vypusteniu došlo, aby zmena odzrkadľovala ustanovenie článku 1 ods. 6 smernice NIS a súčasne táto zmena vyplynula z potrieb aplikačnej praxe, keďže sa uvedené ukázalo ako neefektívne. Ďalej ide o zmeny technického charakteru ako aj zmeny reflektujúce úpravu subjektov, ktoré plnia úlohy ústredného orgánu.

K čl. II (zákon č. 145/1995 Z. z.)

K bodom 1 a 2
Dopĺňa sa sadzobník správnych poplatkov v časti „Kybernetická bezpečnosť“ o položky v súvislosti s certifikáciou na základe implementácie nariadenia.

K čl. III (zákon č. 351/2011 Z. z.)
K bodu 1
Ide o zjednotenie regulácie pri povinnosti podniku, ktorý poskytuje verejné siete alebo verejné služby prijatím bezpečnostných opatrení podľa zákona o kybernetickej bezpečnosti.

K bodu 2
Na účely „nie dvakrát v tej istej veci“ sa ustanovuje, že priestupky a správne delikty za porušenie bezpečnostných opatrení prejednáva Národný bezpečnostný úrad.

K čl. IV (zákon č. 95/2019 Z. z.)
K bodom 1 až 3
Účelom je zjednotenie regulácie bezpečnostných opatrení tak, aby sa na všetky dotknuté subjekty vzťahovali opatrenia podľa zákona o kybernetickej bezpečnosti a následne, aby zákon č. 95/2019 Z. z. obsahoval iba tie bezpečnostné opatrenia, ktoré sú špecifické pre sektor verejnej správy. Účelom novely zákona je teda zjednotenie regulácie s cieľom odstrániť administratívnu záťaž pri zabezpečovaní kybernetickej bezpečnosti a jednoduchšiu a prehľadnejšiu prax.

K bodu 4
Legislatívno-technická úprava

K bodom 5 až 14
Precizovanie ustanovení v nadväznosti na zjednotenie regulácie bezpečnostných opatrení tak, aby sa na všetky dotknuté subjekty vzťahovali opatrenia podľa zákona o kybernetickej bezpečnosti a následne, aby zákon č. 95/2019 Z. z. obsahoval iba tie bezpečnostné opatrenia, ktoré sú špecifické pre sektor verejnej správy.

K bodu 15
Legislatívno-technická úprava

K bodom 16 a 17
Precizovanie ustanovení v nadväznosti na zjednotenie regulácie bezpečnostných opatrení tak, aby sa na všetky dotknuté subjekty vzťahovali opatrenia podľa zákona o kybernetickej bezpečnosti a následne, aby zákon č. 95/2019 Z. z. obsahoval iba tie bezpečnostné opatrenia, ktoré sú špecifické pre sektor verejnej správy.

K bodom 18 a 19
Legislatívno-technická úprava

K bodom 20 až 27

Precizovanie ustanovení v nadväznosti na zjednotenie regulácie bezpečnostných opatrení tak, aby sa na všetky dotknuté subjekty vzťahovali opatrenia podľa zákona o kybernetickej bezpečnosti a následne, aby zákon č. 95/2019 Z. z. obsahoval iba tie bezpečnostné opatrenia, ktoré sú špecifické pre sektor verejnej správy.

K bodom 28 až 32
Legislatívno-technická úprava

K čl. V

Za deň nadobudnutia účinnosti návrhu zákona sa navrhuje 15. apríla 2021.