**TABUĽKA ZHODY**

**právneho predpisu s právom Európskej únie**

|  |  |
| --- | --- |
|  **Právny akt Európskej únie** **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**  | **Právny predpis Slovenskej republiky****Návrh zákona o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov**Zákon č. 10/1996 Z. z. o kontrole v štátnej správe v znení neskorších predpisovZákon č. 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správyZákon č. 40/1964 Z. z. Občiansky zákonník |
|  1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| Článok (Č,O,V, P) | Text | Spôsob transp. | Číslo | Článok (Č, §, O, V, P) | Text | Zhoda | Poznámky  |
| Č:1,O:1  | Touto smernicou sa stanovujú opatrenia na dosiahnutie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v rámci Únie s cieľom zlepšiť fungovanie vnútorného trhu. | N | Návrh zákona | §:2,O:1§:3 P:g) | Tento zákon ustanovuje minimálne požiadavky na zabezpečenie kybernetickej bezpečnosti. kybernetickou bezpečnosťou stav, v ktorom sú siete a informačné systémy schopné odolávať na určitom stupni spoľahlivosti akémukoľvek konaniu, ktoré ohrozuje dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov. | Ú |  |
| C:1,O:2 | Na tento účel sa v tejto smernici: a) stanovujú pre všetky členské štáty povinnosti prijať národnú stratégiu v oblasti bezpečnosti sietí a informačných systémov; b) vytvára skupina pre spoluprácu s cieľom podporiť a uľahčiť strategickú spoluprácu a výmenu informácií medzi členskými štátmi a rozvíjať vzájomnú dôveru medzi nimi; c) vytvárajú sieť jednotiek pre riešenie počítačových bezpečnostných incidentov (Computer Security Incident Response Teams network – ďalej len „sieť jednotiek CSIRT“) s cieľom prispievať k rozvoju dôvery medzi členskými štátmi a podporovať rýchlu a účinnú operačnú spoluprácu; d) stanovujú bezpečnostné a oznamovacie požiadavky pre prevádzkovateľov základných služieb a pre poskytovateľov digitálnych služieb;e) stanovujú povinnosti členských štátov určiť príslušné vnútroštátne orgány, národné jednotné kontaktné miesta a jednotky CSIRT s úlohami súvisiacimi s bezpečnosťou sietí a informačných systémov. | N | Návrh zákona | §:1 | Tento zákon upravuje a) organizáciu, pôsobnosť a povinnosti orgánov verejnej moci v oblasti kybernetickej bezpečnosti, b) národnú stratégiu kybernetickej bezpečnosti, c) jednotný informačný systém kybernetickej bezpečnosti, d) organizáciu a pôsobnosť jednotiek pre riešenie kybernetických bezpečnostných incidentov (ďalej len „jednotka CSIRT“) a ich akreditáciu, e) postavenie a povinnosti prevádzkovateľa základnej služby a poskytovateľa digitálnej služby, f) bezpečnostné opatrenia, g) systém zabezpečenia kybernetickej bezpečnosti, h) kontrolu nad dodržiavaním tohto zákona a audit  | Ú |  |
| Č:1,O:3 | Bezpečnostné a oznamovacie požiadavky stanovené v tejto smernici sa nevzťahujú na podniky, ktoré podliehajú požiadavkám článkov 13a a 13b smernice 2002/21/ES, ani na poskytovateľov dôveryhodných služieb, na ktorých sa vzťahujú požiadavky článku 19 nariadenia (EÚ) č. 910/2014. | N | Návrh zákona | §:2,O:1O:2 | Tento zákon ustanovuje minimálne požiadavky na zabezpečenie kybernetickej bezpečnosti. Tento zákon sa nevzťahuje naa) požiadavky na zabezpečenie sietí a informačných systémov podľa všeobecného predpisu o ochrane utajovaných skutočností,b) osobitné ustanovenia o úlohách a oprávneniach orgánu štátu pri ochrane kybernetického priestoru podľa osobitného predpisu,1)c) ustanovenia osobitných predpisov o vyšetrovaní, odhaľovaní a stíhaní trestných činov,2)d) požiadavky týkajúce sa bezpečnosti sietí a informačných systémov a oznamovania kybernetických bezpečnostných incidentov v sektore bankovníctva, financií alebo finančného systému podľa osobitného predpisu,3) vrátane štandardov a zásad vydaných alebo prijatých Európskou centrálnou bankou, Európskym systémom centrálnych bánk, Eurosystémom alebo európskymi orgánmi dohľadu,4) ak ich účinok je aspoň rovnocenný s účinkom povinností podľa tohto zákona, a vrátane rozhodnutí, štandardov a zásad vydaných alebo prijatých Národnou bankou Slovenska, ak ich cieľom je dosiahnuť vyššiu úroveň bezpečnosti sietí a informačných systémov ako podľa tohto zákona, ani na platobné systémy a na systémy zúčtovania cenných papierov dohliadané alebo prevádzkované Európskou centrálnou bankou alebo Eurosystémom podľa osobitných predpisov,5)e) požiadavky na zabezpečenie sietí a informačných systémov v sektore podľa osobitného predpisu,6) ak ich cieľom je dosiahnuť vyššiu úroveň bezpečnosti sietí a informačných systémov,f) osobitné predpisy.7) | Ú |  |
| Č:1,O:4 | Uplatňovaním tejto smernice nie je dotknutá smernica Rady 2008/114/ES**1** a smernice Európskeho parlamentu a Rady 2011/93/EÚ**2** a 2013/40/EÚ**3**.  |  N  |  | §:2,O:2 | Tento zákon sa nevzťahuje naa) požiadavky na zabezpečenie sietí a informačných systémov podľa všeobecného predpisu o ochrane utajovaných skutočností,b) osobitné ustanovenia o úlohách a oprávneniach orgánu štátu pri ochrane kybernetického priestoru podľa osobitného predpisu,1)c) ustanovenia osobitných predpisov o vyšetrovaní, odhaľovaní a stíhaní trestných činov,2)d) požiadavky týkajúce sa bezpečnosti sietí a informačných systémov a oznamovania kybernetických bezpečnostných incidentov v sektore bankovníctva, financií alebo finančného systému podľa osobitného predpisu,3) vrátane štandardov a zásad vydaných alebo prijatých Európskou centrálnou bankou, Európskym systémom centrálnych bánk, Eurosystémom alebo európskymi orgánmi dohľadu,4) ak ich účinok je aspoň rovnocenný s účinkom povinností podľa tohto zákona, a vrátane rozhodnutí, štandardov a zásad vydaných alebo prijatých Národnou bankou Slovenska, ak ich cieľom je dosiahnuť vyššiu úroveň bezpečnosti sietí a informačných systémov ako podľa tohto zákona, ani na platobné systémy a na systémy zúčtovania cenných papierov dohliadané alebo prevádzkované Európskou centrálnou bankou alebo Eurosystémom podľa osobitných predpisov,5)e) požiadavky na zabezpečenie sietí a informačných systémov v sektore podľa osobitného predpisu,6) ak ich cieľom je dosiahnuť vyššiu úroveň bezpečnosti sietí a informačných systémov,f) osobitné predpisy.7) | U |  |
| Č:1,O:5 | 5. Bez toho, aby bol dotknutý článok 346 ZFEÚ, informácie, ktoré sú dôverné podľa predpisov Únie a vnútroštátnych predpisov, ako napríklad predpisov o obchodnom tajomstve, sa vymieňajú s Komisiou a inými príslušnými orgánmi len v prípade, ak je takáto výmena potrebná na účely uplatňovania tejto smernice. Vymieňané informácie sa obmedzujú na tie, ktoré sú relevantné a primerané účelu takejto výmeny. Pri takejto výmene informácií sa zachováva dôvernosť týchto informácií a chránia sa bezpečnostné a obchodné záujmy prevádzkovateľov základných služieb a poskytovateľov digitálnych služieb. | N | Návrh zákona | § 5 O:1P:e§:5, O:1, P:t §:12, O:1 | Úrad v oblasti kybernetickej bezpečnosti je národným kontaktným miestom pre kybernetickú bezpečnosť pre zahraničie a zabezpečuje spoluprácu s jednotnými kontaktnými miestami iných členských štátov Európskej únie a Organizácie severoatlantickej zmluvy,Úrad v oblasti kybernetickej bezpečnosti prijíma hlásenia o kybernetických bezpečnostných incidentoch zo zahraničia a zabezpečuje spoluprácu s medzinárodnými organizáciami a orgánmi iných štátov pri riešení kybernetických bezpečnostných incidentov s cezhraničným charakterom,Kto plní alebo plnil úlohy na základe tohto zákona alebo v súvislosti s ním, je povinný zachovávať mlčanlivosť o skutočnostiach, o ktorých sa v súvislosti s plnením úloh podľa tohto zákona dozvedel a ktoré nie sú verejne známe. Povinnosť zachovávať mlčanlivosť trvá aj po skončení dohody o spolupráci podľa § 5 ods. 2 alebo § 9 ods. 4, pracovnoprávneho vzťahu alebo obdobného pracovného vzťahu vrátane služobného pomeru.14) Ustanoveniami o povinnosti zachovávať mlčanlivosť podľa tohto zákona nie je dotknutá povinnosť mlčanlivosti alebo zachovania tajomstva podľa osobitných predpisov.15) | Ú | .  |
| Č:1,O:6 | 6. Touto smernicou nie sú dotknuté opatrenia prijímané členskými štátmi na zabezpečenie ich základných štátnych funkcií, najmä na zabezpečenie národnej bezpečnosti vrátane opatrení na ochranu informácií, ktorých sprístupnenie členské štáty považujú za odporujúce základným záujmom ich bezpečnosti, a na udržanie verejného poriadku, najmä na účely umožnenia vyšetrovania, odhaľovania a stíhania trestných činov.  | N |  | §:2,O:2 | Tento zákon sa nevzťahuje naa) požiadavky na zabezpečenie sietí a informačných systémov podľa všeobecného predpisu o ochrane utajovaných skutočností,b) osobitné ustanovenia o úlohách a oprávneniach orgánu štátu pri ochrane kybernetického priestoru podľa osobitného predpisu,1)c) ustanovenia osobitných predpisov o vyšetrovaní, odhaľovaní a stíhaní trestných činov,2)d) požiadavky týkajúce sa bezpečnosti sietí a informačných systémov a oznamovania kybernetických bezpečnostných incidentov v sektore bankovníctva, financií alebo finančného systému podľa osobitného predpisu,3) vrátane štandardov a zásad vydaných alebo prijatých Európskou centrálnou bankou, Európskym systémom centrálnych bánk, Eurosystémom alebo európskymi orgánmi dohľadu,4) ak ich účinok je aspoň rovnocenný s účinkom povinností podľa tohto zákona, a vrátane rozhodnutí, štandardov a zásad vydaných alebo prijatých Národnou bankou Slovenska, ak ich cieľom je dosiahnuť vyššiu úroveň bezpečnosti sietí a informačných systémov ako podľa tohto zákona, ani na platobné systémy a na systémy zúčtovania cenných papierov dohliadané alebo prevádzkované Európskou centrálnou bankou alebo Eurosystémom podľa osobitných predpisov,5)e) požiadavky na zabezpečenie sietí a informačných systémov v sektore podľa osobitného predpisu,6) ak ich cieľom je dosiahnuť vyššiu úroveň bezpečnosti sietí a informačných systémov,f) osobitné predpisy.7) | Ú |  |
| Č:1,O:7 | 7. Ak sa podľa právneho aktu Únie špecifického pre určité odvetvie vyžaduje, aby prevádzkovatelia základných služieb alebo poskytovatelia digitálnych služieb buď zabezpečovali bezpečnosť ich sietí a informačných systémov, alebo aby oznamovali incidenty, uplatňujú sa ustanovenia tohto právneho aktu Únie špecifického pre určité odvetvie pod podmienkou, že tieto požiadavky majú aspoň rovnocenný účinok ako povinnosti stanovené v tejto smernici. | N | Návrh zákona | §:2, O:2 | Tento zákon sa nevzťahuje naa) požiadavky na zabezpečenie sietí a informačných systémov podľa všeobecného predpisu o ochrane utajovaných skutočností,b) osobitné ustanovenia o úlohách a oprávneniach orgánu štátu pri ochrane kybernetického priestoru podľa osobitného predpisu,1)c) ustanovenia osobitných predpisov o vyšetrovaní, odhaľovaní a stíhaní trestných činov,2)d) požiadavky týkajúce sa bezpečnosti sietí a informačných systémov a oznamovania kybernetických bezpečnostných incidentov v sektore bankovníctva, financií alebo finančného systému podľa osobitného predpisu,3) vrátane štandardov a zásad vydaných alebo prijatých Európskou centrálnou bankou, Európskym systémom centrálnych bánk, Eurosystémom alebo európskymi orgánmi dohľadu,4) ak ich účinok je aspoň rovnocenný s účinkom povinností podľa tohto zákona, a vrátane rozhodnutí, štandardov a zásad vydaných alebo prijatých Národnou bankou Slovenska, ak ich cieľom je dosiahnuť vyššiu úroveň bezpečnosti sietí a informačných systémov ako podľa tohto zákona, ani na platobné systémy a na systémy zúčtovania cenných papierov dohliadané alebo prevádzkované Európskou centrálnou bankou alebo Eurosystémom podľa osobitných predpisov,5)e) požiadavky na zabezpečenie sietí a informačných systémov v sektore podľa osobitného predpisu,6) ak ich cieľom je dosiahnuť vyššiu úroveň bezpečnosti sietí a informačných systémov,f) osobitné predpisy.7) | Ú |  |
| Č:2 | Spracúvanie osobných údajov podľa tejto smernice sa vykonáva v súlade so smernicou 95/46/ES. 2. Spracúvanie osobných údajov inštitúciami a orgánmi Únie podľa tejto smernice sa vykonáva v súlade s nariadením (ES) č. 45/2001. | N | Návrh zákona | §:12, O:6O:7O:8 | Na účely riešenia kybernetického bezpečnostného incidentu, v rozsahu potrebnom na jeho identifikáciu a zabezpečenia kybernetickej bezpečnosti, úrad v záujme národnej bezpečnosti spracováva v jednotnom informačnom systéme kybernetickej bezpečnosti na čas nevyhnutne potrebný, osobné údaje spôsobom podľa osobitného predpisu.17)Úrad zabezpečí nepretržitú ochranu osobných údajov a informácie spracúvané podľa tohto zákona pred nezákonným vyzradením, zneužitím, poškodením, neoprávneným zničením, odcudzením a stratou spôsobom podľa osobitného predpisu.18)Informácie a osobné údaje získané na základe tohto zákona alebo v súvislosti sním môže úrad použiť len na plnenie úloh podľa tohto zákona. |  Ú |  |
| Č:3 | Minimálna harmonizácia Bez toho, aby bol dotknutý článok 16 ods. 10 a povinnosti členských štátov podľa práva Únie, členské štáty môžu prijať alebo zachovať ustanovenia, ktorých cieľom je dosiahnuť vyššiu úroveň bezpečnosti sietí a informačných systémov. | n.a. |  |  |  |  |  |
| Č:4,O:1 | „sieť a informačný systém“ je: a) elektronická komunikačná sieť v zmysle článku 2 písm. a) smernice 2002/21/ES; b) každé zariadenie alebo skupina vzájomne prepojených alebo súvisiacich zariadení, z ktorých jedno alebo viaceré vykonávajú na základe programu automatické spracúvanie digitálnych údajov, alebo c) digitálne údaje, ktoré sú uložené, spracúvané, získavané alebo prenášané prostredníctvom prvkov uvedených v písmenách a) a b) na účely ich prevádzkovania, používania, ochrany a udržiavania; | N | Návrh zákona | §:3,P:a | sieťou a informačným systémom elektronická komunikačná sieť, informačný systém, každé zariadenie a komunikačný systém alebo údaje, ktoré sú v nich vytvárané, ukladané, spracúvané, získavané alebo prenášané prostredníctvom elektronickej komunikačnej siete alebo informačného systému, na účely prevádzkovania, používania, ochrany a udržiavania týchto sietí a systémov,  | Ú |  |
| Č:4,O:2 | „bezpečnosť sietí a informačných systémov“ je schopnosť sietí a informačných systémov odolávať na určitom stupni spoľahlivosti akémukoľvek konaniu, ktoré ohrozuje dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov; | N | Návrh zákona | §:3,P:g | kybernetickou bezpečnosťou stav, v ktorom sú siete a informačné systémy schopné odolávať na určitom stupni spoľahlivosti akémukoľvek konaniu, ktoré ohrozuje dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov, | Ú |  |
| Č:4,O:3 | národná stratégia v oblasti bezpečnosti sietí a informačných systémov“ je rámec, v ktorom sa stanovujú strategické ciele a priority v oblasti bezpečnosti sietí a informačných systémov na vnútroštátnej úrovni | N | Návrh zákona | §:7,O:1 | Národná stratégia kybernetickej bezpečnosti je východiskový strategický dokument, ktorý komplexne určuje strategický prístup Slovenskej republiky k zabezpečeniu kybernetickej bezpečnosti. Súčasťou národnej stratégie kybernetickej bezpečnosti je akčný plán ako konkrétny plán čiastkových úloh a zdrojov. | Ú |  |
| Č:4,O:4 | „prevádzkovateľ základných služieb“ je verejný alebo súkromný subjekt, ktorého typ sa uvádza v prílohe II, spĺňajúci kritériá stanovené v článku 5 ods. 2; | N | Návrh zákona | §:3,P:l | prevádzkovateľom základnej služby orgán verejnej moci alebo osoba, ktorá prevádzkuje aspoň jednu službu podľa písmena k) prvého až tretieho bodu, | Ú |  |
| Č:4,O:5 | „digitálna služba“ je služba v zmysle článku 1 ods. 1 písm. b) smernice Európskeho parlamentu a Rady (EÚ) 2015/1535**1**, ktorej druh sa uvádza v prílohe III; | N | Návrh zákona | §: 3, P: m | digitálnou službou služba, ktorej druh je uvedený v prílohe č. 2 |  Ú |  |
| Č:4,O:6 | „poskytovateľ digitálnych služieb“ je každá právnická osoba, ktorá poskytuje digitálnu službu; | N | Návrh zákona | §:3,P:n | poskytovateľom digitálnej služby právnická osoba alebo fyzická osoba - podnikateľ, ktorá poskytuje digitálnu službu a zároveň zamestnáva 50 a viac zamestnancov a má ročný obrat alebo celkovú ročnú bilanciu viac ako 10 000 000 eur,  | Ú |  |
| Č:4,O:7 | „incident“ je každá udalosť, ktorá má skutočne nepriaznivý vplyv na bezpečnosť sietí a informačných systémov; | N | Návrhzákona | §:3,P:j | kybernetickým bezpečnostným incidentom akákoľvek udalosť, ktorá má z dôvodu narušenia bezpečnosti siete a informačného systému, alebo porušenia bezpečnostnej politiky alebo záväznej metodiky negatívny vplyv na kybernetickú bezpečnosť alebo ktorej následkom je1. strata dôvernosti údajov, zničenie údajov alebo narušenie integrity systému,2. obmedzenie alebo odmietnutie dostupnosti základnej služby alebo digitálnej služby,3. vysoká pravdepodobnosť kompromitácie činností základnej služby alebo digitálnej služby alebo4. ohrozenie bezpečnosti informácií, | Ú |  |
| Č:4,O:8 | „riešenie incidentov“ sú všetky postupy na podporu odhaľovania, analýzy a obmedzenia následkov incidentu a reakcie naň; | N | Návrh zákona | §:3,P:o | riešením kybernetického bezpečnostného incidentu všetky postupy súvisiace s oznamovaním, odhaľovaním, analýzou a reakciou na kybernetický bezpečnostný incident a jeho následky. | Ú |  |
| Č:4,O:9 | „riziko“ je každá primerane rozpoznateľná okolnosť alebo udalosť, ktorá môže mať nepriaznivý vplyv na bezpečnosť sietí a informačných systémov; | N | Návrh zákona | §:3, P: h | rizikom miera kybernetického ohrozenia vyjadrená pravdepodobnosťou vzniku nežiaduceho javu a jeho dôsledkami, | Ú |  |
| Č:4,O:10 | „zástupca“ je akákoľvek fyzická alebo právnická osoba usadená v Únii, ktorá je výslovne poverená konať v mene poskytovateľa digitálnej služby, ktorý nie je usadený v Únii, na ktorú sa môže vnútroštátny príslušný orgán alebo jednotka CSIRT obrátiť namiesto poskytovateľa digitálnych služieb, pokiaľ ide o povinnosti uvedeného poskytovateľa digitálnych služieb podľa tejto smernice; | N | Návrh zákona | §:23,O:1 | Zástupcom poskytovateľa digitálnej služby je právnická osoba, ktorá má sídlo v Slovenskej republike alebo fyzická osoba - podnikateľ, ktorá má miesto podnikania v Slovenskej republike, ak odsek 2 neustanovuje inak, a ktorá je poskytovateľom digitálnej služby písomne poverená konať v jeho mene a na jeho zodpovednosť vo vzťahu k povinnostiam podľa tohto zákona. | Ú |  |
| Č:4,O:11 | „norma“ je norma v zmysle článku 2 bodu 1 nariadenia (EÚ) č. 1025/2012; | n.a |  |  |  |  |  |
| Č:4,O:12 | „špecifikácia“ je technická špecifikácia v zmysle článku 2 bodu 4 nariadenia (ES) č. 1025/2012; | n.a |  |  |  |  |  |
| Č:4,O:13 | „internetový prepojovací uzol (IXP)“ je sieťové zariadenie, ktoré umožňuje prepojenie viac než dvoch nezávislých autonómnych systémov, najmä na účely uľahčenia internetového dátového toku; IXP prepojuje len autonómne systémy; pri IXP nemusí internetový dátový tok medzi ktoroukoľvek dvojicou zúčastnených autonómnych systémov prechádzať cez žiaden tretí autonómny systém, pričom tento dátový tok sa nijak nemení ani sa doň nijak nezasahuje;  | N | Návrh zákona  | Príloha č.1 | sieťové zariadenie, ktoré umožňuje prepojenie viac než dvoch nezávislých autonómnych systémov najmä na účely uľahčenia internetového dátového toku; IXP prepojuje len autonómne systémy; pri IXP nemusí internetový dátový tok medzi ktoroukoľvek dvojicou zúčastnených autonómnych systémov prechádzať cez žiadny tretí autonómny systém, pričom tento dátový tok sa nijako nemení ani sa doň nijako nezasahuje | Ú |  |
| Č:4,O:14 | „systém názvov domén (DNS)“ je hierarchický distribuovaný systém pomenovaní v sieti, ktorý prekladá vyhľadávanie názvov domén; | N | Návrh zákona | Príloha č. 1 | hierarchický distribuovaný systém pomenovaní v sieti, ktorý prekladá vyhľadávanie názvov domén. | Ú |  |
| Č:4,O:15 | „poskytovateľ služieb DNS“ je subjekt, ktorý poskytuje na internete služby DNS; | N | Návrh zákona | Príloha č. 1 | poskytovateľ služieb DNS je subjekt, ktorý poskytuje na internete služby DNS | Ú |  |
| Č:4,O:16 | „register domén najvyššej úrovne“ je subjekt, ktorý spravuje a prevádzkuje registráciu názvov internetových domén v rámci určitej domény najvyššej úrovne (TLD); |  | Návrh zákona | Príloha č. 1 | subjekt, ktorý spravuje a prevádzkuje registráciu názvov internetových domén v rámci určitej domény najvyššej úrovne (TLD). | Ú |  |
| Č:4,O:17 | „online trhovisko“ je digitálna služba, ktorá umožňuje spotrebiteľom a/alebo obchodníkom v zmysle článku 4 ods. 1 písm. a) a b) smernice Európskeho parlamentu a Rady 2013/11/EÚ**1** uzavierať online kúpne zmluvy alebo zmluvy o službách s obchodníkmi buď na webovom sídle online trhoviska, alebo na webovom sídle obchodníka, ktoré využíva počítačové služby poskytované online trhoviskom; |  | Návrh zákona | Príloha č. 2 | digitálna služba, ktorá umožňuje spotrebiteľom alebo podnikateľom uzatvárať online kúpne zmluvy alebo zmluvy o službách s podnikateľmi buď na webovom sídle online trhoviska, alebo na webovom sídle podnikateľa, ktoré využíva počítačové služby poskytované online trhoviskom. | Ú |  |
| Č:4,O:18 | „internetový vyhľadávač“ je digitálna služba, ktorá umožňuje používateľom vyhľadávať v zásade na všetkých webových sídlach alebo na webových sídlach v konkrétnom jazyku informácie o akejkoľvek téme na základe kľúčového slova, vety alebo iných zadaných údajov, pričom jeho výsledkom sú linky, prostredníctvom ktorých možno nájsť informácie súvisiace s požadovaným obsahom; |  | Návrh zákona | Príloha č. 2 | digitálna služba, ktorá umožňuje používateľom vyhľadávať v zásade na všetkých webových sídlach alebo na webových sídlach v konkrétnom jazyku informácie o akejkoľvek téme na základe kľúčového slova, vety alebo iných zadaných údajov, pričom jeho výsledkom sú linky, prostredníctvom ktorých možno nájsť informácie súvisiace s požadovaným obsahom. | Ú |  |
| Č:4,O:19 | „služba v oblasti cloud computingu“ je digitálna služba, ktorá umožňuje prístup ku škálovateľnému a pružnému súboru počítačových zdrojov, ktoré možno zdieľať. |  | Návrh zákona | Príloha č. 2 | digitálna služba, ktorá umožňuje prístup ku škálovateľnému a pružnému súboru počítačových zdrojov, ktoré možno zdieľať. | Ú |  |
| Č:5,O:1 | Identifikácia prevádzkovateľov základných služieb 1. Členské štáty do 9. novembra 2018 určia pre každé odvetvie a pododvetvie uvedené v prílohe II prevádzkovateľov základných služieb s prevádzkarňou na ich území. | N | Návrh zákona | §:5,O:1P:k§:9 O:1P:f | Úradna základe oznámenia ústredného orgánu, prevádzkovateľa základnej služby, poskytovateľa digitálnej služby, alebo z vlastnej iniciatívy určuje 1. základnú službu a zaraďuje ju do zoznamu základných služieb, 2. digitálnu službu a zaraďuje ju do zoznamu digitálnych služieb, 3. poskytovateľa digitálnej služby a zaraďuje ho do registra poskytovateľov digitálnych služieb, 4. prevádzkovateľa základnej služby a zaraďuje ho do registra prevádzkovateľov základných služieb, Ústredný orgán identifikuje základnú službu a prevádzkovateľa základnej služby a ich aktuálny zoznam predkladá úradu na účely zaradenia do zoznamu základných služieb a registra prevádzkovateľov základných služieb,  | Ú |  |
| Č:5,O:2 | 2.Kritériá na identifikáciu prevádzkovateľov základných služieb uvedených v článku 4 bode 4 sú tieto: a) subjekt poskytuje službu, ktorá má zásadný význam z hľadiska zachovania kľúčových spoločenských a/alebo hospodárskych činností; b) poskytovanie tejto služby je závislé od sietí a informačných systémov a c) incident by mal závažný rušivý vplyv na poskytovanie uvedenej služby. | N | Návrh zákona | §:17,O:1§:3, P:k§:18O:1O:2O:3O:4 | Ak prevádzkovateľ služby v sektore podľa prílohy č. 1 zistí, že došlo k prekročeniu identifikačných kritérií poskytovanej služby podľa § 18, oznámi to úradu najneskôr do 30 dní odo dňa, kedy prekročenie zistil. základnou službou služba, ktorá je zaradená v zozname základných služieb a1. závisí od sietí a informačných systémov a je činnosťou aspoň v jednom sektore alebo podsektore podľa prílohy č. 1,2. je informačným systémom verejnej správy,8) alebo3. je prvkom kritickej infraštruktúry,9)Identifikačné kritériá poskytovanej služby sú dopadové kritériá a špecifické sektorové kritériá. Dopadové kritériá sú určené všeobecne záväzným právnym predpisom, ktorý vydá úrad a zohľadňujú najmä a) počet používateľov využívajúcich základnú službu, b) závislosť ostatných odvetví podľa prílohy č. 1 od základnej služby c) vplyv, ktorý by mohli mať incidenty z hľadiska rozsahu a trvania a hospodárske a spoločenské činnosti alebo bezpečnosť štátu, d) trhový podiel poskytovateľa služby, e) geografické rozšírenie z hľadiska oblasti, ktorú by kybernetický bezpečnostný incident mohol postihnúť, f) význam poskytovateľa služby z hľadiska zachovania kontinuity poskytovania služby. Špecifické sektorové identifikačné kritériá zohľadňujú kritériá určené všeobecne záväzným právnym predpisom, ktorý vydá úrad. Ak prevádzkovateľ služby podľa prílohy č. 1zistí, že došlo k prekročeniu špecifických sektorových kritérií, oznámi to úradu najneskôr do 30 dní odo dňa, kedy prekročenie zistil spôsobom podľa § 17 ods. 5 aj v prípade, ak neprekročí dopadové kritéria. | Ú |  |
| Č:5,O:3 | Na účely odseku 1 každý členský štát zostaví zoznam služieb uvedených v odseku 2 písm. a). | N | Návrh zákona | §:5,O:1P:k§: 9O:1P:f | Úrad na základe oznámenia ústredného orgánu, prevádzkovateľa základnej služby, poskytovateľa digitálnej služby, alebo z vlastnej iniciatívy určuje 1. základnú službu a zaraďuje ju do zoznamu základných služieb, 2. digitálnu službu a zaraďuje ju do zoznamu digitálnych služieb, 3. poskytovateľa digitálnej služby a zaraďuje ho do registra poskytovateľov digitálnych služieb, 4. prevádzkovateľa základnej služby a zaraďuje ho do registra prevádzkovateľov základných služieb, Ústredný orgán identifikuje základnú službu a prevádzkovateľa základnej služby a ich aktuálny zoznam predkladá úradu na účely zaradenia do zoznamu základných služieb a registra prevádzkovateľov základných služieb,  | Ú |  |
| Č:5,O:4 | Na účely odseku 1, ak subjekt poskytuje službu uvedenú v odseku 2 písm. a) v dvoch alebo viacerých členských štátoch, tieto členské štáty začnú vzájomné konzultácie. Tieto konzultácie sa uskutočnia pred tým, ako sa rozhodne o identifikácii. | N | Návrh zákona | §:19,O:5 | Ak prevádzkovateľ základnej služby túto službu poskytuje aj v inom členskom štáte Európskej únie, úrad v súčinnosti s príslušným orgánom tohto členského štátu rozhodne o tom, podľa kritérií ktorého členského štátu bude prevádzkovateľ základnej služby identifikovaný tak, aby bol jednoznačne identifikovaný ako prevádzkovateľ základnej služby aspoň v jednom z týchto členských štátov. | Ú |  |
| Č:5,O:5 | Členské štáty pravidelne a aspoň každé dva roky od 9. mája 2018 preskúmavajú a v prípade potreby aktualizujú zoznam identifikovaných prevádzkovateľov základných služieb. | N | Návrh zákona | §:5, O:1P:k§:9, O:1P:f§:8O:2 | Úrad na základe oznámenia ústredného orgánu, prevádzkovateľa základnej služby, poskytovateľa digitálnej služby, alebo z vlastnej iniciatívy určuje 1. základnú službu a zaraďuje ju do zoznamu základných služieb, 2. digitálnu službu a zaraďuje ju do zoznamu digitálnych služieb, 3. poskytovateľa digitálnej služby a zaraďuje ho do registra poskytovateľov digitálnych služieb, 4. prevádzkovateľa základnej služby a zaraďuje ho do registra prevádzkovateľov základných služieb, Ústredný orgán identifikuje základnú službu a prevádzkovateľa základnej služby a ich aktuálny zoznam predkladá úradu na účely zaradenia do zoznamu základných služieb a registra prevádzkovateľov základných služieb,Jednotný informačný systém kybernetickej bezpečnosti obsahuje komunikačný systém pre hlásenie a riešenie kybernetických bezpečnostných incidentov a centrálny systém včasného varovania. Jednotný informačný systém pozostáva z verejnej časti a neverejnej časti a prístup k nemu je bezodplatný. Verejná časť jednotného informačného systému kybernetickej bezpečnosti obsahujea) register ústredných orgánov,b) zoznam základných služieb,c) register prevádzkovateľov základných služieb,d) zoznam digitálnych služieb,e) register poskytovateľov digitálnych služieb,f) register kybernetických bezpečnostných incidentov,g) zoznam akreditovaných jednotiek CSIRT,h) metodiky, usmernenia, štandardy, politiky a oznamy,i) informácie a údaje potrebné na používanie jednotného informačného systému kybernetickej bezpečnosti,j) výstrahy a varovania a ďalšie informácie slúžiace na minimalizovanie, odvrátenie alebo nápravu následkov kybernetického bezpečnostného incidentu. | Ú |  |
| Č:5,O:6 | Úlohou skupiny pre spoluprácu je v súlade s úlohami uvedenými v článku 11 podporovať členské štáty, aby v procese identifikácie prevádzkovateľov základných služieb postupovali jednotne. | n.a |  |  |  |  |  |
| Č:5,O:7 | Na účely preskúmania uvedeného v článku 23 a do 9. novembra 2018 a potom každé dva roky členské štáty predložia Komisii informácie, ktoré potrebuje na to, aby mohla posúdiť vykonávanie tejto smernice, najmä jednotnosť postupov členských štátov pri identifikácii prevádzkovateľov základných služieb. Tieto informácie zahŕňajú aspoň: a) vnútroštátne opatrenia umožňujúce identifikáciu prevádzkovateľov základných služieb; b) zoznam služieb uvedený v odseku 3; c) počet prevádzkovateľov základných služieb určených pre každé z odvetví uvedených v prílohe II a ich význam pre dané odvetvie; d) prípadné prahové hodnoty na určenie príslušnej úrovne poskytovania podľa počtu používateľov využívajúcich túto službu, ako sa uvádza v článku 6 ods. 1 písm. a), alebo významu konkrétneho prevádzkovateľa základných služieb, ako sa uvádza v článku 6 ods. 1 písm. f). S cieľom prispieť k poskytovaniu porovnateľných informácií môže Komisia, zohľadňujúc v čo najväčšej miere stanovisko agentúry ENISA, prijať vhodné technické usmernenia týkajúce sa parametrov informácií uvedených v tomto odseku. | ND | Návrh zákon | §:5,O:1P:fP:h) | Úrad plní notifikačné a reportingové povinnosti voči príslušným orgánom Európskej únie a Organizácie severoatlantickej zmluvy a podieľa sa a podporuje vytváranie partnerstiev na národnej a medzinárodnej úrovni v oblasti kybernetickej bezpečnosti, Úrad v spolupráci s Ministerstvom zahraničných vecí a európskych záležitostí Slovenskej republiky rozvíja medzinárodnú spoluprácu a sleduje dopady aktivít v oblasti kybernetickej bezpečnosti na zahraničnopolitické záujmy Slovenskej republiky a partnerov v rámci Európskej únie a Organizácie severoatlantickej zmluvy,  | Ú |  |
| Č:6,O:1 | Článok 6 Závažný rušivý vplyv 1. Pri určovaní závažnosti rušivého vplyvu uvedeného v článku 5 ods. 2 písm. c) členské štáty zohľadňujú aspoň tieto medziodvetvové faktory: a) počet používateľov využívajúcich službu, ktorú poskytuje daný subjekt; b) závislosť ostatných odvetví uvedených v prílohe II od služby, ktorú poskytuje daný subjekt; c) vplyvu, ktorý by mohli mať incidenty z hľadiska rozsahu a trvania na hospodárske a spoločenské činnosti alebo verejnú bezpečnosť; d) trhový podiel daného subjektu; e) geografické rozšírenie z hľadiska oblasti, ktorú by incident mohol postihnúť; f) význam subjektu z hľadiska zachovania dostatočnej úrovne služby, berúc do úvahy dostupnosť alternatívnych spôsobov poskytovania danej služby. | N | Návrh zákona | §:17,O:1§:18O:1O:2O:3O:4 | Ak prevádzkovateľ služby v sektore podľa prílohy č. 1 zistí, že došlo k prekročeniu identifikačných kritérií poskytovanej služby podľa § 18, oznámi to úradu najneskôr do 30 dní odo dňa, kedy prekročenie zistil Identifikačné kritériá poskytovanej služby sú dopadové kritériá a špecifické sektorové kritériá. Dopadové kritériá sú určené všeobecne záväzným právnym predpisom, ktorý vydá úrad a zohľadňujú najmä a) počet používateľov využívajúcich základnú službu, b) závislosť ostatných odvetví podľa prílohy č. 1 od základnej služby c) vplyv, ktorý by mohli mať incidenty z hľadiska rozsahu a trvania a hospodárske a spoločenské činnosti alebo bezpečnosť štátu, d) trhový podiel poskytovateľa služby, e) geografické rozšírenie z hľadiska oblasti, ktorú by kybernetický bezpečnostný incident mohol postihnúť, f) význam poskytovateľa služby z hľadiska zachovania kontinuity poskytovania služby. Špecifické sektorové identifikačné kritériá zohľadňujú kritériá určené všeobecne záväzným právnym predpisom, ktorý vydá úrad. Ak prevádzkovateľ služby podľa prílohy č. 1zistí, že došlo k prekročeniu špecifických sektorových kritérií, oznámi to úradu najneskôr do 30 dní odo dňa, kedy prekročenie zistil spôsobom podľa § 17 ods. 5 aj v prípade, ak neprekročí dopadové kritéria. | Ú |  |
| Č:6,O:2 | Pri určovaní toho, či by mal incident závažný rušivý vplyv, členské štáty zohľadňujú podľa potreby aj faktory špecifické pre jednotlivé odvetvia. | N | Návrh zákona  | §:18,O:3O:4 | Špecifické sektorové kritériá zohľadňujú kritériá určené všeobecne záväzným právnym predpisom, ktorý vydá úrad.Ak prevádzkovateľ služby podľa prílohy č. 1zistí, že došlo k prekročeniu špecifických sektorových kritérií, oznámi to úradu najneskôr do 30 dní odo dňa, kedy prekročenie zistil spôsobom podľa § 17 ods. 5 aj v prípade, ak neprekročí dopadové kritéria. | Ú |  |
| Č:7 | Článok 7 Národná stratégia v oblasti bezpečnosti sietí a informačných systémov 1. Každý členský štát prijme národnú stratégiu v oblasti bezpečnosti sietí a informačných systémov, v ktorej sa vymedzia strategické ciele a vhodné politické a regulačné opatrenia na dosiahnutie a udržanie vysokej úrovne bezpečnosti sietí a informačných systémov a ktorá sa vzťahuje aspoň na odvetvia uvedené v prílohe II a služby uvedené v prílohe III. Národná stratégia v oblasti bezpečnosti sietí a informačných systémov sa venuje najmä týmto otázkam: a) ciele a priority národnej stratégie v oblasti bezpečnosti sietí a informačných systémov; b) rámec riadenia na dosiahnutie cieľov a priorít národnej stratégie v oblasti bezpečnosti sietí a informačných systémov vrátane úloh a zodpovedností vládnych orgánov a ďalších relevantných aktérov; c) identifikácia opatrení týkajúcich sa pripravenosti, reakcie a obnovy, vrátane spolupráce medzi verejným a súkromným sektorom;d) určenie vzdelávacích programov, programov na zvyšovanie informovanosti a programov odbornej prípravy súvisiacich s národnou stratégiou v oblasti bezpečnosti sietí a informačných systémov; e) určenie plánov výskumu a vývoja súvisiacich s národnou stratégiou v oblasti bezpečnosti sietí a informačných systémov; f) plán posudzovania rizika na účely identifikácie rizík; g) zoznam rôznych aktérov zapojených do vykonávania národnej stratégie v oblasti bezpečnosti sietí a informačných systémov. | N | Návrh zákona | §:7,O:1O:2O:3O:4 | Národná stratégia kybernetickej bezpečnosti je východiskový strategický dokument, ktorý komplexne určuje strategický prístup štátu k zabezpečeniu kybernetickej bezpečnosti. Súčasťou národnej stratégie kybernetickej bezpečnosti je akčný plán ako konkrétny plán čiastkových úloh a zdrojov. Národná stratégia kybernetickej bezpečnosti obsahuje najmä a) ciele, priority a rámec riadenia na dosiahnutie týchto cieľov a priorít vrátane úloh a zodpovedností orgánov verejnej moci a ďalších relevantných subjektov, b) identifikáciu opatrení týkajúcich sa pripravenosti, reakcie a obnovy vrátane spolupráce medzi verejným sektorom a súkromným sektorom, c) popis bezpečnostného prostredia, d) definíciu bezpečnostných hrozieb, e) identifikáciu potrebných zdrojov, f) určenie vzdelávacích programov, programov na budovanie bezpečnostného povedomia, zvyšovanie informovanosti a odbornej prípravy, g) určenie plánov výskumu a vývoja, h) plán posudzovania rizika na účely identifikácie rizík, i) zoznam subjektov zapojených do vykonávania národnej stratégie kybernetickej bezpečnosti, j) určenie hlavných zahraničnopolitických partnerov. Ústredné orgány a iné orgány štátnej správy spolupracujú s úradom na vypracovaní národnej stratégie kybernetickej bezpečnosti a na tento účel sú povinné poskytnúť mu informácie v potrebnom rozsahu Národnú stratégiu kybernetickej bezpečnosti schvaľuje vláda Slovenskej republiky  | Ú |  |
| Č:7,O:2 | Členské štáty môžu pri vypracúvaní národných stratégií v oblasti bezpečnosti sietí a informačných systémov požiadať o pomoc agentúru ENISA. | D |  |  |  |  |  |
| Č:7,O:3 | Členské štáty oznámia Komisii svoje národné stratégie v oblasti bezpečnosti sietí a informačných systémov do troch mesiacov od ich prijatia. Členské štáty môžu pritom vylúčiť prvky stratégie, ktoré sa týkajú národnej bezpečnosti. | N | Návrh zákona | §:5,O:1P:f | Úradplní notifikačné a reportingové povinnosti voči príslušným orgánom Európskej únie a Organizácie severoatlantickej zmluvy a podieľa sa a podporuje vytváranie partnerstiev na národnej a medzinárodnej úrovni v oblasti kybernetickej bezpečnosti | Ú |  |
| Č:8,O:1 | Vnútroštátne príslušné orgány a národné jednotné kontaktné miesto 1. Každý členský štát určí jeden alebo viaceré vnútroštátne príslušné orgány pre bezpečnosť sietí a informačných systémov (ďalej len „príslušný orgán“), ktoré sa zaoberajú aspoň odvetviami uvedenými v prílohe II a službami uvedenými v prílohe III. Členské štáty môžu touto úlohou poveriť existujúci orgán alebo orgány.  | N | Návrh zákona | §:4 | Pôsobnosť v oblasti kybernetickej bezpečnosti vykonáva a) Národný bezpečnostný úrad (ďalej len „úrad“), b) úrad, Ministerstvo dopravy a výstavby Slovenskej republiky, Ministerstvo financií Slovenskej republiky, Ministerstvo hospodárstva Slovenskej republiky, Ministerstvo obrany Slovenskej republiky, Ministerstvo vnútra Slovenskej republiky, Ministerstvo zdravotníctva Slovenskej republiky, Ministerstvo životného prostredia Slovenskej republiky, Slovenská informačná služba, Úrad podpredsedu vlády pre investície a informatizáciu a Vojenské spravodajstvo (ďalej ako „ústredný orgán“), c) ministerstvá a ostatné ústredné orgány štátnej správy, 10) ktoré nie sú ústredným orgánom, Generálna prokuratúra Slovenskej republiky, Najvyšší kontrolný úrad Slovenskej republiky, Úrad pre dohľad nad zdravotnou starostlivosťou, Úrad na ochranu osobných údajov Slovenskej republiky, Úrad pre reguláciu elektronických komunikácií a poštových služieb, Úrad pre reguláciu sieťových odvetví a iné štátne orgány v rozsahu svojej pôsobnosti (ďalej len „iný orgán štátnej správy“).  | Ú |  |
| Č:8,O:2 | 2. Príslušné orgány monitorujú uplatňovanie tejto smernice na vnútroštátnej úrovni. |  | Návrh zákona | §:5,O:1P:m§9: O:1P:b | Úrad systematicky získava, sústreďuje, analyzuje a vyhodnocuje informácie o stave kybernetickej bezpečnosti v Slovenskej republike, Ústredný orgán poskytuje úradom požadovanú súčinnosť a informácie získané z vlastnej činnosti dôležité pre zabezpečenie kybernetickej bezpečnosti; informácie sa poskytujú len za podmienky, že ich poskytnutím nedôjde k ohrozeniu plnenia konkrétnej úlohy podľa osobitného predpisu13) alebo k odhaleniu jej zdrojov, prostriedkov, totožnosti osôb konajúcich v jej prospech, alebo k ohrozeniu medzinárodnej spravodajskej spolupráce,  | Ú |  |
| Č:8,O:3 | 3.Každý členský štát určí národné jednotné kontaktné miesto pre bezpečnosť sietí a informačných systémov (ďalej len „jednotné kontaktné miesto“). Členské štáty môžu touto úlohou poveriť existujúci orgán. Ak členský štát určí iba jeden príslušný orgán, tento príslušný orgán je aj jednotným kontaktným miestom. |  | Návrh zákona | §:5,O:1P:e | Úrad je národným kontaktným miestom pre kybernetickú bezpečnosť pre zahraničie a zabezpečuje spoluprácu s jednotnými kontaktnými miestami iných členských štátov Európskej únie a Organizácie severoatlantickej zmluvy | Ú |  |
| Č:8,O:4 | 4.Jednotné kontaktné miesto vykonáva styčnú úlohu, aby zabezpečilo cezhraničnú spoluprácu orgánov členských štátov s príslušnými orgánmi v iných členských štátoch, so skupinou pre spoluprácu uvedenou v článku 11 a sieťou jednotiek CSIRT uvedenou v článku 12 |  | Návrh zákona | §:5,O:1P:eP:f | Úrad je národným kontaktným miestom pre kybernetickú bezpečnosť pre zahraničie a zabezpečuje spoluprácu s jednotnými kontaktnými miestami iných členských štátov Európskej únie a Organizácie severoatlantickej zmluvy, Úrad plní notifikačné a reportingové povinnosti voči príslušným orgánom Európskej únie a Organizácie severoatlantickej zmluvy a podieľa sa a podporuje vytváranie partnerstiev na národnej a medzinárodnej úrovni v oblasti kybernetickej bezpečnosti  | Ú |  |
| Č:8,O:5 | Členské štáty zabezpečia, aby príslušné orgány a jednotné kontaktné miesta mali primerané zdroje na účinné a efektívne vykonávanie zverených úloh, a teda na plnenie cieľov tejto smernice. Členské štáty zabezpečia účinnú, efektívnu a bezpečnú spoluprácu určených zástupcov v rámci skupiny pre spoluprácu. | N | Návrh zákona | §:5,O:1P:e | Úrad je národným kontaktným miestom pre kybernetickú bezpečnosť pre zahraničie a zabezpečuje spoluprácu s jednotnými kontaktnými miestami iných členských štátov Európskej únie a Organizácie severoatlantickej zmluvy, | Ú |  |
| Č:8,O:6 | Príslušné orgány a jednotné kontaktné miesto vždy, keď je to vhodné, a v súlade s vnútroštátnym právom konzultujú a spolupracujú s príslušnými vnútroštátnymi orgánmi presadzovania práva a vnútroštátnymi orgánmi pre ochranu údajov. |  | Zákon č. 575/2001 o organizácii činnosti vlády a organizácii ústrednej štátnej správy  | §:38,O:1 |  Ministerstvá a ostatné ústredné orgány štátnej správy pri plnení svojich úloh úzko spolupracujú. Vymieňajú si potrebné informácie a podklady a prerokúvajú s inými ministerstvami opatrenia, ktoré sa ich dotýkajú. | Ú |  |
| Č:8,O:7 | Každý členský štát bezodkladne oznámi Komisii určenie príslušného orgánu a jednotného kontaktného miesta, ich úlohy a akékoľvek následné zmeny. Každý členský štát zverejní určenie príslušného orgánu a jednotného kontaktného miesta. Komisia uverejní zoznam určených jednotných kontaktných miest. | Nn.a. | Návrh zákona | §:5,O:1P:f | Úrad plní notifikačné a reportingové povinnosti voči príslušným orgánom Európskej únie a Organizácie severoatlantickej zmluvy a podieľa sa a podporuje vytváranie partnerstiev na národnej a medzinárodnej úrovni v oblasti kybernetickej bezpečnosti  | Ú |  |
| Č:9,O:1 | Článok 9 Jednotky pre riešenie počítačových bezpečnostných incidentov (jednotky CSIRT) 1. Každý členský štát určí jednu alebo viac jednotiek CSIRT, ktoré spĺňajú požiadavky stanovené v bode 1 prílohy I, pokrývajú aspoň odvetvia uvedené v prílohe II a služby uvedené v prílohe III a ktoré zodpovedajú za riešenie rizík a incidentov podľa presne stanoveného postupu. Jednotku CSIRT možno zriadiť v rámci príslušného orgánu. |  | Návrh zákona | § 6, O:1§:9 O:2§ 11 | Úrad má postavenie národnej jednotky CSIRT s pôsobnosťou pre Slovenskú republiku, ktorá musí spĺňať podmienky akreditácie podľa § 14 a plniť úlohy jednotky CSIRT podľa § 15 pre všetky sektory a podsektory uvedené v prílohe č. 1 a digitálne služby, okrem tých sektorov a podsektorov, pre ktoré plnia úlohy jednotky CSIRT ústredné orgány. Národná jednotka CSIRT je zaradená v zozname akreditovaných jednotiek CSIRT.Ústredný orgán na účely plnenia úloh podľa odseku 1 písm. a), v rozsahu svojej pôsobnosti pre sektor alebo podsektor podľa prílohy č. 1, zriaďuje a prevádzkuje akreditovanú jednotku CSIRT alebo na tento účel využíva akreditovanú jednotku CSIRT, ktorú zriaďuje a prevádzkuje iný ústredný orgán, okrem vládnej jednotky CSIRT, ak sa tak dohodnú. Využívanie akreditovanej jednotky CSIRT, ktorú zriaďuje a prevádzkuje iný ústredný orgán, sa vykonáva na základe zmluvy. Ústredný orgán, ktorým je Úrad podpredsedu vlády Slovenskej republiky pre investície a informatizáciu zabezpečuje úlohy podľa odseku 1 písm. a) prostredníctvom vládnej jednotky CSIRT.Zriaďuje sa vládna jednotka CSIRT v pôsobnosti Úradu vlády Slovenskej republiky pre podsektor informačné systémy verejnej správy. Vládna jednotka CSIRT musí spĺňať podmienky akreditácie podľa § 14 a plniť úlohy podľa § 15. Vládna jednotka CSIRT sa zaraďuje do zoznamu akreditovaných jednotiek CSIRT. | Ú |  |
| Č:9,,O:2 | Členské štáty zabezpečia, aby mali jednotky CSIRT primerané zdroje na účinné plnenie svojich úloh stanovených v bode 2 prílohy I. Členské štáty zabezpečia účinnú, efektívnu a bezpečnú spoluprácu svojich jednotiek CSIRT v rámci siete jednotiek CSIRT uvedenej v článku 12. |  | Návrh zákona | §:15, O:2 | Preventívne služby sa zameriavajú na prevenciu kybernetických bezpečnostných incidentov a) vytváraním bezpečnostného povedomia, b) výcvikom, c) spoluprácou s ostatnými jednotkami CSIRT, d) monitorovaním a evidenciou kybernetických bezpečnostných incidentov, e) pripojením na jednotný informačný systém kybernetickej bezpečnosti, f) poskytovaním informácií a údajov do jednotného informačného systému kybernetickej bezpečnosti, g) prijímaním a zasielaním včasného varovania pred kybernetickými bezpečnostnými incidentmi prostredníctvom jednotného informačného systému kybernetickej bezpečnosti.  | Ú |  |
| Č:9,O:3 | Členské štáty zabezpečia, aby ich jednotky CSIRT mali prístup k primeranej, bezpečnej a odolnej komunikačnej a informačnej infraštruktúre na vnútroštátnej úrovni. | N | Návrh zákona | §:8, O:5 | K neverejnej časti jednotného informačného systému kybernetickej bezpečnosti má priamy prístup v elektronickej forme v reálnom čase, v rozsahu určenom úradom alebo osobitným predpisom12) a na základe vecnej pôsobnostia) ústredný orgán,b) jednotka CSIRT zaradená v zozname akreditovaných jednotiek CSIRT,c) prevádzkovateľ základnej služby a poskytovateľ digitálnej služby,d) Národná banka Slovenska,e) Úrad na ochranu osobných údajov Slovenskej republiky,f) Ministerstvo obrany Slovenskej republiky,g) iný orgán verejnej moci rozhodnutím úradu. | Ú |  |
| Č:9,O:4 | Členské štáty informujú Komisiu o rozsahu a hlavných prvkoch postupu pri riešení incidentov zo strany ich jednotiek CSIRT. | N | Návrh zákona | §:5,O:1P:f | Úrad plní notifikačné a reportingové povinnosti voči príslušným orgánom Európskej únie a Organizácie severoatlantickej zmluvy a podieľa sa a podporuje vytváranie partnerstiev na národnej a medzinárodnej úrovni v oblasti kybernetickej bezpečnosti  | Ú |  |
| Č:9,O:5 | Členské štáty môžu pri tvorbe vnútroštátnych jednotiek CSIRT požiadať o pomoc agentúru ENISA. | D |  |  |  | N |  |
| Č:10,O:1 | Spolupráca na vnútroštátnej úrovni 1. Ak sú príslušný orgán, jednotné kontaktné miesto a jednotka CSIRT jedného členského štátu samostatnými subjektmi, pri plnení povinností stanovených v tejto smernici spolupracujú.  |  | Návrh zákona | §:5, O:1P:i§:9, O:1P:bP:c§:15,O:2 | Úrad spolupracuje s ústrednými orgánmi a jednotkami CSIRT, prevádzkovateľmi základných služieb a poskytovateľmi digitálnych služieb pri plnení úloh podľa tohto zákona, Ústredný orgán poskytuje úradom požadovanú súčinnosť a informácie získané z vlastnej činnosti dôležité pre zabezpečenie kybernetickej bezpečnosti; informácie sa poskytujú len za podmienky, že ich poskytnutím nedôjde k ohrozeniu plnenia konkrétnej úlohy podľa osobitného predpisu12) alebo k odhaleniu jej zdrojov, prostriedkov, totožnosti osôb konajúcich v jej prospech, alebo k ohrozeniu medzinárodnej spravodajskej spolupráce, spolupracuje s ostatnými ústrednými orgánmi a prevádzkovateľmi základných služieb vo svojej pôsobnosti pri plnení úloh podľa tohto zákona,Preventívne služby sa zameriavajú na prevenciu kybernetických bezpečnostných incidentov a) vytváraním bezpečnostného povedomia, b) výcvikom, c) spoluprácou s ostatnými jednotkami CSIRT, d) monitorovaním a evidenciou kybernetických bezpečnostných incidentov, e) pripojením na jednotný informačný systém kybernetickej bezpečnosti, f) poskytovaním informácií a údajov do jednotného informačného systému kybernetickej bezpečnosti, g) prijímaním a zasielaním včasného varovania pred kybernetickými bezpečnostnými incidentmi prostredníctvom jednotného informačného systému kybernetickej bezpečnosti.  |  Ú |  |
| Č:10,O:2 | Členské štáty zabezpečia, aby ich príslušné orgány alebo jednotky CSIRT dostávali oznámenia o incidentoch predložené podľa tejto smernice. Ak členský štát rozhodne, že jednotka CSIRT nebude dostávať oznámenia, jednotke CSIRT sa v rozsahu potrebnom na plnenie jej úloh poskytne prístup k údajom o incidentoch, ktoré oznámili prevádzkovatelia základných služieb podľa článku 14 ods. 3 a 5 alebo poskytovatelia digitálnych služieb podľa článku 16 ods. 3 a 6. |  | Návrh zákona | §:24,O:1O:4§:25, O:1§:8, O:3O:5 | Prevádzkovateľ základnej služby hlási každý závažný kyberneticky bezpečnostný incident, ktorý identifikuje na základe presiahnutia kritérií pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov určených všeobecne záväzným právnym predpisom, ktorý vydá úrad.Hlásenie kybernetických bezpečnostných incidentov sa vykonáva prostredníctvom jednotného informačného systému kybernetickej bezpečnosti.. Poskytovateľ digitálnej služby je povinný hlásiť kybernetický bezpečnostný incident spôsobom podľa § 24 ods. 4.Komunikačný systém pre hlásenie a riešenie kybernetických bezpečnostných incidentov je komunikačný systém, ktorý zaisťuje systematické získavanie, sústreďovanie, analyzovanie a vyhodnocovanie informácií o kybernetických bezpečnostných incidentov.K neverejnej časti jednotného informačného systému kybernetickej bezpečnosti má priamy prístup v elektronickej forme v reálnom čase, v rozsahu určenom úradom alebo osobitným predpisom12) a na základe vecnej pôsobnostia) ústredný orgán,b) jednotka CSIRT zaradená v zozname akreditovaných jednotiek CSIRT,c) prevádzkovateľ základnej služby a poskytovateľ digitálnej služby,d) Národná banka Slovenska,e) Úrad na ochranu osobných údajov Slovenskej republiky,f) Ministerstvo obrany Slovenskej republiky,g) iný orgán verejnej moci rozhodnutím úradu. | Ú |  |
| Č:10,O:3 | Členské štáty zabezpečia, aby príslušné orgány alebo jednotky CSIRT informovali jednotné kontaktné miesta o oznámeniach o incidentoch predložených podľa tejto smernice. Do 9. augusta 2018 a potom každý rok jednotné kontaktné miesto predkladá skupine pre spoluprácu súhrnnú správu o prijatých oznámeniach, ktorá obsahuje aj počet oznámení a charakter oznámených incidentov a opatrenia prijaté v súlade s článkom 14 ods. 3 a 5 a článkom 16 ods. 3 a 6. |  | Návrh zákona | §:15O:2§:9 O:1P:b | Preventívne služby sa zameriavajú na prevenciu kybernetických bezpečnostných incidentov a) vytváraním bezpečnostného povedomia, b) výcvikom, c) spoluprácou s ostatnými jednotkami CSIRT, d) monitorovaním a evidenciou kybernetických bezpečnostných incidentov, e) pripojením na jednotný informačný systém kybernetickej bezpečnosti, f) poskytovaním informácií a údajov do jednotného informačného systému kybernetickej bezpečnosti, g) prijímaním a zasielaním včasného varovania pred kybernetickými bezpečnostnými incidentmi prostredníctvom jednotného informačného systému kybernetickej bezpečnosti.Ústredný orgán poskytuje úradom požadovanú súčinnosť a informácie získané z vlastnej činnosti dôležité pre zabezpečenie kybernetickej bezpečnosti; informácie sa poskytujú len za podmienky, že ich poskytnutím nedôjde k ohrozeniu plnenia konkrétnej úlohy podľa osobitného predpisu13) alebo k odhaleniu jej zdrojov, prostriedkov, totožnosti osôb konajúcich v jej prospech, alebo k ohrozeniu medzinárodnej spravodajskej spolupráce,  | Ú |  |
| Č:11,O:1 | Skupina pre spoluprácu 1. S cieľom podporiť a uľahčiť strategickú spoluprácu a výmenu informácií medzi členskými štátmi a rozvíjať dôveru a dosiahnuť vysokú spoločnú úroveň bezpečnosti sietí a informačných systémov v Únii sa týmto zriaďuje skupina pre spoluprácu. Skupina pre spoluprácu si plní svoje úlohy na základe dvojročných pracovných programov uvedených v odseku 3 druhom pododseku.  | n.a. |  |  |  |  |  |
| Č:11,O:2 | Skupina pre spoluprácu sa skladá zo zástupcov členských štátov, Komisie a agentúry ENISA. Vo vhodných prípadoch môže skupina pre spoluprácu pozvať na účasť na svojej práci zástupcov príslušných zainteresovaných strán. Sekretariát zabezpečuje Komisia. | n.a |  |  |  |  |  |
| Č:11,O:3 | 3. Skupina pre spoluprácu plní tieto úlohy: a) poskytovanie strategického usmernenia pre činnosť siete jednotiek CSIRT zriadenej podľa článku 12;vymieňanie si najlepších postupov v oblasti výmeny informácií týkajúcich sa oznamovania incidentov podľa článku 14 ods. 3 a 5 a článku 16 ods. 3 a 6; c) vymieňanie si najlepších postupov medzi členskými štátmi a v spolupráci s agentúrou ENISA, pomáhanie členským štátom pri budovaní kapacít na zabezpečenie bezpečnosti sietí a informačných systémov; d) diskutovanie o spôsobilostiach a pripravenosti členských štátov a na dobrovoľnom základe hodnotenie národných stratégií v oblasti bezpečnosti sietí a informačných systémov a účinnosti jednotiek CSIRT, ako aj identifikovanie najlepších postupov; e) vymieňanie si informácií a najlepších postupov v oblasti zvyšovania informovanosti a odbornej prípravy; f) vymieňanie si informácií a najlepších postupov v oblasti výskumu a vývoja bezpečnosti sietí a informačných systémov; g) vo vhodných prípadoch vymieňanie si skúsenosti v otázkach bezpečnosti sietí a informačných systémov s príslušnými inštitúciami, orgánmi, úradmi a agentúrami Únie; h) diskutovanie o normách a špecifikáciách uvedených v článku 19 so zástupcami príslušných európskych organizácií pre normalizáciu; i) zbieranie informácií o najlepších postupoch v súvislosti s rizikami a incidentmi; j) každoročné skúmanie súhrnných správ uvedených v článku 10 ods. 3 druhom pododseku; k) diskutovanie o práci vykonanej v súvislosti s cvičeniami v oblasti bezpečnosti sietí a informačných systémov, vzdelávacími programami a odbornou prípravou vrátane práce vykonanej agentúrou ENISA; l) s pomocou agentúry ENISA vymieňanie si najlepších postupov, pokiaľ ide o identifikáciu prevádzkovateľov základných služieb zo strany členských štátov aj pokiaľ ide o cezhraničnú závislosť v súvislosti s rizikami a incidentmi; m) diskutovanie o spôsoboch informovania o oznámených incidentoch podľa článkov 14 a 16. Do 9. februára 2018 a potom každé dva roky skupina pre spoluprácu zostaví pracovný program týkajúci sa činností, ktoré sa majú uskutočniť v rámci plnenia jej cieľov a úloh, ktoré sú v súlade s cieľmi tejto smernice. | n.a |  |  |  |  |  |
| Č:11,O:4 | Na účely preskúmania uvedeného v článku 23 a do 9. augusta 2018 a potom každý rok a pol skupina pre spoluprácu pripraví správu, v ktorej posúdi skúsenosti získané v rámci strategickej spolupráce vykonávanej podľa tohto článku. | n.a |  |  |  |  |  |
| Č:11,O:5 | Komisia prijme vykonávacie akty stanovujúce procesné opatrenia potrebné na fungovanie skupiny pre spoluprácu. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 22 ods. 2.Na účely prvého pododseku Komisia predloží prvý návrh vykonávacieho aktu výboru uvedenému v článku 22 ods. 1 do 9. februára 2017. | n.a |  |  |  |  |  |
| Č:12,O:1 | Článok 12 Sieť jednotiek CSIRT 1. S cieľom prispieť k rozvoju dôvery medzi členskými štátmi a podporiť rýchlu a účinnú operačnú spoluprácu sa zriaďuje sieť vnútroštátnych jednotiek CSIRT | n.a |  |  |  |  |  |
| Č:12,O:2 | Sieť jednotiek CSIRT sa skladá zo zástupcov jednotiek CSIRT členských štátov a jednotky CERT-EU. Komisia sa zúčastňuje na práci siete jednotiek CSIRT ako pozorovateľ. Agentúra ENISA zabezpečuje sekretariát a aktívne podporuje spoluprácu medzi jednotkami CSIRT. | n.a |  |  |  |  |  |
| Č:12,O:3 | Sieť jednotiek CSIRT plní tieto úlohy: a) vymieňanie si informácií o službách, operáciách a spôsobilostiach spolupráce jednotiek CSIRT; b) na žiadosť zástupcu jednotky CSIRT z členského štátu, ktorý je potenciálne postihnutý incidentom, vymieňanie si a prerokúvanie informácií, ktoré nie sú citlivé z obchodného hľadiska a týkajú sa daného incidentu a súvisiacich rizík; avšak ktorákoľvek jednotka CSIRT členského štátu môže odmietnuť prispieť k tejto diskusii, ak hrozí riziko ovplyvnenia vyšetrovania daného incidentu; c) na dobrovoľnom základe vymieňanie si a sprístupňovanie informácií o jednotlivých incidentoch, ktoré nie sú dôverné; d) na žiadosť zástupcu jednotky CSIRT členského štátu prediskutovanie a pokiaľ možno identifikovanie koordinovanej reakcie na incident, ktorý bol identifikovaný v jurisdikcii tohto členského štátu; e) poskytovanie podpory členským štátom pri riešení cezhraničných incidentov na základe ich dobrovoľnej vzájomnej pomoci; f) diskutovanie o ďalších formách operačnej spolupráce, preskúmavanie a identifikovanie ich, a to aj v súvislosti i) s kategóriami rizík a incidentov; ii) so včasnými varovaniami; iii) so vzájomnou pomocou; iv) so zásadami a spôsobmi koordinácie, keď členské štáty reagujú na cezhraničné riziká a incidenty; g) informovanie skupiny pre spoluprácu o svojej činnosti a o ďalších formách operačnej spolupráce, o ktorých sa diskutuje podľa písmena f), a požadovanie usmernení v tomto ohľade; h) diskutovanie o ponaučeniach z cvičení v oblasti bezpečnosti sietí a informačných systémov vrátane tých, ktoré organizuje agentúra ENISA; i) na žiadosť určitej jednotky CSIRT diskutovanie o spôsobilostiach a pripravenosti tejto jednotky CSIRT; j) vydávanie usmernení s cieľom uľahčiť konvergenciu operačných postupov so zreteľom na uplatňovanie ustanovení tohto článku, pokiaľ ide o operačnú spoluprácu. | n.a |  |  |  |  |  |
| Č:12,O:4 | Na účely preskúmania uvedeného v článku 23 a do 9. augusta 2018 a potom každý rok a pol sieť jednotiek CSIRT vypracuje správu, v ktorej posúdi skúsenosti získané v rámci operačnej spolupráce vykonávanej podľa tohto článku, pričom uvedie aj závery a odporúčania. Táto správa sa tiež predloží skupine pre spoluprácu. | n.a |  |  |  |  |  |
| Č:12,O:5 | Sieť jednotiek CSIRT si stanoví vlastný rokovací poriadok. | n.a |  |  |  |  |  |
| Č:13 | Medzinárodná spolupráca Únia môže uzatvárať medzinárodné dohody v súlade s článkom 218 ZFEÚ s tretími krajinami alebo medzinárodnými organizáciami, ktorými môže povoľovať a organizovať ich účasť na niektorých činnostiach skupiny pre spoluprácu. V takýchto dohodách sa zohľadňuje potreba zabezpečiť primeranú ochranu údajov. | n.a |  |  |  |  |  |
| Č:14,O:1 | **KAPITOLA IV BEZPEČNOSŤ SIETÍ A INFORMAČNÝCH SYSTÉMOV PREVÁDZKOVATEĽOV ZÁKLADNÝCH SLUŽIEB** Článok 14 Bezpečnostné požiadavky a oznamovanie incidentov 1. Členské štáty zabezpečia, aby prevádzkovatelia základných služieb prijali vhodné a primerané technické a organizačné opatrenia na riadenie rizík súvisiacich s bezpečnosťou sietí a informačných systémov, ktoré využívajú vo svojej prevádzke. S ohľadom na najnovší technický vývoj tieto opatrenia zabezpečujú takú úroveň bezpečnosti sietí a informačných systémov, ktorá zodpovedá miere daného rizika. | N | Návrh zákona | §:19, O:1 §:20,O:1O:2O:3O:4O:5 |  Prevádzkovateľ základnej služby je do 30 dní odo dňa oznámenia o zaradení do registra prevádzkovateľov základných služieb povinný prijať a dodržiavať všeobecné bezpečnostné opatrenia najmenej v rozsahu bezpečnostných opatrení podľa § 20 a sektorové bezpečnostné opatrenia, ak sú prijaté. Bezpečnostnými opatreniami na účely tohto zákona sú úlohy, procesy, role a technológie v organizačnej, personálnej a technickej oblasti, ktorých cieľom je zabezpečenie kybernetickej bezpečnosti počas životného cyklu sietí a informačných systémov. Bezpečnostné opatrenia, realizované v závislosti od klasifikácie informácií a kategorizácie sietí a informačných systémov a v súlade s bezpečnostnými štandardami v oblasti kybernetickej bezpečnosti sa prijímajú s cieľom predchádzať kybernetickým bezpečnostným incidentom a minimalizovať vplyv kybernetických bezpečnostných incidentov na kontinuitu prevádzkovania služby. Bezpečnostné opatrenia sú všeobecné, realizované v závislosti od klasifikácie informácií a kategorizácie sietí a informačných systémov a v súlade s bezpečnostnými štandardami v oblasti kybernetickej bezpečnosti pre všetky siete a informačné systémy a sektorové, ktoré sa realizujú na základe špecifík kategorizácie sietí a informačných systémov ústredného orgánu v rozsahu svojej pôsobnosti podľa prílohy č. 1 a v súlade s bezpečnostnými štandardami v oblasti kybernetickej bezpečnosti.Klasifikácia informácií a kategorizácia sietí a informačných systémov podľa odseku 1 sa vykonáva na základe významnosti, funkcie a účelu informácií a informačných systémov s ohľadom na dôvernosť, integritu, dostupnosť, kvalitu služby a kontrolnú činnosť.Bezpečnostné opatrenia sa prijímajú najmä pre oblasťa) organizácie informačnej bezpečnosti,b) riadenia aktív, hrozieb a rizík,c) personálnej bezpečnosti,d) riadenia dodávateľských služieb, akvizície, vývoja a údržby informačných systémov,e) technických zraniteľností systémov a zariadení,f) riadenia bezpečnosti sietí a informačných systémov,g) riadenia prevádzky,h) riadenia prístupov,i) kryptografických opatrení,j) riešenia kybernetických bezpečnostných incidentov,k) monitorovania, testovania bezpečnosti a bezpečnostných auditov,l) fyzickej bezpečnosti a bezpečnosti prostredia,m) riadenia kontinuity procesov.Bezpečnostné opatrenia musia zahŕňať najmeneja) detekciu kybernetických bezpečnostných incidentov,b) evidenciu kybernetických bezpečnostných incidentov,c) postupy riešenia a riešenie kybernetických bezpečnostných incidentov,d) určenie kontaktnej osoby pre prijímanie a evidenciu hlásení,e) pripojenie do komunikačného systému pre hlásenie a riešenie kybernetických bezpečnostných incidentov a centrálneho systému včasného varovania.Bezpečnostné opatrenia sa prijímajú a realizujú na základe schválenej bezpečnostnej dokumentácie, ktorá musí byť aktuálna a musí zodpovedať reálnemu stavu. Rozsah a štruktúru bezpečnostnej dokumentácie určí úrad všeobecne záväzným právnym predpisom. | Ú |  |
| Č:14,O:2 | 2. Členské štáty zabezpečia, aby prevádzkovatelia základných služieb prijali primerané opatrenia na zabránenie a minimalizovanie vplyvu incidentov, ktoré ovplyvňujú bezpečnosť sietí a informačných systémov používaných na poskytovanie týchto základných služieb, s cieľom zabezpečiť ich kontinuitu. | N | Návrh zákona | §27, O:1O:2O:3O:4O:5O:6O:7O:8O:9O:10O:11  | V prípade závažného kybernetického bezpečnostného incidentu alebo jeho hrozby, môže úrad a) vyhlásiť výstrahu a varovanie pred závažným kybernetickým bezpečnostným incidentom,b) uložiť povinnosť riešiť kybernetický bezpečnostný incident,c) uložiť povinnosť vykonať reaktívne opatrenie,d) požadovať návrh opatrení a ich vykonanie určených na zabránenie ďalšieho pokračovania, šírenia a opakovaného výskytu závažného kybernetického bezpečnostného incidentu (ďalej len „ochranné opatrenie“).Výstrahu a varovanie vyhlasuje úrad prostredníctvom jednotného informačného systému kybernetickej bezpečnosti. Ak ide o naliehavý verejný záujem, výstraha a varovanie sa vyhlási aj prostredníctvom hromadných oznamovacích prostriedkov ) a na ústrednom portáli verejnej správy.Povinnosť riešiť kybernetický bezpečnostný incident ukladá úrad rozhodnutím tomu, kto plní úlohy jednotky CSIRT, prevádzkovateľovi základnej služby a poskytovateľovi digitálnej služby.Reaktívne opatrenie je priama odpoveď na závažný kybernetický bezpečnostný incident a zabezpečuje sa službami podľa § 15 ods. 3 písm. b) až g).Povinnosť vykonať reaktívne opatrenie ukladá úrad rozhodnutím prevádzkovateľovi základnej služby alebo poskytovateľovi digitálnej služby, ktorí sú pri riešení závažného kybernetického bezpečnostného incidentu nečinní, alebo ak riešenie závažného kybernetického bezpečnostného incidentu je zjavne neúspešné. Poskytovateľovi digitálnej služby možno povinnosť vykonať reaktívne opatrenie uložiť iba počas krízovej situácie. )Prevádzkovateľ základnej služby alebo poskytovateľ digitálnej služby je povinný bezodkladne oznámiť a preukázať úradu prostredníctvom jednotného informačného systému kybernetickej bezpečnosti vykonanie reaktívneho opatrenia a jeho výsledok.Ochranné opatrenie prijíma prevádzkovateľ základnej služby na základe analýzy riešeného závažného kybernetického bezpečnostného incidentu.Prevádzkovateľ základnej služby je na výzvu úradu v určenej lehote povinný predložiť navrhované ochranné opatrenie na schválenie. Úrad rozhodnutím navrhované opatrenie schváli a určí lehotu na jeho vykonanie. V prípade, ak prevádzkovateľ základnej služby nenavrhne ochranné opatrenie v určenej lehote alebo ak je navrhované ochranné opatrenie zjavne neúspešné, je prevádzkovateľ základnej služby povinný spolupracovať s úradom, s ústredným orgánom a tým, kto prevádzkuje jednotku CSIRT, na jeho návrhu.V prípade, ak úrad na účely zaistenia kybernetickej bezpečnosti vyčerpá všetky spôsoby riešenia závažného kybernetického bezpečnostného incidentu podľa tohto zákona, predloží predsedovi Bezpečnostnej rady Slovenskej republiky informáciu o predpokladaných dopadoch kybernetického bezpečnostného incidentu na bezpečnosť štátu ako podklad na riešenie krízovej situácie. )Z dôvodu neodkladnosti a naliehavosti riešenia závažného kybernetického bezpečnostného incidentu úrad na účely kybernetickej obrany ) informuje Vojenské spravodajstvo, že závažný kybernetický bezpečnostný incident je kategórie tretieho stupňa alebo o skutočnostiach, ktoré nasvedčujú, že závažný kybernetický bezpečnostný incident môže byť kybernetickým terorizmom. Prevádzkovateľ základnej služby a poskytovateľ digitálnej služby, ktorí hlásia tento kybernetický bezpečnostný incident sú na účely zabezpečenia kybernetickej obrany povinní poskytnúť Vojenskému spravodajstvu informácie v potrebnom rozsahu. O postupe podľa prvej vety informuje úrad predsedu Bezpečnostnej rady Slovenskej republiky.Na konanie podľa odseku 3, 5 a 8 sa nevzťahuje všeobecný predpis o správnom konaní. | Ú |  |
| Č:14,O:3 | 3.Členské štáty zabezpečia, aby prevádzkovatelia základných služieb bez zbytočného odkladu oznamovali príslušnému orgánu alebo jednotke CSIRT incidenty, ktoré majú závažný vplyv na kontinuitu základných služieb, ktoré poskytujú. Oznámenia obsahujú informácie umožňujúce príslušnému orgánu alebo jednotke CSIRT určiť prípadný cezhraničný vplyv incidentu. Oznámenie nemá pre oznamujúcu stranu za následok vyššiu zodpovednosť. | N | Návrh zákona | §:19, O:6P:b§:24, O: 1O:4 §:8, O:6 §:24, O:6 | Prevádzkovateľ základnej služby je povinný b) bezodkladne hlásiť kybernetický bezpečnostný incident, Prevádzkovateľ základnej služby hlási každý závažný kyberneticky bezpečnostný incident, ktorý identifikuje na základe presiahnutia kritérií pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov určených všeobecne záväzným právnym predpisom, ktorý vydá úrad. Hlásenie kybernetických bezpečnostných incidentov sa vykonáva prostredníctvom jednotného informačného systému kybernetickej bezpečnosti.Ten, kto je povinný podľa tohto zákona poskytovať informácie, údaje a hlásenia prostredníctvom jednotného informačného systému kybernetickej bezpečnosti je povinný ich poskytovať bezodplatne a bezodkladne po tom, ako sa dozvie o skutočnosti zakladajúcej túto povinnosť. Informácie, údaje a hlásenia sa poskytujú spôsobom určeným funkcionalitou jednotného informačného systému kybernetickej bezpečnosti.Na účely hlásenia kybernetických bezpečnostných incidentov a zaistenia funkcionality jednotného informačného systému kybernetickej bezpečnosti môže úrad namiesto postupu uvedeného v § 8 ods. 6 uzatvoriť písomnú dohodu o spôsobe a forme hlásenia kybernetických bezpečnostných incidentov s prevádzkovateľom základnej služby. | Ú |  |
| Č:14,O:4 | 4. S cieľom určiť závažnosť vplyvu incidentu sa zohľadnia najmä tieto parametre: a) počet používateľov postihnutých narušením základnej služby; b) dĺžka trvania incidentu; c) geografické rozšírenie z hľadiska oblasti, ktorú incident postihol | N |  Návrh zákona  | §:24O:2 | Závažný kybernetický bezpečnostný incident sa člení na kategóriu prvého (I) stupňa, druhého (II) stupňa a tretieho (III) stupňa v závislosti od a) počtu používateľov základnej služby alebo digitálnej služby, postihnutých kybernetickým bezpečnostným incidentom, b) dĺžky trvania kybernetického bezpečnostného incidentu, c) geografického rozšírenia kybernetického bezpečnostného incidentu, d) stupňa narušenia fungovania základnej služby alebo digitálnej služby, e) rozsahu vplyvu kybernetického bezpečnostného incidentu na hospodárske alebo spoločenské činnosti štátu.  | Ú |  |
| Č:14,O:5 | 5.Na základe informácií, ktoré poskytol prevádzkovateľ základných služieb v oznámení, príslušný orgán alebo jednotka CSIRT informuje ostatné postihnuté členské štáty, ak má incident závažný vplyv na kontinuitu základných služieb v týchto členských štátoch. Príslušný orgán alebo jednotka CSIRT pritom v súlade s právom Únie alebo vnútroštátnymi právnymi predpismi, ktoré sú v súlade s právom Únie, chráni bezpečnosť a obchodné záujmy prevádzkovateľa základných služieb, ako aj dôvernosť informácií poskytnutých v jeho oznámení. Pokiaľ to okolnosti umožňujú, príslušný orgán alebo jednotka CSIRT poskytnú oznamujúcemu prevádzkovateľovi základných služieb relevantné informácie týkajúce sa následných opatrení prijatých na základe jeho oznámenia, ako sú napríklad informácie, ktoré by mohli podporiť účinné riešenie incidentu. Na žiadosť príslušného orgánu alebo jednotky CSIRT jednotné kontaktné miesto postúpi oznámenia uvedené v prvom pododseku jednotným kontaktným miestam ostatných postihnutých členských štátov. | N | Návrh zákona | §:5, O:1P: t§:12, O:1O:7§:8 O:3O:5 | Úrad prijíma hlásenia o kybernetických bezpečnostných incidentoch zo zahraničia a zabezpečuje spoluprácu s medzinárodnými organizáciami a orgánmi iných štátov pri riešení kybernetických bezpečnostných incidentov s cezhraničným charakterom,Kto plní alebo plnil úlohy na základe tohto zákona alebo v súvislosti s ním, je povinný zachovávať mlčanlivosť o skutočnostiach, o ktorých sa v súvislosti s plnením úloh podľa tohto zákona dozvedel a ktoré nie sú verejne známe. Povinnosť zachovávať mlčanlivosť trvá aj po skončení dohody o spolupráci podľa § 5 ods. 2 alebo § 9 ods. 4, pracovnoprávneho vzťahu alebo obdobného pracovného vzťahu vrátane služobného pomeru.14) Ustanoveniami o povinnosti zachovávať mlčanlivosť podľa tohto zákona nie je dotknutá povinnosť mlčanlivosti alebo zachovania tajomstva podľa osobitných predpisov.15)Úrad zabezpečí nepretržitú ochranu osobných údajov a informácie spracúvané podľa tohto zákona pred nezákonným vyzradením, zneužitím, poškodením, neoprávneným zničením, odcudzením a stratou spôsobom podľa osobitného predpisu.18)Komunikačný systém pre hlásenie a riešenie kybernetických bezpečnostných incidentov je komunikačný systém, ktorý zaisťuje systematické získavanie, sústreďovanie, analyzovanie a vyhodnocovanie informácií o kybernetických bezpečnostných incidentov.K neverejnej časti jednotného informačného systému kybernetickej bezpečnosti má priamy prístup v elektronickej forme v reálnom čase, v rozsahu určenom úradom alebo osobitným predpisom12) a na základe vecnej pôsobnostia) ústredný orgán,b) jednotka CSIRT zaradená v zozname akreditovaných jednotiek CSIRT,c) prevádzkovateľ základnej služby a poskytovateľ digitálnej služby,d) Národná banka Slovenska,e) Úrad na ochranu osobných údajov Slovenskej republiky,f) Ministerstvo obrany Slovenskej republiky,g) iný orgán verejnej moci rozhodnutím úradu. | Ú |  |
| Č:14,O:6 | 6.Po porade s oznamujúcim prevádzkovateľom základných služieb môže príslušný orgán alebo jednotka CSIRT informovať o jednotlivých incidentoch verejnosť, ak je informovanosť verejnosti potrebná na zabránenie incidentu alebo na riešenie prebiehajúceho incidentu. | N | Návrh zákona | §:27O:2 | Výstrahu a varovanie vyhlasuje úrad prostredníctvom jednotného informačného systému kybernetickej bezpečnosti. Ak ide o naliehavý verejný záujem, výstraha a varovanie sa vyhlási aj prostredníctvom hromadných oznamovacích prostriedkov25) a na ústrednom portáli verejnej správy. | ­Ú |  |
| Č:14,O:7 | 7. Príslušné orgány konajúce spoločne v rámci skupiny pre spoluprácu môžu vypracovať a prijať usmernenia týkajúce sa okolností, za ktorých sú prevádzkovatelia základných služieb povinní oznamovať incidenty, ako aj parametrov na určenie závažnosti vplyvu incidentu, ako sa uvádza v odseku 4. | n.a |  |  |  |  |  |
| Č:15,O:1 | Vykonávanie a presadzovanie 1. Členské štáty zabezpečia, aby príslušné orgány mali právomoci a prostriedky potrebné na posúdenie toho, či prevádzkovatelia základných služieb dodržiavajú svoje povinnosti podľa článku 14, a s tým súvisiacich dôsledkov pre bezpečnosť sietí a informačných systémov.  | N | Návrh zákona | §:28,O:1O:2O:3 | Pri výkone kontroly nad dodržiavaním ustanovení tohto zákona a jeho vykonávacích predpisov postupuje úrad podľa základných pravidiel kontrolnej činnosti ustanovených osobitným predpisom.29)Na účely výkonu kontroly má prevádzkovateľ základnej služby a poskytovateľ digitálnej služby práva a povinnosti kontrolovaného subjektu podľa osobitného predpisu.30)Úrad vykoná kontrolu u poskytovateľa digitálnej služby ak dôvodné podozrenia, že poskytovateľ digitálnej služby nespĺňa požiadavky stanovené týmto zákonom. | Ú |  |
| Č:15,O:2 | 2. Členské štáty zabezpečia, aby príslušné orgány mali právomoci a prostriedky potrebné na to, aby mohli od prevádzkovateľov základných služieb požadovať, aby poskytovali: a) informácie potrebné na posúdenie bezpečnosti svojich sietí a informačných systémov vrátane zdokumentovaných bezpečnostných politík;b) dôkazy o účinnom vykonávaní bezpečnostných politík, ako sú výsledky bezpečnostného auditu, ktorý vykoná príslušný orgán alebo kvalifikovaný audítor, pričom v prípade, že ho vykoná kvalifikovaný audítor, sa výsledky spolu s podkladovými dôkazmi poskytnú príslušnému orgánu. Pri požadovaní takýchto informácií alebo dôkazov príslušný orgán uvedie účel žiadosti a aké informácie sa požadujú.  | N | Návrh zákonaZákon o kontrole 10/1996 Z.z. | §:28,O:1O:2§:11, O:1 |  Pri výkone kontroly nad dodržiavaním ustanovení tohto zákona a jeho vykonávacích predpisov postupuje úrad podľa základných pravidiel kontrolnej činnosti ustanovených osobitným predpisom.29) Na účely výkonu kontroly má prevádzkovateľ základnej služby a poskytovateľ digitálnej služby práva a povinnosti kontrolovaného subjektu podľa osobitného predpisu.30) § 11 Oprávnenia a povinnosti pracovníkov kontroly Pracovníci kontroly sú v súvislosti s výkonom kontroly oprávnení v nevyhnutnom rozsahua)vstupovať do objektov, zariadení a prevádzok, na pozemky a do iných priestorov kontrolovaných subjektov, ak bezprostredne súvisia s predmetom kontroly; nedotknuteľnosť obydlia nesmie byť dotknutá výkonom tohto oprávnenia,14)b)vyžadovať od kontrolovaného subjektu a jeho zamestnancov, aby im v určenej lehote poskytovali doklady15), iné písomnosti, vyjadrenia a informácie (vrátane technických nosičov údajov) potrebné na výkon kontroly, prvopisy dokladov; pri vyžiadaní dokladov a informácií obsahujúcich utajované skutočnosti alebo osobné údaje je potrebné dodržať postup ustanovený osobitnými predpismi,16)c)na účely dokumentácie k protokolu o výsledku kontroly vyhotovovať fotokópie odobratých materiálov, d)v odôvodnených prípadoch odoberať a aj mimo priestorov kontrolovaného subjektu na zabezpečenie dôkazov premiestňovať prvopisy dokladov, ktorých vydanie nie je všeobecne záväzným právnym predpisom zakázané, písomné dokumenty a iné materiály a vykonať ďalšie nevyhnutné úkony súvisiace s kontrolou, e)vyžadovať súčinnosť kontrolovaného subjektu, jeho zamestnancov, ako aj ďalších štátnych orgánov potrebnú na vykonanie kontroly. Od právnických osôb a od fyzických osôb možno vyžadovať súčinnosť v nevyhnutnom rozsahu a s ich súhlasom; v súvislosti so zisťovaním správnosti postupov pri poskytovaní a využití prostriedkov Európskeho spoločenstva vrátane prostriedkov štátneho rozpočtu poskytnutých na plnenie týchto úloh sú tieto osoby povinné poskytnúť požadovanú súčinnosť. Súčinnosť nemožno vyžadovať, ak by tým bol ohrozený život alebo zdravie osôb alebo ak by bola porušená zákonom ustanovená povinnosť mlčanlivosti, pričom kontrolovaný subjekt nebol zbavený oprávneným orgánom povinnosti mlčanlivosti. | Ú |  |
| Č:15,O:3 | Po posúdení informácií alebo výsledkov bezpečnostných auditov uvedených v odseku 2 môže príslušný orgán vydať prevádzkovateľom základných služieb záväzné pokyny na nápravu zistených nedostatkov. | N | Návrh zákonaNávrh zákonaZákon o kontrole 10/1996 Z.z. | §:29,O:1O:2O:3O:4O:5O:6§ 28, O:1O:2 §:13,O:6 | Prevádzkovateľ základnej služby je povinný preveriť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek stanovených týmto zákonom vykonaním auditu kybernetickej bezpečnosti do 24 mesiacov odo dňa zaradenia prevádzkovateľa základnej služby do registra prevádzkovateľov základných služieb.Prevádzkovateľ základnej služby je povinný preveriť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek stanovených týmto zákonom vykonaním auditu kybernetickej bezpečnosti a) po každej zmene majúcej významný vplyv na realizované bezpečnostné opatrenia prijaté podľa § 20, b) v časovom intervale a v rozsahu stanovenom podľa všeobecne záväzného právneho predpisu, ktorý vydá úrad, a to v závislosti od klasifikácie informácií a kategorizácie sietí a informačných systémov. Audit kybernetickej bezpečnosti vykonáva orgán posudzovania zhody podľa osobitného predpisu,29) ktorý je akreditovaný ako orgán príslušný na posudzovanie zhody v oblasti kybernetickej bezpečnosti. Prevádzkovateľ základnej služby je povinný predložiť záverečnú správu o výsledkoch auditu úradu spolu s prípadnými opatreniami na nápravu a s lehotami na ich odstránenie do 30 dní od ukončenia auditu. Bez toho, aby bol dotknutý odsek 1, môže úrad kedykoľvek vykonať audit kybernetickej bezpečnosti u prevádzkovateľa základnej služby, alebo požiadať orgán posudzovania zhody, aby vykonal audit prevádzkovateľa základnej služby s cieľom potvrdiť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek stanovených týmto zákonom. Náklady na audit kybernetickej bezpečnosti podľa odseku 1 znáša prevádzkovateľ základnej služby a náklady na audit kybernetickej bezpečnosti podľa odseku 5 znáša úrad. Pri výkone kontroly nad dodržiavaním ustanovení tohto zákona a jeho vykonávacích predpisov postupuje úrad podľa základných pravidiel kontrolnej činnosti ustanovených osobitným predpisom.27) Na účely výkonu kontroly má prevádzkovateľ základnej služby a poskytovateľ digitálnej služby práva a povinnosti kontrolovaného subjektu podľa osobitného predpisu.28) O prerokovaní protokolu vypracujú pracovníci kontroly zápisnicu, ktorá musí obsahovať dátum oboznámenia vedúceho kontrolovaného subjektu s protokolom, dátum prerokovania protokolu, mená prítomných na prerokovaní a ich vlastnoručné podpisy. Zápisnica o prerokovaní protokolu sa prikladá k protokolu o výsledku kontroly. V zápisnici sa uloží povinnosť vedúcemu kontrolovaného subjektu v určenej lehote a)prijať opatrenia na odstránenie zistených nedostatkov a ich príčin a predložiť ich orgánu kontroly, b)určiť zamestnancov zodpovedných za zistené nedostatky,c)predložiť orgánu kontroly správu o splnení opatrení na odstránenie nedostatkov a ich príčin a uplatnení právnej zodpovednosti, d)uplatniť právnu zodpovednosť za zistené nedostatky voči zamestnancom zodpovedným za tieto nedostatky. | Ú |  |
| Č:15,O:4 | Príslušný orgán pri riešení incidentov, ktoré majú za následok porušenie ochrany osobných údajov, úzko spolupracuje s orgánmi na ochranu údajov. | N | Zákon č. 575/2001 o organizácii činnosti vlády a organizácii ústrednej štátnej správy  | §:38,O:1 |  Ministerstvá a ostatné ústredné orgány štátnej správy pri plnení svojich úloh úzko spolupracujú. Vymieňajú si potrebné informácie a podklady a prerokúvajú s inými ministerstvami opatrenia, ktoré sa ich dotýkajú.o organizácii činnosti vlády a organizácii ústrednej štátnej správy | Ú |  |
| Č:16,O:1 | **KAPITOLA V BEZPEČNOSŤ SIETÍ A INFORMAČNÝCH SYSTÉMOV POSKYTOVATEĽOV DIGITÁLNYCH SLUŽIEB**  Bezpečnostné požiadavky a oznamovanie incidentov 1. Členské štáty zabezpečia, aby poskytovatelia digitálnych služieb identifikovali riziká súvisiace s bezpečnosťou sietí a informačných systémov, ktoré používajú v kontexte poskytovania služieb uvedených v prílohe III v rámci Únie, a aby prijali vhodné a primerané technické a organizačné opatrenia na riadenie týchto rizík. S ohľadom na najnovší technický vývoj musia tieto opatrenia zabezpečiť takú úroveň bezpečnosti sietí a informačných systémov, ktorá zodpovedá miere daného rizika, a zohľadniť tieto prvky: a) bezpečnosť systémov a zariadení; b) riešenie incidentov; c) riadenie kontinuity činnosti; d) monitorovanie, audit a skúšanie; e) súlad s medzinárodnými normami. | N | Návrh zákona+Vykonávacie nariadenie EK | §:22,O:1O:2O:3 | Poskytovateľ digitálnej služby je povinný do šiestich mesiacov odo dňa oznámenia o zaradení do registra poskytovateľov digitálnych služieb prijať a dodržiavať vhodné a primerané bezpečnostné opatrenia podľa osobitného predpisu ) na účely riadenia rizík súvisiacich s ohrozením kontinuity digitálnej služby a procesu riešenia kybernetických bezpečnostných incidentov. Na tento účel je poskytovateľ digitálnej služby povinný vyčleniť dostatočné personálne, materiálno-technické, časové a finančné zdroje s cieľom zabezpečenia kontinuity digitálnej služby.Poskytovateľ digitálnej služby na účely splnenia povinnosti podľa odseku 1 posudzuje najmäa) bezpečnosť sietí a informačného systému a jeho schopnosť predchádzať a riešiť kybernetický bezpečnostný incident,b) spôsob zachovania kontinuity digitálnej služby v prípade kybernetického bezpečnostného incidentu,c) súlad sietí a informačného systému s bezpečnostnými štandardmi v oblasti kybernetickej bezpečnosti.Poskytovateľ digitálnej služby je povinnýa) hlásiť každý kybernetický bezpečnostný incident, ak disponuje informáciami, na základe ktorých je spôsobilý identifikovať, či má tento kybernetický bezpečnostný incident podstatný vplyv podľa osobitného predpisu,24) a to bezodkladne po jeho zistení,b) riešiť hlásený kybernetický bezpečnostný incident,c) spolupracovať s úradom pri riešení hláseného kybernetického bezpečnostného incidentu..  | Ú |  |
| Č:16,O:2 | 2.Členské štáty zabezpečia, aby poskytovatelia digitálnych služieb prijali opatrenia na zabránenie a minimalizovanie vplyvu incidentov ovplyvňujúcich bezpečnosť ich sietí a informačných systémov na služby uvedené v prílohe III, ktoré sa poskytujú v rámci Únie, s cieľom zabezpečiť kontinuitu týchto služieb. | N | Návrh zákona | §:22,O:1O:2 | Poskytovateľ digitálnej služby je povinný do šiestich mesiacov odo dňa oznámenia o zaradení do registra poskytovateľov digitálnych služieb prijať a dodržiavať vhodné a primerané bezpečnostné opatrenia podľa osobitného predpisu ) na účely riadenia rizík súvisiacich s ohrozením kontinuity digitálnej služby a procesu riešenia kybernetických bezpečnostných incidentov. Na tento účel je poskytovateľ digitálnej služby povinný vyčleniť dostatočné personálne, materiálno-technické, časové a finančné zdroje s cieľom zabezpečenia kontinuity digitálnej služby.Poskytovateľ digitálnej služby na účely splnenia povinnosti podľa odseku 1 posudzuje najmäa) bezpečnosť sietí a informačného systému a jeho schopnosť predchádzať a riešiť kybernetický bezpečnostný incident,b) spôsob zachovania kontinuity digitálnej služby v prípade kybernetického bezpečnostného incidentu,c) súlad sietí a informačného systému s bezpečnostnými štandardmi v oblasti kybernetickej bezpečnosti. | Ú |  |
| Č:16,O:3 | 3.Členské štáty zabezpečia, aby poskytovatelia digitálnych služieb bezodkladne oznámili príslušnému orgánu alebo jednotke CSIRT každý incident, ktorý má závažný vplyv na poskytovanie služby uvedenej v prílohe III, ktorú poskytujú v rámci Únie. Oznámenia obsahujú informácie, ktoré umožnia príslušnému orgánu alebo jednotke CSIRT určiť závažnosť prípadného cezhraničného vplyvu. Oznámenie nesmie mať pre oznamujúcu stranu za následok vyššiu zodpovednosť. | N | Návrh zákona | §:22,O:3§:8, O:6§:24, O:6 | (3) Poskytovateľ digitálnej služby je povinnýa) hlásiť každý kybernetický bezpečnostný incident, ak disponuje informáciami, na základe ktorých je spôsobilý identifikovať, či má tento kybernetický bezpečnostný incident podstatný vplyv podľa osobitného predpisu,24) a to bezodkladne po jeho zistení,b) riešiť hlásený kybernetický bezpečnostný incident,c) spolupracovať s úradom pri riešení hláseného kybernetického bezpečnostného incidentu.Ten, kto je povinný podľa tohto zákona poskytovať informácie a údaje prostredníctvom jednotného informačného systému kybernetickej bezpečnosti je povinný ich poskytovať bezodplatne a bezodkladne po tom, ako sa dozvie o skutočnosti zakladajúcej túto povinnosť. Informácie a údaje sa poskytujú spôsobom určeným funkcionalitou jednotného informačného systému kybernetickej bezpečnosti. Na účely hlásenia kybernetických bezpečnostných incidentov a zaistenia funkcionality jednotného informačného systému kybernetickej bezpečnosti môže úrad namiesto postupu uvedeného v § 8 ods. 6 uzatvoriť písomnú dohodu o spôsobe a forme hlásenia kybernetických bezpečnostných incidentov s prevádzkovateľom základnej služby. | Ú |  |
| Č:16,O:4 | 4. Pri určovaní, či je vplyv incidentu závažný, sa zohľadňujú najmä tieto parametre: a) počet používateľov postihnutých incidentom, najmä používateľov využívajúcich danú službu na účely poskytovania vlastných služieb; b) dĺžka trvania incidentu; c) geografické rozšírenie z hľadiska oblasti, ktorú incident postihol; d) stupeň narušenia fungovania služby; e) rozsah vplyvu na hospodárske a spoločenské činnosti. | N | Návrh zákona | §:24,O:2§ 32, O:1  | Závažný kybernetický bezpečnostný incident sa člení na kategóriu prvého (I) stupňa, druhého (II) stupňa a tretieho (III) stupňa v závislosti oda) počtu používateľov základnej služby alebo digitálnej služby, postihnutých kybernetickým bezpečnostným incidentom,b) dĺžky trvania kybernetického bezpečnostného incidentu,c) geografického rozšírenia kybernetického bezpečnostného incidentu,d) stupňa narušenia fungovania základnej služby alebo digitálnej služby,e) rozsahu vplyvu kybernetického bezpečnostného incidentu na hospodárske alebo spoločenské činnosti štátu.Úrad sa splnomocňuje na vydanie všeobecne záväzného právneho predpisu, ktorým ustanovíkategórie a identifikačné kritériá kybernetických bezpečnostných incidentov hlásených prevádzkovateľom základnej služby a poskytovateľom digitálnej služby, | Ú |  |
|  | Povinnosť oznámiť incident sa uplatňuje len v prípade, ak má poskytovateľ digitálnych služieb prístup k informáciám, ktoré sú potrebné na posúdenie dopadu incidentu na základe parametrov uvedených v prvom pododseku. | N | Návrh zákona | §:22,O:3 | (3) Poskytovateľ digitálnej služby je povinnýa) hlásiť každý kybernetický bezpečnostný incident, ak disponuje informáciami, na základe ktorých je spôsobilý identifikovať, či má tento kybernetický bezpečnostný incident podstatný vplyv podľa osobitného predpisu,24) a to bezodkladne po jeho zistení,b) riešiť hlásený kybernetický bezpečnostný incident,c) spolupracovať s úradom pri riešení hláseného kybernetického bezpečnostného incidentu | Ú |  |
| Č:16,O:5 | Ak prevádzkovateľ základných služieb využíva tretiu stranu, ktorou je poskytovateľ digitálnych služieb, na poskytovanie služby, ktorá je základná pre zachovanie rozhodujúcich spoločenských a hospodárskych činností, uvedený prevádzkovateľ oznamuje každý závažný vplyv na kontinuitu základných služieb, ktorý je dôsledkom incidentu, ktorý postihol poskytovateľa digitálnych služieb. | N | Návrh zákona  | §:19, O: 2 | Prevádzkovateľ základnej služby je povinný pri uzatvorení zmluvy s dodávateľom na výkon činností, ktoré priamo súvisia s prevádzkou sietí a informačných systémov pre prevádzkovateľa základnej služby (ďalej len „tretia strana“) uzatvoriť dohodu o zabezpečení plnení bezpečnostných opatrení a notifikačných povinností podľa tohto zákona počas celej doby platnosti zmluvy. Dohoda tvorí neoddeliteľnú súčasť zmluvy s treťou stranou. | Ú |  |
| Č:16,O:6 | Ak je to vhodné, a najmä ak sa incident uvedený v odseku 3 týka dvoch alebo viacerých členských štátov, príslušný orgán alebo jednotka CSIRT informuje ostatné dotknuté členské štáty. Príslušné orgány, jednotky CSIRT a jednotné kontaktné miesta pritom v súlade s právom Únie alebo vnútroštátnymi právnymi predpismi, ktoré sú v súlade s právom Únie, chránia bezpečnosť a obchodné záujmy poskytovateľa digitálnych služieb, ako aj dôvernosť poskytnutých informácií. | N | Návrh zákona | §:5, O:1P:t§ :12, O:7 | Úrad prijíma hlásenia o kybernetických bezpečnostných incidentoch zo zahraničia a zabezpečuje spoluprácu s medzinárodnými organizáciami a orgánmi iných štátov pri riešení kybernetických bezpečnostných incidentov s cezhraničným charakterom, Úrad zabezpečí nepretržitú ochranu osobných údajov a informácie spracúvané podľa tohto zákona pred nezákonným vyzradením, zneužitím, poškodením, neoprávneným zničením, odcudzením a stratou spôsobom podľa osobitného predpisu.17)  | Ú |  |
| Č:16,O:7 | Po porade s dotknutým poskytovateľom digitálnych služieb môže príslušný orgán alebo jednotka CSIRT a prípadne orgány alebo jednotky CSIRT ďalších dotknutých členských štátov informovať verejnosť o jednotlivých incidentoch alebo požiadať o to poskytovateľa digitálnych služieb, ak je informovanosť verejnosti potrebná na zabránenie incidentu alebo riešenie prebiehajúceho incidentu, alebo ak je zverejnenie incidentu vo verejnom záujme z iného dôvodu. | N | Návrh zákona | §:27,O:2 | Výstrahu a varovanie vyhlasuje úrad prostredníctvom jednotného informačného systému kybernetickej bezpečnosti. Ak ide o naliehavý verejný záujem, výstraha a varovanie sa vyhlási aj prostredníctvom hromadných oznamovacích prostriedkov25) a na ústrednom portáli verejnej správy | Ú |  |
| Č:16,O:8 | Komisia prijme vykonávacie akty s cieľom bližšie špecifikovať prvky uvedené v odseku 1 a parametre uvedené v odseku 4 tohto článku. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 22 ods. 2 do ... [1 rok odo dňa nadobudnutia účinnosti tejto smernice]. | n.a |  |  |  |  |  |
| Č:16,O:9 | Komisia môže prijať vykonávacie akty stanovujúce formáty a postupy uplatniteľné na oznamovacie požiadavky. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 22 ods. 2. | n.a |  |  |  |  |  |
| Č:16,O:10 | Bez toho aby bol dotknutý článok 1 ods. 6, členské štáty nesmú ukladať poskytovateľom digitálnych služieb žiadne ďalšie bezpečnostné ani oznamovacie požiadavky. | N |  |  |  |  |  |
| Č:16,O:11 | Kapitola V sa nevzťahuje na mikropodniky a malé podniky, ako sú vymedzené v odporúčaní Komisie 2003/361/ES**1**. | N |  | §3,P:n |  Poskytovateľom digitálnej služby právnická osoba alebo fyzická osoba - podnikateľ, ktorá poskytuje digitálnu službu a zároveň zamestnáva 50 a viac zamestnancov a má ročný obrat alebo celkovú ročnú bilanciu viac ako 10 000 000 eur, | Ú |  |
| Č:17,O:1 | Vykonávanie a presadzovanie 1. Členské štáty zabezpečia, aby príslušné orgány konali, podľa potreby prostredníctvom následných opatrení dohľadu, ak majú k dispozícii dôkazy, že poskytovateľ digitálnych služieb nespĺňa požiadavky stanovené v článku 16. Takéto dôkazy môže predložiť príslušný orgán iného členského štátu, v ktorom sa služba poskytuje | N | Návrh zákonaZákon o kontrole 10/1996 Z.z. | §28,O:1O:2O:3§:11,O:1 | Pri výkone kontroly nad dodržiavaním ustanovení tohto zákona a jeho vykonávacích predpisov postupuje úrad podľa základných pravidiel kontrolnej činnosti ustanovených osobitným predpisom. )Na účely výkonu kontroly má prevádzkovateľ základnej služby a poskytovateľ digitálnej služby práva a povinnosti kontrolovaného subjektu podľa osobitného predpisu. )Úrad vykoná kontrolu u poskytovateľa digitálnej služby ak dôvodné podozrenia, že poskytovateľ digitálnej služby nespĺňa požiadavky stanovené týmto zákonom.Pracovníci kontroly sú v súvislosti s výkonom kontroly oprávnení v nevyhnutnom rozsahua) vstupovať do objektov, zariadení a prevádzok, na pozemky a do iných priestorov kontrolovaných subjektov, ak bezprostredne súvisia s predmetom kontroly; nedotknuteľnosť obydlia nesmie byť dotknutá výkonom tohto oprávnenia,14)b) vyžadovať od kontrolovaného subjektu a jeho zamestnancov, aby im v určenej lehote poskytovali doklady15), iné písomnosti, vyjadrenia a informácie (vrátane technických nosičov údajov) potrebné na výkon kontroly, prvopisy dokladov; pri vyžiadaní dokladov a informácií obsahujúcich utajované skutočnosti alebo osobné údaje je potrebné dodržať postup ustanovený osobitnými predpismi,16)c) na účely dokumentácie k protokolu o výsledku kontroly vyhotovovať fotokópie odobratých materiálov, d) v odôvodnených prípadoch odoberať a aj mimo priestorov kontrolovaného subjektu na zabezpečenie dôkazov premiestňovať prvopisy dokladov, ktorých vydanie nie je všeobecne záväzným právnym predpisom zakázané, písomné dokumenty a iné materiály a vykonať ďalšie nevyhnutné úkony súvisiace s kontrolou, e) vyžadovať súčinnosť kontrolovaného subjektu, jeho zamestnancov, ako aj ďalších štátnych orgánov potrebnú na vykonanie kontroly. Od právnických osôb a od fyzických osôb možno vyžadovať súčinnosť v nevyhnutnom rozsahu a s ich súhlasom; v súvislosti so zisťovaním správnosti postupov pri poskytovaní a využití prostriedkov Európskeho spoločenstva vrátane prostriedkov štátneho rozpočtu poskytnutých na plnenie týchto úloh sú tieto osoby povinné poskytnúť požadovanú súčinnosť. Súčinnosť nemožno vyžadovať, ak by tým bol ohrozený život alebo zdravie osôb alebo ak by bola porušená zákonom ustanovená povinnosť mlčanlivosti, pričom kontrolovaný subjekt nebol zbavený oprávneným orgánom povinnosti mlčanlivosti. | Ú |  |
| Č:17,O:2 | Na účely odseku 1 musia mať príslušné orgány potrebné právomoci a prostriedky na to, aby od poskytovateľov digitálnych služieb požadovali: a) poskytovanie informácií potrebných na posúdenie bezpečnosti ich sietí a informačných systémov vrátane zdokumentovaných bezpečnostných politík; b) napravenie akéhokoľvek nesplnenia požiadaviek stanovených v článku 16. | N | Návrh zákonaZákon o kontrole 10/1996 Z.z. | §:28,O:1O:2O:3§:13,O:6 | Pri výkone kontroly nad dodržiavaním ustanovení tohto zákona a jeho vykonávacích predpisov postupuje úrad podľa základných pravidiel kontrolnej činnosti ustanovených osobitným predpisom. )Na účely výkonu kontroly má prevádzkovateľ základnej služby a poskytovateľ digitálnej služby práva a povinnosti kontrolovaného subjektu podľa osobitného predpisu. )Úrad vykoná kontrolu u poskytovateľa digitálnej služby ak dôvodné podozrenia, že poskytovateľ digitálnej služby nespĺňa požiadavky stanovené týmto zákonom. O prerokovaní protokolu vypracujú pracovníci kontroly zápisnicu, ktorá musí obsahovať dátum oboznámenia vedúceho kontrolovaného subjektu s protokolom, dátum prerokovania protokolu, mená prítomných na prerokovaní a ich vlastnoručné podpisy. Zápisnica o prerokovaní protokolu sa prikladá k protokolu o výsledku kontroly. V zápisnici sa uloží povinnosť vedúcemu kontrolovaného subjektu v určenej lehote a)prijať opatrenia na odstránenie zistených nedostatkov a ich príčin a predložiť ich orgánu kontroly, b)určiť zamestnancov zodpovedných za zistené nedostatky,c)predložiť orgánu kontroly správu o splnení opatrení na odstránenie nedostatkov a ich príčin a uplatnení právnej zodpovednosti, d)uplatniť právnu zodpovednosť za zistené nedostatky voči zamestnancom zodpovedným za tieto nedostatky. | Ú |  |
| Č:17,O:3 | Ak sa hlavná prevádzkareň alebo zástupca poskytovateľa digitálnych služieb nachádza v členskom štáte, ale jeho siete a informačné systémy sú umiestnené v jednom alebo viacerých iných členských štátoch, príslušný orgán členského štátu, v ktorom sa nachádza hlavná prevádzkareň alebo zástupca, a príslušné orgány týchto iných členských štátov spolupracujú a v prípade potreby si navzájom pomáhajú. Takáto pomoc a spolupráca môže zahŕňať výmenu informácií medzi dotknutými príslušnými orgánmi a žiadosti o prijatie opatrení dohľadu uvedených v odseku 2. | N | Návrhzákona  | §:23,O:1O:2O:3§:5, O:1P:e | Zástupcom poskytovateľa digitálnej služby je právnická osoba, ktorá má sídlo v Slovenskej republike alebo fyzická osoba - podnikateľ, ktorá má miesto podnikania v Slovenskej republike, ak odsek 2 neustanovuje inak, a ktorá je poskytovateľom digitálnej služby písomne poverená konať v jeho mene a na jeho zodpovednosť vo vzťahu k povinnostiam podľa tohto zákona.Poskytovateľ digitálnej služby, ktorý poskytuje digitálnu službu v Slovenskej republike, nemá sídlo v Európskej únii a neustanovil si svojho zástupcu v inom členskom štáte Európskej únie, je povinný si ustanoviť svojho zástupcu v Slovenskej republike.Ak má poskytovateľ digitálnej služby sídlo v Slovenskej republike alebo tu má ustanoveného zástupcu, ale jeho siete a informačné systémy sa nachádzajú v inom členskom štáte Európskej únie, úrad pri výkone štátnej správy spolupracuje s príslušným orgánom členského štátu Európskej únie.Úrad je národným kontaktným miestom pre kybernetickú bezpečnosť pre zahraničie a zabezpečuje spoluprácu s jednotnými kontaktnými miestami iných členských štátov Európskej únie a Organizácie severoatlantickej zmluvy,  | Ú |  |
| Č:18,O:1 | Článok 18 Právomoc a teritorialita 1. Na účely tejto smernice sa má za to, že poskytovateľ digitálnych služieb podlieha právomoci členského štátu, v ktorom má hlavnú prevádzkareň. V prípade poskytovateľa digitálnych služieb sa má za to, že hlavnú prevádzkareň má v tom členskom štáte, v ktorom sa nachádza jeho sídlo. | N |  | §:23,O:1O:2O:3 | Zástupcom poskytovateľa digitálnej služby je právnická osoba, ktorá má sídlo v Slovenskej republike alebo fyzická osoba - podnikateľ, ktorá má miesto podnikania v Slovenskej republike, ak odsek 2 neustanovuje inak, a ktorá je poskytovateľom digitálnej služby písomne poverená konať v jeho mene a na jeho zodpovednosť vo vzťahu k povinnostiam podľa tohto zákona.Poskytovateľ digitálnej služby, ktorý poskytuje digitálnu službu v Slovenskej republike, nemá sídlo v Európskej únii a neustanovil si svojho zástupcu v inom členskom štáte Európskej únie, je povinný si ustanoviť svojho zástupcu v Slovenskej republike.Ak má poskytovateľ digitálnej služby sídlo v Slovenskej republike alebo tu má ustanoveného zástupcu, ale jeho siete a informačné systémy sa nachádzajú v inom členskom štáte Európskej únie, úrad pri výkone štátnej správy spolupracuje s príslušným orgánom členského štátu Európskej únie. | Ú |  |
| Č:18,O:2 | Poskytovateľ digitálnych služieb, ktorý nie je usadený v Únii, ale ponúka v nej služby uvedené v prílohe III, určí svojho zástupcu v Únii. Zástupca musí byť usadený v jednom z členských štátov, v ktorých ponúka služby. Má sa za to, že poskytovateľ digitálnych služieb podlieha právomoci toho členského štátu, v ktorom je usadený jeho zástupca. | N |  | §:23,O:1O:2O:3 | Zástupcom poskytovateľa digitálnej služby je právnická osoba, ktorá má sídlo v Slovenskej republike alebo fyzická osoba - podnikateľ, ktorá má miesto podnikania v Slovenskej republike, ak odsek 2 neustanovuje inak, a ktorá je poskytovateľom digitálnej služby písomne poverená konať v jeho mene a na jeho zodpovednosť vo vzťahu k povinnostiam podľa tohto zákona.Poskytovateľ digitálnej služby, ktorý poskytuje digitálnu službu v Slovenskej republike, nemá sídlo v Európskej únii a neustanovil si svojho zástupcu v inom členskom štáte Európskej únie, je povinný si ustanoviť svojho zástupcu v Slovenskej republike.Ak má poskytovateľ digitálnej služby sídlo v Slovenskej republike alebo tu má ustanoveného zástupcu, ale jeho siete a informačné systémy sa nachádzajú v inom členskom štáte Európskej únie, úrad pri výkone štátnej správy spolupracuje s príslušným orgánom členského štátu Európskej únie. |  |  |
| Č:18,O:3 | Určením zástupcu poskytovateľa digitálnych služieb nie sú dotknuté právne kroky, ktoré by mohli byť podniknuté proti samotnému poskytovateľovi digitálnych služieb. | N | Zákon č. 40/1964 Z.z. Občiansky zákoník | §22,O:1O:2§:23§:24 | Zástupcom je ten, kto je oprávnený konať za iného v jeho mene. **Zo zastúpenia vznikajú práva a povinnosti priamo zastúpenému**. Zastupovať iného nemôže ten, kto sám nie je spôsobilý na právny úkon, o ktorý ide, ani ten, záujmy ktorého sú v rozpore so záujmami zastúpeného. Zastúpenie vzniká na základe zákona alebo rozhodnutia štátneho orgánu (zákonné zastúpenie) alebo na základe dohody o plnomocenstve. Zástupca musí konať osobne; ďalšieho zástupcu si môže ustanoviť, len ak je to právnym predpisom ustanovené alebo účastníkmi dohodnuté. Aj z právnych úkonov ďalšieho zástupcu vznikajú práva a povinnosti priamo zastúpenému.  | Ú |  |
| Č:19,O:1 | **KAPITOLA VI NORMALIZÁCIA A DOBROVOĽNÉ OZNAMOVANIE** Normalizácia 1. Členské štáty v záujme presadzovania zbližujúceho sa vykonávania článku 14 ods. 1 a 2 a článku 16 ods. 1 a 2 a bez toho, aby ukladali povinnosť využívať určitý typ technológie alebo diskriminovali v prospech takéhoto využívania, podporujú využívanie európskych alebo medzinárodne uznávaných noriem a špecifikácií, ktoré sú relevantné pre bezpečnosť sietí a informačných systémov.  | N | Návrh zákona  | §:32,O:1 O:2 | (1) Úrad sa splnomocňuje na vydanie všeobecne záväzného právneho predpisu, ktorým ustanovía) podrobnosti o technickom, technologickom a personálnom vybavení jednotky CSIRT,b) identifikačné kritériá základnej služby,c) obsah bezpečnostných opatrení, obsah a štruktúru bezpečnostnej dokumentácie, rozsah všeobecných bezpečnostných opatrení,d) bezpečnostné štandardy a znalostné štandardy v oblasti kybernetickej bezpečnosti,e) kategórie a identifikačné kritériá kybernetických bezpečnostných incidentov hlásených prevádzkovateľom základnej služby a poskytovateľom digitálnej služby,f) pravidlá a rozsah auditu kybernetickej bezpečnosti podľa § 29 ods. 1, podrobnosti o akreditácii orgánov posudzovania zhody podľa tohto zákona a o obsahu záverečnej správy o výsledkoch auditu kybernetickej bezpečnosti podľa § 29.(2) Ústredný orgán v spolupráci s úradom sa splnomocňuje na vydanie všeobecne záväzného právneho predpisu, ktorým ustanovia sektorové bezpečnostné opatrenia v rozsahu svojej pôsobnosti podľa prílohy č. 1 a v súlade s bezpečnostnými štandardami v oblasti kybernetickej bezpečnosti. | Ú |  |
| Č:19,O:2 | 2.Agentúra ENISA v spolupráci s členskými štátmi vypracúva odporúčania a usmernenia týkajúce sa technických oblastí, ktoré sa majú zvážiť v súvislosti s odsekom 1, ako aj odporúčania a usmernenia týkajúce sa už existujúcich noriem vrátane vnútroštátnych noriem členských štátov, ktoré by sa mohli vzťahovať na uvedené oblasti. | n.a |  |  |  |  |  |
| Č:20,O:1 |  Dobrovoľné oznamovanie 1. Bez toho, aby bol dotknutý článok 3, subjekty, ktoré neboli určené ako prevádzkovatelia základných služieb a nie sú poskytovateľmi digitálnych služieb, môžu na dobrovoľnom základe oznamovať incidenty, ktoré majú závažný vplyv na kontinuitu služieb, ktoré poskytujú.  | D |  | §:26, O:1O:2 | Dobrovoľné hlásenie kybernetických bezpečnostných incidentov, bez ohľadu na kategorizáciu kybernetického bezpečnostného incidentu, sa vykonáva prostredníctvom jednotného informačného systému kybernetickej bezpečnosti.Úrad spracováva a analyzuje dobrovoľné hlásenia kybernetických bezpečnostných incidentov v rozsahu, v akom to úradu umožňujú technické podmienky a kapacity tak, aby nedošlo k neprimeranému zaťažovaniu subjektov a neobmedzovala sa medzinárodná spolupráca. |  |  |
| Č:20,O:2 | 2.Pri spracúvaní oznámení členské štáty konajú v súlade s postupom stanoveným v článku 14. Členské štáty môžu uprednostniť spracúvanie povinných oznámení pred dobrovoľnými oznámeniami. Dobrovoľné oznámenia sa spracúvajú len vtedy, ak takéto spracovanie nepredstavuje neprimerané alebo nenáležité zaťaženie dotknutých členských štátov. V dôsledku dobrovoľného oznámenia nevznikajú oznamujúcemu subjektu žiadne povinnosti, ktoré by sa naň neboli vzťahovali, ak by oznámenie nepodal. | D |  | §:26,O:2 | Úrad spracováva a analyzuje dobrovoľné hlásenia kybernetických bezpečnostných incidentov v rozsahu, v akom to úradu umožňujú technické podmienky a kapacity tak, aby nedošlo k neprimeranému zaťažovaniu subjektov a neobmedzovala sa medzinárodná spolupráca. |  |  |
| Č:21 | **KAPITOLA VII ZÁVEREČNÉ USTANOVENIA**Sankcie Členské štáty stanovia pravidlá ukladania sankcií za porušenie vnútroštátnych predpisov prijatých podľa tejto smernice a prijmú všetky opatrenia potrebné na zabezpečenie ich uplatňovania. Stanovené sankcie musia byť účinné, primerané a odrádzajúce. Členské štáty do 9. mája 2018 informujú Komisiu o týchto pravidlách a opatreniach a bezodkladne jej oznámia akékoľvek následné zmeny, ktoré na ne majú vplyv. | N | Návrh zákona | §:31,O:1O:2O:3O:4O:5§:32,O:1O:2O:3O:4O:5O:6O:7O:8O:9O:10O:11O:12 | Priestupku sa dopustí fyzická osoba, ktoráa) poruší povinnosť uvedenú v § 12 ods. 1,b) poskytla nepravdivé údaje podľa § 17 ods. 5,c) poruší povinnosť uvedenú § 19 ods. 1 až 3 a ods. 6 a 7,d) neprijme bezpečnostnú dokumentáciu v zmysle § 20 ods. 5,e) nepostupovala v súlade s technickými, organizačnými alebo personálnymi opatreniami prijatými prevádzkovateľom základnej služby.Za priestupok možno uložiť pokutu od 100 eur do 5 000 eur.Na priestupky a ich prejednávanie sa vzťahuje všeobecný predpis o priestupkoch. )Priestupky prejednáva úrad a pokuty ukladá úrad.Pokuty za priestupky sú príjmom štátneho rozpočtu.Úrad uloží pokutu od 3 000 eur do 30 000 eur prevádzkovateľovi základnej služby, ktorý sa dopustí správneho deliktu tým, že poruší povinnosť podľa § 19 ods. 2 až 4 a 7 alebo nemá bezpečnostnú dokumentáciu v súlade s § 20 ods. 5.Úrad uloží pokutu od 3 000 eur až do výšky 1 % celkového ročného obratu za predchádzajúci účtovný rok, maximálne 300 000 eur, prevádzkovateľovi základnej služby, ktorý sa dopustí správneho deliktu tým, že poruší povinnosť podľa § 17 ods. 1, § 19 ods. 1 a 6, § 24 ods. 1 a 5, § 27 ods. 3, 5,6 a 8 a § 29 ods. 1, 2 a 4 alebo ak nevykoná opatrenia na nápravu v lehote podľa záverečnej správy o výsledkoch auditu.Úrad uloží pokutu od 3 000 eur do 30 000 eur poskytovateľovi digitálnej služby, ktorý sa dopustí správneho deliktu tým, že poruší povinnosť podľa § 21 ods. 5, § 22 ods. 4 a § 23 ods. 2.Úrad uloží pokutu od 3 000 eur až do výšky 1 % celkového ročného obratu za predchádzajúci účtovný rok, maximálne 300 000 eur, poskytovateľovi digitálnej služby, ktorý sa dopustí správneho deliktu tým, že poruší povinnosť podľa § 21 ods. 1, § 22 ods. 3, § 24 ods. 3, § 25 ods. 1 a 2 alebo § 27 ods. 5.Úrad uloží pokutu od 3 000 eur do 100 000 eur tomu, kto na výzvu úradu nesplní povinnosti podľa § 7 ods. 3.Pri ukladaní pokuty za správny delikt úrad prihliadne najmä na závažnosť, spôsob, trvanie a dôsledky porušenia povinnosti.Ak do jedného roka odo dňa nadobudnutia právoplatnosti rozhodnutia o uložení pokuty dôjde k opätovnému porušeniu povinností, za ktoré bola pokuta uložená, úrad uloží pokutu až do dvojnásobku výšky súm uvedených alebo vypočítaných podľa odsekov 1 až 5.Obratom podľa odsekov 2 a 4 sa na účely tohto zákona rozumie súčet všetkých tržieb, výnosov alebo príjmov z predaja tovaru alebo služieb bez nepriamych daní, ku ktorému sa pripočíta poskytnutá finančná pomoc. Obrat vyjadrený v cudzej mene sa prepočíta na eurá, pričom na prepočet cudzej meny na eurá sa použije priemer referenčných výmenných kurzov určených a vyhlásených Európskou centrálnou bankou alebo Národnou bankou Slovenska, ktoré sú platné pre príslušné účtovné obdobie. )Predchádzajúcim účtovným obdobím na účely tohto zákona je účtovné obdobie, za ktoré bola zostavená posledná účtovná závierka.Pokutu za správny delikt možno uložiť do dvoch rokov odo dňa zistenia porušenia povinnosti, najneskôr však do štyroch rokov odo dňa keď k porušeniu povinnosti došlo.Pokuta za správny delikt je splatná do 30 dní odo dňa nadobudnutia právoplatnosti rozhodnutia o jej uložení.Pokuty za správny delikt sú príjmom štátneho rozpočtu. | Ú |  |
| Č:22 | Postup výboru 1. Komisii pomáha Výbor pre bezpečnosť sietí a informačných systémov. Uvedený výbor je výborom v zmysle nariadenia (EÚ) č. 182/2011. 2. Ak sa odkazuje na tento odsek, uplatňuje sa článok 5 nariadenia (EÚ) č. 182/2011. | n.a. |  |  |  |  |  |
| Č:23 | Preskúmanie 1. Komisia do 9. mája 2019 predloží Európskemu parlamentu a Rade správu, v ktorej posúdi jednotnosť prístupu členských štátov pri identifikácii prevádzkovateľov základných služieb. 2. Komisia pravidelne skúma fungovanie tejto smernice a podáva o tom správu Európskemu parlamentu a Rade. Na tento účel a s cieľom ďalej napredovať v strategickej a operačnej spolupráci Komisia zohľadní správy skupiny pre spoluprácu a siete jednotiek CSIRT o skúsenostiach získaných na strategickej a operačnej úrovni. Vo svojom preskúmaní Komisia posúdi aj zoznamy uvedené v prílohách II a III a jednotnosť pri identifikácii prevádzkovateľov základných služieb a služieb v odvetviach uvedených v prílohe II. Prvá správa sa predloží do 9. mája 2021. | n.a |  |  |  |  |  |
| Č:24,O:1 | Prechodné opatrenia 1. Bez toho, aby bol dotknutý článok 25, a s cieľom poskytnúť členským štátom ďalšie možnosti pre vhodnú spoluprácu počas obdobia transpozície začnú skupina pre spoluprácu a sieť jednotiek CSIRT vykonávať úlohy stanovené v článku 11 ods. 3 a článku 12 ods. 3 do 9. februára 2017. | n.a. |  |  |  |  |  |
| Č:24,O:2 | V období od 9. februára 2017 do 9. novembra 2018 a s cieľom podporiť členské štáty, aby zaujímali jednotný prístup k procesu identifikácie prevádzkovateľov základných služieb, skupina pre spoluprácu prerokuje procesný rámec, podstatu a typ vnútroštátnych opatrení, ktoré umožnia identifikáciu prevádzkovateľov základných služieb v konkrétnom odvetví v súlade s kritériami stanovenými v článkoch 5 a 6. Skupina pre spoluprácu na žiadosť členského štátu tiež prerokuje konkrétne návrhy vnútroštátnych opatrení daného členského štátu, ktoré umožňujú identifikáciu prevádzkovateľov základných služieb v konkrétnom odvetví v súlade s kritériami stanovenými v článkoch 5 a 6. | n.a. |  |  |  |  |  |
| Č:24,O:3 | Členské štáty do 9. februára 2017 a na účely tohto článku zabezpečia svoje primerané zastúpenie v skupine pre spoluprácu a sieti jednotiek CSIRT. | N | Návrh zákona | §:5, O:1 P:eP:f | Úrad je národným kontaktným miestom pre kybernetickú bezpečnosť pre zahraničie a zabezpečuje spoluprácu s jednotnými kontaktnými miestami iných členských štátov Európskej únie a Organizácie severoatlantickej zmluvy, Úrad plní notifikačné a reportingové povinnosti voči príslušným orgánom Európskej únie a Organizácie severoatlantickej zmluvy a podieľa sa a podporuje vytváranie partnerstiev na národnej a medzinárodnej úrovni v oblasti kybernetickej bezpečnosti  | Ú |  |
| Č:25,O:1 |  Transpozícia 1. Členské štáty prijmú a uverejnia do 9. mája 2018 zákony, iné právne predpisy a správne opatrenia potrebné na dosiahnutie súladu s touto smernicou. Bezodkladne o tom informujú Komisiu. Tieto opatrenia uplatňujú od 10 mája 2018.Členské štáty uvedú priamo v prijatých opatreniach alebo pri ich úradnom uverejnení odkaz na túto smernicu. Podrobnosti o odkaze upravia členské štáty. | N | Návrh zákona | §:3Príloha č. 3 | Týmto zákonom sa preberajú všeobecne záväzné právne akty EÚ uvedené v prílohe č. 3Zoznam preberaných všeobecne záväzných právnych aktov EÚ: 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. | Ú |  |
| Č:25,O:2 | Členské štáty oznámia Komisii znenie hlavných ustanovení vnútroštátnych právnych predpisov, ktoré prijmú v oblasti pôsobnosti tejto smernice. | N |  | §:5, O:1P:f | Úrad plní notifikačné a reportingové povinnosti voči príslušným orgánom Európskej únie a Organizácie severoatlantickej zmluvy a podieľa sa a podporuje vytváranie partnerstiev na národnej a medzinárodnej úrovni v oblasti kybernetickej bezpečnosti,  | Ú |  |
| Č:26 | Nadobudnutie účinnosti Táto smernica nadobúda účinnosť dvadsiatym dňom po jej uverejnení v Úradnom vestníku Európskej únie | n.a |  |  |  |  |  |
| Č:27 |  Adresáti Táto smernica je určená členským štátom. | n.a |  |  |  |  |  |
| Príloha I. | **PRÍLOHA I** Požiadavky týkajúce sa jednotiek pre riešenie počítačových bezpečnostných incidentov (jednotky CSIRT) a ich úlohy Požiadavky na jednotky CSIRT a ich úlohy musia byť primerane a jasne vymedzené a podporované vnútroštátnymi politikami a/alebo právnymi prepismi. Zahŕňajú: 1. požiadavky na jednotky CSIRT a) Jednotky CSIRT zabezpečujú vysokú úroveň dostupnosti svojich komunikačných služieb, a to tak, že predchádzajú tomu, že zlyhajú ako celok, ak zlyhá ich ľubovoľný jediný bod, a majú k dispozícii niekoľko spôsobov, ktorými ich možno kontaktovať a ktorými môžu oni kedykoľvek kontaktovať iných. Okrem toho sú komunikačné kanály jasne vymedzené a zainteresované strany a spolupracujúci partneri sú o nich dobre informovaní. b) Pracoviská jednotiek CSIRT a podporné informačné systémy sú umiestnené na zabezpečených miestach. c) Zabezpečenie kontinuity činnosti: i) Jednotky CSIRT majú zavedený vhodný systém riadenia a zasielania žiadostí v záujme jednoduchšieho odovzdávania. ii) Jednotky CSIRT sú primerane personálne vybavené, aby sa zabezpečila stála dostupnosť ich služieb. iii) Jednotky CSIRT využívajú infraštruktúru, ktorej kontinuita je zabezpečená. Na tento účel sú k dispozícii záložné systémy a záložný pracovný priestor. d) Jednotky CSIRT musia mať možnosť zapojiť sa do sietí medzinárodnej spolupráce, pokiaľ majú v úmysle byť ich súčasťou. 2. Úlohy jednotiek CSIRT a) Úlohy jednotiek CSIRT zahŕňajú aspoň: i) monitorovanie incidentov na vnútroštátnej úrovni; ii) vydávanie včasného varovania, upozornení, oznamovanie a šírenie informácií o rizikách a incidentoch príslušným zainteresovaným stranám; iii) reagovanie na incidenty; iv) zabezpečovanie dynamickej analýzy rizík a incidentov a získavanie informácií o situácii; v) účasť na činnosti siete jednotiek CSIRT. b) Jednotky CSIRT nadviažu spoluprácu so súkromným sektorom. c) V záujme uľahčenia spolupráce jednotky CSIRT podporujú prijímanie a využívanie spoločnej alebo normalizovanej praxe v oblasti: i) postupov na riešenie incidentov a rizík; ii) systémov klasifikácie incidentov, rizík a informácií. | N | Návrh zákona | §:14§:15, O:1O:2O:3O:4§:16, O:1O:2   O:3 | Žiadateľ o akreditáciu jednotky CSIRT podľa § 13 príslušnou spisovou dokumentáciou preukazuje, že jednotka CSIRT a) má požadované technické, technologické a personálne vybavenie podľa osobitného predpisu, ktorý vydá úrad, b) má vytvorené podmienky umožňujúce chránený prenos a spracovanie údajov spôsobom podľa osobitného predpisu, c) chráni informácie a údaje, ktoré v súvislosti s plnením povinnosti podľa tohto zákona získava a spracováva ich tak, aby nebola narušená ich dostupnosť, dôvernosť, autentickosť a integritad) má umiestnenú dokumentáciu, informačné systémy a ostatné informačno-komunikačné technológie prevádzkované jednotkou CSIRT v zabezpečenom priestore tak, aby nebola narušená ich dôvernosť, autentickosť a integrita.20) Ten, kto plní úlohy jednotky CSIRT v rozsahu svojej pôsobnosti určenej podľa prílohy č. 1 zodpovedá za riešenie kybernetických bezpečnostných incidentov a vykonáva preventívne služby a reaktívne služby.Preventívne služby sa zameriavajú na prevenciu kybernetických bezpečnostných incidentova) vytváraním bezpečnostného povedomia,b) výcvikom,c) spoluprácou s ostatnými jednotkami CSIRT,d) monitorovaním a evidenciou kybernetických bezpečnostných incidentov,e) pripojením na jednotný informačný systém kybernetickej bezpečnosti,f) poskytovaním informácií a údajov do jednotného informačného systému kybernetickej bezpečnosti,g) prijímaním a zasielaním včasného varovania pred kybernetickými bezpečnostnými incidentmi prostredníctvom jednotného informačného systému kybernetickej bezpečnosti.Reaktívne služby sa zameriavajú na riešenie kybernetických bezpečnostných incidentov a sú nimi najmäa) výstraha a varovanie,b) detekcia kybernetických bezpečnostných incidentov,c) analýza kybernetických bezpečnostných incidentov,d) odozva, ohraničenie, riešenie a náprava následkov kybernetických bezpečnostných incidentov,e) asistencia pri riešení na kybernetický bezpečnostný incident na mieste, f) g) reakcia na kybernetický bezpečnostný incident,h) podpora reakcií na kybernetické bezpečnostné incidenty,i) koordinácia reakcií na kybernetické bezpečnostné incidenty,j) návrh opatrení na zabránenie ďalšiemu pokračovaniu, šíreniu a opakovanému výskytu kybernetických bezpečnostných incidentov.Reaktívne služby vykonáva jednotka CSIRT za účasti prevádzkovateľa základnej služby alebo poskytovateľa digitálnej služby.Ten, kto plní úlohy jednotky CSIRTa) musí zabezpečiť, aby jednotka CSIRT v jeho pôsobnosti, ktorá je zaradená v zozname akreditovaných jednotiek CSIRT, nepretržite počas celej doby svojej prevádzky spĺňala podmienky akreditácie jednotky CSIRT podľa § 14 a zároveň plnila všetky úlohy podľa § 15,b) oznamuje úradu všetky zmeny, ktoré majú vplyv na akreditáciu jednotky CSIRT bezodkladne po tom, ako nastali,c) si vyžiada vyjadrenie Národnej banky Slovenska k postupu ústredného orgánu pri plnení úloh podľa tohto zákona, ak prevádzkovateľom základnej služby je dohliadaný subjekt finančného trhu, ) nad ktorým vykonáva dohľad Národná banka Slovenska podľa osobitných predpisov. )) Ak akreditovaná jednotka CSIRT prestane spĺňať podmienky podľa § 14 alebo ak neplní úlohy podľa § 15, ten, kto plní úlohy jednotky CSIRT to bezodkladne oznámi úradu; úrad na základe oznámenia podľa predchádzajúcej vety zruší rozhodnutie o akreditácii a jednotku CSIRT vyradí zo zoznamu akreditovaných jednotiek CSIRT.Úrad môže na základe vlastného zistenia oboznámiť toho, kto plní úlohy jednotky CSIRT o nedostatkoch v plnení podmienok podľa § 14 alebo úloh podľa § 15 s uvedením lehoty na ich odstránenie. Ak tento nedostatky podľa prechádzajúcej vety na základe oznámenia úradu neodstráni v určenej lehote, úrad zruší rozhodnutie o akreditácii a jednotku CSIRT vyradí zo zoznamu akreditovaných jednotiek CSIRT. | Ú |  |
| Príloha II | Typy subjektov na účely článku 4 bodu 4

|  |  |
| --- | --- |
| 1. Energetika  | a) Elektrická energia  |

 b) Ropa  c) Plyn

|  |  |
| --- | --- |
| 2. Doprava  | a) Letecká dopravab) Železničná dopravac) Cestná dopravad) Letecká doprava |
| 3. Bankovníctvo 4. Infraštruktúry finančných trhov

|  |  |
| --- | --- |
| 5. Zdravotníctvo  | Zdravotnícke zariadenia (vrátane nemocníc a súkromných kliník)  |

 |  |

6. Dodávka a distribúcia pitnej vody 7. Digitálna infraštruktúra  | N | Návrh zákona | Príloha č. 1 | Sektory a podsektory v zmysle tohto zákona:

|  |  |
| --- | --- |
|  1. Bankovníctvo | Úverové inštitúcieSprávcovia a prevádzkovatelia informačného systému štátnej pokladnice |

|  |  |
| --- | --- |
|  |  |
| 2. Doprava a) Cestná doprava cestné orgány zodpovedné za  kontrolu riadenia cestnej  premávky  prevádzkovatelia  inteligentných dopravných  systémov b)Letecká doprava leteckí dopravcovia riadiace orgány letiska  prevádzkovatelia  poskytujúci  služby riadenia letovej  prevádzky (ATC)c)Vodná doprava spoločnosti prevádzkujúcee  vnútrozemskú, námornú  a pobrežnú osobnú  a nákladnú, vodnú dopravu,  riadiace orgány prístavu prevádzkovatelia  plavebno-prevádzkových  služiebd)Železničná doprava manažéri infraštruktúry železničné podniky 3. Digitálna infraštruktúra  -internetové prepojovacie uzly (IXP)- poskytovatelia služieb DNS- registre domén najvyššej úrovne (TLD) 4. Elektronické komunikácie a) Satelitná komunikácia b) Siete a služby pevných a mobilných elektronických komunikácií

|  |  |
| --- | --- |
| 5. Energetikaa) Baníctvob) Elektroenergetika - elektroenergetické podniky- prevádzkovatelia distribučnej sústavy- prevádzkovatelia prenosovej sústavyc) Plynárenstvo - dodávateľské podniky - prevádzkovatelia distribučnej siete- prevádzkovatelia prepravnej siete - prevádzkovatelia zásobníkov- prevádzkovatelia zariadení LNG- plynárenské podniky - prevádzkovatelia zariadení na rafinovanie  a spracovanie zemného plynud) Ropa a ropné produkty - prevádzkovatelia ropovodov, - prevádzkovatelia zariadení na ťažbu, rafino- vanie a spracovanie ropy, jej skladovanie  a prepravue) Tepelná energetika |  |

 |  |

 6. Infraštruktúra finančných trhov  - prevádzkovatelia obchodných miest - centrálne protistrany 7. Pošta 8. Priemysel  a) Farmaceutický priemysel b) Hutnícky priemysel c) Chemický priemysel 9. Voda a atmosféra a) Meterologická služby b) Vodné stavby c) Zabezpečovanie pitnej vody  10. Verejná správa a) Bezpečnosť b) ISVS c) Obrana d) Spravodajské služby d) Utajované skutočnosti 11. Zdravotníctvo Zdravotnícke zariadenia vrátane nemocníc a súkromných kliník (poskytovatelia zdravotnej starostlivosti)  | Ú |  |
| Príloha III. | Druhy digitálnych služieb na účely článku 4 bodu 5 1. Online trhovisko 2. Internetový vyhľadávač 3. Služby cloud computingu | N | Návrh zákona  | Príloha č. 2 | **Digitálne služby**Online- trhovisko, Internetového vyhľadávač, Cloud computing | Ú |  |