►B

SMERNICA EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2022/2555

zo 14. decembra 2022

o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (smernica NIS 2)

(Text s významom pre EHP)

(Ú. v. EÚ L 333, 27.12.2022, s. 80)

Opravená a doplnená:

►C1 Korigendum, Ú. v. EÚ L 90349, 12.6.2024, s. 1 (2022/2555)

▼B

SMERNICA EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2022/2555

zo 14. decembra 2022

o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (smernica NIS 2)

(Text s významom pre EHP)

KAPITOLA I

VŠEOBECNÉ USTANOVENIA

Článok 1

Predmet úpravy

1. Touto smernicou sa stanovujú opatrenia, ktorých zámerom je dosiahnuť vysokú spoločnú úroveň kybernetickej bezpečnosti v celej Únii na účely lepšieho fungovania vnútorného trhu.

2. Na uvedený účel sa v tejto smernici stanovujú:

a) povinnosti, ktorými sa od členských štátov vyžaduje, aby prijali národné stratégie kybernetickej bezpečnosti a určili alebo zriadili príslušné orgány, orgány pre riadenie kybernetických kríz, jednotné kontaktné miesta pre kybernetickú bezpečnosť (jednotné kontaktné miesta) a jednotky pre riešenie počítačových bezpečnostných incidentov (jednotky CSIRT);

b) opatrenia na riadenie kybernetických rizík a oznamovacie povinnosti pre subjekty typu uvedeného v prílohe I alebo II, ako aj pre subjekty identifikované ako kritické subjekty podľa smernice (EÚ) 2022/2557;

c) pravidlá a povinnosti výmeny informácií o kybernetickej bezpečnosti;

d) povinnosti členských štátov v oblasti dohľadu a presadzovania práva.

Článok 2

Rozsah pôsobnosti

1. Táto smernica sa vzťahuje na verejné alebo súkromné subjekty typu uvedeného v prílohe I alebo II, ktoré sa považujú za stredné podniky podľa článku 2 prílohy k odporúčaniu 2003/361/ES alebo presahujú limity pre stredné podniky stanovené v odseku 1 uvedeného článku a ktoré poskytujú služby alebo vykonávajú svoje činnosti v Únii.

▼B

Na účely tejto smernice sa článok 3 ods. 4 prílohy k uvedenému odporúčaniu neuplatňuje.

2. Táto smernica sa vzťahuje aj na subjekty typu uvedeného v prílohe I alebo II bez ohľadu na ich veľkosť, ak:

a) služby poskytujú:

   i) poskytovatelia verejných elektronických komunikačných sietí alebo verejne dostupných elektronických komunikačných služieb;

   ii) poskytovatelia dôveryhodných služieb;

   iii) registre názvov domén najvyššej úrovne a poskytovatelia služieb systému názvov domén;

b) subjekt je v členskom štáte jediným poskytovateľom služby, ktorá je kľúčovou pre zachovanie kritických spoločenských alebo hospodárskych činností;

c) narušenie služby poskytovanej subjektom by mohlo mať významný vplyv na verejný poriadok, verejnú bezpečnosť alebo verejné zdravie;

d) narušenie služby poskytovanej subjektom by mohlo vyvolať významné systémové riziko, najmä v odvetviach, v ktorých by takéto narušenie mohlo mať cezhraničný vplyv;

e) subjekt je vzhľadom na svoj osobitný význam na vnútroštátnej alebo regionálnej úrovni kritickým pre konkrétne odvetvie alebo typ služby alebo pre iné vzájomne závislé odvetvia v členskom štáte;

f) subjekt je subjektom verejnej správy:

   i) v ústrednej štátnej správe podľa definície členského štátu v súlade s vnútroštátnym právom; alebo

   ii) na regionálnej úrovni podľa definície členského štátu v súlade s vnútroštátnym právom, ktorý po posúdení na základe rizík poskytuje služby, ktorých narušenie by mohlo mať významný vplyv na kritické spoločenské alebo hospodárske činnosti.

3. Táto smernica sa vzťahuje na subjekty identifikované ako kritické subjekty podľa smernice (EÚ) 2022/2557 bez ohľadu na ich veľkosť.

▼B

4. Táto smernica sa vzťahuje na subjekty poskytujúce služby registrácie názvov domén bez ohľadu na ich veľkosť.

5. Členské štáty môžu ustanoviť, že sa táto smernica vzťahuje na:

a) subjekty verejnej správy na miestnej úrovni;

b) vzdelávacie inštitúcie, najmä tie, v ktorých sa vykonávajú kritické výskumné činnosti.

6. Touto smernicou nie je dotknutá zodpovednosť členských štátov za ochranu národnej bezpečnosti ani ich právomoc chrániť iné základné funkcie štátu vrátane zabezpečenia územnej celistvosti štátu a udržiavania verejného poriadku.

7. Táto smernica sa nevzťahuje na subjekty verejnej správy, ktoré vykonávajú činnosť v oblasti národnej bezpečnosti, verejnej bezpečnosti, obrany alebo presadzovania práva vrátane prevencie, vyšetrovania, odhaľovania a stíhania trestných činov.

8. Členské štáty môžu vyňať konkrétne subjekty, ktoré vykonávajú činnosti v oblastiach národnej bezpečnosti, verejnej bezpečnosti, obrany alebo presadzovania práva vrátane prevencie, vyšetrovania, odhaľovania a stíhania trestných činov, alebo ktoré poskytujú služby výhradne subjektom verejnej správy uvedeným v odseku 7 tohto článku, v súvislosti s danými činnosťami alebo službami z povinností stanovených v článku 21 alebo článku 23. V takýchto prípadoch sa opatrenia dohľadu a presadzovania uvedené v kapitole VII v súvislosti s týmito konkrétnymi činnosťami alebo službami neuplatňujú. Ak subjekty vykonávajú činnosti alebo poskytujú služby výlučne typu uvedeného v tomto odseku, členské štáty sa môžu tiež rozhodnúť vyňať tieto subjekty z povinností stanovených v článkoch 3 a 27.

9. Ak subjekt koná ako poskytovateľ dôveryhodných služieb, odseky 7 a 8 sa neuplatňujú.

10. Táto smernica sa nevzťahuje na subjekty, ktoré členské štáty vyňali z rozsahu pôsobnosti nariadenia (EÚ) 2022/2554 v súlade s článkom 2 ods. 4 uvedeného nariadenia.

11. K povinnostiam ustanoveným v tejto smernici nepatrí poskytovanie informácií, ktorých zverejnenie by bolo v rozpore so základnými záujmami členských štátov v oblasti národnej bezpečnosti, verejnej bezpečnosti alebo obrany.

12. Táto smernica sa uplatňuje bez toho, aby bolo dotknuté nariadenie (EÚ) 2016/679, smernica 2002/58/ES, smernice Európskeho parlamentu a Rady 2011/93/EÚ ([1]) a 2013/40/EÚ ([2]) a smernica (EÚ) 2022/2557.

([1]) Smernica Európskeho parlamentu a Rady 2011/93/EÚ z 13. decembra 2011 o boji proti sexuálnemu zneužívaniu a sexuálnemu vykorisťovaniu detí a proti detskej pornografii, ktorou sa nahrádza rámcové rozhodnutie Rady 2004/68/SVV (Ú. v. EÚ L 335, 17.12.2011, s. 1).

([2]) Smernica Európskeho parlamentu a Rady 2013/40/EÚ z 12. augusta 2013 o útokoch na informačné systémy, ktorou sa nahrádza rámcové rozhodnutie Rady 2005/222/SVV (Ú. v. EÚ L 218, 14.8.2013, s. 8).

▼B

13. Bez toho, aby bol dotknutý článok 346 ZFEÚ, informácie, ktoré sú podľa predpisov Únie alebo vnútroštátnych predpisov dôverné, ako napríklad predpisy o obchodnom tajomstve, sa vymieňajú s Komisiou a inými príslušnými orgánmi v súlade s touto smernicou len vtedy, ak je takáto výmena potrebná na účely uplatňovania tejto smernice. Vymieňané informácie sa obmedzia na také informácie, ktoré sú relevantné a primerané účelu danej výmeny. Pri výmene informácií sa zachováva ich dôvernosť a chránia sa bezpečnostné a komerčné záujmy dotknutých subjektov.

14. Subjekty, príslušné orgány, jednotné kontaktné miesta a jednotky CSIRT spracúvajú osobné údaje v rozsahu potrebnom na účely tejto smernice a v súlade s nariadením (EÚ) 2016/679, pričom takéto spracovanie sa opiera najmä o jeho článok 6.

Spracovanie osobných údajov podľa tejto smernice poskytovateľmi verejných elektronických komunikačných sietí alebo poskytovateľmi verejne dostupných elektronických komunikačných služieb sa vykonáva v súlade s právom Únie v oblasti ochrany údajov a právom Únie v oblasti ochrany súkromia, najmä so smernicou 2002/58/ES.

Článok 3

Kľúčové a dôležité subjekty

1. Na účely tejto smernice sa za kľúčové subjekty považujú:

a) subjekty typu uvedeného v prílohe I, ktoré presahujú limity pre stredné podniky stanovené v článku 2 ods. 1 prílohy k odporúčaniu 2003/361/ES;

b) kvalifikovaní poskytovatelia dôveryhodných služieb a registre názvov domén najvyššej úrovne, ako aj poskytovatelia služieb DNS, bez ohľadu na ich veľkosť;

c) poskytovatelia verejných elektronických komunikačných sietí alebo verejne dostupných elektronických komunikačných služieb, ktoré sú považované za stredné podniky podľa článku 2 prílohy k odporúčaniu 2003/361/ES;

d) subjekty verejnej správy uvedené v článku 2 ods. 2 písm. f) bode i);

e) akékoľvek iné subjekty typu uvedeného v prílohe I alebo II, ktoré členský štát označil za kľúčové subjekty podľa článku 2 ods. 2 písm. b) až e);

f) subjekty označené ako kritické subjekty podľa smernice (EÚ) 2022/2557 uvedenej v článku 2 ods. 3 tejto smernice;

g) ak tak členský štát ustanoví, subjekty, ktoré daný členský štát označil pred 16. januárom 2023 ako prevádzkovateľov základných služieb v súlade so smernicou (EÚ) 2016/1148 alebo vnútroštátnym právom.

▼B

2. Na účely tejto smernice sa subjekty typu uvedeného v prílohe I alebo II, ktoré sa nepovažujú za kľúčové subjekty podľa odseku 1 tohto článku, považujú za dôležité subjekty. Patria sem subjekty označené členskými štátmi ako dôležité subjekty podľa článku 2 ods. 2 písm. b) až e).

3. Do 17. apríla 2025 vypracujú členské štáty zoznam kľúčových a dôležitých subjektov ako aj subjektov poskytujúcich služby registrácie názvov domén. Členské štáty tento zoznam pravidelne prehodnocujú a podľa potreby aktualizujú najmenej každé dva roky po uvedenom dátume.

4. Na účely zostavenia zoznamu uvedeného v odseku 3 členské štáty požadujú od subjektov uvedených v uvedenom odseku, aby príslušným orgánom predložili aspoň tieto informácie:

a) názov subjektu;

b) adresu a aktuálne kontaktné údaje vrátane e-mailových adries, IP adries a telefónnych čísel;

c) podľa potreby príslušné odvetvie a pododvetvie uvedené v prílohe I alebo II; a

d) prípadne zoznam členských štátov, v ktorých poskytujú služby patriace do pôsobnosti tejto smernice.

Subjekty uvedené v odseku 3 bezodkladne a v každom prípade do dvoch týždňov odo dňa zmeny oznámia akékoľvek zmeny údajov zasielaných podľa prvého pododseku tohto odseku.

Komisia s pomocou Agentúry Európskej únie pre kybernetickú bezpečnosť (ENISA) bez zbytočného odkladu poskytne usmernenia a vzory súvisiace s povinnosťami stanovenými v tomto odseku.

Členské štáty môžu zaviesť vnútroštátne mechanizmy, pomocou ktorých by sa subjekty mohli zaregistrovať samé.

5. Do 17. apríla 2025 a potom každé dva roky príslušné orgány nahlasujú:

a) Komisii a skupine pre spoluprácu počet kľúčových a dôležitých subjektov uvedených v odseku 3 za každé odvetvie a pododvetvie uvedené v prílohe I alebo II; a

b) Komisii relevantné informácie o počte kľúčových a dôležitých subjektov označených podľa článku 2 ods. 2 písm. b) až e), odvetvie a pododvetvie uvedené v prílohe I alebo II, do ktorých patria, druh nimi poskytovanej služby a ustanovenie spomedzi ustanovení uvedených v článku 2 ods. 2 písm. b) až e), podľa ktorého boli označené.

▼B

6. Do 17. apríla 2025 a na žiadosť Komisie môžu členské štáty Komisii nahlásiť názvy kľúčových a dôležitých subjektov uvedených v odseku 5 písm. b).

Článok 4

Odvetvové právne akty Únie

1. Ak sa v odvetvových právnych aktoch Únie vyžaduje, aby kľúčové alebo dôležité subjekty prijali opatrenia na riadenie kybernetických rizík alebo aby nahlasovali významné incidenty, a ak majú tieto požiadavky aspoň rovnocenný účinok ako povinnosti stanovené v tejto smernici, príslušné ustanovenia tejto smernice vrátane ustanovení o dohľade a presadzovaní práva v kapitole VII sa na takéto subjekty nevzťahujú. Ak sa odvetvové právne akty Únie nevzťahujú na všetky subjekty v konkrétnom odvetví v pôsobnosti tejto smernice, príslušné ustanovenia tejto smernice sa naďalej vzťahujú na subjekty, na ktoré sa odvetvové právne akty Únie nevzťahujú.

2. Požiadavky uvedené v odseku 1 tohto článku sa považujú za rovnocenné s povinnosťami stanovenými v tejto smernici, ak:

a) opatrenia na riadenie kybernetických rizík majú prinajmenšom rovnocenný účinok ako opatrenia stanovené v článku 21 ods. 1 a 2; alebo

b) odvetvový právny akt Únie poskytuje okamžitý prístup, podľa potreby automatický a priamy, k hláseniam o incidentoch od jednotiek CSIRT, príslušných orgánov alebo jednotných kontaktných miest podľa tejto smernice a ak požiadavky na nahlasovanie závažných incidentov majú prinajmenšom rovnocenný účinok ako požiadavky stanovené v článku 23 ods. 1 až 6 tejto smernice.

3. Komisia do 17. júla 2023 poskytne usmernenia na objasnenie uplatňovania odsekov 1 a 2. Komisia uvedené usmernenia pravidelne prehodnocuje. Pri príprave uvedených usmernení Komisia zohľadňuje všetky pripomienky skupiny pre spoluprácu a agentúry ENISA.

Článok 5

Minimálna harmonizácia

Táto smernica nebráni členským štátom, aby prijali alebo ponechali v platnosti ustanovenia na zaistenie vyššej úrovne kybernetickej bezpečnosti, ak nie sú takéto ustanovenia v rozpore s povinnosťami členských štátov stanovenými v práve Únie.

Článok 6

Vymedzenie pojmov

Na účely tejto smernice sa uplatňuje toto vymedzenie pojmov:

▼B

1. „sieť a informačný systém“ je:

   a) elektronická komunikačná sieť v zmysle vymedzenia v článku 2 bodu 1 smernice (EÚ) 2018/1972;

   b) každé zariadenie alebo skupina vzájomne prepojených alebo súvisiacich zariadení, z ktorých jedno alebo viaceré vykonávajú automatické spracúvanie digitálnych údajov na základe programu; alebo

   c) digitálne údaje, ktoré sa ukladajú, spracúvajú, získavajú alebo prenášajú prostredníctvom prvkov uvedených v písmenách a) a b) na účely ich prevádzkovania, používania, ochrany a udržiavania;

2. „bezpečnosť sietí a informačných systémov“ je schopnosť sietí a informačných systémov odolávať na určitom stupni spoľahlivosti akejkoľvek udalosti, ktorá môže ohroziť dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov;

3. „kybernetická bezpečnosť“ je kybernetická bezpečnosť v zmysle vymedzenia v článku 2 bode 1 nariadenia (EÚ) 2019/881;

4. „národná stratégia kybernetickej bezpečnosti “ je koherentný rámec členského štátu, v ktorom sa stanovujú strategické ciele a priority v oblasti kybernetickej bezpečnosti a systém správy na ich dosiahnutie v danom členskom štáte;

5. „udalosť odvrátená v poslednej chvíli“ je udalosť, ktorá by mohla ohroziť dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov, ale ktorej vzniku sa úspešne zabránilo alebo ku ktorej nedošlo;

6. „incident“ je udalosť ohrozujúca dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo služieb poskytovaných alebo prístupných prostredníctvom sietí a informačných systémov;

7. „rozsiahly kybernetický incident“ je incident, ktorý spôsobí narušenie na úrovni presahujúcej schopnosť členského štátu naň reagovať alebo ktorý má významný vplyv aspoň na dva členské štáty;

8. „riešenie incidentov“ sú akékoľvek kroky a postupy zamerané na prevenciu, odhaľovanie, analýzu a obmedzovanie incidentov alebo na reakciu na incident a zotavenie z neho;

▼B

9. „riziko“ je potenciál straty alebo narušenia v dôsledku incidentu a má byť vyjadrené ako kombinácia rozsahu takejto straty alebo narušenia a pravdepodobnosti výskytu incidentu;

10. „kybernetická hrozba“ je kybernetická hrozba v zmysle vymedzenia v článku 2 bode 8 nariadenia (EÚ) 2019/881;

11. „významná kybernetická hrozba“ je kybernetická hrozba, o ktorej možno na základe jej technických charakteristík predpokladať, že má potenciál mať závažný vplyv na sieť a informačné systémy subjektu alebo používateľov služieb subjektu tým, že spôsobí značnú hmotnú alebo nehmotnú ujmu;

12. „produkt IKT“ je produkt IKT v zmysle vymedzenia v článku 2 bode 12 nariadenia (EÚ) 2019/881;

13. „služba IKT“ je služba IKT v zmysle vymedzenia v článku 2 bode 13 nariadenia (EÚ) 2019/881;

14. „proces IKT“ je proces v zmysle vymedzenia v článku 2 bode 14 nariadenia (EÚ) 2019/881;

15. „zraniteľnosť“ je slabá stránka, náchylnosť alebo chyba produktov IKT alebo služieb IKT, ktorá môže byť zneužitá kybernetickou hrozbou;

16. „norma“ je norma v zmysle vymedzenia v článku 2 bode 1 nariadenia Európskeho parlamentu a Rady (EÚ) č. 1025/2012 ([3]);

17. „technická špecifikácia“ je technická špecifikácia v zmysle vymedzenia v článku 2 bode 4 nariadenia (EÚ) č. 1025/2012;

18. „internetový prepojovací uzol“ je sieťové zariadenie, ktoré umožňuje prepojenie viac než dvoch nezávislých autonómnych sietí (autonómnych systémov) najmä na účely sprostredkovania internetového dátového toku, ktorý prepojuje len autonómne systémy a ktorý nevyžaduje, aby internetový dátový tok medzi ktoroukoľvek dvojicou zúčastnených autonómnych systémov prechádzal cez ľubovoľný tretí autonómny systém, takýto dátový tok menil alebo doň nejako nezasahoval;

19. „systém názvov domén“ alebo „DNS“ je hierarchický distribuovaný systém názvov, ktorý umožňuje identifikáciu internetových služieb a zdrojov a to, aby zariadenia koncových používateľov používali služby smerovania internetu a pripojenia na účely prístupu k týmto službám a zdrojom;

([3]) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 1025/2012 z 25. októbra 2012 o európskej normalizácii, ktorým sa menia a dopĺňajú smernice Rady 89/686/EHS a 93/15/EHS a smernice Európskeho parlamentu a Rady 94/9/ES, 94/25/ES, 95/16/ES, 97/23/ES, 98/34/ES, 2004/22/ES, 2007/23/ES, 2009/23/ES a 2009/105/ES a ktorým sa zrušuje rozhodnutie Rady 87/95/EHS a rozhodnutie Európskeho parlamentu a Rady č. 1673/2006/ES (Ú. v. EÚ L 316, 14.11.2012, s. 12).

▼B

20. „poskytovateľ služieb DNS“ je subjekt, ktorý poskytuje:

    a) verejne dostupné služby rekurzívneho rozlišovania názvov domén pre koncových používateľov internetu; alebo

    b) autoritatívne služby rozlišovania názvov domén pre použitie tretích strán s výnimkou koreňových názvových serverov;

21. „správca názvov domén najvyššej úrovne“ alebo „správca názvov TLD“ je subjekt, ktorému bola pridelená osobitná doména najvyššej úrovne (TLD) a ktorý je zodpovedný za správu TLD vrátane registrácie názvov domén v rámci TLD a za technickú prevádzku TLD vrátane prevádzky názvových serverov, údržby jeho databáz a distribúcie súborov zóny TLD v rámci názvových serverov bez ohľadu na to, či ktorúkoľvek z týchto operácií vykonáva subjekt sám alebo sa vykonáva externe, avšak s vylúčením situácií, kedy názvy TLD používa správca pre vlastnú potrebu;

22. „subjekt poskytujúci služby registrácie názvov domén“ je registrátor alebo zástupca konajúci v mene registrátorov, ako napríklad poskytovateľ alebo predajca služieb registrácie súkromia alebo proxy;

23. „digitálna služba“ je služba v zmysle vymedzenia v článku 1 ods. 1 písm. b) smernice Európskeho parlamentu a Rady (EÚ) 2015/1535 ([4]);

24. „dôveryhodná služba“ je dôveryhodná služba v zmysle vymedzenia v článku 3 bode 16 nariadenia (EÚ) č. 910/2014;

25. „poskytovateľ dôveryhodných služieb“ je poskytovateľ dôveryhodných služieb v zmysle vymedzenia v článku 3 bode 19 nariadenia (EÚ) č. 910/2014;

26. „kvalifikovaná dôveryhodná služba“ je kvalifikovaná dôveryhodná služba v zmysle vymedzenia v článku 3 bode 17 nariadenia (EÚ) č. 910/2014;

27. „poskytovateľ kvalifikovaných dôveryhodných služieb“ je poskytovateľ kvalifikovaných dôveryhodných služieb v zmysle vymedzenia v článku 3 bode 20 nariadenia (EÚ) č. 910/2014;

28. „online trhovisko“ je online trhovisko v zmysle vymedzenia v článku 2 písm. n) smernice Európskeho parlamentu a Rady 2005/29/ES ([5]);

29. „internetový vyhľadávač“ je internetový vyhľadávač v zmysle vymedzenia v článku 2 bodu 5 nariadenia Európskeho parlamentu a Rady (EÚ) 2019/1150 ([6]);

([4]) Smernica Európskeho parlamentu a Rady (EÚ) 2015/1535 z 9. septembra 2015, ktorou sa stanovuje postup pri poskytovaní informácií v oblasti technických predpisov a pravidiel vzťahujúcich sa na služby informačnej spoločnosti (Ú. v. EÚ L 241, 17.9.2015, s. 1).

([5]) Smernica Európskeho parlamentu a Rady 2005/29/ES z 11. mája 2005 o nekalých obchodných praktikách podnikateľov voči spotrebiteľom na vnútornom trhu, a ktorou sa mení a dopĺňa smernica Rady 84/450/EHS, smernice Európskeho parlamentu a Rady 97/7/ES, 98/27/ES a 2002/65/ES a nariadenie Európskeho parlamentu a Rady (ES) č. 2006/2004 („smernica o nekalých obchodných praktikách“) (Ú. v. EÚ L 149, 11.6.2005, s. 22).

([6]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/1150 z 20. júna 2019 o podpore spravodlivosti a transparentnosti pre komerčných používateľov online sprostredkovateľských služieb (Ú. v. EÚ L 186, 11.7.2019, s. 57).

▼B

30. „služba cloud computingu“ je digitálna služba, ktoré umožňuje správu na požiadanie a vzdialený širokopásmový prístup ku škálovateľnému a pružnému súboru zdieľateľných výpočtových zdrojov, a to aj ak sa tieto zdroje nachádzajú na viacerých miestach;

31. „služba dátového centra“ je služba, ktorá zahŕňa štruktúry alebo skupiny štruktúr vyhradené na centralizované umiestnenie, vzájomné prepojenie a prevádzku IT a sieťového vybavenia poskytujúcich služby ukladania, spracovania a prepravy dát spolu so všetkými zariadeniami a infraštruktúrami na distribúciu elektrickej energie a environmentálnu kontrolu;

32. „sieť na sprístupňovanie obsahu“ je sieť geograficky distribuovaných serverov na zabezpečenie vysokej dostupnosti, prístupnosti alebo rýchleho doručenia digitálneho obsahu a služieb používateľom internetu v mene poskytovateľov obsahu a služieb;

33. „platforma služieb sociálnej siete“ je platforma, ktorá koncovým používateľom umožňuje vzájomné prepojenie, zdieľanie, objavovanie a komunikáciu prostredníctvom viacerých zariadení, najmä prostredníctvom chatov, príspevkov, videí a odporúčaní;

34. „zástupca“ je fyzická alebo právnická osoba usadená v Únii, ktorá je výslovne určená konať v mene poskytovateľa služieb DNS, správcu názvov TLD, subjektu poskytujúceho služby registrácie názvov domén, poskytovateľa služieb cloud computingu, poskytovateľa služieb dátových centier, poskytovateľa siete na sprístupňovanie obsahu, poskytovateľa riadených služieb, poskytovateľa riadených bezpečnostných služieb, alebo poskytovateľa online trhoviska, internetového vyhľadávača alebo platformy služieb sociálnych sietí, ktorí nie sú usadení v Únii, a na ktorú sa príslušný orgán alebo jednotka CSIRT môžu obracať namiesto subjektu v súvislosti s jeho povinnosťami podľa tejto smernice;

35. „subjekt verejnej správy“ je subjekt, ktorý je ako taký uznaný v členskom štáte v súlade s vnútroštátnym právom, okrem súdnictva, parlamentov a centrálnych bánk, a ktorý spĺňa tieto kritériá:

    a) je zriadený na účely plnenia potrieb všeobecného záujmu a nemá priemyselný ani komerčný charakter;

    b) má právnu subjektivitu alebo je zo zákona oprávnený konať v mene iného subjektu s právnou subjektivitou;

    c) je financovaný prevažne štátnymi, regionálnymi alebo inými verejnoprávnymi orgánmi, podlieha dohľadu týchto inštitúcií alebo orgánov nad svojím riadením alebo v správnom, riadiacom alebo dozornom orgáne má viac ako polovicu členov menovaných štátnymi alebo regionálnymi orgánmi alebo inými verejnoprávnymi inštitúciami;

    d) má právomoc vydávať fyzickým alebo právnickým osobám správne alebo regulačné rozhodnutia, ktoré majú vplyv na ich práva pri cezhraničnom pohybe osôb, tovarov, služieb alebo kapitálu;

▼B

36. „verejná elektronická komunikačná sieť“ je verejná elektronická komunikačná sieť v zmysle vymedzenia v článku 2 bode 8 smernice (EÚ) 2018/1972;

37. „elektronická komunikačná služba“ je elektronická komunikačná služba v zmysle vymedzenia v článku 2 bode 4 smernice (EÚ) 2018/1972;

38. „subjekt“ je fyzická alebo právnická osoba zriadená a uznaná ako taká podľa vnútroštátneho práva v mieste svojho sídla, ktorá môže vo vlastnom mene vykonávať práva a podliehať povinnostiam;

39. „poskytovateľ riadených služieb“ je subjekt, ktorý poskytuje služby súvisiace s inštaláciou, správou, prevádzkou alebo údržbou produktov IKT, sietí, infraštruktúry, aplikácií alebo akýchkoľvek iných sietí a informačných systémov formou pomoci alebo aktívnej správy vykonávanej buď v priestoroch zákazníka alebo na diaľku;

40. „poskytovateľ riadených bezpečnostných služieb“ je poskytovateľ riadených služieb, ktorý vykonáva alebo poskytuje pomoc pre činnosti súvisiace s riadením kybernetických rizík;

41. „výskumná organizácia“ je subjekt, ktorého hlavným cieľom je vykonávať aplikovaný výskum alebo experimentálny vývoj s cieľom využiť výsledky tohto výskumu na komerčné účely, ktorého súčasťou však nie sú vzdelávacie inštitúcie.

KAPITOLA II

KOORDINOVANÉ RÁMCE KYBERNETICKEJ BEZPEČNOSTI

Článok 7

Národná stratégia kybernetickej bezpečnosti

1. Každý členský štát prijme národnú stratégiu kybernetickej bezpečnosti, v ktorej stanoví strategické ciele, zdroje potrebné na dosiahnutie týchto cieľov a vhodné politické a regulačné opatrenia na dosiahnutie a zachovanie vysokej úrovne kybernetickej bezpečnosti. Národná stratégia kybernetickej bezpečnosti sietí obsahuje:

a) ciele a priority stratégie kybernetickej bezpečnosti členského štátu najmä pre odvetvia uvedené v prílohách I a II;

b) rámec riadenia na dosiahnutie cieľov a priorít uvedených v písmene a) tohto odseku vrátane politík uvedených v odseku 2;

c) rámec riadenia na objasnenie úloh a povinností relevantných zainteresovaných strán na vnútroštátnej úrovni, ktorý je základom spolupráce a koordinácie na vnútroštátnej úrovni medzi príslušnými orgánmi, jednotnými kontaktnými miestami a jednotkami CSIRT podľa tejto smernice, ako aj koordináciu a spoluprácu medzi uvedenými orgánmi a príslušnými orgánmi podľa odvetvových právnych aktov Únie;

▼B

d) mechanizmus na identifikáciu relevantných prostriedkov a hodnotenie rizík v danom členskom štáte;

e) identifikáciu opatrení na zabezpečenie pripravenosti a schopnosti reakcie na incidenty a zotavenia z nich vrátane spolupráce medzi verejným a súkromným sektorom;

f) zoznam rôznych orgánov a zainteresovaných strán zapojených do vykonávania národnej stratégie kybernetickej bezpečnosti;

g) politický rámec pre posilnenú koordináciu medzi príslušnými orgánmi podľa tejto smernice a príslušnými orgánmi podľa smernice (EÚ) 2022/2557 za účelom výmeny informácií o rizikách, kybernetických hrozbách a incidentoch, ako aj o nekybernetických rizikách, hrozbách a incidentoch, prípadne pri plnení úloh dohľadu;

h) plán vrátane potrebných opatrení na zvýšenie všeobecnej úrovne informovanosti občanov o kybernetickej bezpečnosti.

2. Členské štáty v rámci národnej stratégie kybernetickej bezpečnosti prijmú najmä politiky:

a) so zameraním na kybernetickú bezpečnosť v dodávateľskom reťazci produktov IKT a služieb IKT, ktoré subjekty používajú na poskytovanie svojich služieb;

b) týkajúce sa zahrnutia a špecifikácie požiadaviek na kybernetickú bezpečnosť produktov IKT a služieb IKT vo verejnom obstarávaní, a to aj pokiaľ ide o certifikáciu kybernetickej bezpečnosti, šifrovanie a využívanie produktov kybernetickej bezpečnosti s otvoreným zdrojovým kódom;

c) riadenia zraniteľností vrátane podpory a sprostredkovania koordinovaného zverejňovania zraniteľností podľa článku 12 ods. 1;

d) v súvislosti s udržiavaním všeobecnej dostupnosti, integrity a dôvernosti verejného jadra otvoreného internetu, v relevantnom prípade vrátane kybernetickej bezpečnosti podmorských komunikačných káblov;

e) na podporu vývoja a integrácie relevantných pokročilých technológií so zámerom implementovať najmodernejšie opatrenia na riadenie rizík kybernetickej bezpečnosti;

f) na podporu a rozvoj vzdelávania a odbornej prípravy v oblasti kybernetickej bezpečnosti, kvalifikácií v oblasti kybernetickej bezpečnosti, zvyšovania informovanosti a výskumných a vývojových iniciatív v oblasti kybernetickej bezpečnosti, ako aj usmernenia o správnych postupoch a kontrolách kybernetickej hygieny, zamerané na občanov, zainteresované strany a subjekty;

g) na podporu akademických a výskumných inštitúcií pri vývoji, zlepšovaní a zavádzaní nástrojov kybernetickej bezpečnosti a bezpečnej sieťovej infraštruktúry;

▼B

h) vrátane príslušných postupov a vhodných nástrojov zdieľania informácií na podporu dobrovoľného zdieľania informácií o kybernetickej bezpečnosti medzi subjektmi v súlade s právom Únie;

i) na posilnenie kybernetickej odolnosti a základnej kybernetickej hygieny malých a stredných podnikov, najmä podnikov vyňatých z pôsobnosti tejto smernice, poskytovaním ľahko dostupných usmernení a pomoci pre ich špecifické potreby;

j) na podporu aktívnej kybernetickej ochrany.

3. Členské štáty oznámia Komisii svoje národné stratégie kybernetickej bezpečnosti do troch mesiacov od ich prijatia. Členské štáty môžu z takýchto oznámení vylúčiť informácie, ktoré sa týkajú ich národnej bezpečnosti.

4. Členské štáty pravidelne a aspoň každých päť rokov hodnotia svoje národné stratégie kybernetickej bezpečnosti na základe kľúčových ukazovateľov výkonnosti a v prípade potreby ich aktualizujú. Agentúra ENISA pomáha členským štátom na ich žiadosť pri vývoji alebo aktualizácii národnej stratégie kybernetickej bezpečnosti a kľúčových ukazovateľov výkonnosti na posúdenie tejto stratégie s cieľom zosúladiť ju s požiadavkami a povinnosťami stanovenými v tejto smernici.

Článok 8

Príslušné orgány a miesta jednotného kontaktu

1. Každý členský štát určí jeden alebo zriadi jeden alebo viacero príslušných orgánov zodpovedných za kybernetickú bezpečnosť a za úlohy dohľadu uvedené v kapitole VII (príslušné orgány).

2. Príslušné orgány uvedené v odseku 1 monitorujú implementáciu tejto smernice na vnútroštátnej úrovni.

3. Každý členský štát určí alebo zriadi miesto jednotného kontaktu. Ak členský štát určí alebo zriadi iba jeden príslušný orgán podľa odseku 1, uvedený príslušný orgán je aj jednotným kontaktným miestom v danom členskom štáte.

4. Každé jednotné kontaktné miesto vykonáva styčnú funkciu s cieľom zabezpečiť cezhraničnú spoluprácu orgánov daného členského štátu s príslušnými orgánmi iných členských štátov a v prípade potreby s Komisiou a agentúrou ENISA, ako aj s cieľom zabezpečiť medziodvetvovú spoluprácu s inými príslušnými orgánmi v rámci daného členského štátu.

5. Členské štáty zabezpečia, aby ich príslušné orgány a jednotné kontaktné miesta mali primerané zdroje na účinné a efektívne vykonávanie zverených úloh, a teda na plnenie cieľov tejto smernice.

6. Každý členský štát bez zbytočného odkladu informuje Komisiu o identite príslušného orgánu uvedeného v odseku 1 a jednotného kontaktného miesta uvedeného v odseku 3, o úlohách uvedených orgánov a o všetkých ich následných zmenách. Každý členský štát totožnosť svojho príslušného orgánu zverejní. Komisia zostaví verejne dostupný zoznam jednotných kontaktných miest.

▼B

Článok 9

Národné rámce pre riadenie kybernetických kríz

1. Každý členský štát určí alebo zriadi jeden alebo viac príslušných orgánov zodpovedných za riadenie rozsiahlych kybernetických incidentov a kríz (orgány pre riadenie kybernetických kríz). Členské štáty zabezpečujú, aby uvedené orgány mali primerané zdroje na účinný a efektívny výkon zverených úloh. Súlad s platnými rámcami pre všeobecné vnútroštátne krízové riadenie zabezpečujú členské štáty.

2. Ak členský štát určí alebo zriadi viac ako jeden orgán pre riadenie kybernetických kríz podľa odseku 1, jasne uvedie, ktorý z týchto príslušných orgánov má slúžiť ako koordinátor riadenia rozsiahlych kybernetických incidentov a kríz.

3. Každý členský štát určí spôsobilosti, aktíva a postupy, ktoré možno použiť na účely tejto smernice v prípade krízy.

4. Každý členský štát prijme národný plán reakcie na rozsiahle kybernetické incidenty a krízy, v ktorom sa stanovia ciele a spôsoby riadenia rozsiahlych kybernetických incidentov a kríz. V uvedenom pláne sa stanovia najmä:

a) ciele vnútroštátnych opatrení a činností v oblasti pripravenosti;

b) úlohy a povinnosti orgánov pre riadenie kybernetických kríz;

c) postupy riadenia kybernetických kríz vrátane ich začlenenia do všeobecného vnútroštátneho rámca krízového riadenia a kanálov na výmenu informácií;

d) vnútroštátne opatrenia v oblasti pripravenosti vrátane cvičení a činností odbornej prípravy;

e) príslušné verejné a súkromné zainteresované strany a potrebná infraštruktúra;

f) vnútroštátne postupy a dojednania medzi príslušnými vnútroštátnymi orgánmi a inštitúciami s cieľom zabezpečiť účinnú účasť členského štátu na koordinovanom riadení rozsiahlych kybernetických incidentov a kríz na úrovni Únie, ako aj jeho podporu tohto riadenia.

5. Do troch mesiacov od určenia alebo zriadenia orgánu pre riadenie kybernetických kríz uvedeného v odseku 1 informuje každý členský štát Komisiu o totožnosti svojho orgánu a o všetkých jeho následných zmenách. Členské štáty zasielajú Komisii a Európskej sieti kontaktných organizácií pre kybernetickú krízu (EU-CyCLONe) relevantné informácie v súvislosti s požiadavkami odseku 4 o svojich vnútroštátnych plánoch reakcie na rozsiahle kybernetické incidenty a krízy do troch mesiacov od prijatia uvedených plánov. Členské štáty môžu vylúčiť informácie v prípade a v rozsahu, v akom je takéto vylúčenie potrebné pre ich národnú bezpečnosť.

▼B

Článok 10

Jednotky pre riešenie počítačových bezpečnostných incidentov (jednotky CSIRT)

1. Každý členský štát určí alebo zriadi jednu alebo viacero jednotiek CSIRT. Jednotky CSIRT možno určiť alebo zriadiť v rámci príslušného orgánu. Jednotky CSIRT sú povinné spĺňať požiadavky stanovené v článku 11 ods. 1, pokrývať aspoň odvetvia, pododvetvia alebo druhy subjektov uvedených v prílohách I a II a zodpovedajú za riešenie incidentov podľa presne stanoveného postupu.

2. Členské štáty zabezpečia, aby každá jednotka CSIRT mala primerané zdroje na účinné plnenie svojich úloh stanovených v článku 11 ods. 3.

3. Členské štáty zabezpečia, aby každá jednotka CSIRT mala k dispozícii vhodnú, bezpečnú a odolnú komunikačnú a informačnú infraštruktúru na výmenu informácií s kľúčovými a dôležitými subjektmi a ďalšími relevantnými zainteresovanými stranami. Členské štáty na uvedený účel zabezpečia, aby každá jednotka CSIRT prispievala k zavádzaniu bezpečných nástrojov na výmenu informácií.

4. Jednotky CSIRT spolupracujú a v prípade potreby si vymieňajú relevantné informácie v súlade s článkom 29 s odvetvovými alebo medziodvetvovými komunitami kľúčových a dôležitých subjektov.

5. Jednotky CSIRT sa zúčastňujú na partnerských preskúmaniach organizovaných podľa článku 19.

6. Členské štáty zabezpečia účinnú, efektívnu a bezpečnú spoluprácu svojich jednotiek CSIRT v sieti jednotiek CSIRT.

7. Jednotky CSIRT môžu nadväzovať spoluprácu s národnými jednotkami reakcie na počítačové bezpečnostné incidenty tretích krajín. Ako súčasť takýchto vzťahov spolupráce členské štáty sprostredkujú účinnú, efektívnu a bezpečnú výmenu informácií s uvedenými národnými jednotkami reakcie na počítačové bezpečnostné incidenty z tretích krajín, pričom použijú relevantné protokoly na výmenu informácií vrátane semaforového protokolu. Jednotky CSIRT si môžu vymieňať relevantné informácie s národnými jednotkami reakcie na počítačové bezpečnostné incidenty tretích krajín vrátane osobných údajov v súlade s právom Únie v oblasti ochrany údajov.

8. Jednotky CSIRT môžu spolupracovať s národnými jednotkami reakcie na počítačové bezpečnostné incidenty tretích krajín alebo rovnocennými orgánmi tretích krajín najmä na účely poskytovania pomoci v oblasti kybernetickej bezpečnosti.

9. Každý členský štát bez zbytočného odkladu informuje Komisiu o identite jednotky CSIRT uvedenej v odseku 1 tohto článku a jednotky CSIRT určenej za koordinátora podľa článku 12 ods. 1, o úlohách uvedených orgánov v súvislosti s kľúčovými a dôležitými subjektmi a o všetkých následných zmenách.

10. Členské štáty môžu pri zriaďovaní svojich jednotiek CSIRT požiadať o pomoc agentúru ENISA.

▼B

Článok 11

Požiadavky na jednotky CSIRT a ich technické spôsobilosti a úlohy

1. Jednotky CSIRT sú povinné spĺňať tieto požiadavky:

a) zabezpečovať vysokú úroveň dostupnosti svojich komunikačných kanálov prevenciou jediných bodov zlyhania a mať k dispozícii niekoľko spôsobov, ktorými ich možno kedykoľvek kontaktovať a ktorými môžu tieto jednotky kontaktovať iných; jasne špecifikovať komunikačné kanály a oboznámiť s nimi zainteresované strany a spolupracujúcich partnerov;

b) mať svoje pracoviská a podporné informačné systémy umiestnené na zabezpečených miestach;

c) byť vybavené vhodným systémom riadenia a smerovania žiadostí, najmä na sprostredkovanie ich účinného a efektívneho odovzdávania;

d) zabezpečovať dôvernosť a dôveryhodnosť svojich operácií;

e) byť primerane personálne vybavené na zabezpečenie stálej dostupnosti svojich služieb a zabezpečovať patričnú odbornú prípravu pre svojich zamestnancov;

f) byť vybavené redundantnými systémami a záložným pracovným priestorom na zabezpečenie kontinuity svojich služieb.

Jednotky CSIRT môžu byť zapojené do sietí medzinárodnej spolupráce.

2. Členské štáty zabezpečia, aby ich jednotky CSIRT spoločne mali technické spôsobilosti potrebné na výkon úloh uvedených v odseku 3. Aby jednotky CSIRT mohli rozvíjať svoje technické spôsobilosti, členské štáty zabezpečia prídel dostatočných zdrojov pre svoje jednotky CSIRT na zaistenie primeraného počtu zamestnancov.

3. Jednotky CSIRT plnia tieto úlohy:

a) monitorujú a analyzujú kybernetické hrozby, zraniteľnosti a incidenty na vnútroštátnej úrovni a na požiadanie poskytujú pomoc dotknutým kľúčovým a dôležitým subjektom s ohľadom na monitorovanie ich sietí a informačných systémov v reálnom alebo takmer v reálnom čase;

b) zasielajú včasné varovania, výstrahy a oznámenia a šíria informácie o kybernetických hrozbách, zraniteľnostiach a incidentoch dotknutým kľúčovým a dôležitým subjektom, ako aj príslušným orgánom a ďalším relevantným zainteresovaným stranám pokiaľ možno takmer v reálnom čase;

c) podľa potreby reagujú na incidenty a poskytujú pomoc dotknutým kľúčovým a dôležitým subjektom;

▼B

d) zhromažďujú a analyzujú forenzné údaje a poskytujú dynamickú analýzu rizík a incidentov a informácie o situácii v kybernetickej bezpečnosti;

e) na žiadosť kľúčového alebo dôležitého subjektu umožňujú aktívne skenovanie siete a informačných systémov dotknutého subjektu s cieľom odhaľovať zraniteľnosti s potenciálnym významným dosahom;

f) účasť v sieti jednotiek CSIRT a poskytovanie vzájomnej pomoci podľa svojich kapacít a kompetencií ostatným členom siete jednotiek CSIRT na ich žiadosť;

g) v prípade potreby pôsobia ako koordinátor na účely koordinovaného zverejňovania zraniteľností podľa článku 12 ods. 1;

h) prispievajú k zavádzaniu bezpečných nástrojov na výmenu informácií podľa článku 10 ods. 3.

Jednotky CSIRT môžu vykonávať aktívne nerušivé skenovanie verejne prístupných sietí a informačných systémov kľúčových a dôležitých subjektov. Takéto skenovanie sa vykonáva s cieľom odhaliť zraniteľné alebo nezabezpečene nakonfigurované siete a informačné systémy a informovať dotknuté subjekty. Takéto skenovanie nesmie mať negatívny vplyv na fungovanie služieb subjektov.

Pri výkone úloh uvedených v prvom pododseku môžu jednotky CSIRT uprednostňovať konkrétne úlohy na základe prístupu založeného na rizikách.

4. Jednotky CSIRT nadviažu spoluprácu s príslušnými zainteresovanými stranami v súkromnom sektore s cieľom dosiahnuť ciele tejto smernice.

5. Jednotky CSIRT v záujme sprostredkovania spolupráce uvedenej v odseku 4 podporujú prijímanie a využívanie spoločných alebo normalizovaných postupov, režimov utajenia a taxonómie v súvislosti s:

a) postupmi riešenia incidentov;

b) krízovým riadením; a

c) koordinovaným zverejňovaním zraniteľností podľa článku 12 ods. 1.

Článok 12

Koordinované zverejňovanie zraniteľností a európska databáza zraniteľností

1. Na účely koordinovaného zverejňovania zraniteľností určí každý členský štát jednu zo svojich jednotiek CSIRT za koordinátora. Jednotka CSIRT určená za koordinátora koná ako dôveryhodný sprostredkovateľ, ktorý v prípade potreby sprostredkuje interakciu medzi fyzickou alebo právnickou osobou, ktorá na žiadosť niektorej zo strán oznamuje zraniteľnosť a výrobcom alebo poskytovateľom potenciálne zraniteľných produktov IKT alebo služieb IKT. K úlohám jednotky CSIRT určenej za koordinátora patrí:

▼B

a) identifikácia a kontaktovanie dotknutých subjektov;

b) pomoc fyzickým alebo právnickým osobám oznamujúcim zraniteľnosti a

c) vyjednávanie harmonogramu zverejňovania a riadenie zraniteľností, ktoré majú dosah na viaceré subjekty.

Členské štáty zabezpečia, aby fyzické alebo právnické osoby mohli na požiadanie nahlásiť zraniteľnosť jednotke CSIRT určenej za koordinátora anonymne. Jednotka CSIRT určená za koordinátora zabezpečí v súvislosti s oznámenou zraniteľnosťou vykonanie dôsledných následných opatrení a zabezpečí anonymitu fyzickej alebo právnickej osoby, ktorá túto zraniteľnosť oznámila. Ak by oznámená zraniteľnosť mohla by mať významný vplyv na subjekty vo viac ako jednom členskom štáte, jednotka CSIRT každého dotknutého členského štátu určená za koordinátora v prípade potreby spolupracuje s inými jednotkami CSIRT určenými za koordinátorov v rámci siete jednotiek CSIRT.

2. Po porade so skupinou pre spoluprácu agentúra ENISA vytvorí a vedie európsku databázu zraniteľností. Na uvedený účel agentúra ENISA zriaďuje a udržiava vhodné informačné systémy, politiky a postupy a prijíma nevyhnutné technické a organizačné opatrenia na zaistenie bezpečnosti a integrity európskej databázy zraniteľností, aby subjektom, bez ohľadu na to či patria do rozsahu pôsobnosti tejto smernice, a ich dodávateľom sietí a informačných systémov umožnila najmä dobrovoľne zverejňovať a do registra zaraďovať verejne známe zraniteľnosti produktov IKT alebo služieb IKT. Prístup k informáciám o zraniteľnostiach v európskej databáze zraniteľností sa poskytuje všetkým zainteresovaným stranám. Uvedená databáza obsahuje:

a) informácie s opisom zraniteľností;

b) zasiahnuté produkty IKT alebo služby IKT a závažnosť zraniteľnosti z hľadiska okolností, za ktorých ju možno zneužiť;

c) dostupnosť súvisiacich záplat a v prípade absencie dostupných záplat usmernenia poskytnuté príslušnými orgánmi alebo jednotkami CSIRT určené používateľom zraniteľných produktov IKT a služieb IKT o tom, ako možno zmierniť riziká vyplývajúce zo zverejnených zraniteľností.

Článok 13

Spolupráca na vnútroštátnej úrovni

1. Ak sú príslušné orgány, jednotné kontaktné miesto a jednotky CSIRT jedného členského štátu samostatnými subjektmi, pri plnení povinností stanovených v tejto smernici navzájom spolupracujú.

▼B

2. Členské štáty zabezpečia, aby ich jednotky CSIRT, prípadne ich príslušné orgány dostávali oznámenia o významných incidentoch podľa článku 23 a o incidentoch, kybernetických hrozbách a udalostiach odvrátených v poslednej chvíli podľa článku 30.

3. Členské štáty zabezpečia, aby ich jednotky CSIRT, prípadne príslušné orgány poskytovali ich jednotným kontaktným miestam hlásenia o incidentoch, kybernetických hrozbách a udalostiach odvrátených v poslednej chvíli zasielané podľa tejto smernice.

4. S cieľom zabezpečiť, aby sa úlohy a povinnosti príslušných orgánov, jednotných kontaktných miest a jednotiek CSIRT vykonávali efektívne, členské štáty v rámci možností zabezpečia primeranú spoluprácu medzi uvedenými orgánmi a orgánmi presadzovania práva, orgánmi na ochranu údajov, vnútroštátnymi orgánmi podľa nariadení (ES) č. 300/2008 a (EÚ) 2018/1139, dozornými orgánmi podľa nariadenia (EÚ) č. 910/2014, príslušnými orgánmi podľa nariadenia (EÚ) 2022/2554, národnými regulačnými orgánmi podľa smernice (EÚ) 2018/1972, príslušnými orgánmi podľa smernice (EÚ) 2022/2557, ako aj príslušnými orgánmi podľa iných odvetvových právnych aktov Únie v danom členskom štáte.

5. Členské štáty zabezpečia, aby ich príslušné orgány podľa tejto smernice a ich príslušné orgány podľa smernice (EÚ) 2022/2557 pravidelne spolupracovali a vymieňali si informácie, pokiaľ ide o identifikáciu kritických subjektov, o rizikách, kybernetických hrozbách a incidentoch, ako aj o nekybernetických rizikách, hrozbách a incidentoch s dosahom na kľúčové subjekty označené ako kritické podľa smernice (EÚ) 2022/2557 a o opatreniach prijatých v reakcii na takéto riziká, hrozby a incidenty. Členské štáty tiež zabezpečia, aby si ich príslušné orgány podľa tejto smernice a ich príslušné orgány podľa nariadenia (EÚ) č. 910/2014, nariadenia (EÚ) 2022/2554 a smernice (EÚ) 2018/1972 pravidelne vymieňali relevantné informácie, a to aj o relevantných incidentoch a kybernetických hrozbách.

6. Pre oznamovanie uvedené v článkoch 23 a 30 zjednodušia členské štáty oznamovanie technickými prostriedkami.

KAPITOLA III

SPOLUPRÁCA NA ÚROVNI ÚNIE A NA MEDZINÁRODNEJ ÚROVNI

Článok 14

Skupina pre spoluprácu

1. S cieľom podporiť a sprostredkovať strategickú spoluprácu a výmenu informácií medzi členskými štátmi, ako aj posilniť vzájomnú dôveru, sa zriaďuje skupina pre spoluprácu.

2. Skupina pre spoluprácu vykonáva svoje úlohy na základe dvojročných pracovných programov uvedených v odseku 7.

▼B

3. Skupinu pre spoluprácu tvoria zástupcovia členských štátov, Komisie a agentúry ENISA. Na činnostiach skupiny pre spoluprácu sa ako pozorovateľ zúčastňuje Európska služba pre vonkajšiu činnosť. Európske orgány dohľadu (ESA) a príslušné orgány podľa nariadenia (EÚ) 2022/2554 sa môžu zúčastňovať na činnostiach skupiny pre spoluprácu v súlade s článkom 47 ods. 1 uvedeného nariadenia.

Podľa potreby môže skupina pre spoluprácu prizvať k práci Európsky parlament a zástupcov príslušných zainteresovaných strán.

Sekretariát zabezpečuje Komisia.

4. Skupina pre spoluprácu plní tieto úlohy:

a) poskytuje usmernenia príslušným orgánom v súvislosti s transpozíciou a vykonávaním tejto smernice;

b) poskytuje usmernenia príslušným orgánom v súvislosti s prípravou a implementáciou politík koordinovaného zverejňovania zraniteľností, ako sa uvádza v článku 7 ods. 2 písm. c);

c) vymieňa si najlepšie postupy a informácie v súvislosti s implementáciou tejto smernice, a to aj o kybernetických hrozbách, incidentoch, zraniteľnostiach, udalostiach odvrátených v poslednej chvíli, iniciatívy na zvyšovanie informovanosti, odbornú prípravu, cvičenia a kvalifikácie, budovanie kapacít, normy a technické špecifikácie, ako aj identifikáciu kľúčových a dôležitých subjektov podľa článku 2 ods. 2 písm. b) až e);

d) vymieňa si rady a spolupracuje s Komisiou v súvislosti s novými politickými iniciatívami pre kybernetickú bezpečnosť a celkovou konzistentnosťou odvetvových požiadaviek na kybernetickú bezpečnosť;

e) vymieňa si rady a spolupracuje s Komisiou v súvislosti s návrhom delegovaných alebo vykonávacích aktov prijímaných podľa tejto smernice;

f) vymieňa si najlepšie postupy a informácie s relevantnými inštitúciami, orgánmi, úradmi a agentúrami Únie;

g) vymieňa si názory na implementáciu odvetvových právnych aktov Únie, ktoré obsahujú ustanovenia o kybernetickej bezpečnosti;

h) v prípade potreby rokuje o správach o partnerskom hodnotení uvedenom v článku 19 ods. 9 a pripravuje závery a odporúčania;

i) vykonáva koordinované hodnotenia bezpečnostných rizík kritických dodávateľských reťazcov v súlade s článkom 22 ods. 1;

▼B

j) rokuje o prípadoch vzájomnej pomoci vrátane skúseností a výsledkov z cezhraničných spoločných opatrení dohľadu uvedených v článku 37;

k) na žiadosť jedného alebo viacerých dotknutých členských štátov rokuje o konkrétnych žiadostiach o vzájomnú pomoc podľa článku 37;

l) poskytuje strategické usmernenia pre sieť jednotiek CSIRT a EU-CyCLONe v otázkach konkrétnych vznikajúcich problémov;

m) vymieňa si názory na politiku nadväzných opatrení po rozsiahlych kybernetických incidentoch a krízach na základe skúseností siete jednotiek CSIRT a EU-CyCLONe;

n) prispieva k spôsobilostiam kybernetickej bezpečnosti v celej Únii sprostredkovaním výmen vnútroštátnych úradníkov prostredníctvom programu budovania kapacít, do ktorého sú zapojení zamestnanci príslušných orgánov alebo jednotiek CSIRT;

o) organizuje pravidelné spoločné stretnutia s príslušnými súkromnými zainteresovanými stranami z celej Únie s cieľom rokovať o činnostiach skupiny a zhromažďovať informácie o nových politických výzvach;

p) rokuje o práci vykonanej v súvislosti s cvičeniami kybernetickej bezpečnosti, ako aj o práci agentúry ENISA;

q) stanovuje metodiku a organizačné aspekty partnerských preskúmaní uvedených v článku 19 ods. 1, ako aj stanovuje metodiku sebahodnotenia pre členské štáty v súlade s článkom 19 ods. 5 za pomoci Komisie a agentúry ENISA a v spolupráci s Komisiou a agentúrou ENISA vypracovať kódexy správania, ktoré budú základom pracovných metód určených expertov na kybernetickú bezpečnosť v súlade s článkom 19 ods. 6;

r) vyhotovuje správy o skúsenostiach získaných na strategickej úrovni a z partnerských preskúmaní na účely preskúmania uvedeného v článku 40;

s) pravidelne vedie diskusiu o súčasnom stave kybernetických hrozieb alebo incidentov, ako je ransomvér, a vykonávať jeho hodnotenie.

Skupina pre spoluprácu predkladá správy uvedené v prvom pododseku písm. r) Komisii, Európskemu parlamentu a Rade.

5. Členské štáty zabezpečia účinnú, efektívnu a bezpečnú spoluprácu svojich zástupcov v rámci skupiny pre spoluprácu.

6. Skupina pre spoluprácu môže od siete jednotiek CSIRT požadovať technickú správu na vybrané témy.

7. Skupina pre spoluprácu do 1. februára 2024 a potom každé dva roky zostaví pracovný program týkajúci sa činností, ktoré sa majú uskutočniť v rámci dosahovania jej cieľov a úloh.

▼B

8. Komisia môže prijať vykonávacie akty stanovujúce procesné opatrenia potrebné na fungovanie skupiny pre spoluprácu.

Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 39 ods. 2.

Pokiaľ ide o návrhy vykonávacích aktov uvedených v prvom pododseku tohto odseku, Komisia sa radí a spolupracuje so skupinou pre spoluprácu v súlade s odsekom 4 písm. e).

9. Skupina pre spoluprácu sa pravidelne a v každom prípade aspoň raz ročne stretáva so skupinou pre odolnosť kritických subjektov zriadenou podľa smernice (EÚ) 2022/2557 s cieľom podporovať a sprostredkovať strategickú spoluprácu a výmenu informácií.

Článok 15

Sieť jednotiek CSIRT

1. S cieľom prispieť k zvyšovaniu dôvery a podporiť rýchlu a účinnú operačnú spoluprácu medzi členskými štátmi sa zriaďuje sieť národných jednotiek CSIRT.

2. Sieť jednotiek CSIRT sa skladá zo zástupcov jednotiek CSIRT určených alebo zriadených podľa článku 10 a tímu reakcie na núdzové počítačové situácie v inštitúciách, orgánoch a agentúrach Únie (CERT-EU). Komisia sa zúčastňuje na práci siete jednotiek CSIRT ako pozorovateľ. Agentúra ENISA zabezpečuje sekretariát a aktívne pomáha so spoluprácou medzi jednotkami CSIRT.

3. Sieť jednotiek CSIRT plní tieto úlohy:

a) výmena informácií o spôsobilostiach jednotiek CSIRT;

b) sprostredkovanie spoločného používania, transferu a výmeny technológií a príslušných opatrení, politík, nástrojov, procesov, najlepších postupov a rámcov medzi jednotkami CSIRT;

c) výmena relevantných informácií o incidentoch, udalostiach odvrátených v poslednej chvíli, kybernetických hrozbách, rizikách a zraniteľnostiach;

d) výmena informácií v súvislosti s publikáciami a odporúčaniami o kybernetickej bezpečnosti;

e) zabezpečovanie interoperability, pokiaľ ide o špecifikácie a protokoly výmeny informácií;

f) na žiadosť člena siete jednotiek CSIRT potenciálne zasiahnutej incidentom výmena a prediskutovanie informácií o danom incidente a súvisiacich kybernetických hrozbách, rizikách a zraniteľnostiach;

g) na žiadosť člena siete jednotiek CSIRT prediskutovanie a v rámci možností vykonanie koordinovanej reakcie na incident, ktorý bol identifikovaný v oblasti patriacej do právomoci daného členského štátu;

▼B

h) poskytovanie pomoci členským štátom pri riešení cezhraničných incidentov podľa tejto smernice;

i) spolupráca, výmena najlepších postupov a poskytovanie pomoci jednotkám CSIRT určeným za koordinátorov podľa článku 12 ods. 1, pokiaľ ide o riadenie koordinovaného zverejňovania informácií o zraniteľnostiach, ktoré by mohli mať významný dosah na subjekty vo viac ako jednom členskom štáte;

j) prediskutovanie a určovanie ďalších foriem operačnej spolupráce, a to aj v súvislosti:

   i) s kategóriami kybernetických hrozieb a incidentov;

   ii) so včasnými varovaniami;

   iii) so vzájomnou pomocou;

   iv) so zásadami a dojednaniami koordinácie pri reakcii na cezhraničné riziká a incidenty;

   v) na žiadosť členského štátu s príspevkom k národnému plánu reakcie na rozsiahle kybernetické incidenty a krízy uvedeného v článku 9 ods. 4;

k) informovanie skupiny pre spoluprácu o svojej činnosti a o ďalších formách operačnej spolupráce prediskutovaných podľa písmena j) a v prípade potreby požadovanie usmernení v tomto ohľade;

l) bilancia kybernetických bezpečnostných cvičení vrátane cvičení organizovaných agentúrou ENISA;

m) na žiadosť niektorej jednotky CSIRT prediskutovanie spôsobilostí a pripravenosti tejto jednotky CSIRT;

n) spolupráca a výmena informácií s regionálnymi a únijnými centrami bezpečnostných operácií (SOC) s cieľom zlepšiť spoločné situačné povedomie o incidentoch a kybernetických hrozbách v celej Únii;

o) v príslušných prípadoch prediskutovanie správ o partnerskom preskúmaní uvedených v článku 19 ods. 9;

p) poskytovanie usmernení s cieľom uľahčiť zbližovanie operačných postupov so zreteľom na uplatňovanie ustanovení tohto článku, pokiaľ ide o operačnú spoluprácu.

4. Na účely preskúmania uvedeného v článku 40 sieť jednotiek CSIRT do 17. januára 2025 a potom každé dva roky posúdi pokrok dosiahnutý s ohľadom na operačnú spoluprácu a prijme správu. V správe sa predovšetkým vyvodia závery a odporúčania na základe výsledkov partnerských preskúmaní uvedených v článku 19 a vykonaných v súvislosti s národnými jednotkami CSIRT. Táto správa sa predloží skupine pre spoluprácu.

5. Sieť jednotiek CSIRT prijme svoj rokovací poriadok.

6. Sieť jednotiek CSIRT a sieť EU-CyCLONe sa dohodnú na procesných opatreniach a v súlade s nimi spolupracujú.

▼B

Článok 16

Európska sieť styčných organizácií pre kybernetické krízy (EU-CyCLONe)

1. Sieť EU-CyCLONe sa zriaďuje s cieľom podporiť koordinované riadenie rozsiahlych kybernetických incidentov a kríz na operačnej úrovni a zabezpečiť pravidelnú výmenu relevantných informácií medzi členskými štátmi a inštitúciami, orgánmi, úradmi a agentúrami Únie.

2. Sieť EU-CyCLONe tvoria zástupcovia orgánov členských štátov pre riadenie kybernetických kríz a v prípadoch, keď potenciálny alebo prebiehajúci rozsiahly kybernetický incident má alebo pravdepodobne bude mať významný vplyv na služby a činnosti patriace do rozsahu pôsobnosti tejto smernice, aj zástupcovia Komisie. Vo všetkých ostatných prípadoch sa Komisia zúčastňuje na činnostiach siete EU-CyCLONe ako pozorovateľ.

Agentúra ENISA zabezpečuje sekretariát siete EU-CyCLONe, podporuje bezpečnú výmenu informácií a poskytuje potrebné nástroje na podporu spolupráce medzi členskými štátmi zaistením bezpečnej výmeny informácií.

V náležitých prípadoch môže sieť EU-CyCLONe prizvať ako pozorovateľov k svojej práci zástupcov príslušných zainteresovaných strán.

3. Sieť EU-CyCLONe plní tieto úlohy:

a) zvyšovanie úrovne pripravenosti na riadenie rozsiahlych kybernetických incidentov a kríz;

b) rozvíjanie spoločného situačného povedomia o rozsiahlych kybernetických incidentoch a krízach;

c) posudzovanie dôsledkov a vplyvu relevantných rozsiahlych kybernetických incidentov a kríz a navrhovanie možných zmierňujúcich opatrení;

d) koordinácia riadenia rozsiahlych kybernetických incidentov a kríz a podpora rozhodovania na politickej úrovni v súvislosti s takýmito incidentmi a krízami;

e) na žiadosť príslušného členského štátu prediskutovanie národných plánov reakcie na rozsiahle kybernetické incidenty a krízy uvedených v článku 9 ods. 4;

4. Sieť EU-CyCLONe prijme vlastný rokovací poriadok.

5. Sieť EU-CyCLONe podáva skupine pre spoluprácu pravidelne správy o riadení rozsiahlych kybernetických incidentov a kríz, ako aj o trendoch, pričom sa zameriava najmä na ich vplyv na kľúčové a dôležité subjekty.

▼B

6. Sieť EU-CyCLONe spolupracuje so sieťou jednotiek CSIRT na základe dohodnutých procesných opatrení stanovených v článku 15 ods. 6.

7. Sieť EU-CyCLONe do 17. júla 2024 a potom každých 18 mesiacov predloží Európskemu parlamentu a Rade správu, v ktorej posúdi svoju prácu.

Článok 17

Medzinárodná spolupráca

Únia môže v prípade potreby v súlade s článkom 218 ZFEÚ uzatvárať medzinárodné dohody s tretími krajinami alebo medzinárodnými organizáciami, ktorými môže povoľovať a organizovať ich účasť na konkrétnych činnostiach skupiny pre spoluprácu, siete jednotiek CSIRT a siete EU-CyCLONe. Takéto dohody musia byť v súlade s právom Únie v oblasti ochrany údajov.

Článok 18

Správa o stave kybernetickej bezpečnosti v Únii

1. Agentúra ENISA v spolupráci s Komisiou a skupinou pre spoluprácu prijme každé dva roky správu o stave kybernetickej bezpečnosti v Únii a predkladá a prezentuje ju Európskemu parlamentu. Správa sa vydáva aj v strojovo čitateľnom formáte a obsahuje:

a) posúdenie kybernetických rizík na úrovni Únie s prihliadnutím na panorámu kybernetických hrozieb;

b) posúdenie rozvoja spôsobilostí v oblasti kybernetickej bezpečnosti vo verejnom a súkromnom sektore v celej Únii;

c) posúdenie všeobecnej úrovne informovanosti o kybernetickej bezpečnosti a kybernetickej hygieny medzi občanmi a subjektmi vrátane malých a stredných podnikov;

d) súhrnné posúdenie výsledkov partnerského preskúmania uvedeného v článku 19;

e) súhrnné posúdenie úrovne vyspelosti spôsobilostí a zdrojov v oblasti kybernetickej bezpečnosti v celej Únii vrátane spôsobilostí a zdrojov na úrovni odvetví, ako aj rozsahu, v akom sú národné stratégie kybernetickej bezpečnosti členských štátov zosúladené.

2. Správa obsahuje konkrétne politické odporúčania na riešenie problémov a zvýšenie úrovne kybernetickej bezpečnosti v celej Únii a zhrnutie zistení za konkrétne obdobie z technických situačných správ o kybernetickej bezpečnosti v EÚ o incidentoch a kybernetických hrozbách, ktoré vypracúva agentúra ENISA v súlade s článkom 7 ods. 6 nariadenia (EÚ) 2019/881.

3. Agentúra ENISA v spolupráci s Komisiou, skupinou pre spoluprácu a sieťou jednotiek CSIRT pripraví metodiku súhrnného posúdenia uvedeného v prvom odseku písm. e) vrátane príslušných premenných, ako sú kvantitatívne a kvalitatívne ukazovatele.

▼B

Článok 19

Partnerské preskúmania

1. Skupina pre spoluprácu do 17. januára 2025 s pomocou Komisie a agentúry ENISA a v prípade potreby siete jednotiek CSIRT vypracuje metodiku a organizačné aspekty partnerských preskúmaní s cieľom čerpať zo spoločných skúseností, posilniť vzájomnú dôveru, dosiahnuť vysokú spoločnú úroveň kybernetickej bezpečnosti, ako aj posilniť spôsobilosti kybernetickej bezpečnosti a politiky členských štátov potrebné na vykonávanie tejto smernice. Účasť na partnerských preskúmaniach je dobrovoľná. Partnerské preskúmania vykonávajú experti na kybernetickú bezpečnosť. Expertov na kybernetickú bezpečnosť určia minimálne dva iné členské štáty, než je členský štát, ktorý je predmetom preskúmania.

Partnerské preskúmania sa týkajú aspoň jedného z týchto aspektov:

a) úrovne vykonávania opatrení na riadenie kybernetických rizík a oznamovacích povinností stanovených v článkoch 21 a 23;

b) úrovne spôsobilostí vrátane dostupných finančných, technických a ľudských zdrojov a účinnosť plnenia úloh príslušných orgánov;

c) operačných spôsobilostí jednotiek CSIRT;

d) úrovne vykonávania vzájomnej pomoci uvedenej v článku 37;

e) úrovne vykonávania dohôd o výmene informácií o kybernetickej bezpečnosti uvedených v článku 29;

f) konkrétnych záležitostí cezhraničného alebo medziodvetvového charakteru.

2. Metodika uvedená v odseku 1 zahŕňa objektívne, nediskriminačné, spravodlivé a transparentné kritériá, na základe ktorých členské štáty určia expertov na kybernetickú bezpečnosť oprávnených vykonávať partnerské preskúmania. Komisia agentúra ENISA sa zúčastňujú na partnerských preskúmaniach ako pozorovatelia.

3. Členské štáty môžu určiť konkrétne záležitosti uvedené v odseku 1 písm. f) na účely partnerského preskúmania.

4. Pred začatím partnerského preskúmania uvedeného v odseku 1 členské štáty oznámia zúčastneným členským štátom jeho rozsah vrátane konkrétnych záležitostí určených podľa odseku 3.

5. Pred začatím partnerského preskúmania môžu členské štáty vykonať sebahodnotenie skúmaných aspektov a toto sebahodnotenie poskytnúť určeným expertom na kybernetickú bezpečnosť. Metodiku sebahodnotenia členských štátov stanoví skupina pre spoluprácu s pomocou Komisie a agentúry ENISA.

▼B

6. Partnerské preskúmania zahŕňajú osobné alebo virtuálne návštevy na mieste a výmenu informácií na diaľku. Členský štát, ktorý je predmetom partnerského preskúmania, poskytne v súlade so zásadou dobrej spolupráce určeným expertom na kybernetickú bezpečnosť informácie potrebné na hodnotenie, a to bez toho, aby bolo dotknuté právo Únie alebo vnútroštátne právo týkajúce sa ochrany dôverných alebo utajovaných skutočností a ochrany základných funkcií štátu, ako je národná bezpečnosť. Skupina pre spoluprácu v spolupráci s Komisiou a agentúrou ENISA vypracuje vhodné kódexy správania na podporu pracovných metód určených expertov na kybernetickú bezpečnosť. Všetky informácie získané v rámci partnerského preskúmania sa použijú výlučne na uvedený účel. Experti na kybernetickú bezpečnosť, ktorí sa zúčastňujú na partnerskom preskúmaní, nesmú sprístupniť tretím stranám žiadne citlivé alebo dôverné informácie získané v priebehu tohto partnerského preskúmania.

7. Tie isté aspekty, ktoré už boli predmetom partnerského preskúmania v členskom štáte, nepodliehajú ďalšiemu partnerskému preskúmaniu v tomto členskom štáte najbližšie dva roky od ukončenia partnerského preskúmania, pokiaľ o to členský štát nepožiada alebo nedôjde k dohode po návrhu skupiny pre spoluprácu.

8. Členské štáty zabezpečia, aby každé riziko konfliktu záujmov týkajúce sa určených expertov na kybernetickú bezpečnosť bolo oznámené ostatným členským štátom, skupine pre spoluprácu, Komisii a agentúre ENISA pred začatím postupu partnerského preskúmania. Členský štát, ktorý je predmetom partnerského preskúmania, môže na základe riadne opodstatnených dôvodov, ktoré oznámi určujúcemu členskému štátu, podať námietku proti určeniu konkrétnych expertov na kybernetickú bezpečnosť.

9. Experti na kybernetickú bezpečnosť zúčastňujúci sa na partnerských preskúmaniach vypracujú správy o zisteniach a záveroch partnerských preskúmaní. Členské štáty, ktoré sú predmetom partnerského preskúmania, môžu predložiť pripomienky k návrhom správ, ktoré sa ich týkajú, a takéto pripomienky sa priložia k správam. Správy obsahujú odporúčania s cieľom umožniť zlepšenie aspektov, ktoré sú predmetom partnerského preskúmania. Správy sú v náležitých prípadoch postúpené skupine pre spoluprácu a sieti jednotiek CSIRT. Členský štát, ktorý je predmetom partnerského preskúmania, sa môže rozhodnúť, že svoju správu alebo jej upravenú verziu sprístupní verejnosti.

KAPITOLA IV

OPATRENIA NA RIADENIE KYBERNETICKÝCH RIZÍK A OZNAMOVACIE POVINNOSTI

Článok 20

Riadenie

1. Členské štáty zabezpečia, aby riadiace orgány kľúčových a dôležitých subjektov schválili opatrenia na riadenie kybernetických rizík, ktoré tieto subjekty prijali s cieľom dosiahnuť súlad s článkom 21, dohliadali na jeho vykonávanie a aby mohli byť brané na zodpovednosť, ak subjekty porušujú uvedený článok.

Uplatňovaním tohto odseku nie je dotknuté vnútroštátne právo, pokiaľ ide o pravidlá zodpovednosti uplatniteľné na verejné inštitúcie, ako aj zodpovednosť štátnych zamestnancov a volených alebo menovaných činiteľov.

▼B

2. Členské štáty zabezpečia, aby členovia riadiacich orgánov kľúčových a dôležitých subjektov boli povinní absolvovať odbornú prípravu, a kľúčové a dôležité subjekty podporia v tom, aby svojim zamestnancom pravidelne poskytovali podobnú odbornú prípravu a ich zamestnanci tak získali dostatočné znalosti a zručnosti a vedeli rozpoznať riziká a posúdiť postupy riadenia kybernetických rizík a ich vplyv na služby poskytované subjektom.

Článok 21

Opatrenia na riadenie kybernetických rizík

1. Členské štáty zabezpečia, aby kľúčové a dôležité subjekty prijali vhodné a primerané technické, operačné a organizačné opatrenia na riadenie rizík súvisiacich s bezpečnosťou sietí a informačných systémov, ktoré tieto subjekty využívajú na svoju činnosť alebo na poskytovanie svojich služieb a na prevenciu alebo minimalizáciu vplyvu incidentov na príjemcov ich služieb a na ďalšie služby.

S prihliadnutím na najnovšie, resp. na relevantné európske a medzinárodné normy, ako aj na náklady na vykonávanie sa opatreniami uvedenými v prvom pododseku zabezpečí úroveň bezpečnosti sietí a informačných systémov primeraná rizikám, ktoré predstavujú. Pri posudzovaní primeranosti týchto opatrení sa náležite zohľadní miera vystavenia subjektu rizikám, veľkosť subjektu a pravdepodobnosť výskytu incidentov a ich závažnosti vrátane ich spoločenského a hospodárskeho dosahu.

2. Opatrenia uvedené v odseku 1 sú založené na prístupe zohľadňujúcom všetky riziká, ktorého cieľom je chrániť siete a informačné systémy a fyzické prostredie uvedených systémov pred incidentmi, a zahŕňajú aspoň:

a) zásady analýzy rizík a bezpečnosti informačných systémov;

b) riešenie incidentov;

c) kontinuitu činností, ako je riadenie zálohovania a obnova systému po havárii, a krízové riadenie;

d) bezpečnosť dodávateľského reťazca vrátane bezpečnostných aspektov týkajúcich sa vzťahov medzi jednotlivými subjektmi a ich priamymi dodávateľmi alebo poskytovateľmi služieb;

e) bezpečnosť pri nadobúdaní, vývoji a údržbe siete a informačných systémov vrátane riešenia zraniteľností a zverejňovania informácií o zraniteľnostiach;

f) zásady a postupy posudzovania účinnosti opatrení na riadenie kybernetických rizík;

g) základné postupy kybernetickej hygieny a odborná príprava v oblasti kybernetickej bezpečnosti;

▼B

h) zásady a postupy používania kryptografie, prípadne šifrovania;

i) bezpečnosť ľudských zdrojov, zásady kontroly prístupu a správu aktív;

j) v prípade potreby používanie riešení viacstupňovej alebo kontinuálnej autentifikácie, zabezpečenej hlasovej, obrazovej a textovej komunikácie a zabezpečených systémov komunikácie v núdzových situáciách v rámci subjektu.

3. Členské štáty zabezpečia, aby subjekty pri zvažovaní toho, ktoré opatrenia uvedené v odseku 2 písm. d) tohto článku sú vhodné, zohľadňovali zraniteľnosti špecifické pre každého priameho dodávateľa a poskytovateľa služieb a celkovú kvalitu produktov a postupy svojich dodávateľov a poskytovateľov služieb kybernetickej bezpečnosti vrátane ich postupov bezpečného vývoja. Členské štáty tiež zabezpečia, aby subjekty pri zvažovaní toho, ktoré opatrenia uvedené v uvedenom písmene sú vhodné, boli povinné zohľadňovať výsledky koordinovaných posúdení bezpečnostných rizík kritických dodávateľských reťazcov vykonaných v súlade s článkom 22 ods. 1.

4. Členské štáty zabezpečia, aby subjekt, ktorý zistí, že nedodržiava opatrenia stanovené v odseku 2, prijal bez zbytočného odkladu všetky potrebné, vhodné a primerané nápravné opatrenia.

5. Komisia do 17. októbra 2024 prijme vykonávacie akty, ktorými stanoví technické a metodické požiadavky na opatrenia uvedené v odseku 2, pokiaľ ide o poskytovateľov služieb DNS, správcov názvov TLD, poskytovateľov služieb cloud computingu, poskytovateľov služieb dátového centra, poskytovateľov sietí na sprístupňovanie obsahu, poskytovateľov riadených služieb, poskytovateľov riadených bezpečnostných služieb, poskytovateľov online trhov, internetových vyhľadávačov a platforiem služieb sociálnej siete a poskytovateľov dôveryhodných služieb.

Komisia môže prijať vykonávacie akty, ktorými podľa potreby stanoví technické, metodické, ako aj odvetvové požiadavky na opatrenia uvedené v odseku 2, pokiaľ ide o iné kľúčové a dôležité subjekty, než sú subjekty uvedené v prvom pododseku tohto odseku.

Komisia pri príprave vykonávacích aktov uvedených v prvom a druhom pododseku tohto odseku sa v čo najväčšej možnej miere riadi európskymi a medzinárodnými normami, ako aj príslušnými technickými špecifikáciami. Komisia sa radí a spolupracuje so skupinou pre spoluprácu a agentúrou ENISA v súlade s článkom 14 ods. 4 písm. e), pokiaľ ide o návrhy vykonávacích aktov.

Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 39 ods. 2.

Článok 22

Koordinované posúdenia bezpečnostných rizík kritických dodávateľských reťazcov na úrovni Únie

1. Skupina pre spoluprácu môže v spolupráci s Komisiou a agentúrou ENISA vykonávať koordinované posúdenia bezpečnostných rizík dodávateľských reťazcov konkrétnych kritických služieb IKT, systémov IKT alebo produktov IKT, pričom zohľadní technické a prípadne aj netechnické faktory rizík.

▼B

2. Komisia po konzultácii so skupinou pre spoluprácu a agentúrou ENISA a v prípade potreby s príslušnými zainteresovanými stranami určí konkrétne kritické služby IKT, systémy IKT alebo produkty IKT, ktoré môžu podliehať koordinovanému posúdeniu bezpečnostných rizík uvedenému v odseku 1.

Článok 23

Oznamovacie povinnosti

1. Každý členský štát zabezpečí, aby kľúčové a dôležité subjekty bez zbytočného odkladu oznámili svojej jednotke CSIRT alebo v náležitých prípadoch svojmu príslušnému orgánu v súlade s odsekom 4 každý incident s významným vplyvom na poskytovanie ich služieb ako sa uvádza v odseku 3 (významný incident). V prípade potreby dotknuté subjekty bez zbytočného odkladu oznámia príjemcom svojich služieb významné incidenty, ktoré by mohli nepriaznivo ovplyvniť poskytovanie daných služieb. Každý členský štát zabezpečí, aby tieto subjekty oznamovali okrem iného informácie umožňujúce jednotke CSIRT alebo v náležitých prípadoch príslušnému orgánu určiť cezhraničný vplyv incidentu. Samotný akt oznámenia nezakladá zvýšenú zodpovednosť oznamujúceho subjektu.

Ak dotknuté subjekty oznámia príslušnému orgánu významný incident podľa prvého pododseku, členský štát zabezpečí, aby uvedený príslušný orgán postúpil toto oznámenie po jeho prijatí jednotke CSIRT.

V prípade cezhraničného alebo medziodvetvového významného incidentu členské štáty zabezpečia, aby sa ich jednotným kontaktným miestam včas poskytli príslušné informácie oznámené v súlade s odsekom 4.

2. Členské štáty v náležitých prípadoch zabezpečia, aby kľúčové a dôležité subjekty bez zbytočného odkladu oznámili príjemcom svojich služieb, ktorí potenciálne čelia významnej kybernetickej hrozbe, všetky opatrenia alebo nápravné kroky, ktoré títo príjemcovia môžu v reakcii na danú hrozbu prijať. Subjekty v prípade potreby týchto príjemcov informujú aj o samotnej významnej kybernetickej hrozbe.

3. Incident sa považuje za významný, ak:

a) spôsobil alebo má schopnosť spôsobiť dotknutému subjektu závažné prevádzkové narušenie služieb alebo finančnú stratu;

b) zasiahol alebo má schopnosť zasiahnuť iné fyzické alebo právnické osoby tým, že im spôsobí značnú majetkovú alebo nemajetkovú ujmu.

4. Členské štáty zabezpečia, aby dotknuté subjekty na účely oznámenia podľa odseku 1 postúpili jednotke CSIRT alebo v náležitých prípadoch príslušnému orgánu:

a) bez zbytočného odkladu a v každom prípade do 24 hodín od zistenia významného incidentu včasné varovanie, v ktorom sa prípadne uvedie, či významný incident pravdepodobne spôsobilo konanie, ktoré je nezákonné alebo so zlým úmyslom, alebo či môže mať cezhraničný dosah;

▼B

b) bez zbytočného odkladu a v každom prípade do 72 hodín po tom, ako sa dozvedeli o významnom incidente, oznámenie o incidente, ktorým v prípade potreby aktualizujú informácie uvedené v písmene a) a uvedú prvotné posúdenie významného incidentu, vrátane jeho závažnosti a vplyvu, ako aj prípadne indikátory kompromitácie.

c) na žiadosť jednotky CSIRT alebo v náležitých prípadoch príslušného orgánu priebežnú správu s relevantnou aktualizáciou daného stavu;

d) najneskôr jeden mesiac po postúpení oznámenia o incidente podľa písmena b) záverečnú správu, ktorá obsahuje tieto informácie:

i) podrobný opis incidentu vrátane jeho závažnosti a vplyvu;

ii) druh hrozby alebo hlavnú príčinu, ktorá pravdepodobne incident spôsobila;

iii) zavedené a prebiehajúce zmierňujúce opatrenia;

iv) v náležitých prípadoch cezhraničný vplyv incidentu;

e) v prípade, že v čase predkladania záverečnej správy uvedenej v písmene d) incident ešte prebieha, členské štáty zabezpečia, aby dotknuté subjekty predložili v uvedenom čase ďalšiu priebežnú správu a záverečnú správu do jedného mesiaca odo dňa, keď incident vyriešili.

Odchylne od prvého pododseku písm. b) poskytovateľ dôveryhodných služieb informuje jednotku CSIRT alebo v náležitých prípadoch príslušný orgán o významných incidentoch, ktoré majú vplyv na poskytovanie jeho dôveryhodných služieb, a to bez zbytočného odkladu a v každom prípade do 24 hodín od zistenia významného incidentu.

5. Jednotka CSIRT alebo príslušný orgán bez zbytočného odkladu a v rámci možností do 24 hodín od doručenia včasného varovania uvedeného v odseku 4 písm. a) poskytne oznamujúcemu subjektu odpoveď vrátane prvotnej spätnej väzby k významnému incidentu a na žiadosť subjektu usmernenie alebo operačné pokyny k vykonávaniu možných zmierňujúcich opatrení. Ak jednotka CSIRT nie je prvotným príjemcom oznámenia uvedeného v odseku 1, usmernenie poskytne príslušný orgán v spolupráci s jednotkou CSIRT. Jednotka CSIRT poskytne doplňujúcu technickú podporu, ak o to dotknutý subjekt požiada. Ak existuje podozrenie, že významný incident je trestnoprávnej povahy, jednotka CSIRT alebo príslušný orgán poskytne aj usmernenie, ako významný incident oznámiť orgánom presadzovania práva.

6. V prípade potreby, a najmä ak sa významný incident týka dvoch alebo viacerých členských štátov, jednotka CSIRT, príslušný orgán alebo jednotné kontaktné miesto bez zbytočného odkladu informuje o významnom incidente ostatné zasiahnuté členské štáty a agentúru ENISA. Takéto informácie obsahujú informácie toho typu, ktoré boli doručené v súlade s odsekom 4. Jednotka CSIRT, príslušný orgán alebo jednotné kontaktné miesto pritom v súlade s právom Únie alebo vnútroštátnymi právom chránia bezpečnosť a obchodné záujmy subjektu, ako aj dôvernosť poskytnutých informácií.

▼B

7. Po porade s dotknutým subjektom môže jednotka CSIRT, prípadne príslušný orgán členského štátu a v náležitých prípadoch jednotky CSIRT alebo príslušné orgány ďalších dotknutých členských štátov informovať o významnom incidente verejnosť alebo požiadať o to daný subjekt, ak je informovanie verejnosti potrebné na zabránenie významnému incidentu alebo riešenie prebiehajúceho incidentu alebo ak je zverejnenie významného incidentu vo verejnom záujme z iného dôvodu.

8. Na žiadosť jednotky CSIRT alebo príslušného orgánu jednotné kontaktné miesto postúpi doručené oznámenia podľa odseku 1 jednotným kontaktným miestam ostatných zasiahnutých členských štátov.

9. Jednotné kontaktné miesto predkladá agentúre ENISA každé tri mesiace súhrnnú správu s anonymizovanými a agregovanými údajmi o významných incidentoch, incidentoch, kybernetických hrozbách a udalostiach odvrátených v poslednej chvíli oznámených v súlade s odsekom 1 tohto článku a s článkom 30. S cieľom prispieť k poskytovaniu porovnateľných informácií môže agentúra ENISA prijať technické usmernenia k parametrom informácií, ktoré sa majú uvádzať v súhrnnej správe. Agentúra ENISA každých šesť mesiacov informuje skupinu pre spoluprácu a sieť jednotiek CSIRT o svojich zisteniach týkajúcich sa doručených oznámení.

10. Jednotky CSIRT alebo v náležitých prípadoch príslušné orgány poskytujú príslušným orgánom podľa smernice (EÚ) 2022/2557 informácie o významných incidentoch, incidentoch, kybernetických hrozbách a udalostiach odvrátených v poslednej chvíli, ktoré v súlade s odsekom 1 tohto článku a s článkom 30 oznámili subjekty označené ako kritické subjekty podľa smernice (EÚ) 2022/2557.

11. Komisia môže prijať vykonávacie akty, v ktorých bližšie určí druh informácií, formát a postup oznámenia predkladaného podľa odseku 1 tohto článku a článku 30 a komunikácie predkladanej podľa odseku 2 tohto článku.

Komisia do 17. októbra 2024 vo vzťahu k poskytovateľom služieb DNS, správcom názvov TLD, poskytovateľom služieb cloud computingu, poskytovateľom služieb dátového centra, poskytovateľom sietí na sprístupňovanie obsahu, poskytovateľom riadených služieb, poskytovateľom riadených bezpečnostných služieb, ako aj poskytovateľom online trhov, internetových vyhľadávačov a platforiem služieb sociálnych sietí prijme vykonávacie akty, v ktorých bližšie určí prípady, v ktorých sa incident považuje za významný, ako sa uvádza v odseku 3. Komisia môže prijať takéto vykonávacie akty vo vzťahu k iným kľúčovým a dôležitým subjektom.

Komisia sa radí a spolupracuje so skupinou pre spoluprácu v súlade s článkom 14 ods. 4 písm. e), pokiaľ ide o návrhy vykonávacích aktov uvedených v prvom a druhom pododseku tohto odseku.

Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 39 ods. 2.

▼B

Článok 24

Používanie európskych systémov certifikácie kybernetickej bezpečnosti

1. S cieľom preukázať súlad s určitými požiadavkami článku 21 môžu členské štáty vyžadovať, aby kľúčové a dôležité subjekty používali určité produkty IKT, služby IKT a procesy IKT, ktoré vyvinul kľúčový alebo dôležitý subjekt alebo boli obstarané od tretích strán certifikovaných podľa európskych systémov certifikácie kybernetickej bezpečnosti prijatých podľa článku 49 nariadenia (EÚ) 2019/881. Členské štáty navyše podporujú kľúčové a dôležité subjekty v tom, aby využívali kvalifikované dôveryhodné služby.

2. Komisia je splnomocnená prijímať delegované akty v súlade s článkom 38 s cieľom doplniť túto smernicu a bližšie určiť kategórie kľúčových a dôležitých subjektov, od ktorých sa má vyžadovať používanie určitých certifikovaných produktov IKT, služieb IKT a procesov IKT alebo získanie certifikátu v rámci európskeho systému certifikácie kybernetickej bezpečnosti prijatého podľa článku 49 nariadenia (EÚ) 2019/881. Uvedené delegované akty sa prijmú v prípade, že sa zistí nedostatočná úroveň kybernetickej bezpečnosti, a stanoví sa v nich obdobie vykonávania.

Komisia pred prijatím takýchto delegovaných aktov vykoná posúdenie vplyvov a uskutoční konzultácie v súlade s článkom 56 nariadenia (EÚ) 2019/881.

3. V prípadoch, keď nie je k dispozícii žiadny európsky systém certifikácie kybernetickej bezpečnosti na účely odseku 2 tohto článku, Komisia po porade so skupinou pre spoluprácu a európskou skupinou pre certifikáciu kybernetickej bezpečnosti môže požiadať agentúru ENISA, aby vypracovala kandidátsky systém podľa článku 48 ods. 2 nariadenia (EÚ) 2019/881.

Článok 25

Normalizácia

1. Členské štáty v záujme harmonizovaného vykonávania článku 21 ods. 1 a 2 a bez toho, aby ukladali povinnosť využívať určitý typ technológie alebo diskriminovali v prospech takéhoto využívania, podporujú využívanie európskych a medzinárodných noriem a technických špecifikácií, ktoré sú relevantné pre bezpečnosť sietí a informačných systémov.

2. Agentúra ENISA v spolupráci s členskými štátmi a v prípade potreby po konzultácii s príslušnými zainteresovanými stranami vypracuje odporúčania a usmernenia pre technické oblasti, ktoré sa majú zvážiť v súvislosti s odsekom 1, ako aj odporúčania a usmernenia k už existujúcim normám vrátane vnútroštátnych noriem, ktoré by sa mohli vzťahovať na uvedené oblasti.

KAPITOLA V

PRÁVOMOC A REGISTRÁCIA

Článok 26

Právomoc a teritorialita

1. Subjekty, ktoré patria do rozsahu pôsobnosti tejto smernice sa považujú za subjekty podliehajúce právomoci členského štátu, v ktorom sú usadené, s výnimkou:

▼B

a) poskytovateľov verejných elektronických komunikačných sietí alebo poskytovateľov verejne dostupných elektronických komunikačných služieb, ktorí sa považujú za poskytovateľov podliehajúcich právomoci členského štátu, v ktorom poskytujú svoje služby;

b) poskytovateľov služieb DNS, správcov názvov TLD, subjektov poskytujúcich služby registrácie názvov domén, poskytovateľov služieb cloud computingu, poskytovateľov služieb dátového centra, poskytovateľov sietí na sprístupňovanie obsahu, poskytovateľov riadených služieb, poskytovateľov riadených bezpečnostných služieb, ako aj poskytovateľov online trhov, internetových vyhľadávačov a platforiem služieb sociálnej siete, ktorí sa považujú za subjekty podliehajúce právomoci toho členského štátu, v ktorom majú hlavnú prevádzkareň v Únii podľa odseku 2;

c) subjektov verejnej správy, ktoré sa považujú za subjekty podliehajúce právomoci členského štátu, ktorý ich zriadil.

2. Na účely tejto smernice platí, že subjekt uvedený v odseku 1 písm. b) má svoju hlavnú prevádzkareň v Únii v členskom štáte, v ktorom najčastejšie prijíma rozhodnutia týkajúce sa opatrení na riadenie kybernetických rizík. Ak takýto členský štát nemožno určiť alebo ak sa takéto rozhodnutia neprijímajú v Únii, za hlavnú prevádzkareň sa považuje členský štát, v ktorom sa vykonávajú operácie kybernetickej bezpečnosti. Ak takýto členský štát nemožno určiť, za hlavnú prevádzkareň sa považuje členský štát, v ktorom má dotknutý subjekt prevádzkareň s najvyšším počtom zamestnancov v Únii.

3. Ak subjekt uvedený v odseku 1 písm. b) nie je usadený v Únii, ale ponúka služby v rámci Únie, určí zástupcu v Únii. Zástupca musí byť usadený v jednom z tých členských štátov, v ktorých subjekt ponúka služby. Takýto subjekt sa považuje za subjekt podliehajúci právomoci toho členského štátu, v ktorom je usadený jeho zástupca. Ak v Únii nie je určený zástupca podľa tohto odseku, ktorýkoľvek členský štát, v ktorom subjekt poskytuje služby, môže proti tomuto subjektu podniknúť právne kroky za porušenie tejto smernice.

4. Tým, že subjekt uvedený v odseku 1 písm. b) určí svojho zástupcu, nie sú dotknuté právne kroky, ktoré by mohli byť podniknuté proti samotnému subjektu.

5. Členské štáty, ktorým bola doručená žiadosť o vzájomnú pomoc týkajúcu sa subjektu uvedeného v odseku 1 písm. b), môžu v medziach uvedenej žiadosti prijať primerané opatrenia dohľadu a presadzovania práva vo vzťahu k dotknutému subjektu, ktorý poskytuje služby alebo má sieť a informačný systém na ich území.

Článok 27

Register subjektov

1. Agentúra ENISA zriadi a vedie register poskytovateľov služieb DNS, správcov názvov TLD, subjektov poskytujúcich služby registrácie názvov domén, poskytovateľov služieb cloud computingu, poskytovateľov služieb dátového centra, poskytovateľov sietí na sprístupňovanie obsahu, poskytovateľov riadených služieb, poskytovateľov riadených bezpečnostných služieb, ako aj poskytovateľov online trhov, internetových vyhľadávačov a platforiem služieb sociálnych sietí na základe informácií

▼B

získaných od jednotných kontaktných miest v súlade s odsekom 4. Agentúra ENISA umožní príslušným orgánom na požiadanie prístup do uvedeného registra, pričom v náležitých prípadoch zabezpečí ochranu dôvernosti informácií.

2. Členské štáty do 17. januára 2025 požiadajú subjekty uvedené v odseku 1, aby príslušným orgánom predložili tieto informácie:

a) názov subjektu;

b) podľa potreby príslušné odvetvie, pododvetvie a typ subjektu, ako sú uvedené v prílohe I alebo II;

c) adresu hlavnej prevádzkarne subjektu a jeho iných zákonných prevádzkarní v Únii, alebo ak subjekt nie je usadený v Únii, adresu svojho zástupcu určeného podľa článku 26 ods. 3;

d) aktuálne kontaktné údaje vrátane e-mailových adries a telefónnych čísel subjektu a v náležitom prípade jeho zástupcu určeného podľa článku 26 ods. 3;

e) členské štáty, v ktorých subjekt poskytuje služby; a

f) rozsahy IP adries subjektu.

3. Členské štáty zabezpečia, aby subjekty uvedené v odseku 1 oznámili príslušnému orgánu všetky zmeny údajov, ktoré predložili podľa odseku 2, a to bezodkladne a v každom prípade do troch mesiacov odo dňa zmeny.

4. Po doručení informácií uvedených v odsekoch 2 a 3, s výnimkou informácií uvedených v odseku 2 písm. f), jednotné kontaktné miesto dotknutého členského štátu postúpi tieto informácie bez zbytočného odkladu agentúre ENISA.

5. Informácie uvedené v odsekoch 2 a 3 tohto článku sa prípadne podávajú prostredníctvom vnútroštátneho mechanizmu uvedeného v článku 3 ods. 4 štvrtom pododseku.

Článok 28

Databáza registračných údajov názvov domén

1. S cieľom prispieť k bezpečnosti, stabilite a odolnosti DNS členské štáty požadujú, aby správcovia názvov TLD a subjekty poskytujúce služby registrácie názvov domén s náležitou starostlivosťou zhromažďovali a uchovávali presné a úplné registračné údaje názvov domén vo vyhradenej databáze v súlade s právom Únie v oblasti ochrany údajov, pokiaľ ide o údaje, ktoré sú osobnými údajmi.

2. Na účely odseku 1 členské štáty požadujú, aby databáza registračných údajov názvov domén obsahovala nevyhnutné informácie na identifikáciu a kontaktovanie držiteľov názvov domén a kontaktných miest spravujúcich názvy domén v rámci TLD. Takéto informácie zahŕňajú:

▼B

a) názov domény;

b) dátum registrácie;

c) meno/názov žiadateľa o registráciu, kontaktnú e-mailovú adresu a telefónne číslo;

d) kontaktnú e-mailovú adresu a telefónne číslo kontaktného miesta spravujúceho názov domény v prípade, že sa líšia od adresy a čísla žiadateľa o registráciu.

3. Členské štáty požadujú, aby správcovia názvov TLD a subjekty poskytujúce služby registrácie názvov domén mali zavedené politiky a postupy vrátane postupov overovania s cieľom zabezpečiť, aby databázy uvedené v odseku 1 obsahovali presné a úplné informácie. Členské štáty požadujú, aby takéto politiky a postupy boli verejne dostupné.

4. Členské štáty požadujú, aby správcovia názvov TLD a subjekty poskytujúce služby registrácie názvov domén bez zbytočného odkladu po registrácii názvu domény zverejnili registračné údaje názvu domény, ktoré nie sú osobnými údajmi.

5. Členské štáty požadujú, aby správcovia názvov TLD a subjekty poskytujúce služby registrácie názvov domén poskytovali prístup k špecifickým registračným údajom názvov domén na základe zákonných a riadne odôvodnených žiadostí ►C1 oprávnených žiadateľov o prístup ◄ v súlade s právom Únie v oblasti ochrany údajov. Členské štáty požadujú, aby správcovia názvov TLD a subjekty poskytujúce služby registrácie názvov domén odpovedali bez zbytočného odkladu a v každom prípade do 72 hodín od doručenia akýchkoľvek žiadostí o prístup. Členské štáty požadujú, aby politiky a postupy zverejňovania takýchto údajov boli verejne dostupné.

6. Dodržiavanie povinností stanovených v odsekoch 1 až 5 nesmie viesť k duplicitnému zberu registračných údajov názvov domén. Na tento účel členské štáty požadujú, aby správcovia názvov TLD a subjekty poskytujúce služby registrácie názvov domén navzájom spolupracovali.

KAPITOLA VI

VÝMENA INFORMÁCIÍ

Článok 29

Dohody o výmene informácií o kybernetickej bezpečnosti

1. Členské štáty zabezpečia, aby si subjekty, ktoré patria do rozsahu pôsobnosti tejto smernice, a v náležitých prípadoch ďalšie subjekty, ktoré nepatria do rozsahu pôsobnosti tejto smernice, mohli dobrovoľne medzi sebou vymieňať relevantné informácie o kybernetickej bezpečnosti vrátane informácií o kybernetických hrozbách, udalostiach odvrátených v poslednej chvíli, zraniteľnostiach, technikách a postupoch, indikátoroch kompromitácie, nepriateľských taktikách, informácie špecifické pre jednotlivé hrozby a aktérov, výstrahy a odporúčania týkajúce sa konfigurácie kybernetických bezpečnostných nástrojov na odhaľovanie kybernetických útokov, ak takáto výmena informácií:

▼B

a) má za cieľ predchádzať incidentom, odhaľovať ich, reagovať na ne alebo zotaviť sa z nich, alebo zmierniť ich vplyv;

b) zvyšuje úroveň kybernetickej bezpečnosti, najmä zvyšovaním informovanosti o kybernetických hrozbách, obmedzovaním alebo zabraňovaním možnosti šírenia takýchto hrozieb, podporou celej škály obranných spôsobilostí, nápravou zraniteľností a zverejňovaním informácií o nich, odhaľovaním hrozieb, technikami na zamedzenie ich šírenia a na ich predchádzanie, stratégiami zmierňovania alebo fázami reakcie a zotavenia, resp. podporou spoločného výskumu kybernetických hrozieb verejnými a súkromnými subjektmi.

2. Členské štáty zabezpečia, aby sa výmena informácií uskutočňovala v rámci komunít kľúčových a dôležitých subjektov, prípadne ich dodávateľov alebo poskytovateľov služieb. Takáto výmena sa uskutočňuje na základe dohôd o výmene informácií o kybernetickej bezpečnosti s ohľadom na potenciálne citlivú povahu vymieňaných informácií.

3. Uzavretie dohôd o výmene informácií o kybernetickej bezpečnosti uvedených v odseku 2 tohto článku sprostredkujú členské štáty. V takýchto dohodách sa môžu špecifikovať operačné prvky vrátane využívania špecializovaných platforiem IKT a nástrojov automatizácie, ako aj obsah a podmienky dohôd o výmene informácií. Tým, že členské štáty stanovia podrobnosti o zapojení orgánov verejnej moci do takýchto dohôd, môžu uložiť podmienky zverejňovania informácií príslušnými orgánmi alebo jednotkami CSIRT. Členské štáty pomáhajú s uplatňovaním takýchto dohôd v súlade so svojimi politikami uvedenými v článku 7 ods. 2 písm. h).

4. Členské štáty zabezpečia, aby kľúčové a dôležité subjekty oznamovali príslušným orgánom svoju účasť na dohodách o výmene informácií o kybernetickej bezpečnosti uvedených v odseku 2 hneď, ako takéto dohody uzatvoria, prípadne ich odstúpenie od takýchto dohôd hneď, ako odstúpenie nadobudne účinnosť.

5. Agentúra ENISA poskytuje pomoc pri uzatváraní dohôd o výmene informácií o kybernetickej bezpečnosti uvedených v odseku 2 tým, že umožňuje výmenu najlepších postupov a poskytuje rady.

Článok 30

Dobrovoľné oznámenie relevantných informácií

1. Členské štáty zabezpečia, aby okrem oznamovacej povinnosti stanovenej v článku 23 mohli jednotkám CSIRT alebo prípadne príslušným orgánom podávať oznámenia dobrovoľne tieto subjekty:

a) kľúčové a dôležité subjekty v súvislosti s incidentmi, kybernetickými hrozbami a udalosťami odvrátenými v poslednej chvíli;

▼B

b) iné subjekty, než sú subjekty uvedené v písmene a), bez ohľadu na to, či patria do rozsahu pôsobnosti tejto smernice, v súvislosti s významnými incidentmi, kybernetickými hrozbami a udalosťami odvrátenými v poslednej chvíli.

2. Členské štáty spracujú oznámenie uvedené v odseku 1 tohto článku v súlade s postupom stanoveným v článku 23. Členské štáty môžu spracovanie povinných oznámení uprednostniť pred dobrovoľnými oznámeniami.

V prípade potreby jednotky CSIRT a v náležitom prípade príslušné orgány poskytnú jednotným kontaktným miestam informácie o oznámeniach doručených podľa tohto článku, pričom zabezpečia dôvernosť a primeranú ochranu informácií poskytnutých oznamujúcim subjektom. Bez toho, aby bola dotknutá prevencia, vyšetrovanie, odhaľovanie a stíhanie trestných činov, oznamujúcemu subjektu nevznikajú v dôsledku dobrovoľného oznámenia žiadne ďalšie povinnosti, ktoré by sa naň neboli vzťahovali, ak by oznámenie nepodal.

KAPITOLA VII

DOHĽAD A PRESADZOVANIE PRÁVA

Článok 31

Všeobecné aspekty dohľadu a presadzovania práva

1. Členské štáty zabezpečia, aby ich príslušné orgány účinne dohliadali a prijímali opatrenia potrebné na zabezpečenie súladu s touto smernicou.

2. Členské štáty môžu povoliť svojim príslušným orgánom, aby uprednostnili úlohy dohľadu. Takéto uprednostňovanie vychádza z prístupu založeného na rizikách. Príslušné orgány môžu na tento účel pri vykonávaní svojich úloh dohľadu stanovených v článkoch 32 a 33 stanoviť metodiky dohľadu, ktoré umožnia uprednostnenie takýchto úloh podľa prístupu založeného na rizikách.

3. Príslušné orgány pri riešení incidentov, ktoré majú za následok porušenie ochrany osobných údajov, úzko spolupracujú s orgánmi dohľadu podľa nariadenia (EÚ) 2016/679 bez toho, aby boli dotknuté kompetencie a úlohy orgánov dohľadu podľa uvedeného nariadenia.

4. Bez toho, aby boli dotknuté vnútroštátne legislatívne a inštitucionálne rámce, členské štáty zabezpečia, aby príslušné orgány mali pri dohľade nad dodržiavaním tejto smernice subjektami verejnej správy a pri ukladaní opatrení presadzovania práva v súvislosti s porušeniami tejto smernice primerané právomoci na plnenie takýchto úloh s operačnou nezávislosťou od dohliadaných subjektov verejnej správy. Členské štáty môžu rozhodnúť o uložení vhodných, primeraných a účinných opatrení v oblasti dohľadu a na presadzovanie práva vo vzťahu k týmto subjektom v súlade s vnútroštátnymi legislatívnymi a inštitucionálnymi rámcami.

▼B

Článok 32

Opatrenia dohľadu a presadzovania práva týkajúce sa kľúčových subjektov

1. Členské štáty zabezpečia, aby opatrenia dohľadu alebo presadzovania práva uložené kľúčovým subjektom v súvislosti s povinnosťami stanovenými v tejto smernici boli účinné, primerané a odrádzajúce a zároveň zohľadňovali okolnosti každého jednotlivého prípadu.

2. Členské štáty zabezpečia, aby príslušné orgány pri vykonávaní svojich úloh dohľadu nad kľúčovými subjektmi mali právomoc podrobiť tieto subjekty prinajmenšom:

a) inšpekciám na mieste a dohľadu na diaľku vrátane náhodných kontrol, ktoré vykonávajú vyškolení odborníci;

b) pravidelným a cieleným bezpečnostným auditom, ktoré vykonáva nezávislý orgán alebo príslušný orgán;

c) auditom ad hoc, a to v prípadoch odôvodnených významným incidentom alebo porušením tejto smernice kľúčovým subjektom;

d) bezpečnostným kontrolám podľa objektívnych, nediskriminačných, spravodlivých a transparentných kritérií posudzovania rizík, v prípade potreby v spolupráci s dotknutým subjektom;

e) žiadostiam o informácie potrebné na posúdenie opatrení na riadenie kybernetických rizík, ktoré dotknutý subjekt prijal, vrátane zdokumentovaných politík kybernetickej bezpečnosti, ako aj dodržiavania povinnosti predložiť informácie príslušným orgánom podľa článku 27;

f) žiadostiam o prístup k údajom, dokumentom a informáciám potrebným na plnenie ich úloh dohľadu;

g) žiadostiam o dôkazy vykonávania politík kybernetickej bezpečnosti, ako sú výsledky bezpečnostných auditov uskutočnených kvalifikovaným audítorom a príslušné podkladové dôkazy.

Cielené bezpečnostné audity uvedené v prvom pododseku písm. b) sú založené na posúdeniach rizík, ktoré vypracoval príslušný orgán alebo auditovaný subjekt, alebo na iných dostupných informáciách týkajúcich sa rizík.

Výsledky každého cieleného bezpečnostného auditu sa sprístupnia príslušnému orgánu. Náklady na takýto cielený bezpečnostný audit, ktorý vykonáva nezávislý orgán, hradí auditovaný subjekt, s výnimkou riadne odôvodnených prípadov, keď príslušný orgán rozhodne inak.

3. Príslušné orgány pri vykonávaní svojich právomocí podľa odseku 2 písm. e), f) alebo g) uvedú účel žiadosti a konkretizujú požadované informácie.

4. Členské štáty zabezpečia, aby ich príslušné orgány pri vykonávaní svojich právomocí presadzovania práva v súvislosti s kľúčovými subjektmi mali právomoc prinajmenšom:

▼B

a) vydávať varovania o porušeniach tejto smernice dotknutými subjektmi;

b) prijímať záväzné pokyny, a to aj v súvislosti s opatreniami potrebnými na prevenciu alebo nápravu incidentu, ako aj lehotami na vykonávanie takýchto opatrení a podávanie správ o ich vykonávaní, alebo príkaz, ktorým sa od dotknutých subjektov vyžaduje napraviť zistené nedostatky alebo porušenia tejto smernice;

c) nariadiť dotknutým subjektom, aby upustili od konania, ktoré porušuje túto smernicu, a takéto konanie neopakovali;

d) nariadiť dotknutým subjektom, aby určeným spôsobom a v určenej lehote zosúladili svoje opatrenia na riadenie kybernetických rizík s článkom 21 alebo splnili oznamovacie povinnosti stanovené v článku 23;

e) nariadiť dotknutým subjektom, aby informovali fyzické alebo právnické osoby, v súvislosti s ktorými poskytujú služby alebo vykonávajú činnosti, ktoré sú potenciálne zasiahnuté významnou kybernetickou hrozbou, o povahe hrozby, ako aj o akýchkoľvek možných ochranných alebo nápravných opatreniach, ktoré môžu tieto fyzické alebo právnické osoby prijať v reakcii na danú hrozbu;

f) nariadiť dotknutým subjektom, aby v primeranej lehote vykonali odporúčania poskytnuté na základe bezpečnostného auditu;

g) určiť monitorujúceho úradníka s presne vymedzenými úlohami na určité obdobie, ktorý bude dohliadať na dodržiavanie článkov 21 a 23 dotknutými subjektmi;

h) nariadiť dotknutým subjektom, aby určeným spôsobom zverejnili aspekty porušovania tejto smernice;

i) uložiť správnu pokutu podľa článku 34 alebo požiadať o jej uloženie príslušné orgány, súdy alebo tribunály v súlade s vnútroštátnym právom, a to popri ktoromkoľvek z opatrení uvedených v písmenách a) až h) tohto odseku.

5. Ak sa opatrenia na presadzovanie práva prijaté podľa odseku 4 písm. a) až d) a f) ukážu ako neúčinné, členské štáty zabezpečia, aby ich príslušné orgány mali právomoc stanoviť lehotu, v rámci ktorej je kľúčový subjekt povinný prijať potrebné opatrenia na nápravu nedostatkov alebo splniť požiadavky týchto orgánov. Ak sa požadované opatrenie v stanovenej lehote neprijme, členské štáty zabezpečia, aby ich príslušné orgány mali právomoc:

a) dočasne pozastaviť certifikáciu alebo povoľovanie alebo požiadať certifikačný alebo povoľujúci subjekt, súd, alebo tribunál v súlade s vnútroštátnym právom, aby dočasne pozastavil certifikáciu alebo povoľovanie časti alebo všetkých relevantných služieb, ktoré kľúčový subjekt poskytuje, alebo činností, ktoré kľúčový subjekt vykonáva;

b) od príslušných orgánov, súdov alebo tribunálov v súlade s vnútroštátnym právom požadovať uloženie dočasného zákazu vykonávať riadiace funkcie v tomto kľúčovom subjekte, a to akejkoľvek fyzickej osobe zodpovednej za vykonávanie riadiacich úloh na úrovni výkonného riaditeľa alebo právneho zástupcu v tomto kľúčovom subjekte.

▼B

Dočasné pozastavenia alebo zákazy podľa tohto odseku sa uplatňujú len dovtedy, kým dotknutý subjekt neprijme potrebné opatrenia na nápravu nedostatkov alebo nesplní požiadavky príslušného orgánu, ktorý takéto opatrenia presadzovania práva uložil. Ukladanie takýchto dočasných pozastavení alebo zákazov musí podliehať primeraným procesným zárukám podľa všeobecných zásad práva Únie a charty vrátane práva na účinný prostriedok nápravy a na spravodlivý proces, prezumpciu neviny a práva na obhajobu.

Opatrenia presadzovania práva stanovené v tomto odseku sa neuplatňujú na subjekty verejnej správy, na ktoré sa vzťahuje táto smernica.

6. Členské štáty zabezpečia, aby každá fyzická osoba zodpovedná za kľúčový subjekt alebo konajúca ako jeho právny zástupca na základe právomoci zastupovať ho, prijímať rozhodnutia v jeho mene alebo vykonávať kontrolu nad ním mala právomoc zabezpečiť dodržiavanie tejto smernice. Členské štáty zabezpečia, aby bolo možné brať takéto fyzické osoby na zodpovednosť za porušenie ich úloh zabezpečovať dodržiavanie tejto smernice.

Pokiaľ ide o subjekty verejnej správy, týmto odsekom nie je dotknuté vnútroštátne právo, pokiaľ ide o zodpovednosť štátnych zamestnancov a volených alebo menovaných činiteľov.

7. Príslušné orgány pri prijímaní ktoréhokoľvek z opatrení na presadzovanie práva uvedených v odseku 4 alebo 5 dodržiavajú právo na obhajobu a zohľadňujú okolnosti každého jednotlivého prípadu a prinajmenšom náležite zohľadňujú:

a) závažnosť porušenia a dôležitosť porušených ustanovení, pričom za závažné porušenie sa okrem iného považujú v každom prípade tieto porušenia:

   i) opakované porušenia;

   ii) neoznámenie významných incidentov alebo nevykonanie ich nápravy;

   iii) nevykonanie nápravy nedostatkov po prijatí záväzných pokynov príslušných orgánov;

   iv) marenie auditov alebo monitorovacích činností nariadených príslušným orgánom na základe zistenia porušenia;

   v) poskytovanie nepravdivých alebo hrubo nepresných informácií týkajúcich sa opatrení na riadenie kybernetických rizík alebo oznamovacích povinností stanovených v článkoch 21 a 23;

b) dĺžku trvania porušenia;

c) akékoľvek relevantné predchádzajúce prípady porušenia dotknutého subjektu;

d) akúkoľvek spôsobenú majetkovú alebo nemajetkovú ujmu vrátane finančných alebo hospodárskych strát, účinkov na iné služby a počtu dotknutých používateľov;

▼B

e) akýkoľvek úmysel alebo nedbanlivosť páchateľa porušenia;

f) akékoľvek opatrenia, ktoré subjekt prijal na zabránenie alebo zmiernenie majetkovej alebo nemajetkovej ujmy;

g) akékoľvek dodržiavanie schválených kódexov správania alebo schválených mechanizmov certifikácie;

h) úrovne spolupráce zodpovednej fyzickej alebo právnickej osoby s príslušným orgánom.

8. Príslušné orgány uvedú podrobné odôvodnenie svojich opatrení na presadzovanie práva. Príslušné orgány pred prijatím takýchto opatrení oznámia dotknutým subjektom svoje predbežné zistenia. Takisto poskytnú týmto subjektom primeraný čas na predloženie pripomienok, s výnimkou riadne odôvodnených prípadov, ak by to bránilo prijatiu okamžitých opatrení na predchádzanie incidentom alebo reakciu na ne.

9. Členské štáty zabezpečia, aby ich príslušné orgány podľa tejto smernice informovali relevantné príslušné orgány v tom istom členskom štáte podľa smernice (EÚ) 2022/2557 vtedy, keď vykonávajú svoje právomoci v oblasti dohľadu a presadzovania práva, ktorých cieľom je zabezpečiť, aby subjekt identifikovaný ako kritický subjekt podľa smernice (EÚ) 2022/2557 dodržiaval túto smernicu. Príslušné orgány podľa smernice (EÚ) 2022/2557 môžu v náležitých prípadoch požiadať príslušné orgány podľa tejto smernice o vykonanie ich právomocí dohľadu a presadzovania práva vo vzťahu k subjektu, ktorý je identifikovaný ako kritický subjekt podľa smernice (EÚ) 2022/2557.

10. Členské štáty zabezpečia, aby ich príslušné orgány podľa tejto smernice spolupracovali s relevantnými príslušnými orgánmi dotknutého členského štátu podľa nariadenia (EÚ) 2022/2554. Členské štáty najmä zabezpečia, aby ich príslušné orgány podľa tejto smernice informovali fórum pre dozor zriadený podľa článku 32 ods. 1 nariadenia (EÚ) 2022/2554 pri vykonávaní svojich právomocí dohľadu a presadzovania práva, ktorých cieľom je zabezpečiť, aby kľúčový subjekt, ktorý je identifikovaný ako externý poskytovateľ kritických IKT služieb podľa článku 31 nariadenia (EÚ) 2022/2554, dodržiaval túto smernicu.

Článok 33

Opatrenia dohľadu a presadzovania práva týkajúce sa dôležitých subjektov

1. Ak členské štáty získajú dôkaz, indíciu alebo informáciu, že dôležitý subjekt údajne nedodržiava túto smernicu, a najmä jej články 21 a 23, zabezpečia, aby príslušné orgány konali v prípade potreby prostredníctvom *ex post* opatrení v oblasti dohľadu. Členské štáty zabezpečia, aby tieto opatrenia boli účinné, primerané a odrádzajúce, pričom zohľadnia okolnosti každého jednotlivého prípadu.

2. Členské štáty zabezpečia, aby príslušné orgány pri vykonávaní svojich úloh dohľadu nad dôležitými subjektmi mali právomoc podrobiť tieto subjekty prinajmenšom:

▼B

a) inšpekciám na mieste a *ex post* dohľadu na diaľku, ktoré vykonávajú vyškolení odborníci;

b) cieleným bezpečnostným auditom, ktoré vykonáva nezávislý orgán alebo príslušný orgán;

c) bezpečnostným kontrolám založeným na objektívnych, nediskriminačných, spravodlivých a transparentných kritériách posudzovania rizík, v prípade potreby v spolupráci s dotknutým subjektom;

d) žiadostiam o informácie potrebné na *ex post* posúdenie opatrení na riadenie kybernetických rizík, ktoré dotknutý subjekt prijal, vrátane zdokumentovaných politík kybernetickej bezpečnosti, ako aj dodržiavania povinnosti predkladať informácie príslušným orgánom podľa článku 27;

e) žiadostiam o prístup k údajom, dokumentom a informáciám potrebným na plnenie ich úloh dohľadu;

f) žiadostiam o dôkazy vykonávania politík kybernetickej bezpečnosti, ako sú výsledky bezpečnostných auditov uskutočnených kvalifikovaným audítorom a príslušné podkladové dôkazy.

Cielené bezpečnostné audity uvedené v prvom pododseku písm. b) sú založené na posúdení rizík, ktoré vykonal príslušný orgán alebo auditovaný subjekt, alebo na iných dostupných informáciách týkajúcich sa rizík.

Výsledky každého cieleného bezpečnostného auditu sa sprístupnia príslušnému orgánu. Náklady na takýto cielený bezpečnostný audit, ktorý vykonáva nezávislý orgán, hradí auditovaný subjekt, s výnimkou riadne odôvodnených prípadov, keď príslušný orgán rozhodne inak.

3. Príslušné orgány pri vykonávaní svojich právomocí podľa odseku 2 písm. d), e) alebo f) uvedú účel žiadosti a konkretizujú požadované informácie.

4. Členské štáty zabezpečia, aby príslušné orgány pri vykonávaní svojich právomocí presadzovania práva v súvislosti s dôležitými subjektmi mali právomoc prinajmenšom:

a) vydávať varovania o porušeniach tejto smernice dotknutými subjektmi;

b) prijímať záväzné pokyny alebo príkaz, ktorým sa od dotknutých subjektov vyžaduje napraviť zistené nedostatky alebo porušenie tejto smernice;

c) nariadiť dotknutým subjektom, aby upustili od konania, ktoré porušuje túto smernicu, a neopakovali takéto konanie;

d) nariadiť dotknutým subjektom, aby určeným spôsobom a v určenej lehote zabezpečili zosúladenie svojich opatrení na riadenie kybernetických rizík s článkom 21 alebo splnili oznamovacie povinnosti stanovené v článku 23;

▼B

e) nariadiť dotknutým subjektom, aby informovali fyzické alebo právnické osoby, v súvislosti s ktorými poskytujú služby alebo vykonávajú činnosti, ktoré sú potenciálne zasiahnuté významnou kybernetickou hrozbou, o povahe hrozby, ako aj o akýchkoľvek možných ochranných alebo nápravných opatreniach, ktoré môžu tieto fyzické alebo právnické osoby prijať v reakcii na túto hrozbu;

f) nariadiť dotknutým subjektom, aby v primeranej lehote vykonali odporúčania vydané na základe bezpečnostného auditu;

g) nariadiť dotknutým subjektom, aby určeným spôsobom zverejnili aspekty porušovania tejto smernice;

h) uložiť správnu pokutu podľa článku 34 alebo požiadať o jej uloženie príslušné orgány, súdy alebo tribunály v súlade s vnútroštátnym právom, a to popri ktoromkoľvek z opatrení uvedených v písmenách a) až g) tohto odseku.

5. *Článok 32* ods. 6, 7 a 8 sa uplatňuje *mutatis mutandis* na opatrenia dohľadu a presadzovania práva stanovené v tomto článku v súvislosti s dôležitými subjektmi.

6. Členské štáty zabezpečia, aby ich príslušné orgány podľa tejto smernice spolupracovali s relevantnými príslušnými orgánmi dotknutého členského štátu podľa nariadenia (EÚ) 2022/2554. Členské štáty najmä zabezpečia, aby ich príslušné orgány podľa tejto smernice informovali fórum pre dozor zriadený podľa článku 32 ods. 1 nariadenia (EÚ) 2022/2554 pri vykonávaní svojich právomocí dohľadu a presadzovania práva, ktorých cieľom je zabezpečiť, aby dôležitý subjekt, ktorý je identifikovaný ako externý poskytovateľ kritických IKT služieb podľa článku 31 nariadenia (EÚ) 2022/2554, dodržiaval túto smernicu.

Článok 34

Všeobecné podmienky ukladania správnych pokút kľúčovým a dôležitým subjektom

1. Členské štáty zabezpečia, aby správne pokuty uložené kľúčovým a dôležitým subjektom podľa tohto článku v súvislosti s porušeniami tejto smernice boli účinné, primerané a odrádzajúce a zároveň zohľadňovali okolnosti každého jednotlivého prípadu.

2. Správne pokuty sa ukladajú navyše ku ktorémukoľvek z opatrení uvedených v článku 32 ods. 4 písm. a) až h), článku 32 ods. 5 a článku 33 ods. 4 písm. a) až g).

3. Pri rozhodovaní o uložení správnej pokuty, ako aj pri rozhodovaní o jej výške v každom jednotlivom prípade sa náležite zohľadnia aspoň prvky stanovené v článku 32 ods. 7.

4. Členské štáty zabezpečia, aby kľúčovým subjektom v prípade porušenia článku 21 alebo 23 boli v súlade s odsekmi 2 a 3 tohto článku uložené správne pokuty v maximálnej výške aspoň 10 000 000 EUR alebo v maximálnej výške aspoň 2 % celkového celosvetového ročného obratu v predchádzajúcom finančnom roku podniku, ku ktorému kľúčový subjekt patrí, podľa toho, ktorá suma je vyššia.

▼B

5. Členské štáty zabezpečia, aby dôležitým subjektom v prípade porušenia článku 21 alebo 23 boli v súlade s odsekmi 2 a 3 tohto článku uložené správne pokuty v maximálnej výške aspoň 7 000 000 EUR alebo v maximálnej výške aspoň 1,4 % celkového celosvetového ročného obratu v predchádzajúcom finančnom roku podniku, ku ktorému dôležitý subjekt patrí, podľa toho, ktorá suma je vyššia.

6. Členské štáty môžu stanoviť právomoc ukladať pravidelné penále s cieľom prinútiť kľúčový alebo dôležitý subjekt, aby prestal porušovať túto smernicu v súlade s predchádzajúcim rozhodnutím príslušného orgánu.

7. Bez toho, aby boli dotknuté právomoci príslušných orgánov podľa článkov 32 a 33, každý členský štát môže stanoviť pravidlá, či a v akom rozsahu sa správne pokuty môžu uložiť subjektom verejnej správy.

8. Ak sa v právnom systéme členského štátu nestanovujú správne pokuty, uvedený členský štát zabezpečí, aby sa tento článok uplatňoval tak, že uloženie pokuty iniciuje príslušný orgán a uložia ju príslušné vnútroštátne súdy alebo tribunály, pričom sa zabezpečí, aby tieto právne prostriedky nápravy boli účinné a mali rovnocenný účinok ako správne pokuty ukladané príslušnými orgánmi. Ukladané pokuty musia byť v každom prípade účinné, primerané a odrádzajúce. Členský štát oznámi Komisii ustanovenia právnych predpisov, ktoré prijíma podľa tohto odseku, do 17. októbra 2024 a bezodkladne všetky následné pozmeňujúce právne predpisy či zmeny, ktoré sa ich týkajú.

Článok 35

Porušenia povinností, pri ktorých došlo k porušeniu ochrany osobných údajov

1. Ak príslušné orgány počas výkonu dohľadu alebo presadzovania práva zistia, že porušenie povinností stanovených v článkoch 21 a 23 tejto smernice kľúčovým alebo dôležitým subjektom môže mať za následok porušenie ochrany osobných údajov, ako je vymedzené v článku 4 bode 12 nariadenia (EÚ) 2016/679, pričom takéto porušenie sa oznamuje podľa článku 33 uvedeného nariadenia, bez zbytočného odkladu o tom informujú orgány dohľadu podľa článku 55 alebo 56 uvedeného nariadenia.

2. Ak orgány dohľadu uvedené v článku 55 alebo 56 nariadenia (EÚ) 2016/679 uložia správnu pokutu podľa článku 58 ods. 2 písm. i) uvedeného nariadenia, príslušné orgány neuložia správnu pokutu podľa článku 34 tejto smernice za porušenie uvedené v odseku 1 tohto článku spôsobené rovnakým konaním, ktoré bolo dôvodom správnej pokuty podľa článku 58 ods. 2 písm. i) nariadenia (EÚ) 2016/679. Príslušné orgány však môžu uložiť opatrenia na presadzovanie práva stanovené v článku 32 ods. 4 písm. a) až h), v článku 32 ods. 5 a v článku 33 ods. 4 písm. a) až g) tejto smernice.

3. Ak je orgán dohľadu, príslušný podľa nariadenia (EÚ) 2016/679, usadený v inom členskom štáte než príslušný orgán, príslušný orgán informuje orgán dohľadu so sídlom v jeho vlastnom členskom štáte o možnom porušení ochrany údajov podľa odseku 1.

▼B

Článok 36

Sankcie

Členské štáty stanovia pravidlá, pokiaľ ide o sankcie uplatniteľné pri porušení vnútroštátnych opatrení prijatých podľa tejto smernice, a prijmú všetky opatrenia potrebné na zabezpečenie ich uplatňovania. Stanovené sankcie musia byť účinné, primerané a odrádzajúce. Členské štáty o týchto pravidlách a opatreniach do 17. januára 2025 informujú Komisiu a bezodkladne jej oznámia každú nasledujúcu zmenu, ktorá ich ovplyvní.

Článok 37

Vzájomná pomoc

1. Ak subjekt poskytuje služby vo viac ako jednom členskom štáte alebo poskytuje služby v jednom alebo viacerých členských štátoch a jeho siete a informačné systémy sú umiestnené v niektorom inom alebo vo viacerých iných členských štátoch, príslušné orgány dotknutých členských štátov spolupracujú a v prípade potreby si navzájom pomáhajú. Táto spolupráca zahŕňa aspoň tieto prvky:

a) príslušné orgány, ktoré uplatňujú opatrenia dohľadu alebo presadzovania práva v členskom štáte, informujú prostredníctvom jednotného kontaktného miesta príslušné orgány v ostatných dotknutých členských štátoch a konzultujú s nimi prijaté opatrenia dohľadu a presadzovania práva;

b) príslušný orgán môže požiadať iný príslušný orgán, aby prijal opatrenia dohľadu alebo presadzovania práva;

c) príslušný orgán po prijatí odôvodnenej žiadosti od iného príslušného orgánu poskytne tomuto inému príslušnému orgánu vzájomnú pomoc primeranú jeho vlastným zdrojom, aby sa opatrenia dohľadu alebo presadzovania práva mohli vykonávať účinne, efektívne a konzistentne.

Vzájomná pomoc uvedená v prvom pododseku písm. c) sa môže vzťahovať na žiadosti o informácie a na opatrenia v oblasti dohľadu vrátane žiadostí o vykonanie inšpekcií na mieste alebo dohľadu na diaľku, alebo cielených bezpečnostných auditov. Príslušný orgán, ktorému je adresovaná žiadosť o pomoc, túto žiadosť neodmietne, pokiaľ sa nepreukáže, že nemá právomoc poskytnúť požadovanú pomoc, že požadovaná pomoc nie je primeraná úlohám príslušného orgánu v oblasti dohľadu, alebo že sa žiadosť týka informácií alebo zahŕňa činnosti, ktoré by v prípade zverejnenia alebo vykonania boli v rozpore so základnými záujmami členských štátov v oblasti národnej bezpečnosti, verejnej bezpečnosti alebo obrany. Príslušný orgán pred zamietnutím takejto žiadosti konzultuje s ostatnými dotknutými príslušnými orgánmi a v prípade, že o to jeden z dotknutých členských štátov požiada, aj s Komisiou a agentúrou ENISA.

▼B

2. V prípade potreby a po vzájomnej dohode môžu príslušné orgány z rôznych členských štátov vykonávať spoločné opatrenia v oblasti dohľadu.

KAPITOLA VIII

DELEGOVANÉ A VYKONÁVACIE AKTY

Článok 38

Vykonávanie delegovania právomoci

1. Komisii sa udeľuje právomoc prijímať delegované akty za podmienok stanovených v tomto článku.

2. Právomoc prijímať delegované akty uvedené v článku 24 ods. 2 sa Komisii udeľuje na obdobie piatich rokov od 16. januára 2023.

3. Delegovanie právomoci uvedené v článku 24 ods. 2 môže Európsky parlament alebo Rada kedykoľvek odvolať. Rozhodnutím o odvolaní sa ukončuje delegovanie právomoci, ktoré sa v ňom uvádza. Rozhodnutie nadobúda účinnosť dňom nasledujúcim po jeho uverejnení v *Úradnom vestníku Európskej únie* alebo k neskoršiemu dátumu, ktorý je v ňom určený. Nie je ním dotknutá platnosť delegovaných aktov, ktoré už nadobudli účinnosť.

4. Komisia pred prijatím delegovaného aktu konzultuje s expertami určenými jednotlivými členskými štátmi v súlade so zásadami stanovenými v Medziinštitucionálnej dohode z 13. apríla 2016 o lepšej tvorbe práva.

5. Komisia oznamuje delegovaný akt hneď po jeho prijatí súčasne Európskemu parlamentu a Rade.

6. Delegovaný akt prijatý podľa článku 24 ods. 2 nadobudne účinnosť, len ak Európsky parlament alebo Rada voči nemu nevzniesli námietku v lehote dvoch mesiacov odo dňa oznámenia uvedeného aktu Európskemu parlamentu a Rade alebo ak pred uplynutím uvedenej lehoty Európsky parlament a Rada informovali Komisiu o svojom rozhodnutí nevzniesť námietku. Na podnet Európskeho parlamentu alebo Rady sa táto lehota predĺži o dva mesiace.

Článok 39

Postup výboru

1. Komisii pomáha výbor. Uvedený výbor je výborom v zmysle nariadenia (EÚ) č. 182/2011.

▼B

2. Ak sa odkazuje na tento odsek, uplatňuje sa článok 5 nariadenia (EÚ) č. 182/2011.

3. Ak sa má stanovisko výboru získať písomným postupom, uvedený postup sa ukončí bez výsledku, ak tak v rámci lehoty na vydanie stanoviska rozhodne predseda výboru alebo ak o to požiada člen výboru.

KAPITOLA IX

ZÁVEREČNÉ USTANOVENIA

Článok 40

Preskúmanie

Komisia do 17. októbra 2027 a následne každých 36 mesiacov preskúma fungovanie tejto smernice a podá o tom správu Európskemu parlamentu a Rade. V správe sa posúdi najmä relevantnosť veľkosti dotknutých subjektov a odvetví, pododvetví a typov subjektu uvedených v prílohách I a II pre fungovanie hospodárstva a spoločnosti v súvislosti s kybernetickou bezpečnosťou. 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. K správe sa podľa potreby pripojí legislatívny návrh.

Článok 41

Transpozícia

1. Členské štáty prijmú a uverejnia do 17. októbra 2024 opatrenia potrebné na dosiahnutie súladu s touto smernicou. Bezodkladne o tom informujú Komisiu.

Tieto opatrenia sa uplatňujú od 18. októbra 2024.

2. Členské štáty uvedú priamo v prijatých opatreniach uvedených v odseku 1 alebo pri ich úradnom uverejnení odkaz na túto smernicu. Podrobnosti o odkaze upravia členské štáty.

Článok 42

Zmena nariadenia (EÚ) č. 910/2014

V nariadení (EÚ) č. 910/2014 sa vypúšťa článok 19 s účinnosťou od 18. októbra 2024.

Článok 43

Zmena smernice (EÚ) 2018/1972

V smernici (EÚ) 2018/1972 sa vypúšťajú články 40 a 41 s účinnosťou od 18. októbra 2024.

▼B

Článok 44

Zrušenie

Smernica (EÚ) 2016/1148 sa zrušuje s účinnosťou od 18. októbra 2024.

Odkazy na zrušenú smernicu sa považujú za odkazy na túto smernicu a znejú v súlade s tabuľkou zhody uvedenou v prílohe III.

Článok 45

Nadobudnutie účinnosti

Táto smernica nadobúda účinnosť dvadsiatym dňom nasledujúcim po jej uverejnení v *Úradnom vestníku Európskej únie*.

Článok 46

Adresáti

Táto smernica je určená členským štátom.

▼B

PRÍLOHA I

ODVETVIA S VYSOKOU ÚROVŇOU KRITICKOSTI

Odvetvie	Pododvetvie	Typ subjektu
1. Energetika	a) elektrická energia	— elektroenergetické podniky, ako sú vymedzené v článku 2 bode 57 smernice Európskeho parlamentu a Rady (EÚ) 2019/944 ([1]), ktoré vykonávajú funkciu „dodávky“, ako je vymedzená v článku 2 bode 12 uvedenej smernice
		— prevádzkovatelia distribučnej sústavy, ako sú vymedzení v článku 2 bode 29 smernice (EÚ) 2019/944
		— prevádzkovatelia prenosovej sústavy, ako sú vymedzení v článku 2 bode 35 smernice (EÚ) 2019/944
		— výrobcovia, ako sú vymedzení v článku 2 bode 38 smernice (EÚ) 2019/944
		— nominovaní organizátori trhu s elektrinou, ako sú vymedzení v článku 2 bode 8 nariadenia Európskeho parlamentu a Rady (EÚ) 2019/943 ([2]) — účastníci trhu, ako sú vymedzení v článku 2 bode 25 nariadenia (EÚ) 2019/943, ktorí poskytujú služby agregácie, riadenia odberu alebo uskladňovania energie, ako sú vymedzené v článku 2 bodoch 18, 20 a 59 smernice (EÚ) 2019/944 — prevádzkovatelia nabíjacieho bodu, ktorí sú zodpovední za správu a prevádzku nabíjacieho bodu, ktorý koncovým používateľom poskytuje nabíjaciu službu, a to aj v mene a na účet poskytovateľa služieb mobility
	b) diaľkové vykurovanie a chladenie	— prevádzkovatelia diaľkového vykurovania alebo diaľkového chladenia, ako sú vymedzení v článku 2 bode 19 smernice Európskeho parlamentu a Rady (EÚ) 2018/2001 ([3])
	c) ropa	— prevádzkovatelia ropovodov
		— prevádzkovatelia zariadení na ťažbu, rafinovanie a spracovanie ropy, jej skladovanie a prepravu
		— ústredné subjekty správy zásob, ako sú vymedzené v článku 2 písm. f) smernice Rady 2009/119/ES ([4])
	d) plyn	— dodávateľské podniky, ako sú vymedzené v článku 2 bode 8 smernice Európskeho parlamentu a Rady 2009/73/ES ([5])
		— prevádzkovatelia distribučnej siete, ako sú vymedzení v článku 2 bode 6 smernice 2009/73/ES
		— prevádzkovatelia prepravnej siete, ako sú vymedzení v článku 2 bode 4 smernice 2009/73/ES
		— prevádzkovatelia zásobníkov, ako sú vymedzení v článku 2 bode 10 smernice 2009/73/ES

▼B

Odvetvie	Pododvetvie	Typ subjektu
		— prevádzkovatelia zariadení LNG, ako sú vymedzení v článku 2 bode 12 smernice 2009/73/ES
		— plynárenské podniky, ako sú vymedzené v článku 2 bode 1 smernice 2009/73/ES
		— prevádzkovatelia zariadení na rafinovanie a spracovanie zemného plynu
	e) vodík	— prevádzkovatelia zariadení na výrobu, skladovanie a prepravu vodíka
2. Doprava	a) letecká doprava	— leteckí dopravcovia, ako sú vymedzení v článku 3 bode 4 nariadenia (ES) č. 300/2008, využívaní na komerčné účely
		— riadiace orgány letiska, ako sú vymedzené v článku 2 bode 2 smernice Európskeho parlamentu a Rady 2009/12/ES ([6]), letiská, ako sú vymedzené v článku 2 bode 1 uvedenej smernice, vrátane hlavných letísk uvedených v oddiele 2 prílohy II k nariadeniu Európskeho parlamentu a Rady (EÚ) č. 1315/2013 ([7]), a subjekty prevádzkujúce pomocné zariadenia nachádzajúce sa na letiskách
		— prevádzkovatelia kontroly riadenia dopravy poskytujúci služby riadenia letovej prevádzky (ATC), ako sú vymedzení v článku 2 bode 1 nariadenia Európskeho parlamentu a Rady (ES) č. 549/2004 ([8])
	b) železničná doprava	— manažéri infraštruktúry, ako sú vymedzení v článku 3 bode 2 smernice Európskeho parlamentu a Rady 2012/34/EÚ ([9])
		— železničné podniky, ako sú vymedzené v článku 3 bode 1 smernice 2012/34/EÚ, vrátane prevádzkovateľov servisných zariadení, ako sú vymedzené v článku 3 bode 12 uvedenej smernice
	c) vodná doprava	— spoločnosti prevádzkujúce vnútrozemskú, námornú a pobrežnú osobnú a nákladnú vodnú dopravu, ako sú vymedzené pre námornú dopravu v prílohe I k nariadeniu Európskeho parlamentu a Rady (ES) č. 725/2004 ([10]), bez jednotlivých plavidiel, ktoré tieto spoločnosti prevádzkujú

▼B

Odvetvie	Pododvetvie	Typ subjektu
		— riadiace orgány prístavov, ako sú vymedzené v článku 3 bode 1 smernice Európskeho parlamentu a Rady 2005/65/ES ([11]), vrátane ich prístavných zariadení, ako sú vymedzené v článku 2 bode 11 nariadenia (ES) č. 725/2004, a subjekty prevádzkujúce činnosti a zariadenia v rámci prístavu
		— prevádzkovatelia plavebno-prevádzkových služieb (VTS), ako sú vymedzené v článku 3 písm. o) smernice Európskeho parlamentu a Rady 2002/59/ES ([12])
	d) cestná doprava	— cestné orgány, ako sú vymedzené v článku 2 bode 12 delegovaného nariadenia Komisie (EÚ) 2015/962 ([13]), zodpovedné za kontrolu riadenia dopravy, s výnimkou verejných subjektov, v prípade ktorých je riadenie dopravy alebo prevádzkovanie inteligentných dopravných systémov nepodstatnou súčasťou ich celkovej činnosti
		— prevádzkovatelia inteligentných dopravných systémov, ako sú vymedzené v článku 4 bode 1 smernice Európskeho parlamentu a Rady 2010/40/EÚ ([14])
3. Bankovníctvo		úverové inštitúcie, ako sú vymedzené v článku 4 bode 1 nariadenia Európskeho parlamentu a Rady (EÚ) č. 575/2013 ([15])
4. Infraštruktúra finančných trhov		— prevádzkovatelia obchodných miest, ako sú vymedzení v článku 4 bode 24 smernice Európskeho parlamentu a Rady 2014/65/EÚ ([16])
		— centrálne protistrany (CCP), ako sú vymedzené v článku 2 bode 1 nariadenia Európskeho parlamentu a Rady (EÚ) č. 648/2012 ([17])
5. Zdravotníctvo		— poskytovatelia zdravotnej starostlivosti, ako sú vymedzení v článku 3 písm. g) smernice Európskeho parlamentu a Rady 2011/24/EÚ ([18])
		— referenčné laboratóriá EÚ uvedené v článku 15 nariadenia Európskeho parlamentu a Rady (EÚ) .../... ([19])
		— subjekty vykonávajúce činnosti vo výskume a vývoji liekov, ako sú vymedzené v článku 1 bode 2 smernice Európskeho parlamentu a Rady 2001/83/ES ([20]) — subjekty vyrábajúce základné farmaceutické výrobky a farmaceutické prípravky uvedené v sekcii C divízii 21 NACE Rev. 2 — subjekty vyrábajúce zdravotnícke pomôcky považované za kritické v núdzovej situácii v oblasti verejného zdravia (ďalej len „zoznam kritických pomôcok v núdzovej situácii v oblasti verejného zdravia“) v zmysle článku 22 nariadenia Európskeho parlamentu a Rady (EÚ) 2022/123 ([21])

▼B

Odvetvie	Pododvetvie	Typ subjektu
6. Pitná voda		dodávatelia a distribútori vody určenej na ľudskú spotrebu, ako je vymedzená v článku 2 bode 1 písm. a) smernice Európskeho parlamentu a Rady (EÚ) 2020/2184 ([22]), s výnimkou distribútorov, pre ktorých je distribúcia vody určenej na ľudskú spotrebu nepodstatnou súčasťou ich celkovej činnosti v oblasti distribúcie iných komodít a tovaru
7. Odpadová voda		podniky zaoberajúce sa zberom, likvidáciou alebo úpravou komunálnych odpadových vôd, odpadových vôd z domácností alebo priemyselných odpadových vôd, ako sú vymedzené v článku 2 bodoch 1, 2 a 3 smernice Rady 91/271/EHS ([23]), s výnimkou podnikov, pre ktoré je zber, likvidácia alebo úprava komunálnych odpadových vôd, odpadových vôd z domácností alebo priemyselných odpadových vôd nepodstatnou súčasťou ich celkovej činnosti
8. Digitálna infraštruktúra		— poskytovatelia internetových prepojovacích uzlov
		— poskytovatelia služieb DNS, s výnimkou prevádzkovateľov koreňových názvových serverov
		— správcovia názvov TLD
		— poskytovatelia služieb cloud computingu
		— poskytovatelia služieb dátového centra
		— poskytovatelia sietí na sprístupňovanie obsahu
		— poskytovatelia dôveryhodných služieb
		— poskytovatelia verejných elektronických komunikačných sietí
		— poskytovatelia verejne dostupných elektronických komunikačných služieb
9. Riadenie služieb IKT (medzi podnikmi)		— poskytovatelia riadených služieb — poskytovatelia riadených bezpečnostných služieb
10. Verejná správa		— subjekty verejnej správy na úrovni ústrednej štátnej správy, ako ich vymedzuje členský štát v súlade s vnútroštátnym právom
		— subjekty verejnej správy na regionálnej úrovni, ako ich vymedzuje členský štát v súlade s vnútroštátnym právom

▼B

Odvetvie	Pododvetvie	Typ subjektu
11. Vesmír		prevádzkovatelia pozemnej infraštruktúry, ktorú vlastnia, riadia a prevádzkujú členské štáty alebo súkromné subjekty, ktorí prispievajú k poskytovaniu vesmírnych služieb, s výnimkou poskytovateľov verejných elektronických komunikačných sietí

([1]) Smernica Európskeho parlamentu a Rady (EÚ) 2019/944 z 5. júna 2019 o spoločných pravidlách pre vnútorný trh s elektrinou a o zmene smernice 2012/27/EÚ (Ú. v. EÚ L 158, 14.6.2019, s. 125).
([2]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/943 z 5. júna 2019 o vnútornom trhu s elektrinou (Ú. v. EÚ L 158, 14.6.2019, s. 54).
([3]) Smernica Európskeho parlamentu a Rady (EÚ) 2018/2001 z 11. decembra 2018 o podpore využívania energie z obnoviteľných zdrojov (Ú. v. EÚ L 328, 21.12.2018, s. 82).
([4]) Smernica Rady 2009/119/ES zo 14. septembra 2009, ktorou sa členským štátom ukladá povinnosť udržiavať minimálne zásoby ropy a/alebo ropných výrobkov (Ú. v. EÚ L 265, 9.10.2009, s. 9).
([5]) Smernica Európskeho parlamentu a Rady 2009/73/ES z 13. júla 2009 o spoločných pravidlách pre vnútorný trh so zemným plynom, ktorou sa zrušuje smernica 2003/55/ES (Ú. v. EÚ L 211, 14.8.2009, s. 94).
([6]) Smernica Európskeho parlamentu a Rady 2009/12/ES z 11. marca 2009 o letiskových poplatkoch (Ú. v. EÚ L 70, 14.3.2009, s. 11).
([7]) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 1315/2013 z 11. decembra 2013 o usmerneniach Únie pre rozvoj transeurópskej dopravnej siete a o zrušení rozhodnutia č. 661/2010/EÚ (Ú. v. EÚ L 348, 20.12.2013, s. 1).
([8]) Nariadenie Európskeho parlamentu a Rady (ES) č. 549/2004 z 10. marca 2004, ktorým sa stanovuje rámec na vytvorenie jednotného európskeho neba (rámcové nariadenie) (Ú. v. EÚ L 96, 31.3.2004, s. 1).
([9]) Smernica Európskeho parlamentu a Rady 2012/34/EÚ z 21. novembra 2012, ktorou sa zriaďuje jednotný európsky železničný priestor (Ú. v. EÚ L 343, 14.12.2012, s. 32).
([10]) Nariadenie Európskeho parlamentu a Rady (ES) č. 725/2004 z 31. marca 2004 o zvýšení bezpečnosti lodí a prístavných zariadení (Ú. v. EÚ L 129, 29.4.2004, s. 6).
([11]) Smernica Európskeho parlamentu a Rady 2005/65/ES z 26. októbra 2005 o zvýšení bezpečnosti prístavov (Ú. v. EÚ L 310, 25.11.2005, s. 28).
([12]) Smernica Európskeho parlamentu a Rady 2002/59/ES z 27. júna 2002, ktorou sa zriaďuje monitorovací a informačný systém spoločenstva pre lodnú dopravu a ktorou sa zrušuje smernica Rady 93/75/EHS (Ú. v. ES L 208, 5.8.2002, s. 10).
([13]) Delegované nariadenie Komisie (EÚ) 2015/962 z 18. decembra 2014, ktorým sa dopĺňa smernica Európskeho parlamentu a Rady 2010/40/EÚ, pokiaľ ide o poskytovanie informačných služieb o doprave v reálnom čase v celej EÚ (Ú. v. EÚ L 157, 23.6.2015, s. 21).
([14]) Smernica Európskeho parlamentu a Rady 2010/40/EÚ zo 7. júla 2010 o rámci na zavedenie inteligentných dopravných systémov v oblasti cestnej dopravy a na rozhrania s inými druhmi dopravy (Ú. v. EÚ L 207, 6.8.2010, s. 1).
([15]) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 575/2013 z 26. júna 2013 o prudenciálnych požiadavkách na úverové inštitúcie a o zmene nariadenia (EÚ) č. 648/2012 (Ú. v. EÚ L 176, 27.6.2013, s. 1).
([16]) Smernica Európskeho parlamentu a Rady 2014/65/EÚ z 15. mája 2014 o trhoch s finančnými nástrojmi, ktorou sa mení smernica 2002/92/ES a smernica 2011/61/EÚ (Ú. v. EÚ L 173, 12.6.2014, s. 349).
([17]) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 648/2012 zo 4. júla 2012 o mimoburzových derivátoch, centrálnych protistranách a archívoch obchodných údajov (Ú. v. EÚ L 201, 27.7.2012, s. 1).
([18]) Smernica Európskeho parlamentu a Rady 2011/24/EÚ z 9. marca 2011 o uplatňovaní práv pacientov pri cezhraničnej zdravotnej starostlivosti (Ú. v. EÚ L 88, 4.4.2011, s. 45).
([19]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2371 z 23. novembra 2022 o závažných cezhraničných ohrozeniach zdravia, ktorým sa zrušuje rozhodnutie č. 1082/2013/EÚ (Ú. v. EÚ L 314, 6.12.2022, s. 26).
([20]) Smernica Európskeho parlamentu a Rady 2001/83/ES zo 6. novembra 2001, ktorou sa ustanovuje zákonník spoločenstva o humánnych liekoch (Ú. v. ES L 311, 28.11.2001, s. 67).
([21]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/123 z 25. januára 2022 o posilnenej úlohe Európskej agentúry pre lieky z hľadiska pripravenosti na krízy a krízového riadenia v oblasti liekov a zdravotníckych pomôcok (Ú. v. EÚ L 20, 31.1.2022, s. 1).
([22]) Smernica Európskeho parlamentu a Rady (EÚ) 2020/2184 zo 16. decembra 2020 o kvalite vody určenej na ľudskú spotrebu (Ú. v. EÚ L 435, 23.12.2020, s. 1).
([23]) Smernica Rady 91/271/EHS z 21. mája 1991 o čistení komunálnych odpadových vôd (Ú. v. ES L 135, 30.5.1991, s. 40).

▼B

PRÍLOHA II

INÉ KRITICKÉ ODVETVIA

Odvetvie	Pododvetvie	Typ subjektu
1. Poštové a kuriérske služby		poskytovatelia poštových služieb, ako sú vymedzení v článku 2 bode 1a smernice 97/67/ES, vrátane poskytovateľov kuriérskych služieb
2. Odpadové hospodárstvo		podniky vykonávajúce činnosti nakladania s odpadom, ako je vymedzené v článku 3 bodu 9 smernice Európskeho parlamentu a Rady 2008/98/ES ([1]), s výnimkou podnikov, pre ktoré nakladanie s odpadom nepredstavuje hlavnú hospodársku činnosť
3. Výroba a distribúcia chemických látok		podniky vyrábajúce látky a distribuujúce látky alebo zmesi, ako je uvedené v článku 3 bodoch 9 a 14 nariadenia Európskeho parlamentu a Rady (ES) č. 1907/2006 ([2]), a podniky vyrábajúce výrobky, ako sú vymedzené v článku 3 bode 3 uvedeného nariadenia, z látok a zmesí
4. Výroba, spracovanie a distribúcia potravín		potravinárske podniky, ako sú vymedzené v článku 3 bode 2 nariadenia Európskeho parlamentu a Rady (ES) č. 178/2002 ([3]), ktoré sa zaoberajú veľkoobchodnou distribúciou a priemyselnou výrobou a spracovaním
5. Výroba	a) výroba zdravotníckych pomôcok a diagnostických zdravotníckych pomôcok *in vitro*	subjekty vyrábajúce zdravotnícke pomôcky, ako sú vymedzené v článku 2 bode 1 nariadenia Európskeho parlamentu a Rady (EÚ) 2017/745 ([4]), a subjekty vyrábajúce diagnostické zdravotnícke pomôcky in vitro, ako sú vymedzené v článku 2 bode 2 nariadenia Európskeho parlamentu a Rady (EÚ) 2017/746 ([5]), s výnimkou subjektov vyrábajúcich zdravotnícke pomôcky uvedených v piatej zarážke bodu 5 prílohy I tejto smernice
	b) výroba počítačových, elektronických a optických výrobkov	subjekty vykonávajúce akúkoľvek hospodársku činnosť uvedenú v sekcii C divízii 26 NACE Rev. 2
	c) výroba elektrických zariadení	subjekty vykonávajúce akúkoľvek hospodársku činnosť uvedenú v sekcii C divízii 27 NACE Rev. 2

▼B

Odvetvie	Pododvetvie	Typ subjektu
	d) výroba strojov a zariadení i. n.	subjekty vykonávajúce akúkoľvek hospodársku činnosť uvedenú v sekcii C divízii 28 NACE Rev. 2
	e) výroba motorových vozidiel, návesov a prívesov	subjekty vykonávajúce akúkoľvek hospodársku činnosť uvedenú v sekcii C divízii 29 NACE Rev. 2
	f) výroba ostatných dopravných prostriedkov	subjekty vykonávajúce akúkoľvek hospodársku činnosť uvedenú v sekcii C divízii 30 NACE Rev. 2
6. Poskytovatelia digitálnych služieb		— poskytovatelia online trhov
		— poskytovatelia internetových vyhľadávačov
		— poskytovatelia platforiem služieb sociálnej siete
7. Výskum		výskumné organizácie

([1]) Smernica Európskeho parlamentu a Rady 2008/98/ES z 19. novembra 2008 o odpade a o zrušení určitých smerníc (Ú. v. EÚ L 312, 22.11.2008, s. 3).
([2]) Nariadenie Európskeho parlamentu a Rady (ES) č. 1907/2006 z 18. decembra 2006 o registrácii, hodnotení, autorizácii a obmedzovaní chemikálií (REACH) a o zriadení Európskej chemickej agentúry, o zmene a doplnení smernice 1999/45/ES a o zrušení nariadenia Rady (EHS) č. 793/93 a nariadenia Komisie (ES) č. 1488/94, smernice Rady 76/769/EHS a smerníc Komisie 91/155/EHS, 93/67/EHS, 93/105/ES a 2000/21/ES (Ú. v. EÚ L 396, 30.12.2006, s. 1).
([3]) Nariadenie Európskeho parlamentu a Rady (ES) č. 178/2002 z 28. januára 2002, ktorým sa ustanovujú všeobecné zásady a požiadavky potravinového práva, zriaďuje Európsky úrad pre bezpečnosť potravín a stanovujú postupy v záležitostiach bezpečnosti potravín (Ú. v. ES L 31, 1.2.2002, s. 1).
([4]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2017/745 z 5. apríla 2017 o zdravotníckych pomôckach, zmene smernice 2001/83/ES, nariadenia (ES) č. 178/2002 a nariadenia (ES) č. 1223/2009 a o zrušení smerníc Rady 90/385/EHS a 93/42/EHS (Ú. v. EÚ L 117, 5.5.2017, s. 1).
([5]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2017/746 z 5. apríla 2017 o diagnostických zdravotníckych pomôckach in vitro a o zrušení smernice 98/79/ES a rozhodnutia Komisie 2010/227/EÚ (Ú. v. EÚ L 117, 5.5.2017, s. 176).

▼B

PRÍLOHA III

TABUĽKA ZHODY

Smernica (EÚ) 2016/1148	Táto smernica
článok 1 ods. 1	článok 1 ods. 1
článok 1 ods. 2	článok 1 ods. 2
článok 1 ods. 3	–
článok 1 ods. 4	článok 2 ods. 12
článok 1 ods. 5	článok 2 ods. 13
článok 1 ods. 6	článok 2 ods. 6 a 11
článok 1 ods. 7	článok 4
článok 2	článok 2 ods. 14
článok 3	článok 5
článok 4	článok 6
článok 5	–
článok 6	–
článok 7 ods. 1	článok 7 ods. 1 a 2
článok 7 ods. 2	článok 7 ods. 4
článok 7 ods. 3	článok 7 ods. 3
článok 8 ods. 1 až 5	článok 8 ods. 1 až 5
článok 8 ods. 6	článok 13 ods. 4
článok 8 ods. 7	článok 8 ods. 6
článok 9 ods. 1, 2 a 3	článok 10 ods. 1, 2 a 3
článok 9 ods. 4	článok 10 ods. 9
článok 9 ods. 5	článok 10 ods. 10
článok 10 ods. 1, 2 a 3 prvý pododsek	článok 13 ods. 1, 2 a 3
článok 10 ods. 3 druhý pododsek	článok 23 ods. 9
článok 11 ods. 1	článok 14 ods. 1 a 2
článok 11 ods. 2	článok 14 ods. 3
článok 11 ods. 3	článok 14 ods. 4 prvý pododsek písm. a) až q) a písm. s) a ods. 7

▼B

Smernica (EÚ) 2016/1148	Táto smernica
článok 11 ods. 4	článok 14 ods. 4 prvý pododsek písm. r) a druhý pododsek
článok 11 ods. 5	článok 14 ods. 8
článok 12 ods. 1 až 5	článok 15 ods. 1 až 5
článok 13	článok 17
článok 14 ods. 1 a 2	článok 21 ods. 1 až 4
článok 14 ods. 3	článok 23 ods. 1
článok 14 ods. 4	článok 23 ods. 3
článok 14 ods. 5	článok 23 ods. 5, 6 a 8
článok 14 ods. 6	článok 23 ods. 7
článok 14 ods. 7	článok 23 ods. 11
článok 15 ods. 1	článok 31 ods. 1
článok 15 ods. 2 prvý pododsek písm. a)	článok 32 ods. 2 písm. e)
článok 15 ods. 2 prvý pododsek písm. b)	článok 32 ods. 2 písm. g)
článok 15 ods. 2 druhý pododsek	článok 32 ods. 3
článok 15 ods. 3	článok 32 ods. 4 písm. b)
článok 15 ods. 4	článok 31 ods. 3
článok 16 ods. 1 a 2	článok 21 ods. 1 až 4
článok 16 ods. 3	článok 23 ods. 1
článok 16 ods. 4	článok 23 ods. 3
článok 16 ods. 5	–
článok 16 ods. 6	článok 23 ods. 6
článok 16 ods. 7	článok 23 ods. 7
článok 16 ods. 8 a 9	článok 21 ods. 5 a článok 23 ods. 11
článok 16 ods. 10	–
článok 16 ods. 11	článok 2 ods. 1, 2 a 3
článok 17 ods. 1	článok 33 ods. 1
článok 17 ods. 2 písm. a)	článok 32 ods. 2 písm. e)
článok 17 ods. 2 písm. b)	článok 32 ods. 4 písm. b)

▼B

Smernica (EÚ) 2016/1148	Táto smernica
článok 17 ods. 3	článok 37 ods. 1 písm. a) a b)
článok 18 ods. 1	článok 26 ods. 1 písm. b) a ods. 2
článok 18 ods. 2	článok 26 ods. 3
článok 18 ods. 3	článok 26 ods. 4
článok 19	článok 25
článok 20	článok 30
článok 21	článok 36
článok 22	článok 39
článok 23	článok 40
článok 24	–
článok 25	článok 41
článok 26	článok 45
článok 27	článok 46
príloha I bod 1	článok 11 ods. 1
príloha I bod 2 písm. a) podbody i) až iv)	článok 11 ods. 2 písm. a) až d)
príloha I bod 2 písm. a) podbod v)	článok 11 ods. 2 písm. f)
príloha I bod 2 písm. b)	článok 11 ods. 4
príloha I bod 2 písm. c) podbody i) a ii)	článok 11 ods. 5 písm. a)
príloha II	príloha I
príloha III body 1 a 2	príloha II bod 6
príloha III bod 3	príloha I bod 8