



EURÓPSKA
KOMISIA

V Bruseli 16. 12. 2020
COM(2020) 823 final

2020/0359 (COD)

Návrh

SMERNICA EURÓPSKEHO PARLAMENTU A RADY

**o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti
v Únii a o zrušení smernice (EÚ) 2016/1148**

(Text s významom pre EHP)

{SEC(2020) 430 final} - {SWD(2020) 344 final} - {SWD(2020) 345 final}

DÔVODOVÁ SPRÁVA

1. KONTEXT NÁVRHU

• Dôvody a ciele návrhu

Tento návrh je súčasťou balíka opatrení na ďalšie zlepšenie odolnosti a kapacít, pokiaľ ide o reakcie na incidenty verejných a súkromných subjektov, príslušných orgánov a Únie ako celku, v oblasti kybernetickej bezpečnosti a ochrany kritickej infraštruktúry. Je v súlade s prioritami Komisie pripraviť Európu na digitálny vek a vybudovať perspektívne hospodárstvo, ktoré bude slúžiť ľuďom. Kybernetická bezpečnosť je prioritou, pokiaľ ide o reakciu Komisie na krízu spôsobenú pandémiou COVID-19. Balík opatrení zahŕňa novú stratégiu v oblasti kybernetickej bezpečnosti, ktorej cieľom je posilniť strategickú autonómiu Únie zameranú na zlepšenie jej odolnosti a spoločnej reakcie a na vybudovanie otvoreného a globálneho internetu. Napokon balík zahŕňa návrh smernice o odolnosti kritických prevádzkovateľov základných služieb, ktorého cieľom je zmierniť fyzické hrozby voči takýmto prevádzkovateľom.

Tento návrh vychádza zo smernice (EÚ) 2016/1148 o bezpečnosti sietí a informačných systémov (smernica NIS) a zrušuje ju, pričom táto smernica je prvým právnym predpisom o kybernetickej bezpečnosti platným v celej EÚ a poskytuje právne opatrenia na zvyšovanie celkovej úrovne kybernetickej bezpečnosti v Únii. Smernica NIS 1. prispela k zlepšeniu spôsobilostí v oblasti kybernetickej bezpečnosti na vnútroštátnej úrovni tým, že sa v nej od členských štátov vyžaduje prijatie vnútroštátnych stratégií v oblasti kybernetickej bezpečnosti a vymenovanie orgánov kybernetickej bezpečnosti; 2. zvýšila mieru spolupráce medzi členskými štátmi na úrovni Únie zriadením rôznych fór na uľahčenie výmeny strategických a operačných informácií a 3. zlepšila kybernetickú odolnosť verejných a súkromných subjektov v siedmich špecifických odvetviach (energetika, doprava, bankovníctvo, infraštruktúra finančných trhov, zdravotníctvo, dodávka a distribúcia pitnej vody a digitálne infraštruktúry) a v troch digitálnych službách (online trhy, internetové vyhľadávače a služby cloud computingu) tým, že sa v nej od členských štátov vyžaduje, aby zabezpečili, že prevádzkovatelia základných služieb a poskytovatelia digitálnych služieb zavedú požiadavky v oblasti kybernetickej bezpečnosti a budú oznamovať incidenty.

Návrhom sa modernizuje existujúci právny rámec, pričom sa zohľadňuje rastúca digitalizácia vnútorného trhu počas posledných rokov a vyvíjajúce sa hrozby v oblasti kybernetickej bezpečnosti. Vývoj v oboch oblastiach sa od vypuknutia krízy spôsobenej pandémiou COVID-19 ďalej zintenzívnili. Návrh sa zaoberá aj niekoľkými nedostatkami, ktoré bránili využiť plný potenciál smernice NIS.

Smernica NIS, ktorá viedla k významnej zmene v zmýšľaní o kybernetickej bezpečnosti, ako aj v inštitucionálnom a regulačnom prístupe ku kybernetickej bezpečnosti v mnohých členských štátoch, aj napriek svojim významným výsledkom už ukázala svoje obmedzenia. Digitálna transformácia spoločnosti (posilnená krízou spôsobenou pandémiou COVID-19) rozšírila panorámu hrozieb a prináša nové výzvy, ktoré si vyžadujú prispôbené a inovačné reakcie. Počet kybernetických útokov naďalej narastá, pričom sú tieto útoky čoraz dômyselnejšie a pochádzajú zo širokej škály zdrojov v rámci EÚ aj mimo nej.

V rámci hodnotenia o fungovaní smernice NIS, ktoré bolo vykonané na účely posúdenia vplyvu, sa identifikovali tieto problémy: 1. nízka úroveň kybernetickej odolnosti podnikov pôsobiacich v EÚ; 2. nejednotná úroveň odolnosti v jednotlivých členských štátoch a odvetviach; a 3. nízka úroveň spoločnej situačnej informovanosti a nedostatočná spoločná reakcia na krízu. Napríklad určité veľké nemocnice v členskom štáte nepatria do rozsahu pôsobnosti smernice NIS, a preto sa od nich nevyžaduje, aby vykonávali z nej vyplývajúce

bezpečnostné opatrenia, zatiaľ čo v inom členskom štáte sa na takmer každého jedného poskytovateľa zdravotnej starostlivosti v krajine vzťahujú bezpečnostné požiadavky smernice NIS.

Návrh sa ako iniciatíva v rámci Programu regulačnej vhodnosti a efektívnosti (REFIT) zameriava na zníženie regulačného zaťaženia pre príslušné orgány, ako aj nákladov na dodržiavanie predpisov pre verejné a súkromné subjekty. To sa predovšetkým dosiahne zrušením povinnosti príslušných orgánov identifikovať prevádzkovateľov základných služieb a zvýšením úrovne harmonizácie požiadaviek týkajúcich sa bezpečnosti a oznamovania s cieľom uľahčiť dodržiavanie predpisov pre subjekty poskytujúce cezhraničné služby. Príslušné orgány zároveň dostanú nové úlohy vrátane dohľadu nad subjektmi v odvetviach, na ktoré sa zatiaľ nevzťahuje smernica NIS.

- **Súlad s existujúcimi ustanoveniami v tejto oblasti politiky**

Tento návrh je súčasťou širšieho súboru existujúcich právnych nástrojov a pripravovaných iniciatív na úrovni Únie, ktoré majú za cieľ zvýšiť odolnosť verejných a súkromných subjektov proti hrozbám.

V oblasti kybernetickej bezpečnosti je to najmä smernica (EÚ) 2018/1972, ktorou sa stanovuje európsky kódex elektronických komunikácií (ktorej ustanovenia týkajúce sa kybernetickej bezpečnosti nahradia ustanovenia tohto návrhu) a návrh nariadenia o digitálnej prevádzkovej odolnosti finančného sektora [COM(2020) 595 final], ktoré sa bude považovať za *lex specialis* vo vzťahu k tomuto návrhu, keď oba akty nadobudnú účinnosť.

V oblasti fyzickej bezpečnosti sa týmto návrhom dopĺňa návrh smernice o odolnosti kritických subjektov, ktorou sa reviduje smernica 2008/114/ES o identifikácii a označení európskych kritických infraštruktúr a zhodnotení potreby zlepšiť ich ochranu (smernica ECI), ktorou sa ustanovuje postup Únie na identifikáciu a označenie európskych kritických infraštruktúr a stanovuje sa prístup na zlepšenie ich ochrany. V júli 2020 Komisia prijala stratégiu EÚ pre bezpečnostnú úniu¹, v ktorej uznala zvýšené prepojenie a vzájomnú závislosť medzi fyzickými a digitálnymi infraštruktúrami. Zdôraznila sa v nej potreba ucelenejšieho a konzistentnejšieho prístupu medzi smernicou ECI a smernicou (EÚ) 2016/1148, ktorá sa týka opatrení na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii.

Návrh je preto úzko zosúladený s návrhom smernice o odolnosti kritických subjektov, ktorého cieľom je posilniť odolnosť kritických subjektov proti fyzickým hrozbám vo veľkom počte odvetví. Cieľom návrhu je zabezpečiť, aby príslušné orgány v zmysle oboch právnych aktov prijali doplnkové opatrenia a podľa potreby si vymieňali informácie, pokiaľ ide o kybernetickú a nekybernetickú odolnosť, a aby mimoriadne kritickí prevádzkovatelia v odvetviach, ktoré sa v tomto návrhu považujú za „kľúčové“, takisto podliehali povinnostiam súvisiacim so všeobecnejším zvyšovaním odolnosti s dôrazom na nekybernetické riziká.

- **Súlad s ostatnými politikami Únie**

Ako sa stanovuje v oznámení Komisie „Formovanie digitálnej budúcnosti Európy“², je pre Európu kľúčové využívať všetky výhody digitálneho veku a posilniť svoju priemyselnú

¹ COM(2020) 605 final.

² COM(2020) 67 final.

a inovačnú kapacitu v rámci bezpečných a etických hraníc. V rámci Európskej dátovej stratégie sa stanovujú štyri piliere – ochrana údajov, základné práva, bezpečnosť a kybernetická bezpečnosť – ktoré sú základnými predpokladmi pre spoločnosť posilnenú využívaním údajov.

V uznesení z 12. marca 2019 Európsky parlament „[...] vyzýva Komisiu, aby posúdila potrebu ďalšieho rozšírenia pôsobnosti smernice NIS na ďalšie kritické odvetvia a služby, na ktoré sa nevzťahujú osobitné odvetvové právne predpisy“.³ Rada vo svojich záveroch z 9. júna 2020 uvítala „[...] plány Komisie zabezpečiť konzistentné pravidlá pre účastníkov trhu a uľahčiť bezpečnú, spoľahlivú a vhodnú výmenu informácií o hrozbách, ako aj o incidentoch, a to aj prostredníctvom preskúmania smernice o sieťovej a informačnej bezpečnosti (smernica NIS), s cieľom hľadať možnosti na zvýšenie kybernetickej odolnosti a účinnejšie reakcie na kybernetické útoky, najmä pokiaľ ide o základné hospodárske a spoločenské činnosti, pričom sa budú rešpektovať právomoci členských štátov vrátane ich zodpovednosti za vlastnú národnú bezpečnosť.“⁴ Okrem toho navrhovaným právnym aktom nie je dotknuté uplatňovanie pravidiel hospodárskej súťaže, ktoré sú stanovené v Zmluve o fungovaní Európskej únie (ZFEÚ).

S ohľadom na skutočnosť, že významná časť kybernetických hrozieb má pôvod mimo EÚ, je potrebný ucelený prístup v rámci medzinárodnej spolupráce. Táto smernica predstavuje referenčný model, ktorý sa má podporovať v kontexte spolupráce EÚ s tretími krajinami, a to najmä pri poskytovaní externej technickej pomoci.

2. PRÁVNY ZÁKLAD, SUBSIDIARITA A PROPORCIONALITA

• Právny základ

Právnym základom smernice NIS je článok 114 Zmluvy o fungovaní Európskej únie, ktorého cieľom je vytváranie a fungovanie vnútorného trhu prostredníctvom posilňovania opatrení na aproximáciu vnútroštátnych pravidiel. Ako sa konštatuje v rozsudku Súdneho dvora Európskej únie vo veci C-58/08 Vodafone a i., použitie článku 114 ZFEÚ je odôvodnené, ak sú medzi vnútroštátnymi pravidlami rozdiely, ktoré majú priamy vplyv na fungovanie vnútorného trhu. Rovnako Súdny dvor konštatoval, že ak akt, ktorý sa zakladá na článku 114 ZFEÚ, už odstránil všetky prekážky obchodu v oblasti, ktorú harmonizuje, normotvorcu Únie nemožno pozbaviť možnosti prispôbiť tento akt akýmkoľvek zmenám okolností alebo akémukoľvek vývoju poznatkov vzhľadom na úlohu, ktorá mu prislúcha pri zabezpečení ochrany všeobecných záujmov uznaných Zmluvou. Súdny dvor nakoniec konštatoval, že opatrenia na aproximáciu, ktoré sú zahrnuté v článku 114 ZFEÚ, majú za cieľ ponechať priestor na voľné konanie v závislosti od všeobecného kontextu a osobitných okolností v oblasti, ktorá sa má harmonizovať, a to pokiaľ ide o posúdenie najvhodnejšej techniky aproximácie na dosiahnutie požadovaného výsledku. Navrhovaný právny akt by odstránil prekážky vnútorného trhu pre kľúčové a dôležité subjekty, a zlepšil by jeho vytváranie a fungovanie, a to prostredníctvom: stanovenia jasných, všeobecne uplatniteľných pravidiel o rozsahu pôsobnosti smernice NIS, ako aj harmonizovania pravidiel uplatniteľných v oblasti riadenia kybernetického rizika a oznamovania incidentov. Súčasné rozdiely v tejto oblasti na legislatívnej úrovni aj úrovni dohľadu, ako aj na vnútroštátnej úrovni a úrovni EÚ, sú prekážkami vnútorného trhu, keďže subjekty, ktoré sú zapojené do cezhraničných činností,

³ https://www.europarl.europa.eu/doceo/document/TA-8-2019-0156_SK.html.

⁴ <https://data.consilium.europa.eu/doc/document/ST-8711-2020-INIT/sk/pdf>.

musia čeliť rôznym regulačným požiadavkám, ktoré sa môžu vzájomne prekryvať, a/alebo ich uplatňovať, a to na úkor vykonávania ich slobody usadiť sa a poskytovať služby. Rôzne pravidlá majú takisto negatívny vplyv na podmienky hospodárskej súťaže na vnútornom trhu, pokiaľ ide o subjekty rovnakého typu v rôznych členských štátoch.

- **Subsidiarita (v prípade inej ako výlučnej právomoci)**

Kybernetická odolnosť v rámci Únie nemôže byť účinná, ak sa k nej prostredníctvom vnútroštátnych alebo regionálnych dátových síl pristupuje odlišným spôsobom. Smernica NIS čiastočne riešila tento nedostatok stanovením rámca pre bezpečnosť sietí a informačných systémov na vnútroštátnej úrovni a úrovni Únie. Jej transpozícia a vykonávanie však takisto odhalili charakteristické nedostatky a obmedzenia istých ustanovení alebo prístupov, ako je napríklad nejasné vymedzenie rozsahu pôsobnosti smernice, čo vedie k významným rozdielom, pokiaľ ide o rozsah a hĺbku *de facto* intervencie EÚ na úrovni členských štátov. Okrem toho je od začiatku krízy spôsobenej pandemiou COVID-19 európske hospodárstvo dokonca viac ako kedykoľvek predtým závislé od sietí a informačných systémov a odvetvia a služby sú čoraz viac prepojené. Intervenciu EÚ nad rámec súčasných opatrení smernice NIS možno odôvodniť najmä týmito skutočnosťami: i) čoraz viac cezhraničný charakter hrozieb a výziev týkajúcich sa NIS; ii) potenciál opatrení Únie zlepšiť a uľahčiť účinné a koordinované vnútroštátne politiky; a iii) príspevok zosúladeného postupu založeného na spolupráci k účinnej ochrane údajov a súkromia.

- **Proporcionalita**

Pravidlá navrhnuté v tejto smernici neprekračujú rámec nevyhnutný na uspokojivé plnenie osobitných cieľov. Plánované zosúladenie a zefektívnenie bezpečnostných opatrení a oznamovacích povinností sa týka požiadaviek členských štátov a podnikov na zlepšenie súčasného rámca.

V návrhu sa zohľadňujú už existujúce postupy v členských štátoch. Posilnená úroveň ochrany, ktorá sa dosiahla prostredníctvom takýchto zjednodušených a koordinovaných požiadaviek, je primeraná čoraz väčším rizikám, ktorým je nutné čeliť, ako aj tým, ktoré predstavujú cezhraničný prvok; požiadavky sú primerané a vo všeobecnosti zodpovedajú záujmu subjektov zapojených do zabezpečovania kontinuity a kvality ich služieb. Náklady na zabezpečenie systematickej spolupráce medzi členskými štátmi by boli nízke v porovnaní s hospodárskymi a spoločenskými stratami a škodami spôsobenými kybernetickými incidentmi. Okrem toho konzultácie so zainteresovanými stranami, ktoré sa uskutočnili v kontexte preskúmania smernice NIS, ako aj výsledky otvorenej verejnej konzultácie a cielených prieskumov ukazujú podporu revízie smernice NIS podľa uvedených bodov.

- **Výber nástroja**

Návrh ďalej zjednoduší povinnosti uložené podnikom a zabezpečí vyššiu úroveň ich harmonizácie. Cieľom návrhu je zároveň poskytnúť členským štátom flexibilitu potrebnú nato, aby zohľadnili vnútroštátne špecifiká (napríklad možnosť identifikovať dodatočné kľúčové alebo dôležité subjekty nad rámec základného scenára stanoveného v rámci právneho aktu). Budúcim právnym nástrojom by preto mala byť smernica, keďže tento právny nástroj umožňuje cielenú lepšiu harmonizáciu, ako aj určitý stupeň flexibility pre príslušné orgány.

3. VÝSLEDKY HODNOTENÍ EX POST, KONZULTÁCIÍ SO ZAJINTERESOVANÝMI STRANAMI A POSÚDENÍ VPLYVU

• Hodnotenia ex post/kontroly vhodnosti existujúcich právnych predpisov

Komisia vykonala hodnotenie fungovania smernice NIS.⁵ Analyzovala jej relevantnosť, pridanú hodnotu EÚ, koherentnosť, účinnosť a efektívnosť. Hlavné zistenia tejto analýzy sú:

- Rozsah pôsobnosti smernice NIS je príliš obmedzený, pokiaľ ide o odvetvia, na ktoré sa vzťahuje, a to najmä z týchto dôvodov: i) zvýšená digitalizácia v posledných rokoch a vyšší stupeň vzájomného prepojenia; ii) v rozsahu pôsobnosti smernice NIS sa už viac neodzrkadľujú všetky digitalizované odvetvia poskytujúce kľúčové služby pre hospodárstvo a spoločnosť ako celok.
- Smernica NIS nie je dostatočne jasná, pokiaľ ide o rozsah pôsobnosti pre prevádzkovateľov základných služieb a jej ustanovenia neposkytujú dostatočnú zrozumiteľnosť, pokiaľ ide o vnútroštátnu právomoc nad poskytovateľmi digitálnych služieb. To vedie k situácii, v ktorej určité typy subjektov nie sú vo všetkých členských štátoch identifikované, a preto sa od nich nevyžaduje, aby zaviedli bezpečnostné opatrenia a oznamovali incidenty.
- V smernici NIS sa členským štátom pri stanovovaní bezpečnostných požiadaviek a požiadaviek na oznamovanie incidentov pre prevádzkovateľov základných služieb umožnil široký priestor na voľné konanie. Z hodnotenia vyplýva, že v niektorých prípadoch členské štáty tieto požiadavky zaviedli značne odlišnými spôsobmi, pričom vytvorili dodatočné zaťaženie pre spoločnosti pôsobiace vo viac ako jednom členskom štáte.
- Systém dohľadu a presadzovania smernice NIS je neúčinný. Napríklad členské štáty sa veľmi zdráhajú uplatňovať sankcie voči subjektom, ktoré nezaviedli bezpečnostné požiadavky alebo neoznámili incidenty. To môže mať negatívne následky na kybernetickú odolnosť jednotlivých subjektov.
- Finančné a ľudské zdroje vyčlenené členskými štátmi na vykonávanie ich úloh (ako je identifikácia prevádzkovateľov základných služieb alebo dohľad nad nimi) a následne rôzne úrovne pokročilosti pri riešení kybernetických rizík sa výrazne líšia. To ešte viac prehľbuje rozdiely v oblasti kybernetickej odolnosti medzi členskými štátmi.
- Členské štáty si informácie medzi sebou nevymieňajú systematicky, čo má negatívne následky, najmä pokiaľ ide o účinnosť opatrení v oblasti kybernetickej bezpečnosti a mieru spoločnej situačnej informovanosti na úrovni EÚ. Platí to aj pre výmenu informácií medzi súkromnými subjektmi a pre interakciu medzi štruktúrami spolupráce na úrovni EÚ a súkromnými subjektmi.
- **Konzultácie so zainteresovanými stranami**

Komisia viedla konzultácie so širokým spektrom zainteresovaných strán. Členské štáty a zainteresované strany boli vyzvané, aby sa zúčastnili otvorenej verejnej konzultácie a prieskumov a seminárov organizovaných dodávateľmi Wavestone, CEPS a ICF, ktorých Komisia poverila vykonaním štúdie na podporu preskúmania smernice NIS. Medzi zainteresované strany, ktoré sa zúčastnili na konzultáciách, patria aj príslušné orgány, orgány Únie zaoberajúce sa kybernetickou bezpečnosťou, prevádzkovatelia základných služieb,

⁵ [Príloha 5 k posúdeniu vplyvu].

poskytovatelia digitálnych služieb, subjekty poskytujúce služby mimo rozsahu pôsobnosti súčasnej smernice NIS, odborové združenia, spotrebiteľské organizácie a občania.

Okrem toho Komisia je neustále v kontakte s príslušnými orgánmi zodpovednými za vykonávanie smernice NIS. Skupina pre spoluprácu sa podrobne zaoberala rôznymi prierezovými aspektmi a aspektmi sektorového vykonávania. Napokon Komisia počas svojich návštev krajín v rámci smernice NIS v rokoch 2019 a 2020 uskutočnila rozhovory so 154 verejnými a súkromnými subjektmi, ako aj so 117 príslušnými orgánmi.

- **Získavanie a využívanie expertízy**

Komisia uzatvorila zmluvy s konzorciom dodávateľov Wavestone, CEPS a ICF, aby podporili Komisiu v preskúmaní smernice NIS.⁶ Dodávateľ nielenže oslovil zainteresované strany priamo dotknuté smernicou NIS prostredníctvom cielených prieskumov a seminárov, ale takisto konzultoval so širokým spektrom expertov v oblasti kybernetickej bezpečnosti, akými sú výskumníci v oblasti kybernetickej bezpečnosti a odborníci v odvetví kybernetickej bezpečnosti.

- **Posúdenie vplyvu**

K tomuto návrhu je pripojené posúdenie vplyvu⁷, ktoré bolo 23. októbra 2020 predložené výboru pre kontrolu regulácie a ktoré 20. novembra 2020 získalo pozitívne stanovisko s pripomienkami od výboru pre kontrolu regulácie. Výbor pre kontrolu regulácie odporučil zlepšenia v niektorých oblastiach s cieľom: 1. lepšie zohľadniť úlohu cezhraničných účinkov presahovania v rámci analýzy problému; 2. lepšie vysvetliť, ako by vyzeral úspech iniciatívy; 3. bližšie zdôvodniť zoznam možností politiky; 4. ďalej rozpracovať náklady na navrhované opatrenia. Posúdenie vplyvu bolo prispôbené s cieľom riešiť tieto body, ako aj podrobnejšie pripomienky výboru pre kontrolu regulácie. V súčasnosti zahŕňa podrobnejšie vysvetlenia úlohy cezhraničných účinkov presahovania v oblasti kybernetickej bezpečnosti, jasnejší prehľad o tom, ako možno merať úspech, podrobnejšie vysvetlenie koncepcie a logiky, pokiaľ ide o rôzne možnosti politiky a opatrenia, ktoré sa v rámci týchto možností zvažujú, podrobnejšie vysvetlenie analyzovaných aspektov v súvislosti s rozsahom odvetvovej pôsobnosti smernice NIS, ako aj ďalšie objasnenia, pokiaľ ide o náklady.

Komisia zvažila niekoľko možností politiky na zlepšenie právneho rámca v oblasti kybernetickej odolnosti a reakcie na kybernetický incident:

- „Nevykonať žiadne opatrenia“: Smernica NIS by zostala nezmenená a neprijali by sa žiadne iné opatrenia nelegislatívnej povahy na odstránenie problémov zistených pri hodnotení smernice NIS.
- Možnosť 1: Na legislatívnej úrovni by sa nevykonali žiadne zmeny. Namiesto toho by Komisia vydala odporúčania a usmernenia (napríklad, pokiaľ ide o identifikáciu prevádzkovateľov základných služieb, bezpečnostné požiadavky, postupy oznamovania incidentov a dohľad), a to po konzultácii so skupinou pre spoluprácu, s agentúrou EÚ pre kybernetickú bezpečnosť (ENISA) a prípadne so sieťou jednotiek pre riešenie počítačových bezpečnostných incidentov (jednotky CSIRT).

⁶ Štúdia na podporu revízie smernice (EÚ) 2016/1148 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (ďalej len „smernica NIS“) – č. 2020 – 665. Wavestone, CEPS a ICF.

⁷ [Doplňa sa odkazy na záverečný dokument a na zhrnutie.]

- Možnosť 2: Táto možnosť zahŕňa ciele zmeny smernice NIS vrátane rozšírenia rozsahu jej pôsobnosti a niekoľkých ďalších zmien, ktorých cieľom by bolo zaistiť určité okamžité riešenia zistených problémov, pričom by poskytovali väčšiu zrozumiteľnosť a ďalšiu harmonizáciu (ako napríklad ustanovenia na harmonizáciu prahových hodnôt na identifikáciu). V zmenenej smernici NIS by však zostali zachované hlavné stavebné prvky, prístup a hodnoty.
- Možnosť 3: V tomto scenári sú zahrnuté systémové a štrukturálne zmeny smernice NIS (prostredníctvom novej smernice), v rámci ktorých sa plánuje zásadnejšia zmena prístupu, a to v podobe zahrnutia širšej oblasti hospodárstiev v Únii, ale zároveň aj cielenejší dohľad zameraný na veľkých a kľúčových účastníkov. Takisto by sa tým zefektívnili povinnosti uložené podnikom a zabezpečila by sa vyššia úroveň ich harmonizácie, vytvorilo by sa účinnejšie nastavenie prevádzkových aspektov a takisto by vznikol jasný základ pre posilnenú spoločnú zodpovednosť a zodpovednosť rôznych zainteresovaných strán, pokiaľ ide o opatrenia v oblasti kybernetickej bezpečnosti.

Z posúdenia vplyvu vyplýva, že uprednostňovaná je možnosť 3 (t. j. systémové a štrukturálne zmeny rámca smernice NIS). Pokiaľ ide o účinnosť, uprednostňovaná možnosť by jasne stanovila rozsah pôsobnosti smernice NIS, ktorý by sa rozšíril na reprezentatívnejšiu časť hospodárstiev a spoločností v EÚ, a zefektívnila požiadavky a takisto lepšie vymedzila rámec pre dohľad a presadzovanie predpisov, ktorý by mal za cieľ zvýšiť úroveň dodržiavania pravidiel. Táto možnosť takisto zahŕňa opatrenia zamerané na zlepšenie prístupov v oblasti tvorby politík na úrovni členských štátov a na zmenu ich paradigmy, pričom podporuje nové rámce pre riadenie rizika v rámci vzťahov s dodávateľmi a koordinované zverejňovanie informácií o zraniteľnosti. V uprednostňovanej možnosti sa zároveň stanovuje jasný základ pre spoločnú zodpovednosť a plánujú sa mechanizmy zamerané na zvyšovanie dôvery medzi členskými štátmi, medzi orgánmi aj v rámci priemyslu, na stimulovanie výmeny informácií a zabezpečenie operatívnejšieho prístupu, ako sú mechanizmy vzájomnej pomoci a partnerského preskúmania. Táto možnosť by takisto stanovila rámec EÚ pre krízové riadenie založený na nedávno spustenej operačnej sieti EÚ, a zabezpečila by lepšie zapojenie agentúry ENISA v rámci jej súčasného mandátu, a to presným prehľadom o stave kybernetickej bezpečnosti Únie.

Pokiaľ ide o efektívnosť, zatiaľ čo uprednostňovaná možnosť by so sebou prinášala dodatočné náklady pre podniky a členské štáty na dodržiavanie pravidiel a presadzovanie, viedla by takisto k účinným kompromisom a synergiám, keďže má najlepší potenciál zo všetkých analyzovaných možností politiky na zabezpečenie zvýšenej a konzistentnej úrovne kybernetickej odolnosti kľúčových subjektov v Únii, čo by v konečnom dôsledku viedlo k úspore nákladov pre podniky aj spoločnosť. Táto možnosť politiky by viedla k určitému dodatočnému administratívne zaťaženiu a dodatočným nákladom na dodržiavanie predpisov pre orgány členských štátov. Avšak po dôkladnom zvážení, v strednodobom a dlhodobom horizonte by táto možnosť takisto priniesla značné výhody prostredníctvom zvýšenej spolupráce medzi členskými štátmi, a to aj na operačnej úrovni, ako aj stimulovanie k celkovému nárastu kapacít v oblasti kybernetickej bezpečnosti na vnútroštátnej a regionálnej úrovni prostredníctvom vzájomnej pomoci, mechanizmov partnerského preskúmania a lepšieho prehľadu o kľúčových podnikoch a lepšej interakcie s nimi. Uprednostňovaná možnosť politiky by takisto do veľkej miery zabezpečila súlad s inými právnymi predpismi, iniciatívami alebo politickými opatreniami vrátane odvetvových *lex specialis*.

Riešenie súčasnej pretrvávajúcej nedostatočnej pripravenosti v oblasti kybernetickej bezpečnosti na úrovni členských štátov a na úrovni spoločností a iných organizácií by mohlo

viest' k zvýšeniu efektívnosti a zníženiu dodatočných nákladov, ktoré vyplývajú z kybernetických incidentov.

- Pokiaľ ide o kľúčové a dôležité subjekty, narastajúca úroveň kybernetickobezpečnostnej pripravenosti by mohla viesť k zmierneniu prípadnej straty príjmov z dôvodu narušenia – aj z dôvodu priemyselnej špionáže – a mohla by znížiť vysoké výdavky na zmiernovanie *ad hoc* hrozieb. Také zisky pravdepodobne prevýšia potrebné investičné náklady. Zníženie fragmentácie na vnútornom trhu by takisto zlepšilo rovnaké podmienky medzi prevádzkovateľmi.
- Pokiaľ ide o členské štáty, takisto by mohlo ďalej znižovať riziko narastajúcich rozpočtových výdavkov na zmiernovanie *ad hoc* hrozieb a dodatočných nákladov v prípade núdzových situácií súvisiacich s kybernetickými incidentmi.
- Pokiaľ ide o občanov, očakáva sa, že riešenie kybernetických incidentov povedie k zníženiu straty príjmu z dôvodu hospodárskych výkyvov.

Zvýšená úroveň kybernetickej bezpečnosti v členských štátoch a schopnosť spoločností a orgánov rýchlo reagovať na incident a zmierniť jeho vplyv s najväčšou pravdepodobnosťou povedie k zvýšeniu celkovej miery dôvery občanov v digitálne hospodárstvo, čo môže mať pozitívny vplyv na rast a investície.

Zvýšenie celkovej úrovne kybernetickej bezpečnosti pravdepodobne povedie k zvýšenej celkovej bezpečnosti a plynulému, nepretržitému fungovaniu základných služieb, ktoré sú pre spoločnosť kľúčové. Iniciatíva môže takisto prispieť k ďalším sociálnym vplyvom, ako je znížená úroveň počítačovej kriminality a terorizmu a zvýšená úroveň civilnej ochrany. Vďaka zvyšovaniu úrovne kybernetickej pripravenosti podnikov a iných organizácii je možné sa vyhnúť prípadným finančným stratám, ktoré sú dôsledkom kybernetických útokov, a zabrániť tak nutnosti prepustiť zamestnancov.

Zvyšovanie celkovej úrovne kybernetickej bezpečnosti by takisto mohlo viesť k predchádzaniu environmentálnym rizikám/poškodzovania životného prostredia v prípade útoku na základnú službu. To by mohlo platiť najmä pre sektor energetiky, sektor dodávok a distribúcie vody alebo dopravy. Posilnením spôsobilostí v oblasti kybernetickej bezpečnosti by iniciatíva mohla viesť k zvýšenému využívaniu najnovšej generácie infraštruktúr a služieb IKT, ktoré sú aj z hľadiska životného prostredia udržateľnejšie, ako aj k výmene neefektívnych a menej bezpečných tradičných infraštruktúr. Očakáva sa, že toto prispeje aj k zníženiu počtu nákladných kybernetických incidentov, čím sa uvoľnia prostriedky dostupné pre udržateľné investície.

• Regulačná vhodnosť a zjednodušenie

V návrhu sa predpokladá všeobecné vyňatie mikrosubjektov a malých subjektov z rozsahu pôsobnosti smernice NIS, ako aj jednoduchší režim dohľadu *ex post*, ktorý sa uplatňuje na veľké množstvo nových subjektov podľa revidovaného rozsahu (tzv. dôležité subjekty). Tieto opatrenia majú za cieľ minimalizovať a vyvážiť záťaž pre podniky a subjekty verejnej správy. Okrem toho návrh nahrádza komplikovaný systém identifikácie pre prevádzkovateľov základných služieb všeobecne uplatniteľnou povinnosťou a zavádza vyššiu úroveň harmonizácie povinností v oblasti bezpečnosti a oznamovania, čím by sa znížila záťaž spojená s dodržiavaním predpisov, a to najmä pokiaľ ide o subjekty poskytujúce cezhraničné služby.

Návrhom sa minimalizujú náklady na dodržiavanie predpisov pre MSP, keďže od subjektov sa vyžaduje, aby prijali len tie opatrenia, ktoré sú potrebné na zabezpečenie úrovne bezpečnosti sietí a informačných systémov, ktorá je primeraná existujúcemu riziku.

- **Základné práva**

EÚ sa zaviazala, že bude dodržiavať vysoké normy ochrany základných práv. Všetky dobrovoľné opatrenia na výmenu informácií medzi subjektmi, ktoré táto smernica podporuje, by sa vykonali v dôveryhodnom prostredí pri úplnom dodržiavaní pravidiel Únie o ochrane údajov, a najmä nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679⁸.

4. VPLYV NA ROZPOČET

Pozri finančný výkaz

5. ĎALŠIE PRVKY

- **Plány vykonávania, spôsob monitorovania, hodnotenia a podávania správ**

Návrh zahŕňa všeobecný plán monitorovania a hodnotenia vplyvu na osobitné ciele, v rámci ktorého sa od Komisie vyžaduje, aby aspoň [54 mesiacov] po dátume nadobudnutia jeho účinnosti vykonala jeho revíziu a podala správu Európskemu parlamentu a Rade o svojich hlavných zisteniach.

Revízia sa vykoná v súlade s usmerneniami Komisie o lepšej právnej regulácii.

- **Podrobné vysvetlenie konkrétnych ustanovení návrhu**

Návrh zahŕňa sedem hlavných oblastí politiky, ktoré vzájomne súvisia a slúžia na zvyšovanie úrovne kybernetickej bezpečnosti v Únii.

Predmet úpravy a rozsah pôsobnosti (článok 1 a článok 2)

Smernicou sa najmä: a) stanovujú povinnosti pre členské štáty prijať vnútroštátne stratégie kybernetickej bezpečnosti, určiť príslušné vnútroštátne orgány, jednotné kontaktné miesta a jednotky CSIRT; b) stanovuje, aby členské štáty uložili povinnosti v oblasti riadenia kybernetického rizika a oznamovacie povinnosti pre subjekty označované ako kľúčové subjekty v prílohe I a dôležité subjekty v prílohe II; c) stanovuje, aby členské štáty uložili povinnosti v oblasti výmeny informácií o kybernetickej bezpečnosti.

Vzťahuje sa na určité verejné alebo súkromné kľúčové subjekty pôsobiace v odvetviach uvedených v prílohe I (energetika, doprava, bankovníctvo, infraštruktúry finančných trhov, zdravotníctvo, pitná voda, odpadová voda, digitálna infraštruktúra, verejná správa a kozmonautika) a na určité dôležité subjekty pôsobiace v odvetviach uvedených v prílohe II (poštové a kuriérske služby, odpadové hospodárstvo, výroba a distribúcia chemických látok, výroba, spracovanie a distribúcia potravín, výroba a digitálni poskytovatelia). Mikrosubjekty a malé subjekty v zmysle odporúčania Komisie 2003/361/ES zo 6. mája 2003 sú vyňaté z rozsahu pôsobnosti smernice, okrem poskytovateľov elektronických komunikačných sietí alebo poskytovateľov verejne dostupných elektronických komunikačných služieb, poskytovateľov dôveryhodných služieb, správcov mien domény najvyššej úrovne a subjektov verejnej správy a určitých iných subjektov, ako je napríklad jediný poskytovateľ služieb v členskom štáte.

Vnútroštátne rámce pre kybernetickú bezpečnosť (články 5 až 11)

⁸

Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (Ú. v. EÚ L 119, 4.5.2016, s. 1)

Od členských štátov sa vyžaduje, aby prijali vnútroštátnu stratégiu kybernetickej bezpečnosti, v ktorej sa vymedzia strategické ciele a vhodné politické a regulačné opatrenia, s cieľom dosiahnuť a zachovať vysokú úroveň kybernetickej bezpečnosti.

V smernici sa takisto stanovuje rámec pre koordinované zverejňovanie informácií o zraniteľnostiach a od členských štátov sa vyžaduje, aby poverili jednotky CSIRT, aby konali ako dôveryhodní sprostredkovatelia a uľahčili interakciu medzi oznamujúcimi subjektmi a výrobcami alebo poskytovateľmi produktov IKT a služieb IKT. Od agentúry ENISA sa vyžaduje, aby pre zistené zraniteľnosti vyvinula a spravovala európsky register zraniteľnosti.

Od členských štátov sa vyžaduje, aby zaviedli národné rámce krízového riadenia kybernetickej bezpečnosti, okrem iného určením príslušných vnútroštátnych orgánov zodpovedných za riadenie incidentov a kríz kybernetickej bezpečnosti veľkého rozsahu.

Od členských štátov sa takisto vyžaduje, aby určili jeden alebo dva príslušné vnútroštátne orgány pre oblasť kybernetickej bezpečnosti na úlohy týkajúce sa dohľadu v súlade s touto smernicou, ako aj národné jednotné kontaktné miesto pre kybernetickú bezpečnosť na vykonávanie styčnej úlohy s cieľom zabezpečiť cezhraničnú spoluprácu orgánov členských štátov. Od členských štátov sa takisto vyžaduje, aby určili jednotky CSIRT.

Spolupráca (články 12 až 16)

Smernicou sa zriaďuje skupina pre spoluprácu na podporu a uľahčenie strategickej spolupráce a výmeny informácií medzi členskými štátmi a na rozvoj vzájomnej dôvery. Takisto sa ňou zriaďuje sieť jednotiek CSIRT s cieľom prispieť k rozvoju dôvery medzi členskými štátmi a podporiť rýchlu a účinnú operačnú spoluprácu.

Európska sieť styčných organizácií pre kybernetické krízy (EÚ – CyCLONe) bola zriadená s cieľom podporiť koordinované riadenie incidentov a kríz veľkého rozsahu v oblasti kybernetickej bezpečnosti a zabezpečiť pravidelnú výmenu informácií medzi členskými štátmi a inštitúciami EÚ.

Od agentúry ENISA sa vyžaduje, aby v spolupráci s Komisiou vydala dvojročnú správu o stave kybernetickej bezpečnosti v Únii.

Od Komisie sa vyžaduje, aby zriadila systém partnerského preskúmania, v rámci ktorého sa umožnia pravidelné partnerské preskúmania účinnosti politík v oblasti kybernetickej bezpečnosti členských štátov.

Riadenie rizík v oblasti kybernetickej bezpečnosti a oznamovacie povinnosti (články 17 až 23)

V smernici sa od členských štátov vyžaduje, aby zabezpečili, že riadiace orgány všetkých subjektov v rámci rozsahu pôsobnosti schvália opatrenia na riadenie kybernetických rizík prijaté príslušnými subjektmi, a absolvovali osobitnú odbornú prípravu v súvislosti s kybernetickou bezpečnosťou.

Od členských štátov sa vyžaduje, aby zabezpečili, že subjekty v rozsahu pôsobnosti prijímú náležité a primerané technické a organizačné opatrenia na riadenie kybernetických rizík súvisiacich s bezpečnosťou sietí a informačných systémov. Takisto sa od nich vyžaduje, aby

zabezpečili, že subjekty upovedomia vnútroštátne príslušné orgány alebo jednotky CSIRT v prípade, že kybernetický incident má významný vplyv na nimi poskytovanú službu.

Správcovia mien domény najvyššej úrovne a subjekty poskytujúce služby registrácie doménových mien pre doménu najvyššej úrovne budú zbierať a uchovávať presné a úplné údaje o registrácii doménových mien. Okrem toho sa od takýchto subjektov vyžaduje, aby oprávneným žiadateľom o prístup poskytli účinný prístup k registračným údajom domény.

Právomoc a registrácia (články 24 a 25)

Kľúčové a dôležité subjekty spravidla podliehajú právomoci toho členského štátu, v ktorom poskytujú svoje služby. Určité druhy subjektov (poskytovatelia služieb DNS, správcovia mien domény najvyššej úrovne, poskytovatelia služieb cloud computingu, poskytovatelia služieb dátového centra a poskytovatelia siete na sprístupňovanie obsahu, ako aj určití digitálni poskytovatelia) však podliehajú právomoci členského štátu, v ktorom majú svoje hlavné miesto podnikateľskej činnosti v Únii. Dôvodom je zabezpečiť, aby také subjekty nemuseli plniť viaceré rôzne právne požiadavky, keďže poskytujú služby za hranicami v obzvlášť vysokej miere. Od agentúry ENISA sa vyžaduje, aby vytvorila a spravovala register uvedeného druhu subjektov.

Výmena informácií (články 26 a 27)

Členské štáty stanovujú pravidlá, ktoré umožnia subjektom zapojiť sa do výmeny informácií súvisiacich s kybernetickou bezpečnosťou, a to v rámci špecifických opatrení na výmenu informácií v oblasti kybernetickej bezpečnosti v súlade s článkom 101 ZFEÚ. Okrem toho členské štáty umožnia subjektom mimo rozsahu pôsobnosti tejto smernice na dobrovoľnej báze oznamovať významné incidenty, kybernetické hrozby alebo udalosti odvrátené v poslednej chvíli.

Dohľad a presadzovanie predpisov (články 28 až 34)

Od príslušných orgánov sa vyžaduje, aby vykonávali dohľad nad subjektmi v rozsahu pôsobnosti smernice, a najmä aby zabezpečili ich súlad s bezpečnostnými požiadavkami a požiadavkami o oznamovaní incidentov. V smernici sa rozlišuje medzi režimom dohľadu *ex ante* pre kľúčové subjekty a režimom dohľadu *ex post* pre dôležité subjekty, pričom režim dohľadu *ex post* vyžaduje od príslušných orgánov prijatie opatrení v prípade, že získajú dôkazy alebo indície o tom, že dôležitý subjekt nespĺňa bezpečnostné požiadavky a požiadavky o oznamovaní incidentov.

V smernici sa takisto od členských štátov vyžaduje, aby ukladali kľúčovým a dôležitým subjektom správne pokuty a vymedzujú sa v nej určité maximálne pokuty.

Od členských štátov sa vyžaduje, aby spolupracovali a prípadne si vzájomne pomáhali, ak subjekty poskytujú služby vo viac ako jednom členskom štáte alebo ak sa hlavné miesto podnikateľskej činnosti subjektu alebo jeho zástupca nachádza v určitom členskom štáte, ale jeho sieť a informačné systémy sa nachádzajú v inom členskom štáte alebo vo viacerých iných členských štátoch.

Návrh

SMERNICA EURÓPSKEHO PARLAMENTU A RADY**o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii a o zrušení smernice (EÚ) 2016/1148**

(Text s významom pre EHP)

EURÓPSKY PARLAMENT A RADA EURÓPSKEJ ÚNIE,

so zreteľom na Zmluvu o fungovaní Európskej únie, a najmä na jej článok 114,

so zreteľom na návrh Európskej komisie,

po postúpení návrhu legislatívneho aktu národným parlamentom,

so zreteľom na stanovisko Európskeho hospodárskeho a sociálneho výboru⁹,so zreteľom na stanovisko Výboru regiónov¹⁰,

konajúc v súlade s riadnym legislatívnym postupom,

keďže:

- (1) Cieľom smernice Európskeho parlamentu a Rady (EÚ) 2016/1148¹¹ bolo budovať kybernetickobezpečnostné kapacity v celej Únii, zmierňovať hrozby pre siete a informačné systémy používané na poskytovanie základných služieb v kľúčových odvetviach a zabezpečiť kontinuitu takýchto služieb pri riešení kybernetickobezpečnostných incidentov, a tým prispievať k efektívnemu fungovaniu spoločnosti a hospodárstva Únie.
- (2) Od nadobudnutia účinnosti smernice (EÚ) 2016/1148 sa pri zvyšovaní úrovne odolnosti Únie v oblasti kybernetickej bezpečnosti dosiahol významný pokrok. Preskúmanie uvedenej smernice ukázalo, že slúžila ako katalyzátor inštitucionálneho a regulačného prístupu ku kybernetickej bezpečnosti v Únii a pripravila pôdu pre dôležitú zmenu v zmýšľaní. Uvedenou smernicou sa zabezpečilo dokončenie vnútroštátnych rámcov vymedzením národných stratégií kybernetickej bezpečnosti, stanovením vnútroštátnych kapacít a vykonávaním regulačných opatrení vzťahujúcich sa na kľúčové infraštruktúry a aktérov identifikovaných v každom členskom štáte. Prispela aj k spolupráci na úrovni Únie zriadením skupiny pre spoluprácu¹² a siete národných jednotiek pre riešenie počítačových bezpečnostných incidentov (ďalej len „sieť jednotiek CSIRT“) ¹³. Bez ohľadu na tieto úspechy sa pri preskúmaní smernice

⁹ Ú. v. EÚ C ..., ..., s.¹⁰ Ú. v. EÚ C ..., ..., s.¹¹ Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (Ú. v. EÚ L 194/1, 19.7.2016, s. 1).¹² Článok 11 smernice (EÚ) 2016/1148.¹³ Článok 12 smernice (EÚ) 2016/1148.

(EÚ) 2016/1148 odhalili prirodzené nedostatky, ktoré jej bránia účinne riešiť súčasne a vznikajúce výzvy v oblasti kybernetickej bezpečnosti.

- (3) Siete a informačné systémy sa spolu s rýchlou digitálnou transformáciou a prepojenosťou spoločnosti, a to aj pri cezhraničných výmenách, stali bežnou súčasťou každodenného života. Tento vývoj viedol k nárastu kybernetickobezpečnostných hrozieb a prináša nové výzvy, ktoré si vyžadujú prispôbené, koordinované a inovatívne reakcie vo všetkých členských štátoch. Počet, rozsah, sofistikovanosť, frekvencia a vplyv kybernetickobezpečnostných incidentov sa zvyšujú a pre fungovanie sietí a informačných systémov predstavujú veľkú hrozbu. Vo výsledku môžu takéto incidenty zabraňovať realizácii ekonomických aktivít na vnútornom trhu, spôsobovať finančné straty, narušovať dôveru používateľov a spôsobovať značné škody spoločnosti a hospodárstvu Únie. Pripravenosť a účinnosť v oblasti kybernetickej bezpečnosti sú preto teraz pre riadne fungovanie vnútorného trhu dôležitejšie ako kedykoľvek predtým.
- (4) Právnym základom smernice (EÚ) 1148/2016 bol článok 114 Zmluvy o fungovaní Európskej únie (ZFEÚ), ktorého cieľom je vytvorenie a fungovanie vnútorného trhu posilnením opatrení na aproximáciu vnútroštátnych pravidiel. Požiadavky na kybernetickú bezpečnosť uložené subjektom poskytujúcim služby alebo ekonomicky relevantné činnosti sa v jednotlivých členských štátoch značne líšia, pokiaľ ide o typ požiadaviek, ich úroveň podrobnosti a metódu dohľadu. Tieto rozdiely spôsobujú dodatočné náklady a podnikom, ktoré cezhranične ponúkajú tovar alebo služby, spôsobujú ťažkosti. Požiadavky jedného členského štátu, ktoré sa líšia od požiadaviek iného členského štátu alebo sú s nimi dokonca v rozpore, môžu tieto cezhraničné činnosti podstatne ovplyvniť. Okrem toho môžu mať suboptimálne navrhnuté alebo zavedené kybernetickobezpečnostné normy v jednom členskom štáte vplyv na úroveň kybernetickej bezpečnosti v iných členských štátoch, najmä vzhľadom na intenzívne cezhraničné výmeny. Preskúmanie smernice (EÚ) 2016/1148 ukázalo, že pri jej implementácii členskými štátmi existujú veľké rozdiely, a to aj pokiaľ ide o jej rozsah pôsobnosti, ktorého určenie bolo do veľkej miery ponechané na voľnom uvážení členských štátov. Smernica (EÚ) 2016/1148 poskytla členským štátom veľmi široký priestor na voľné konanie, aj pokiaľ ide o implementáciu povinností týkajúcich sa bezpečnosti a oznamovania incidentov, ktoré sú v nej stanovené. Tieto povinnosti boli preto na vnútroštátnej úrovni implementované značne odlišne. Podobné rozdiely v implementácii sa vyskytli aj v súvislosti s ustanoveniami uvedenej smernice o dohľade a presadzovaní práva.
- (5) Všetky tieto rozdiely spôsobujú fragmentáciu vnútorného trhu a môžu mať škodlivý vplyv na jeho fungovanie, a to najmä pokiaľ ide o cezhraničné poskytovanie služieb a úroveň kybernetickobezpečnostnej odolnosti v dôsledku uplatňovania rôznych noriem. Cieľom tejto smernice je odstrániť takéto veľké rozdiely medzi členskými štátmi, a to najmä stanovením minimálnych pravidiel týkajúcich sa fungovania koordinovaného regulačného rámca, stanovením mechanizmov účinnej spolupráce medzi zodpovednými orgánmi v každom členskom štáte, aktualizáciou zoznamu odvetví a činností podliehajúcich povinnostiam v oblasti kybernetickej bezpečnosti a poskytnutím účinných nápravných opatrení a sankcií, ktoré sú nevyhnutné na účinné presadzovanie týchto povinností. Smernica (EÚ) 2016/1148 by sa preto mala zrušiť a nahradiť touto smernicou.
- (6) Táto smernica neovplyvňuje možnosť členských štátov prijať potrebné opatrenia na zaručenie ochrany základných záujmov vlastnej bezpečnosti, chrániť verejný poriadok a verejnú bezpečnosť a umožniť vyšetrovanie a odhaľovanie trestných činov, ako aj

stíhanie ich páchatel'ov, a to v súlade s právom Únie. V súlade s článkom 346 ZFEÚ nemá byť žiaden členský štát povinný poskytovať informácie, ktorých sprístupnenie by odporovalo základným záujmom jeho verejnej bezpečnosti. V tejto súvislosti sú relevantné pravidlá Únie a členských štátov na ochranu utajovaných skutočností, dohody o zachovaní mlčanlivosti a neformálne dohody o zachovaní mlčanlivosti, ako napríklad semaforový protokol¹⁴.

- (7) Zrušením smernice (EÚ) 2016/1148 by sa rozsah uplatňovania podľa odvetví mal rozšíriť na väčšiu časť hospodárstva vzhľadom na úvahy uvedené v odôvodneniach 4 až 6. Odvetvia, na ktoré sa vzťahuje smernica (EÚ) 2016/1148, by sa preto mali rozšíriť tak, aby boli komplexne pokryté odvetvia a služby, ktoré majú zásadný význam pre kľúčové spoločenské a hospodárske činnosti v rámci vnútorného trhu. Pravidlá by sa nemali líšiť podľa toho, či sú subjekty prevádzkovateľmi základných služieb alebo poskytovateľmi digitálnych služieb. Takéto rozlišovanie sa ukázalo ako zastarané, pretože neodráža skutočný význam odvetví alebo služieb pre spoločenské a hospodárske činnosti na vnútornom trhu.
- (8) V súlade so smernicou (EÚ) 2016/1148 boli členské štáty zodpovedné za určenie tých subjektov, ktoré spĺňajú kritériá, aby mohli pôsobiť ako prevádzkovatelia základných služieb („proces identifikácie“). S cieľom odstrániť v tejto súvislosti veľké rozdiely medzi členskými štátmi a zabezpečiť právnu istotu, pokiaľ ide o požiadavky na riadenie rizík a oznamovacie povinnosti pre všetky príslušné subjekty, by sa malo stanoviť jednotné kritérium, ktorým sa určia subjekty, ktoré patria do rozsahu pôsobnosti tejto smernice. Toto kritérium by malo spočívať v uplatňovaní pravidla obmedzenia veľkosti, podľa ktorého všetky stredné a veľké podniky, ako sú vymedzené v odporúčaní Komisie 2003/361/ES¹⁵, ktoré pôsobia v rámci takých odvetví alebo poskytujú taký druh služieb, na ktoré sa vzťahuje táto smernica, patria do rozsahu jej pôsobnosti. Od členských štátov by sa nemalo vyžadovať, aby zostavili zoznam subjektov, ktoré spĺňajú toto všeobecne uplatniteľné kritérium týkajúce sa veľkosti.
- (9) Táto smernica by sa však mala vzťahovať aj na malé subjekty alebo mikrosubjekty spĺňajúce určité kritériá, ktoré sú ukazovateľom kľúčovej úlohy pre hospodárstva alebo spoločnosti členských štátov alebo pre určité odvetvia či druhy služieb. Členské štáty by mali byť zodpovedné za vypracovanie zoznamu takýchto subjektov a mali by ho predložiť Komisii.
- (10) Komisia môže v spolupráci so skupinou pre spoluprácu vydať usmernenia o vykonávaní kritérií uplatniteľných na mikropodniky a malé podniky.
- (11) Subjekty, ktoré patria do rozsahu pôsobnosti tejto smernice, by sa v závislosti od odvetvia, v ktorom pôsobia, alebo druhu služieb, ktoré poskytujú, mali rozdeliť do dvoch kategórií: kľúčové a dôležité. Táto kategorizácia by mala zohľadňovať úroveň kritickosti daného odvetvia alebo druhu služby, ako aj úroveň závislosti iných odvetví alebo druhov služieb. Na kľúčové aj dôležité subjekty by sa mali vzťahovať rovnaké požiadavky na riadenie rizík a oznamovacie povinnosti. Malo by sa rozlišovať medzi

¹⁴ Semaforový protokol (Traffic Light Protocol, TLP) slúži pri sprístupňovaní informácií na informovanie príjemcov o akýchkoľvek obmedzeniach pri ďalšom šírení týchto informácií. Používa sa takmer vo všetkých komunitách jednotiek CSIRT a v niektorých strediskách pre výmenu a analýzu informácií (ISAC).

¹⁵ Odporúčanie Komisie 2003/361/ES zo 6. mája 2003 o vymedzení pojmov mikropodnik, malý a stredný podnik (Ú. v. EÚ L 124, 20.5.2003, s. 36).

režimom dohľadu a sankcií, pokiaľ ide o tieto dve kategórie subjektov, aby sa zabezpečila spravodlivá rovnováha medzi požiadavkami a povinnosťami na jednej strane a administratívnou záťažou vyplývajúcou z dohľadu nad dodržiavaním predpisov na strane druhej.

- (12) Právne predpisy a nástroje špecifické pre jednotlivé odvetvia môžu prispieť k zabezpečeniu vysokej úrovne kybernetickej bezpečnosti pri plnom zohľadnení špecifik a zložitosti týchto odvetví. Ak sa v právnom akte Únie špecifickom pre určité odvetvia vyžaduje, aby kľúčové alebo dôležité subjekty prijali opatrenia na riadenie kybernetickobezpečnostných rizík, alebo aby oznamovali incidenty alebo závažné kybernetické hrozby a táto povinnosť má mať aspoň rovnocenný účinok ako povinnosti stanovené v tejto smernici, mali by sa uplatňovať dané ustanovenia pre určité odvetvia vrátane ustanovení o dohľade a presadzovaní práva. Komisia môže vydať usmernenia týkajúce sa vykonávania *lex specialis*. Touto smernicou sa nebráni prijatiu ďalších odvetvových aktov Únie, ktoré sa zaoberajú opatreniami na riadenie kybernetickobezpečnostných rizík a oznamovaním incidentov. Touto smernicou nie sú dotknuté existujúce vykonávacie právomoci, ktoré boli Komisii udelené vo viacerých odvetviach vrátane dopravy a energetiky.
- (13) Nariadenie Európskeho parlamentu a Rady XXXX/XXXX¹⁶ by sa v súvislosti s touto smernicou malo považovať za odvetvový právny akt Únie, pokiaľ ide o subjekty finančného odvetvia. Namiesto ustanovení tejto smernice by sa mali uplatňovať ustanovenia nariadenia XXXX/XXXX týkajúce sa opatrení na riadenie rizík v oblasti informačných a komunikačných technológií (IKT), riadenia incidentov súvisiacich s IKT, a najmä oznamovania incidentov, ako aj testovania digitálnej prevádzkovej odolnosti, mechanizmov zdieľania informácií a rizík týkajúcich sa IKT zabezpečovaných tretími stranami. Členské štáty by preto nemali uplatňovať ustanovenia tejto smernice týkajúce sa riadenia kybernetickobezpečnostných rizík a oznamovacích povinností, zdieľania informácií, dohľadu a presadzovania práva na žiadne finančné subjekty, na ktoré sa vzťahuje nariadenie XXXX/XXXX. Zároveň je dôležité zachovať pevné vzťahy a výmenu informácií s finančným odvetvím podľa tejto smernice. Na tento účel nariadenie XXXX/XXXX umožňuje všetkým orgánom finančného dohľadu, európskym orgánom dohľadu (ESA) vo finančnom odvetví a príslušným vnútroštátnym orgánom podľa nariadenia XXXX/XXXX zúčastňovať sa na strategických politických diskusiách a technických prácach skupiny pre spoluprácu a vymieňať si informácie a spolupracovať s jednotnými kontaktnými miestami určenými podľa tejto smernice a s vnútroštátnymi jednotkami CSIRT. Príslušné orgány podľa nariadenia XXXX/XXXX by mali zasielať podrobnosti o závažných incidentoch súvisiacich s IKT aj jednotným kontaktným miestam určeným podľa tejto smernice. Členské štáty by okrem toho mali naďalej začleňovať finančné odvetvie do svojich stratégií kybernetickej bezpečnosti a vnútroštátne jednotky CSIRT môžu zahrnúť finančné odvetvie do svojich činností.
1. Vzhľadom na prepojenia medzi kybernetickou bezpečnosťou a fyzickou bezpečnosťou subjektov by sa mal zabezpečiť jednotný prístup medzi smernicou Európskeho parlamentu a Rady (EÚ) XXX/XXX¹⁷ a touto smernicou. Na dosiahnutie tohto cieľa by členské štáty mali zabezpečiť, aby sa kritické subjekty (a rovnocenné subjekty) podľa smernice (EÚ) XXX/XXX považovali za kľúčové subjekty podľa tejto smernice. Členské štáty by tiež mali zabezpečiť, aby ich

¹⁶ [vložte celý názov a odkaz na uverejnenie v ú. v., keď budú známe]

¹⁷ [vložte celý názov a odkaz na uverejnenie v ú. v., keď budú známe]

stratégie kybernetickej bezpečnosti poskytovali politický rámec pre posilnenú koordináciu medzi príslušným orgánom podľa tejto smernice a príslušným orgánom podľa smernice (EÚ) XXX/XXX v kontexte zdieľania informácií o incidentoch a kybernetických hrozbách, ako aj vykonávania úloh dohľadu. Orgány, na ktoré sa obe smernice vzťahujú, by mali spolupracovať a vymieňať si informácie, najmä pokiaľ ide o identifikáciu kritických subjektov, kybernetické hrozby, kybernetickobezpečnostné riziká, incidenty ovplyvňujúce kritické subjekty, ako aj o kybernetickobezpečnostných opatreniach prijatých kritickými subjektmi. Príslušné orgány podľa tejto smernice by na žiadosť príslušných orgánov podľa smernice (EÚ) XXX/XXX mali byť oprávnené vykonávať svoje právomoci v oblasti dohľadu a presadzovania práva vo vzťahu ku kľúčovému subjektu identifikovanému ako kritický subjekt. Na tento účel by oba orgány mali spolupracovať a vymieňať si informácie.

- (14) Potvrdenie a udržanie spoľahlivého, odolného a bezpečného systému doménových mien (DNS) je kľúčovým faktorom zachovania integrity internetu a je nevyhnutné pre jeho nepretržité a stabilné fungovanie, od ktorého závisí digitálne hospodárstvo a spoločnosť. Táto smernica by sa preto mala vzťahovať na všetkých poskytovateľov služieb DNS v rozlišovacom reťazci DNS vrátane prevádzkovateľov koreňových menných serverov, menných serverov domén najvyššej úrovne (TLD), autoritatívnych menných serverov pre doménové mená a rekurzívne resolvers.
- (15) Služby cloud computingu by sa mali vzťahovať na služby, ktoré umožňujú správu na požiadanie a vzdialený širokopásmový prístup ku škálovateľnému a pružnému súboru zdieľateľných a distribuovaných počítačových zdrojov. Uvedené počítačové zdroje zahŕňajú zdroje, ako sú napríklad siete, servery alebo iná infraštruktúra, operačné systémy, softvér, úložiská, aplikácie a služby. Modely zavádzania cloud computingu by mali zahŕňať súkromný, komunitný, verejný a hybridný cloud. Uvedené modely služieb a zavádzania majú rovnaký význam ako podmienky poskytovania služieb a modely zavádzania vymedzené v norme ISO/IEC 17788:2014. Schopnosť používateľa cloud computingu jednostranne si zabezpečovať počítačové kapacity, ako je serverový čas alebo sieťové úložisko, bez ľudskej interakcie zo strany poskytovateľa služieb cloud computingu by sa mohla opísať ako správa na požiadanie. Pojem „širokopásmový vzdialený prístup“ sa používa na opis toho, že cloudové kapacity sú poskytované cez sieť a prístupné prostredníctvom mechanizmov na podporu využívania heterogénnych tenkých alebo hrubých klientskych platforiem (vrátane mobilných telefónov, tabletov, laptopov, pracovných staníc). Pojem „škálovateľné“ odkazuje na počítačové zdroje, ktoré pružne prideluje poskytovateľ cloudových služieb bez ohľadu na zemepisnú polohu zdrojov s cieľom zvládať výkyvy v dopyte. Pojem „pružný súbor“ sa používa na označenie tých počítačových zdrojov, ktoré sa poskytujú a uvoľňujú na základe dopytu s cieľom rýchlo zvýšiť a znížiť dostupné zdroje v závislosti od záťaže. Pojem „zdieľateľný“ sa používa na označenie tých počítačových zdrojov, ktoré sa poskytujú viacerým používateľom, ktorí zdieľajú spoločný prístup k službe, ale spracúvanie sa vykonáva oddelene pre každého používateľa, hoci sa služba poskytuje z toho istého elektronického zariadenia. Pojem „distribuovaný“ sa používa na opis tých počítačových zdrojov, ktoré sa nachádzajú v rôznych sieťových počítačoch alebo zariadeniach a ktoré navzájom komunikujú a koordinujú sa prenosom správ.
- (16) Vzhľadom na vznik inovačných technológií a nových obchodných modelov sa očakáva, že sa na trhu objavajú nové modely zavádzania cloud computingu a služieb v reakcii na vyvíjajúce sa potreby zákazníkov. V tejto súvislosti sa služby cloud

computingu môžu poskytovať vo vysoko distribuovanej forme, ešte bližšie k miestu, kde sa údaje generujú alebo zhromažďujú, čím sa prechádza od tradičného modelu k vysoko distribuovanému modelu („edge computing“).

- (17) Služby ponúkané poskytovateľmi služieb dátového centra sa nemusia vždy poskytovať vo forme služby cloud computingu. Dátové centrá preto nemusia vždy tvoriť súčasť infraštruktúry cloud computingu. S cieľom zvládnuť všetky riziká spojené s bezpečnosťou sietí a informačných systémov by sa táto smernica mala vzťahovať aj na poskytovateľov takých služieb dátového centra, ktoré nie sú službami cloud computingu. Na účely tejto smernice by sa pojem „služba dátového centra“ mal vzťahovať na poskytovanie služby, ktorá zahŕňa štruktúry alebo skupiny štruktúr určené na centralizované umiestnenie, vzájomné prepojenie a prevádzku informačných technológií a sieťového vybavenia poskytujúcich služby ukladania, spracovania a prepravy dát spolu so všetkými zariadeniami a infraštruktúrami na distribúciu elektrickej energie a environmentálnu kontrolu. Pojem „služba dátového centra“ sa nevzťahuje na interné, podnikové dátové centrá vlastnené a prevádzkované na vlastné účely príslušného subjektu.
- (18) Poskytovatelia poštových služieb v zmysle smernice Európskeho parlamentu a Rady 97/67/ES¹⁸, ako aj poskytovatelia expresných a kuriérskych doručovacích služieb by mali podliehať tejto smernici, ak zabezpečujú aspoň jeden z krokov v reťazci poštového doručovania, a to najmä vyberanie, triedenie alebo distribúciu vrátane služieb zberu. Dopravné služby, ktoré sa nevykonávajú v spojení s jedným z týchto krokov, by nemali patriť do rozsahu poštových služieb.
- (19) Táto rastúca previazanosť je výsledkom čoraz väčšej cezhraničnej a previazanej siete poskytovania služieb s využitím kľúčových infraštruktúr v celej Únii v odvetviach energetiky, dopravy, digitálnej infraštruktúry, pitnej a odpadovej vody, zdravia, určitých aspektov verejnej správy, ako aj kozmického priestoru, pokiaľ ide o poskytovanie určitých služieb v závislosti od pozemných infraštruktúr, ktoré vlastní, spravujú a prevádzkujú členské štáty alebo súkromné strany, a preto sa nevzťahujú na infraštruktúry vlastnené, spravované alebo prevádzkované Úniou alebo v jej mene ako súčasť jej vesmírnych programov. Táto previazanosť znamená, že akékoľvek narušenie, dokonca aj také, ktoré sa pôvodne obmedzovalo na jeden subjekt alebo jedno odvetvie, môže mať širšie kaskádovité účinky, čo môže viesť k d'alekosiahlym a dlhotrvajúcim negatívnym vplyvom na poskytovanie služieb na celom vnútornom trhu. Pandémia ochorenia COVID-19 ukázala zraniteľnosť našich čoraz previazanejších spoločností voči rizikám s nízkou pravdepodobnosťou.
- (20) Vzhľadom na rozdiely vo vnútroštátnych štruktúrach riadenia a s cieľom chrániť už existujúce odvetvové dohody alebo orgány dohľadu a regulačné orgány Únie by členské štáty mali mať možnosť určiť viac než jeden vnútroštátny príslušný orgán zodpovedný za vykonávanie úloh súvisiacich s bezpečnosťou sietí a informačných systémov kľúčových a dôležitých subjektov podľa tejto smernice. Členské štáty by mali mať možnosť poveriť touto úlohou existujúci orgán.
- (21) V záujme uľahčenia cezhraničnej spolupráce a komunikácie orgánov a s cieľom umožniť účinné vykonávanie tejto smernice je potrebné, aby každý členský štát určil vnútroštátne jednotné kontaktné miesto zodpovedné za koordináciu záležitostí

¹⁸

Smernica Európskeho parlamentu a Rady 97/67/ES z 15. decembra 1997 o spoločných pravidlách rozvoja vnútorného trhu poštových služieb Spoločenstva a zlepšovaní kvality služieb (Ú. v. ES L 15, 21.1.1998, s. 14).

týkajúcich sa bezpečnosti sietí a informačných systémov a cezhraničnú spoluprácu na úrovni Únie.

- (22) Príslušné orgány alebo jednotky CSIRT by mali dostávať oznámenia o incidentoch od subjektov účinným a efektívnym spôsobom. Malo by byť úlohou jednotných kontaktných miest postupovať oznámenia o incidentoch jednotným kontaktným miestam ostatných dotknutých členských štátov. Na úrovni orgánov členských štátov by na zabezpečenie jedného kontaktného bodu v každom členskom štáte mali byť jednotné kontaktné miesta aj adresátmi relevantných informácií o incidentoch týkajúcich sa subjektov finančného odvetvia od príslušných orgánov podľa nariadenia XXXX/XXXX, ktoré by mali byť podľa potreby schopné postúpiť príslušným vnútroštátnym orgánom alebo jednotkám CSIRT podľa tejto smernice.
- (23) Členské štáty by mali mať primerané vybavenie, pokiaľ ide o technické a organizačné kapacity, aby mohli predchádzať incidentom a rizikám v oblasti sietí a informačných systémov, odhaľovať ich, reagovať na ne a zmierňovať ich. Členské štáty by preto mali zabezpečiť, aby mali dobre fungujúce jednotky CSIRT, známe aj ako jednotky reakcie na núdzové počítačové situácie (ďalej len „jednotky CERT“), ktoré budú dodržiavať základné požiadavky s cieľom zaručiť účinné a zlučiteľné kapacity na riešenie incidentov a rizík a zabezpečiť účinnú spoluprácu na úrovni Únie. S cieľom posilniť dôverný vzťah medzi subjektmi a jednotkami CSIRT v prípadoch, keď je jednotka CSIRT súčasťou príslušného orgánu, by členské štáty mali zvážiť funkčné oddelenie operačných úloh poskytovaných jednotkami CSIRT, najmä pokiaľ ide o zdieľanie informácií a podporu subjektov, od činností dohľadu príslušných orgánov.
- (24) Pokiaľ ide o osobné údaje, jednotky CSIRT by mali mať možnosť vykonávať v súlade s nariadením Európskeho parlamentu a Rady (EÚ) 2016/679¹⁹ v mene subjektu a na jeho žiadosť podľa tejto smernice proaktívnu kontrolu sietí a informačných systémov používaných na poskytovanie jeho služieb. Členské štáty by sa mali zamerať na zabezpečenie rovnakej úrovne technických kapacít pre všetky odvetvové jednotky CSIRT. Členské štáty môžu pri tvorbe vnútroštátnych jednotiek CSIRT požiadať o pomoc Agentúru Európskej únie pre kybernetickú bezpečnosť (ENISA).
- (25) Vzhľadom na význam medzinárodnej spolupráce v oblasti kybernetickej bezpečnosti by sa malo jednotkám CSIRT umožniť, aby sa okrem siete jednotiek CSIRT zriadenej podľa tejto smernice mohli stať súčasťou sietí medzinárodnej spolupráce.
- (26) V súlade s prílohou k odporúčaniu Komisie (EÚ) 2017/1548 o koordinovanej reakcii na kybernetické incidenty a krízy veľkého rozsahu (ďalej len „konceptia“)²⁰ by incident veľkého rozsahu mal znamenať incident s významným dosahom na najmenej dva členské štáty alebo ktorý svojím narušením presahuje schopnosť členského štátu reagovať naň. Incidenty veľkého rozsahu sa v závislosti od svojej príčiny a dosahu môžu vystupňovať a naplno prepuknúť v krízu, ktorá neumožňuje riadne fungovanie vnútorného trhu. Vzhľadom na široký rozsah a vo väčšine prípadov cezhraničný charakter takýchto incidentov by členské štáty a príslušné inštitúcie, orgány a agentúry Únie mali spolupracovať na technickej, prevádzkovej a politickej úrovni s cieľom riadne koordinovať reakciu v celej únii.

¹⁹ Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (Ú. v. EÚ L 119, 4.5.2016, s. 1).

²⁰ Odporúčanie Komisie (EÚ) 2017/1584 z 13. septembra 2017 o koordinovanej reakcii na kybernetické incidenty a krízy veľkého rozsahu (Ú. v. EÚ L 239, 19.9.2017, s. 36).

- (27) Keďže využívanie zraniteľností v sieťach a informačných systémoch môže spôsobiť značné narušenie a škody, rýchla identifikácia a náprava týchto zraniteľností je dôležitým faktorom pri znižovaní kybernetickobezpečnostného rizika. Subjekty, ktoré takéto systémy vyvíjajú, by preto mali zaviesť vhodné postupy na riešenie zistených zraniteľností. Keďže zraniteľnosti často odhaľujú a oznamujú (zverejňujú) tretie strany (oznamujúce subjekty), výrobca alebo poskytovateľ produktov alebo služieb IKT by mal zaviesť aj potrebné postupy na získavanie informácií o zraniteľnosti od tretích strán. V tejto súvislosti sa v medzinárodnej norme ISO/IEC 30111 poskytujú usmernenia na riešenie zraniteľností a v medzinárodnej norme ISO/IEC 29417 zasa usmernenia na zverejňovanie informácií o zraniteľnosti. Pokiaľ ide o zverejňovanie informácií o zraniteľnosti, obzvlášť dôležitá je koordinácia medzi oznamujúcimi subjektmi a výrobcami alebo poskytovateľmi produktov alebo služieb IKT. Koordinované zverejňovanie informácií o zraniteľnosti sa riadi štruktúrovaným procesom, v rámci ktorého sa zraniteľnosti hlásia organizáciám takým spôsobom, ktorým sa danej organizácii umožňuje diagnostikovať zraniteľnosť a zabezpečiť jej nápravu pred tým, ako sa podrobné informácie o zraniteľnosti poskytnú tretím stranám alebo verejnosti. Koordinované zverejňovanie informácií o zraniteľnosti by malo zahŕňať aj koordináciu medzi oznamujúcim subjektom a organizáciou, pokiaľ ide o načasovanie nápravy a zverejnenie zraniteľností.
- (28) Členské štáty by preto mali prijať opatrenia na uľahčenie koordinovaného zverejňovania informácií o zraniteľnostiach zavedením príslušnej vnútroštátnej politiky. V tejto súvislosti by členské štáty mali určiť jednotku CSIRT, ktorá by prevzala úlohu „koordinátora“, ktorý by v prípade potreby pôsobil ako sprostredkovateľ medzi oznamujúcimi subjektmi a výrobcami alebo poskytovateľmi produktov alebo služieb IKT. Úlohy koordinátora jednotiek CSIRT by mali zahŕňať najmä identifikáciu a kontaktovanie dotknutých subjektov, podporu oznamujúcich subjektov, rokovania o harmonograme zverejňovania informácií a riadenie koordinovaného zverejňovania informácií o zraniteľnosti, ktoré majú vplyv na viaceré organizácie (zverejňovanie informácií o zraniteľnosti viacerých strán). Ak majú zraniteľnosti vplyv na viacerých výrobcov alebo poskytovateľov produktov alebo služieb IKT usadených vo viac ako jednom členskom štáte, určené jednotky CSIRT z každého dotknutého členského štátu by mali spolupracovať v rámci siete jednotiek CSIRT.
- (29) Prístup k správnym a včasným informáciám o zraniteľnostiach ovplyvňujúcich produkty a služby IKT prispieva k lepšiemu riadeniu kybernetickobezpečnostných rizík. V tejto súvislosti sú zdroje verejne dostupných informácií o zraniteľnostiach dôležitým nástrojom pre subjekty a ich používateľov, ale aj pre príslušné vnútroštátne orgány a jednotky CSIRT. Agentúra ENISA by preto mala zriadiť register zraniteľností, v ktorom by kľúčové a dôležité subjekty a ich dodávatelia, ako aj subjekty, ktoré nepatria do rozsahu pôsobnosti tejto smernice, mohli dobrovoľne zverejňovať zraniteľnosti a poskytovať o nich informácie, ktoré používateľom umožnia prijať vhodné zmierňujúce opatrenia.
- (30) Hoci podobné registre alebo databázy zraniteľností existujú, ich hostiteľmi a správcami sú subjekty, ktoré nie sú usadené v Únii. Európsky register zraniteľností, ktorý vedie agentúra ENISA, by zabezpečil lepšiu transparentnosť, pokiaľ ide o proces uverejňovania pred tým, ako je daná zraniteľnosť oficiálne oznámená, ako aj odolnosť v prípade narušenia alebo prerušenia poskytovania podobných služieb. Agentúra ENISA by mala preskúmať možnosť uzatvorenia dohôd o štruktúrovanej spolupráci s

podobnými registrami v jurisdikciách tretích krajín s cieľom zabrániť duplicite úsilia a usilovať sa v čo najväčšej možnej miere o komplementaritu.

- (31) Skupina pre spoluprácu by mala každé dva roky vypracovať pracovný program vrátane opatrení, ktoré má skupina vykonať na plnenie svojich cieľov a úloh. Časový rámec prvého programu prijatého podľa tejto smernice by sa mal zosúladiť s časovým rámcom posledného programu prijatého podľa smernice (EÚ) 2016/1148 s cieľom zabrániť možným narušeniam práce skupiny.
- (32) Pri vypracúvaní usmerňujúcich dokumentov by skupina pre spoluprácu mala dôsledne: zmapovať vnútroštátne riešenia a skúsenosti, posúdiť vplyv výstupov skupiny pre spoluprácu na vnútroštátne prístupy, diskutovať o výzvach pri vykonávaní a formulovať konkrétne odporúčania, ktorými sa má dosiahnuť lepšie vykonávanie existujúcich pravidiel.
- (33) Skupina pre spoluprácu by mala zostať flexibilným fórom a mala by byť schopná reagovať na meniace sa a nové politické priority a výzvy a zároveň zohľadňovať dostupnosť zdrojov. Mala by organizovať pravidelné spoločné stretnutia s príslušnými súkromnými zainteresovanými stranami z celej Únie s cieľom prediskutovať činnosti skupiny a zhromažďovať informácie o nových politických výzvach. S cieľom posilniť spoluprácu na úrovni Únie by skupina mala zväziť prizývanie orgánov a agentúr Únie zapojených do politiky v oblasti kybernetickej bezpečnosti, ako je Európske centrum boja proti počítačovej kriminalite (EC3), Agentúra Európskej únie pre bezpečnosť letectva (EASA) a Agentúra Európskej únie pre vesmírny program (EUSPA), k účasti na jej práci.
- (34) Príslušné orgány a jednotky CSIRT by mali mať možnosť zúčastňovať sa na výmenných programoch pre úradníkov z iných členských štátov s cieľom zlepšovať spoluprácu. Príslušné orgány by mali prijať potrebné opatrenia, ktoré úradníkom z iných členských štátov umožnia zohrávať účinnú úlohu v činnostiach hostiteľského príslušného orgánu.
- (35) Únia by v prípade potreby mala v súlade s článkom 218 ZFEÚ uzatvárať medzinárodné dohody s tretími krajinami alebo medzinárodnými organizáciami, ktorými môže povoliť a organizovať ich účasť na niektorých činnostiach skupiny pre spoluprácu a siete jednotiek CSIRT. Takýmito dohodami by sa mala zabezpečiť primeraná ochrana údajov.
- (36) Členské štáty by mali prispieť k vytvoreniu rámca EÚ pre reakciu na kybernetické krízy stanoveného v odporúčaní (EÚ) 2017/1584 prostredníctvom existujúcich sietí spolupráce, najmä siete styčných organizácií pre kybernetické krízy (EU-CyCLONe), siete jednotiek CSIRT a skupiny pre spoluprácu. Sieť EU-CyCLONe a sieť jednotiek CSIRT by mali spolupracovať na základe procedurálnych opatrení, v ktorých sa vymedzujú podmienky spolupráce. V rokovacom poriadku siete EU-CyCLONe by sa mali ďalej spresniť spôsoby fungovania siete, okrem iného vrátane úloh, spôsobov spolupráce, interakcií s inými relevantnými aktérmi a vzorových formulárov na zdieľanie informácií, ako aj komunikačných prostriedkov. Pokiaľ ide o krízové riadenie na úrovni Únie, príslušné strany by sa mali opierať o integrované dojednania o politickej reakcii na krízu (IPCR). Komisia by mala na tento účel využiť ARGUS – medziodvetvový krízový koordinačný proces na vysokej úrovni. Ak má kríza výrazný externý rozmer alebo sa týka spoločnej bezpečnostnej a obrannej politiky, mal by sa aktivovať mechanizmus reakcie Európskej služby pre vonkajšiu činnosť na krízy.

- (37) Na účely tejto smernice by sa pojem „riziko“ mal vzťahovať na potenciál straty alebo narušenia v dôsledku kybernetickobezpečnostného incidentu a mal by sa vyjadriť ako kombinácia rozsahu takejto straty alebo narušenia a pravdepodobnosti výskytu daného incidentu.
- (38) Na účely tejto smernice by sa pojem „udalosti odvrátené v poslednej chvíli“ mal vzťahovať na udalosť, ktorá by mohla spôsobiť škodu, ale úspešne sa zabránilo jej prejavu v plnej miere.
- (39) Opatrenia na riadenie rizika by mali zahŕňať opatrenia na identifikáciu rizika incidentov, opatrenia na predchádzanie incidentom a ich odhaľovanie a zvládanie, ako aj opatrenia na zmiernenie ich vplyvu. Bezpečnosť sietí a informačných systémov by mala zahŕňať bezpečnosť uchovávaných, prenášaných a spracúvaných údajov.
- (40) S cieľom vyhnúť sa neprimeranému finančnému a administratívne zaťaženiu kľúčových a dôležitých subjektov by požiadavky na riadenie kybernetickobezpečnostných rizík mali byť primerané riziku, ktorým čelí daná sieť a daný informačný systém, berúc pritom do úvahy najnovší technický vývoj v oblasti takýchto opatrení.
- (41) Kľúčové a dôležité subjekty by mali zaistiť bezpečnosť sietí a informačných systémov, ktoré používajú vo svojich činnostiach. Ide predovšetkým o súkromné siete a informačné systémy, ktoré spravujú ich interní pracovníci IT alebo ktorých bezpečnosť zaisťujú externí dodávatelia. Požiadavky na riadenie kybernetickobezpečnostných rizík a na oznamovanie podľa tejto smernice by sa mali vzťahovať na príslušné kľúčové a dôležité subjekty bez ohľadu na to, či vykonávajú údržbu svojich sietí a informačných systémov interne alebo ju nechávajú vykonávať externe.
- (42) Riešenie kybernetickobezpečnostných rizík vyplývajúcich z dodávateľského reťazca subjektu a jeho vzťahu s dodávateľmi je obzvlášť dôležité vzhľadom na výskyt incidentov, keď sa subjekty stali obeťami kybernetických útokov a keď aktéri s nekalými úmyslami dokázali ohroziť bezpečnosť sietí a informačných systémov subjektu využívaním zraniteľností a zasiahnuť tak produkty a služby tretích strán. Subjekty by preto mali posúdiť a zohľadniť celkovú kvalitu produktov a postupy svojich dodávateľov a poskytovateľov služieb v oblasti kybernetickej bezpečnosti vrátane ich bezpečných vývojových postupov.
- (43) Spomedzi poskytovateľov služieb zohrávajú poskytovatelia riadených bezpečnostných služieb (MSSP) osobitne dôležitú úlohu v pomoci subjektom v ich úsilí o odhaľovanie incidentov a reakciu na ne, a to v takých oblastiach, ako je reakcia na incidenty, penetračné testovanie, bezpečnostné audity a poradenstvo. Avšak aj samotní poskytovatelia MSSP boli cieľom kybernetických útokov a ich úzke zapojenie do činnosti prevádzkovateľov predstavuje osobitné kybernetickobezpečnostné riziko. Subjekty by preto mali výberu poskytovateľa MSSP venovať zvýšenú pozornosť.
- (44) Subjekty by mali riešiť aj kybernetickobezpečnostné riziká vyplývajúce z ich interakcií a vzťahov s inými zainteresovanými stranami v rámci širšieho ekosystému. Predovšetkým by mali prijať vhodné opatrenia, aby sa ich spolupráca s akademickými a výskumnými inštitúciami uskutočňovala v súlade s ich politikami v oblasti kybernetickej bezpečnosti a aby sa riadila osvedčenými postupmi, pokiaľ ide o bezpečný prístup k informáciám a ich šírenie vo všeobecnosti, a najmä o ochranu duševného vlastníctva. Podobne by subjekty, ktoré závisia od služieb v oblasti transformácie údajov a analýzy údajov od tretích strán, mali prijať všetky vhodné

kybernetickobezpečnostné opatrenia, a to vzhľadom na význam a hodnotu údajov pre činnosti subjektov.

- (45) V záujme ďalšieho riešenia rizík kľúčového dodávateľského reťazca a pomoci subjektom pôsobiacim v odvetviach, na ktoré sa vzťahuje táto smernica, pri náležitom riadení kybernetickobezpečnostných rizík súvisiacich s dodávateľským reťazcom a dodávateľmi, by skupina pre spoluprácu, do ktorej sú zapojené príslušné vnútroštátne orgány, mala v spolupráci s Komisiou a agentúrou ENISA vykonať koordinované odvetvové posúdenia rizík dodávateľského reťazca, ktoré sa už vykonali v prípade sietí 5G v nadväznosti na odporúčanie (EÚ) 2019/534 o kybernetickej bezpečnosti sietí 5G²¹ s cieľom identifikovať za každé odvetvie kritické služby, systémy alebo produkty IKT, relevantné hrozby a zraniteľnosti.
- (46) Pri posudzovaní rizík v dodávateľskom reťazci by sa vzhľadom na vlastnosti dotknutého odvetvia mali zohľadniť technické a v relevantných prípadoch aj netechnické faktory vrátane tých, ktoré sú vymedzené v odporúčaní (EÚ) 2019/534, v celoeurópskom koordinovanom posúdení rizika bezpečnosti sietí 5G a v súbore nástrojov EÚ pre kybernetickú bezpečnosť 5G, na ktorom sa dohodla skupina pre spoluprácu. Pri určovaní dodávateľských reťazcov, ktoré by mali podliehať koordinovanému posúdeniu rizika, by sa mali zohľadniť tieto kritériá: i) rozsah, v akom kľúčové a dôležité subjekty využívajú konkrétne kritické služby, systémy alebo produkty IKT a spoliehajú sa na ne; ii) relevantnosť konkrétnych kritických služieb, systémov alebo produktov IKT pre vykonávanie kritických alebo citlivých funkcií vrátane spracúvania osobných údajov; iii) dostupnosť alternatívnych služieb, systémov alebo produktov IKT; iv) odolnosť celkového dodávateľského reťazca služieb, systémov alebo produktov IKT voči rušivým udalostiam a v) v prípade vznikajúcich služieb, systémov alebo produktov IKT ich potenciálny budúci význam pre činnosti subjektov.
- (47) S cieľom zefektívniť právne povinnosti uložené poskytovateľom verejných elektronických komunikačných sietí alebo verejne dostupných elektronických komunikačných služieb a poskytovateľom dôveryhodných služieb v súvislosti s bezpečnosťou ich sietí a informačných systémov, ako aj umožniť týmto subjektom a ich príslušným orgánom využívať právny rámec stanovený touto smernicou (vrátane určenia jednotiek CSIRT zodpovedných za riešenie rizík a incidentov, účasť príslušných orgánov a subjektov na práci skupiny pre spoluprácu a siete jednotiek CSIRT), mali by sa tieto povinnosti zahrnúť do rozsahu pôsobnosti tejto smernice. Zodpovedajúce ustanovenia v nariadení Európskeho parlamentu a Rady (EÚ) č. 910/2014²² a v smernici Európskeho parlamentu a Rady (EÚ) 2018/1972²³ týkajúce sa stanovenia požiadavky na bezpečnosť a oznamovanie pre tieto typy subjektov by sa preto mali zrušiť. Pravidlami týkajúcimi sa oznamovacích povinností by nemali byť

²¹ Odporúčanie Komisie (EÚ) 2019/534 z 26. marca 2019 Kybernetická bezpečnosť sietí 5G (Ú. v. EÚ L 88, 29.3.2019, s. 42).

²² Nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES (Ú. v. EÚ L 257, 28.8.2014, s. 73).

²³ Smernica Európskeho parlamentu a Rady (EÚ) 2018/1972 z 11. decembra 2018, ktorou sa stanovuje európsky kódex elektronických komunikácií (Ú. v. EÚ L 321, 17.12.2018, s. 36).

dotknuté nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 a smernica Európskeho parlamentu a Rady 2002/58/ES²⁴.

- (48) V prípade potreby a s cieľom zabrániť zbytočnému narušeniu by príslušné orgány zodpovedné za dohľad a presadzovanie práva mali naďalej používať existujúce vnútroštátne usmernenia a vnútroštátne právne predpisy prijaté na účely transpozície pravidiel týkajúcich sa bezpečnostných opatrení stanovených v článku 40 ods. 1 smernice (EÚ) 2018/1772, ako aj požiadaviek v článku 40 ods. 2 uvedenej smernice týkajúcich sa parametrov súvisiacich s významom incidentu.
- (49) Vzhľadom na rastúci význam interpersonálnych komunikačných služieb nezávislých od číslovania je potrebné zabezpečiť, aby takéto služby tiež podliehali príslušným bezpečnostným požiadavkám vzhľadom na ich špecifický charakter a hospodársky význam. Poskytovatelia takýchto služieb by preto mali takisto zabezpečiť takú úroveň bezpečnosti sietí a informačných systémov, ktorá zodpovedá miere daného rizika. Vzhľadom na to, že poskytovatelia interpersonálnych komunikačných služieb nezávislých od číslovania obvyčajne nevykonávajú samotnú kontrolu nad prenosom signálov v sieťach, stupeň rizika sa v prípade takýchto služieb môže v niektorých aspektoch považovať za nižší ako v prípade tradičných elektronických komunikačných služieb. To isté platí pre interpersonálne komunikačné služby, ktoré využívajú čísla a ktoré nevykonávajú skutočnú kontrolu nad prenosom signálu.
- (50) Vnútrošný trh je viac než kedykoľvek predtým závislý od fungovania internetu. Služby prakticky všetkých kľúčových a dôležitých subjektov sú závislé od služieb poskytovaných cez internet. V záujme zabezpečenia bezproblémového poskytovania služieb kľúčovými a dôležitými subjektmi je dôležité, aby verejné elektronické komunikačné siete, ako sú napríklad internetové chrbticové siete alebo podmorské komunikačné káble, mali zavedené vhodné kybernetickobezpečnostné opatrenia a aby oznamovali incidenty, ktoré sa ich týkajú.
- (51) V prípade potreby by subjekty mali informovať príjemcov svojich služieb o konkrétnych a významných hrozbách a o opatreniach, ktoré môžu prijať na zmiernenie vyplývajúceho rizika. Požiadavka informovať týchto príjemcov o takýchto hrozbách by nemala subjekty zbaviť povinnosti na vlastné náklady prijať vhodné a okamžité opatrenia na prevenciu alebo odstránenie akýchkoľvek kybernetických hrozieb a obnovenie bežnej úrovne bezpečnosti služby. Takéto informácie o bezpečnostných hrozbách by sa mali príjemcom poskytovať bezplatne.
- (52) Poskytovatelia verejných elektronických komunikačných sietí alebo verejne dostupných elektronických komunikačných služieb by mali predovšetkým informovať príjemcov služieb o konkrétnych a významných kybernetických hrozbách a o opatreniach, ktoré môžu prijať na ochranu bezpečnosti svojej komunikácie, napríklad použitím určitých typov softvéru alebo šifrovacích technológií.
- (53) S cieľom zaistiť bezpečnosť elektronických komunikačných sietí a služieb by sa malo podporovať používanie šifrovania, a najmä šifrovania medzi koncovými bodmi, a v prípade potreby by malo byť povinné pre poskytovateľov takýchto služieb a sietí v súlade so zásadami štandardnej a špecificky navrhutej bezpečnosti a ochrany súkromia na účely článku 18. Používanie šifrovania medzi koncovými bodmi by sa

²⁴

Smernica Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002, týkajúca sa spracovávanía osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách) (Ú. v. ES L 201, 31.7.2002, s. 37).

malo zosúladiť s právomocami členských štátov na zabezpečenie ochrany ich základných bezpečnostných záujmov a verejnej bezpečnosti a na umožnenie vyšetrovania, odhaľovania a stíhania trestných činov v súlade s právom Únie. Riešenia na účely zákonného prístupu k informáciám v koncovej šifrovanej komunikácii by mali zachovať účinnosť šifrovania pri ochrane súkromia a bezpečnosti komunikácií a zároveň poskytovať účinnú reakciu na trestnú činnosť.

- (54) V tejto smernici sa stanovuje dvojfázový prístup k oznamovaniu incidentov s cieľom nájsť správnu rovnováhu medzi rýchlym oznamovaním na jednej strane, ktoré pomáha zmierniť potenciálne šírenie incidentov a umožňuje subjektom hľadať podporu, a na druhej strane podávaním podrobných správ, v ktorých sa čerpajú cenné ponaučenia z jednotlivých incidentov a časom sa zlepšuje odolnosť jednotlivých podnikov a celých odvetví voči kybernetickým hrozbám. Ak sa subjekty dozvedia o incidente, malo by sa od nich vyžadovať, aby do 24 hodín predložili prvotné oznámenie, po ktorom bude najneskôr do jedného mesiaca nasledovať konečná správa. Prvotné oznámenie by malo obsahovať len informácie, ktoré sú nevyhnutne potrebné na to, aby sa príslušné orgány dozvedeli o incidente a v prípade potreby umožnili subjektu požiadať o pomoc. V takomto oznámení by sa prípadne malo uviesť, či je incident pravdepodobne spôsobený protiprávnym alebo zlomyseľným konaním. Členské štáty by mali zabezpečiť, aby požiadavka na predloženie tohto prvotného oznámenia neodklonila zdroje oznamujúceho subjektu od činností súvisiacich s riešením incidentov, ktoré by sa mali uprednostniť. S cieľom zabrániť tomu, aby sa z dôvodu povinností oznamovania incidentov odklákali zdroje od riešenia reakcie na incidenty alebo aby sa inak ohrozilo úsilie subjektov v tejto súvislosti, by členské štáty mali takisto stanoviť, že v riadne odôvodnených prípadoch a po dohode s príslušnými orgánmi alebo jednotkami CSIRT sa dotknutý subjekt môže odchýliť od lehoty 24 hodín pre prvotné oznámenie a od lehoty jedného mesiaca pre záverečnú správu.
- (55) Kľúčové a dôležité subjekty sa často nachádzajú v situácii, keď sa konkrétny incident z dôvodu jeho charakteristík musí oznámiť rôznym orgánom v dôsledku oznamovacej povinnosti zahrnutej v rôznych právnych nástrojoch. Takéto prípady vytvárajú dodatočnú záťaž a môžu viesť aj k nejasnostiam, pokiaľ ide o formát a postupy takéhoto oznamovania. Vzhľadom na to a na účely zjednodušenia oznamovania bezpečnostných incidentov by členské štáty mali zriadiť *jednotné kontaktné miesto* pre všetky oznámenia požadované podľa tejto smernice, ako aj podľa iných právnych predpisov Únie, ako napríklad nariadenie (EÚ) 2016/679 a smernica 2002/58/ES. Agentúra ENISA by spolu so skupinou pre spoluprácu mala vypracovať spoločné vzorové formuláre oznámení prostredníctvom usmernení, ktoré by zjednodušili a zefektívnili oznamovanie informácií požadovaných v právnych predpisoch Únie a znížili záťaž pre podniky.
- (56) Ak existuje podozrenie, že incident súvisí so závažnou trestnou činnosťou podľa práva Únie alebo vnútroštátneho práva, členské štáty by mali nabádať kľúčové a dôležité subjekty na základe platných pravidiel trestného konania v súlade s právom Únie, aby príslušným orgánom presadzovania práva oznamovali incidenty, pri ktorých existuje podozrenie o ich súvisi so závažnou trestnou činnosťou. V prípade potreby a bez toho, aby boli dotknuté pravidlá ochrany osobných údajov, ktoré sa vzťahujú na Europol, je žiaduce, aby centrum EC3 a agentúra ENISA uľahčili koordináciu medzi príslušnými orgánmi a orgánmi presadzovania práva jednotlivých členských štátov.
- (57) V dôsledku incidentov je v mnohých prípadoch ohrozená ochrana osobných údajov. V tejto súvislosti by príslušné orgány mali spolupracovať a vymieňať si informácie o

všetkých relevantných záležitostiach s orgánmi pre ochranu osobných údajov a dozornými orgánmi podľa smernice 2002/58/ES.

- (58) Udržiavanie presných a úplných databáz doménových mien a registračných údajov (tzv. údajov WHOIS) a poskytovanie zákonného prístupu k takýmto údajom je nevyhnutné na zaistenie bezpečnosti, stability a odolnosti DNS, čo zase prispieva k vysokej spoločnej úrovni kybernetickej bezpečnosti v Únii. Ak spracúvanie zahŕňa osobné údaje, takéto spracúvanie musí byť v súlade s právnymi predpismi Únie o ochrane údajov.
- (59) Dostupnosť a včasná prístupnosť týchto údajov pre orgány verejnej moci vrátane príslušných orgánov podľa práva Únie alebo vnútroštátneho práva na predchádzanie trestným činom, ich vyšetrovanie alebo stíhanie, pre jednotky CERT, jednotky CSIRT, a pokiaľ ide o údaje ich klientov pre poskytovateľov elektronických komunikačných sietí a služieb a poskytovateľov kybernetickobezpečnostných technológií a služieb konajúcich v mene týchto klientov, je nevyhnutná na predchádzanie zneužívaniu systému doménových mien a boj proti tomuto zneužívaniu, najmä na predchádzanie kybernetickobezpečnostným incidentom, ich odhaľovanie a reakciu na ne. Takýto prístup by mal byť v súlade s právnymi predpismi Únie o ochrane údajov, pokiaľ ide o osobné údaje.
- (60) S cieľom zabezpečiť dostupnosť presných a úplných údajov o registrácii doménových mien by mali správcovia TLD a subjekty poskytujúce služby registrácie doménových mien pre TLD (tzv. registrátori) zhromažďovať registračné údaje o menách domén a zaručovať ich integritu a dostupnosť. Správcovia TLD a subjekty poskytujúce služby registrácie doménových mien pre TLD by mali najmä stanoviť politiky a postupy na zhromažďovanie a uchovávanie presných a úplných registračných údajov, ako aj na predchádzanie nepresným registračným údajom a ich opravu v súlade s pravidlami Únie v oblasti ochrany údajov.
- (61) Správcovia TLD a subjekty, ktoré pre nich poskytujú služby registrácie doménových mien, by mali zverejňovať registračné údaje o doménových menách, ktoré nepatria do rozsahu pôsobnosti pravidiel Únie v oblasti ochrany údajov, ako sú údaje, ktoré sa týkajú právnických osôb²⁵. Správcovia TLD a subjekty poskytujúce služby registrácie doménových mien pre TLD by tiež mali oprávneným záujemcom o prístup umožniť zákonný prístup k špecifickým registračným údajom o doménových menách týkajúcim sa fyzických osôb v súlade s právnymi predpismi Únie o ochrane údajov. Členské štáty by mali zabezpečiť, aby správcovia TLD a subjekty, ktoré pre nich poskytujú služby registrácie doménových mien, bezodkladne reagovali na žiadosti oprávnených záujemcov o prístup týkajúcich sa zverejnenia registračných údajov o doménových menách. Správcovia TLD a subjekty, ktoré pre nich poskytujú služby registrácie doménových mien, by mali stanoviť politiky a postupy uverejňovania a sprístupňovania registračných údajov vrátane dohôd o úrovni poskytovaných služieb na vybavovanie žiadostí o prístup od oprávnených záujemcov o prístup. Postup týkajúci sa udelenia prístupu môže zahŕňať aj použitie rozhrania, portálu alebo iného technického nástroja na zabezpečenie účinného systému na podávanie žiadostí o registračné údaje a prístup k nim. S cieľom podporovať harmonizované postupy na

²⁵

Odôvodnenie 14 nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679: „Toto nariadenie sa nevzťahuje na spracúvanie osobných údajov, ktoré sa týka právnických osôb, a najmä podnikov založených ako právnické osoby vrátane názvu, formy a kontaktných údajov právnickej osoby.“

celom vnútornom trhu môže Komisia prijať usmernenia o takýchto postupoch bez toho, aby boli dotknuté právomoci Európskeho výboru pre ochranu údajov.

- (62) Všetky kľúčové a dôležité subjekty podľa tejto smernice by mali patriť do jurisdikcie členského štátu, v ktorom poskytujú svoje služby. Ak subjekt poskytuje služby vo viac ako jednom členskom štáte, mal by patriť do samostatnej a súbežnej jurisdikcie každého z týchto členských štátov. Príslušné orgány týchto členských štátov by mali spolupracovať, vzájomne si pomáhať a v prípade potreby vykonávať spoločné opatrenia dohľadu.
- (63) S cieľom zohľadniť cezhraničný charakter služieb a operácií poskytovateľov služieb DNS, správcov mien TLD, poskytovateľov sietí na sprístupňovanie obsahu, poskytovateľov služieb cloud computingu, poskytovateľov služieb dátového centra a poskytovateľov digitálnych služieb by mal mať právomoc nad týmito subjektmi len jeden členský štát. Právomoc by sa mala udeliť členskému štátu, v ktorom má príslušný subjekt hlavné miesto podnikateľskej činnosti v Únii. Kritérium miesta podnikateľskej činnosti na účely tejto smernice zahŕňa účinné vykonávanie činnosti prostredníctvom stabilných dojednaní. Právna forma takýchto dojednaní, či už ide o pobočku alebo dcérsku spoločnosť s právnou subjektivitou, nie je v tomto ohľade určujúcim faktorom. Splňanie tohto kritéria by nemalo závisieť od toho, či sa sieť a informačné systémy fyzicky nachádzajú na danom mieste; samotná prítomnosť a používanie takýchto systémov nepredstavuje hlavné miesto podnikateľskej činnosti, a preto nejde o rozhodujúce kritériá na určenie hlavného miesta podnikateľskej činnosti. Hlavným miestom podnikateľskej činnosti by malo byť miesto v Únii, kde sa prijímajú rozhodnutia týkajúce sa opatrení na riadenie kybernetickobezpečnostných rizík. Zvyčajne zodpovedá miestu ústredia spoločností v Únii. Ak sa takéto rozhodnutia neprijímajú v Únii, predpokladá sa, že hlavné miesto podnikateľskej činnosti by malo byť v členských štátoch, v ktorých majú subjekty miesto podnikateľskej činnosti s najvyšším počtom zamestnancov v Únii. Ak služby vykonáva skupina podnikov, hlavné miesto podnikateľskej činnosti riadiaceho podniku by sa malo považovať za hlavné miesto podnikateľskej činnosti skupiny podnikov.
- (64) V prípadoch, keď poskytovateľ služieb DNS, správca mien TLD, poskytovateľ siete na sprístupňovanie obsahu, poskytovateľ služieb cloud computingu, poskytovateľ služieb dátového centra a poskytovateľ digitálnych služieb, ktorí nie sú usadení v Únii, ponúkajú služby v rámci Únie, mal by sa určiť zástupca. Aby bolo možné určiť, či takýto subjekt ponúka služby v Únii, malo by sa zistiť, či je zřejmé, že daný subjekt plánuje ponúkať služby osobám v jednom alebo vo viacerých členských štátoch. Samotná dostupnosť webového sídla subjektu alebo jeho sprostredkovateľa v Únii alebo e-mailovej adresy a iných kontaktných údajov alebo použitie jazyka, ktorý sa všeobecne používa v tretej krajine, v ktorej je subjekt usadený, nepostačuje na potvrdenie takého úmyslu. Na základe faktorov, ako je používanie jazyka alebo meny bežne používaných v jednom alebo vo viacerých členských štátoch s možnosťou objednania služieb v tomto inom jazyku alebo zmienka o zákazníkoch alebo používateľoch, ktorí sa nachádzajú v Únii, môže byť však zjavné, že subjekt plánuje ponúkať služby v Únii. Zástupca by mal konať v mene subjektu a príslušné orgány alebo jednotky CSIRT by mali mať možnosť zástupcu kontaktovať. Subjekt by mal prostredníctvom písomného mandátu výslovne určiť zástupcu oprávneného konať v mene subjektu v súvislosti s jeho povinnosťami podľa tejto smernice vrátane oznamovania incidentov.

- (65) Ak sa informácie, ktoré sa považujú za utajované podľa vnútroštátneho práva alebo práva Únie, vymieňajú, oznamujú alebo inak zdieľajú podľa ustanovení tejto smernice, mali by sa uplatňovať zodpovedajúce osobitné pravidlá zaobchádzania s utajovanými skutočnosťami.
- (66) Keďže kybernetické hrozby sú čoraz zložitejšie a sofistikovanejšie, dobré opatrenia na odhaľovanie a prevenciu do značnej miery závisia od pravidelného zdieľania spravodajských informácií medzi subjektmi o hrozbách a zraniteľnosti. Zdieľanie informácií prispieva k zvýšenej informovanosti o kybernetických hrozbách, čo zase zvyšuje schopnosť subjektov predchádzať tomu, aby sa hrozby stali skutočnými incidentmi, a subjektom umožňuje lepšie obmedziť vplyvy incidentov a účinnejšie sa z nich zotavovať. Keďže na úrovni Únie neexistujú príslušné usmernenia, zdá sa, že takémuto zdieľaniu spravodajských informácií bránia viaceré faktory, najmä neistota týkajúca sa zlučiteľnosti s pravidlami hospodárskej súťaže a pravidlami týkajúcimi sa zodpovednosti.
- (67) Subjekty by sa mali nabádať, aby kolektívne využívali svoje individuálne znalosti a praktické skúsenosti na strategickej, taktickej a operačnej úrovni s cieľom zlepšiť svoje schopnosti primerane posudzovať kybernetické hrozby, monitorovať ich, brániť sa proti nim a reagovať na ne. Preto treba umožniť, aby sa na úrovni Únie vytvorili mechanizmy dohôd o dobrovoľnom zdieľaní informácií. Na tento účel by členské štáty mali aktívne podporovať a podnecovať aj príslušné subjekty, na ktoré sa nevzťahuje rozsah pôsobnosti tejto smernice, aby sa na takýchto mechanizmoch zdieľania informácií zúčastňovali. Tieto mechanizmy by sa mali vykonávať v plnom súlade s pravidlami Únie týkajúcimi sa hospodárskej súťaže, ako aj právnymi predpismi Únie v oblasti ochrany údajov.
- (68) Spracúvanie osobných údajov v rozsahu, ktorý je nevyhnutne potrebný a primeraný na účely zaistenia bezpečnosti sietí a informácií subjektmi, orgánmi verejnej moci, jednotkami CERT, jednotkami CSIRT a poskytovateľmi bezpečnostných technológií a služieb, by malo predstavovať oprávnený záujem dotknutého prevádzkovateľa, ako sa uvádza v nariadení (EÚ) 2016/679. To by malo zahŕňať opatrenia týkajúce sa prevencie, odhaľovania a analýzy incidentov a reakcie na ne, opatrenia na zvýšenie informovanosti o konkrétnych kybernetických hrozbách, výmenu informácií v kontexte nápravy zraniteľnosti a koordinovaného zverejňovania, ako aj dobrovoľnú výmenu informácií o týchto incidentoch, ako aj o kybernetických hrozbách a zraniteľnostiach, ukazovatele kompromitácie, taktiky, techniky a postupy, kybernetickobezpečnostné varovania a konfiguračné nástroje. Takéto opatrenia si môžu vyžadovať spracovanie týchto druhov osobných údajov: IP adresy, jednotné vyhľadávače prostriedkov (URL), doménové mená a e-mailové adresy.
- (69) S cieľom posilniť právomoci a opatrenia v oblasti dohľadu, ktoré pomáhajú zabezpečiť účinné dodržiavanie predpisov, by sa v tejto smernici mal stanoviť minimálny zoznam opatrení a prostriedkov dohľadu, prostredníctvom ktorých môžu príslušné orgány vykonávať dohľad nad kľúčovými a dôležitými subjektmi. Okrem toho by sa touto smernicou malo zaviesť rozlišovanie režimu dohľadu medzi kľúčovými a dôležitými subjektmi s cieľom zabezpečiť spravodlivú rovnováhu povinností pre subjekty aj príslušné orgány. Kľúčové subjekty by preto mali podliehať plnohodnotnému režimu dohľadu (*ex ante* a *ex post*), zatiaľ čo na dôležité subjekty by sa mal vzťahovať zjednodušený režim dohľadu, a to len *ex post*. V druhom prípade to znamená, že dôležité subjekty by nemali systematicky dokumentovať súlad s požiadavkami na riadenie kybernetickobezpečnostných rizík, zatiaľ čo príslušné

orgány by mali k dohľadu uplatňovať reaktívny prístup *ex post*, a preto by nemali mať všeobecnú povinnosť vykonávať nad týmito subjektmi dohľad.

- (70) Aby bolo presadzovanie povinností účinné, mal by sa stanoviť minimálny zoznam správnych sankcií za porušenie povinností v oblasti riadenia kybernetickobezpečnostných rizík a oznamovania stanovených v tejto smernici, ktorým sa stanoví jasný a konzistentný rámec pre takéto sankcie v celej Únii. Náležitá pozornosť by sa mala venovať povahe, závažnosti a trvaniu porušenia, skutočnej spôsobenej škode alebo vzniknutým stratám alebo potenciálnym škodám či stratám, ktoré mohli vzniknúť, úmyselnému alebo nedbanlivostnému charakteru porušenia, opatreniam prijatým na zabránenie alebo zmiernenie vzniknutej škody a/alebo strát, miere zodpovednosti alebo akémukoľvek relevantnému predchádzajúcemu porušeniu, miere spolupráce s príslušným orgánom a akýmkoľvek ďalším príťažujúcim alebo poľahčujúcim faktorom. Ukladanie sankcií vrátane správnych pokút by malo podliehať primeraným procesným zárukám v súlade so všeobecnými zásadami práva Únie a Charty základných práv Európskej únie vrátane účinnej súdnej ochrany a riadneho procesu.
- (71) S cieľom zabezpečiť účinné presadzovanie povinností stanovených v tejto smernici by mal mať každý príslušný orgán právomoc uložiť správne pokuty alebo požiadať o ich uloženie.
- (72) Keď sa správne pokuty ukladajú podniku, podnik by sa mal na tieto účely považovať za podnik v súlade s článkami 101 a 102 ZFEÚ. Ak sa správne pokuty ukladajú osobám, ktoré nie sú podnikom, dozorný orgán by mal pri rozhodovaní o primeranej výške pokuty zohľadniť všeobecnú úroveň príjmov v členskom štáte, ako aj majetkové pomery danej osoby. Členské štáty by mali rozhodnúť, či orgány verejnej moci budú podliehať správnym pokutám a do akej miery. Uloženie správnej pokuty nemá vplyv na uplatňovanie iných právomocí príslušnými orgánmi alebo iných sankcií stanovených vo vnútroštátnych predpisoch, ktorými sa transponuje táto smernica.
- (73) Členské štáty by mali mať možnosť stanoviť pravidlá o trestných sankciách za porušenie vnútroštátnych pravidiel, ktorými sa transponuje táto smernica. Uloženie trestných sankcií za porušenia takýchto vnútroštátnych predpisov a uloženie súvisiacich správnych sankcií by však nemalo viesť k porušeniu zásady *ne bis in idem*, ako ju vykladá Súdny dvor.
- (74) Členské štáty by mali zaviesť systém, ktorým sa zabezpečia účinné, primerané a odrádzajúce sankcie v prípadoch, keď sa touto smernicou neharmonizujú správne sankcie alebo, ak je to potrebné, aj v iných prípadoch, napríklad v prípade závažného porušenia povinností stanovených v tejto smernici. Povaha týchto sankcií, trestná alebo správna, by sa mala určiť v právnom predpise členského štátu.
- (75) S cieľom ďalej posilniť účinnosť a odrádzajúci účinok sankcií za porušenie povinností stanovených podľa tejto smernice by príslušné orgány mali byť oprávnené uplatňovať sankcie pozostávajúce z pozastavenia certifikácie alebo povolenia časti alebo všetkých služieb, ktoré poskytuje kľúčový subjekt, a uloženia dočasného zákazu fyzickej osobe vykonávať riadiace funkcie. Takéto sankcie by sa vzhľadom na svoju závažnosť a vplyv na činnosti subjektov a v konečnom dôsledku na ich spotrebiteľov mali uplatňovať len úmerne k závažnosti porušenia a s prihliadnutím na osobitné okolnosti každého prípadu vrátane úmyselného alebo nedbanlivostného charakteru porušenia, opatrení prijatých na zabránenie alebo zmiernenie vzniknutej škody a/alebo strát. Takéto sankcie by sa mali uplatňovať len ako *ultima ratio*, čo znamená až po vyčerpaní ostatných príslušných opatrení na presadzovanie povinností stanovených v

tejto smernici, a len na obdobie, kým subjekty, na ktoré sa vzťahujú, neprijmú potrebné opatrenia na nápravu nedostatkov alebo na splnenie požiadaviek príslušného orgánu, v prípade ktorých sa takéto sankcie uplatnili. Ukladanie takýchto sankcií by malo podliehať primeraným procesným zárukám v súlade so všeobecnými zásadami práva Únie a Charty základných práv Európskej únie vrátane účinnej súdnej ochrany, riadneho procesu, prezumpcie nevinu a práva na obhajobu.

- (76) Touto smernicou by sa mali stanoviť pravidlá spolupráce medzi príslušnými orgánmi a dozornými orgánmi v súlade s nariadením (EÚ) 2016/679 s cieľom riešiť porušenia týkajúce sa osobných údajov.
- (77) Cieľom tejto smernice by malo byť zabezpečenie vysokej úrovne zodpovednosti za opatrenia v oblasti riadenia kybernetickobezpečnostných rizík a oznamovacích povinností na úrovni organizácií. Z týchto dôvodov by riadiace orgány subjektov, ktoré patria do rozsahu pôsobnosti tejto smernice, mali schvaľovať opatrenia v oblasti kybernetickobezpečnostných rizík a dohliadať na ich vykonávanie.
- (78) Mal by sa zaviesť mechanizmus partnerského preskúmania, ktorý odborníkom určeným členskými štátmi umožní posúdiť vykonávanie politík v oblasti kybernetickej bezpečnosti vrátane úrovne schopností a dostupných zdrojov členských štátov.
- (79) S cieľom zohľadniť nové kybernetické hrozby, technologický vývoj alebo odvetvové špecifiká by sa mala na Komisiu delegovať právomoc prijímať akty v súlade s článkom 290 ZFEÚ, pokiaľ ide o prvky týkajúce sa opatrení na riadenie rizík, ktoré sa vyžadujú v tejto smernici. Komisia by mala byť splnomocnená prijímať aj delegované akty, v ktorých stanoví, od ktorých kategórií kľúčových subjektov sa vyžaduje získanie certifikátu a v rámci ktorých konkrétnych európskych systémov certifikácie kybernetickej bezpečnosti. Je osobitne dôležité, aby Komisia počas prípravných prác uskutočnila príslušné konzultácie, a to aj na úrovni expertov, a aby tieto konzultácie vykonávala v súlade so zásadami stanovenými v Medziinštitucionálnej dohode z 13. apríla 2016 o lepšej tvorbe práva²⁶. Predovšetkým, v záujme rovnakého zastúpenia pri príprave delegovaných aktov, sa všetky dokumenty doručujú Európskemu parlamentu a Rade v rovnakom čase ako expertom z členských štátov, a experti Európskeho parlamentu a Rady majú systematický prístup na zasadnutia skupín expertov Komisie, ktoré sa zaoberajú prípravou delegovaných aktov.
- (80) S cieľom zabezpečiť jednotné podmienky vykonávania príslušných ustanovení tejto smernice týkajúcich sa procedurálnych opatrení potrebných na fungovanie skupiny pre spoluprácu, technických prvkov týkajúcich sa opatrení na riadenie rizík alebo druhu informácií, formátu a postupu oznamovania incidentov by sa mali na Komisiu preniesť vykonávacie právomoci. Uvedené právomoci by sa mali vykonávať v súlade s nariadením Európskeho parlamentu a Rady (EÚ) č. 182/2011²⁷.
- (81) Komisia by mala túto smernicu pravidelne preskúmavať a radiť sa pritom so zainteresovanými subjektmi najmä s cieľom určiť, či ju treba zmeniť na základe zmien spoločenských, politických, technologických alebo trhových podmienok.
- (82) Keďže cieľ tejto smernice, a to dosiahnutie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, nie je možné uspokojivo dosiahnuť na úrovni samotných

²⁶ Ú. v. EÚ L 123, 12.5.2016, s. 1.

²⁷ Nariadenie Európskeho parlamentu a Rady (EÚ) č. 182/2011 zo 16. februára 2011, ktorým sa ustanovujú pravidlá a všeobecné zásady mechanizmu, na základe ktorého členské štáty kontrolujú vykonávanie vykonávacích právomocí Komisie (Ú. v. EÚ L 55, 28.2.2011, s. 13).

členských štátov, ale z dôvodu účinku tohto opatrenia ho možno lepšie dosiahnuť na úrovni Únie, môže Únia prijať opatrenia v súlade so zásadou subsidiarity podľa článku 5 Zmluvy o Európskej únii. V súlade so zásadou proporcionality podľa uvedeného článku táto smernica neprekračuje rámec nevyhnutný na dosiahnutie tohto cieľa.

- (83) V tejto smernici sa dodržiavajú základné práva a zásady uznané Chartou základných práv Európskej únie, najmä právo na rešpektovanie súkromného života a komunikácie, ochrana osobných údajov, sloboda podnikania, právo vlastníť majetok, právo na účinný prostriedok nápravy pred súdom a právo na vypočutie. Táto smernica by sa mala vykonávať v súlade s uvedenými právami a zásadami,

PRIJALI TÚTO SMERNICU:

KAPITOLA I

Všeobecné ustanovenia

Článok 1

Predmet úpravy

1. Touto smernicou sa stanovujú opatrenia na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v rámci Únie.
2. Na tento účel sa v tejto smernici:
 - a) stanovujú povinnosti členských štátov prijať národné stratégie kybernetickej bezpečnosti, určiť príslušné vnútroštátne orgány, jednotné kontaktné miesta a jednotky pre riešenie počítačových bezpečnostných incidentov (CSIRT);
 - b) stanovujú pre subjekty, ktoré sa podľa svojho typu označujú v prílohe I ako kľúčové subjekty a v prílohe II ako dôležité subjekty, povinnosti riadenia kybernetickobezpečnostných rizík a oznamovania;
 - c) stanovujú povinnosti týkajúce sa zdieľania informácií o kybernetickej bezpečnosti.

Článok 2

Rozsah pôsobnosti

1. Táto smernica sa uplatňuje na verejné a súkromné subjekty, a to typu, ktorý sa v prílohe I označuje ako kľúčové subjekty a v prílohe II ako dôležité subjekty. Táto smernica sa neuplatňuje na subjekty, ktoré v zmysle odporúčania Komisie 2003/361/ES²⁸ spĺňajú kritériá mikropodniku alebo malého podniku.

²⁸

Odporúčanie Komisie 2003/361/ES zo 6. mája 2003 o vymedzení pojmov mikropodnik, malý a stredný podnik (Ú. v. EÚ L 124, 20.5.2003, s. 36).

2. Táto smernica sa však bez ohľadu na ich veľkosť uplatňuje aj na subjekty uvedené v prílohe I a II, keď:
- a) služby poskytuje jeden z týchto subjektov:
 - i) verejné elektronické komunikačné siete alebo verejne dostupné elektronické komunikačné služby uvedené v bode 8 prílohy I;
 - ii) poskytovatelia dôveryhodných služieb uvedených v bode 8 prílohy I;
 - iii) správcovia mien domény najvyššej úrovne a poskytovatelia služby systému doménových mien (DNS) uvedených v bode 8 prílohy I;
 - b) subjekt je subjektom verejnej správy podľa vymedzenia v článku 4 bode 23;
 - c) subjekt je jediným poskytovateľom služby v členskom štáte;
 - d) potenciálne narušenie služby poskytovanej subjektom by mohlo mať vplyv na ochranu verejnosti, verejnú bezpečnosť alebo verejné zdravie;
 - e) potenciálne narušenie služby poskytovanej subjektom by mohlo vyvolať systémové riziká, najmä v odvetviach, v ktorých by takéto narušenie mohlo mať cezhraničný vplyv;
 - f) subjekt je vzhľadom na svoj osobitný význam na regionálnej alebo celoštátnej úrovni kritický pre konkrétne odvetvie alebo typ služby alebo pre iné previazané odvetvia v členskom štáte;
 - g) subjekt je identifikovaný ako kritický subjekt podľa smernice Európskeho parlamentu a Rady (EÚ) XXXX/XXXX²⁹ [smernica o odolnosti kritických subjektov] alebo ako subjekt rovnocenný s kritickým subjektom podľa článku 7 uvedenej smernice.

Členské štáty vypracujú zoznam subjektov identifikovaných podľa písmen b) až f) a predložia ho Komisii do [6 mesiacov po uplynutí lehoty na transpozíciu]. Členské štáty zoznam pravidelne preskúmajú, a to následne aspoň každé dva roky a v prípade potreby ho aktualizujú.

3. Touto smernicou nie sú dotknuté právomoci členských štátov týkajúce sa udržiavania verejnej bezpečnosti, obrany a národnej bezpečnosti v súlade s právom Únie.
4. Táto smernica sa uplatňuje bez toho, aby boli dotknuté smernica Rady 2008/114/ES³⁰ a smernice Európskeho parlamentu a Rady 2011/93/EÚ³¹ a 2013/40/EÚ³².
5. Bez toho, aby bol dotknutý článok 346 ZFEÚ, informácie, ktoré sú dôverné podľa predpisov Únie a vnútroštátnych predpisov, ako napríklad predpisov o obchodnom tajomstve, sa vymieňajú s Komisiou a inými príslušnými orgánmi len v prípade, ak je takáto výmena potrebná na účely uplatňovania tejto smernice. Vymieňané informácie

²⁹ [vlozte celý názov a odkaz na uverejnenie v ú. v., keď budú známe]

³⁰ Smernica Rady 2008/114/ES z 8. decembra 2008 o identifikácii a označení európskych kritických infraštruktúr a zhodnotení potreby zlepšiť ich ochranu (Ú. v. EÚ L 345, 23.12.2008, s. 75).

³¹ 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).

³² 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).

sa obmedzujú na také informácie, ktoré sú relevantné a primerané účelu takejto výmeny. Pri výmene informácií sa zachováva dôvernosť týchto informácií a chráni sa bezpečnostné a obchodné záujmy kľúčových alebo dôležitých subjektov.

6. Ak sa v ustanoveniach právnych aktov Únie špecifických pre určité odvetvie vyžaduje, aby kľúčové alebo dôležité subjekty buď prijali opatrenia na riadenie kybernetickobezpečnostných rizík, alebo aby oznamovali incidenty alebo závažné kybernetické hrozby, 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 VI sa neuplatňujú.

Článok 3

Minimálna harmonizácia

Členské štáty môžu v súlade s touto smernicou a bez toho, aby boli dotknuté ich povinnosti podľa práva Únie, prijať alebo zachovať ustanovenia na dosiahnutie vyššej úrovne kybernetickej bezpečnosti.

Článok 4

Vymedzenie pojmov

Na účely tejto smernice sa uplatňuje toto vymedzenie pojmov:

1. „sieť a informačný systém“ je:
 - a) elektronická komunikačná sieť v zmysle článku 2 bodu 1 smernice (EÚ) 2018/1972;
 - b) každé zariadenie alebo skupina vzájomne prepojených alebo súvisiacich zariadení, z ktorých jedno alebo viaceré vykonávajú na základe programu automatické spracúvanie digitálnych údajov;
 - 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 akémukoľvek konaniu, ktoré ohrozuje dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov;
3. „kybernetická bezpečnosť“ je kybernetická bezpečnosť v zmysle článku 2 bodu 1 nariadenia Európskeho parlamentu a Rady (EÚ) 2019/881³³;

³³

Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/881 zo 17. apríla 2019 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013 (akt o kybernetickej bezpečnosti) (Ú. v. EÚ L 151, 7.6.2019, s. 15).

4. „národná stratégia kybernetickej bezpečnosti“ je súdržný rámec členského štátu, v ktorom sa stanovujú strategické ciele a priority v oblasti bezpečnosti sietí a informačných systémov v danom členskom štáte;
5. „incident“ je každá udalosť ohrozujúca dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov;
6. „riešenie incidentov“ sú všetky kroky a postupy zamerané na odhaľovanie, analýzu a obmedzovanie následkov incidentu a reakcie naň;
7. „kybernetická hrozba“ je kybernetická hrozba v zmysle článku 2 bodu 8 nariadenia (EÚ) 2019/881;
8. „zraniteľnosť“ je slabé miesto, náchylnosť alebo chyba prostriedku, systému, procesu alebo kontroly, ktoré môžu byť zneužitú v rámci kybernetickej hrozby;
9. „zástupca“ je každá fyzická alebo právnická osoba usadená v Únii, ktorá je výslovne určená konať v mene i) poskytovateľa služieb DNS, správcu mien domény najvyššej úrovne (TLD), poskytovateľa služieb cloud computingu, poskytovateľa služieb dátových centier, poskytovateľa siete na sprístupňovanie obsahu podľa bodu 8 prílohy I alebo ii) subjektov uvedených v bode 6 prílohy II, ktoré nie sú usadené v Únii, a vnútroštátny príslušný orgán alebo jednotka CSIRT sa môžu na túto osobu obracať namiesto subjektu, pokiaľ ide o povinnosti daného subjektu podľa tejto smernice;
10. „norma“ je norma v zmysle článku 2 bodu 1 nariadenia Európskeho parlamentu a Rady (EÚ) č. 1025/2012³⁴;
11. „technická špecifikácia“ je technická špecifikácia v zmysle článku 2 bodu 4 nariadenia (EÚ) č. 1025/2012;
12. „internetový prepojovací uzol (IXP)“ je sieťové zariadenie, ktoré umožňuje prepojenie viac než dvoch nezávislých sietí (autonómnych systémov), najmä na účely uľahčenia internetového dátového toku; IXP prepojuje len autonómne systémy; pri IXP nemusí internetový dátový tok medzi ktoroukoľvek dvojicou zúčastnených autonómnych systémov prechádzať cez žiadny tretí autonómny systém, pričom tento dátový tok sa nijako nemení ani sa doň nijako nezasahuje;
13. „systém doménových mien (DNS)“ je hierarchický distribuovaný systém pomenovaní, ktorý umožňuje koncovým používateľom dostať sa k službám a zdrojom na internete;
14. „poskytovateľ služieb DNS“ je subjekt, ktorý koncovým používateľom internetu a iným poskytovateľom služieb DNS poskytuje služby rekurzívneho alebo autoritatívneho rozlišovania doménových mien;
15. „správca mien domény najvyššej úrovne“ je subjekt, ktorému bola udelená osobitná doména najvyššej úrovne (TLD) a ktorý je zodpovedný za správu TLD vrátane registrácie doménových mien v rámci TLD a za technickú prevádzku TLD vrátane

³⁴ 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).

prevádzky menných serverov, údržby databáz a distribúcie zónových súborov TLD v rámci menných serverov;

16. „digitálna služba“ je služba v zmysle článku 1 ods. 1 písm. b) smernice Európskeho parlamentu a Rady (EÚ) 2015/1535³⁵;
17. „online trh“ sú digitálne služby v zmysle článku 2 písm. n) smernice Európskeho parlamentu a Rady 2005/29/ES³⁶;
18. „internetový vyhľadávač“ je digitálna služba v zmysle článku 2 bodu 5 nariadenia Európskeho parlamentu a Rady (EÚ) 2019/1150³⁷;
19. „služba cloud computingu“ je digitálna služba, ktorá umožňuje správu na požiadanie a vzdialený širokopásmový prístup ku škálovateľnému a pružnému súboru zdieľateľných a distribuovaných počítačových zdrojov;
20. „služba dátového centra“ je služba, ktorá zahŕňa štruktúry alebo skupiny štruktúr vyhradené na centralizované umiestnenie, vzájomné prepojenie a prevádzku informačných technológií a sieťového vybavenia poskytujúcich služby ukladania, spracovania a prepravy dát spolu so všetkými zariadeniami a infraštruktúrami na distribúciu elektrickej energie a environmentálnu kontrolu;
21. „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;
22. „platforma služieb sociálnej siete“ je platforma, ktorá koncovým používateľom umožňuje vzájomné prepojenie, zdieľanie, objavovanie a komunikáciu prostredníctvom viacerých zariadení, a najmä prostredníctvom chatov, príspevkov, videí a odporúčaní;
23. „subjekt verejnej správy“ je subjekt v členskom štáte spĺňajúci tieto kritériá:
 - a) je zriadený na účely plnenia potrieb všeobecného záujmu a nemá priemyselný ani komerčný charakter;
 - b) má právnu subjektivitu;
 - c) je z väčšej časti financovaný štátnymi, regionálnymi alebo inými verejnoprávnymi inštitúciami; alebo jeho riadenie podlieha dohľadu týchto orgánov alebo inštitúcií; alebo má správnu, riadiacu alebo dozornú radu, v ktorej viac ako polovicu členov menujú štátne, regionálne alebo iné verejnoprávne inštitúcie;

³⁵ 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).

³⁶ 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).

³⁷ 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).

- d) má právomoc vydávať pre fyzické alebo právnické osoby správne alebo regulačné rozhodnutia, ktoré majú vplyv na ich práva pri cezhraničnom pohybe osôb, tovaru, služieb alebo kapitálu.

Vylúčené sú subjekty verejnej správy, ktoré vykonávajú činnosti v oblasti verejnej bezpečnosti, presadzovania práva, obrany alebo národnej bezpečnosti;

24. „subjekt“ je každá fyzická alebo právnická osoba zriadená a uznaná za takú podľa vnútroštátneho práva v mieste svojho usadenia, ktorá môže vo vlastnom mene vykonávať práva a podliehať povinnostiam;
25. „kľúčový subjekt“ je subjekt typu označeného ako kľúčový subjekt v prílohe I;
26. „dôležitý subjekt“ je subjekt typu označeného ako dôležitý subjekt v prílohe II.

KAPITOLA II

Koordinované regulačné rámce kybernetickej bezpečnosti

Článok 5

Národná stratégia kybernetickej bezpečnosti

1. Každý členský štát prijme národnú stratégiu kybernetickej bezpečnosti, v ktorej sa vymedzia strategické ciele a vhodné politické a regulačné opatrenia na dosiahnutie a zachovanie vysokej úrovne kybernetickej bezpečnosti. Národná stratégia kybernetickej bezpečnosti sietí obsahuje najmä tieto prvky:
- a) vymedzenie cieľov a priorít stratégie členského štátu v oblasti kybernetickej bezpečnosti;
 - b) riadiaci rámec na dosiahnutie týchto cieľov a priorít vrátane politík uvedených v odseku 2, ako aj úloh a zodpovedností vládnych orgánov, inštitúcií a ďalších relevantných aktérov;
 - c) posúdenie s cieľom identifikovať relevantné prostriedky a riziká v oblasti kybernetickej bezpečnosti v danom členskom štáte;
 - d) identifikáciu opatrení na zabezpečenie pripravenosti a reakcie na incidenty a obnovy vrátane spolupráce medzi verejným a súkromným sektorom;
 - e) zoznam rôznych orgánov a aktérov zapojených do vykonávania národnej stratégie kybernetickej bezpečnosti;
 - f) politický rámec pre posilnenú koordináciu medzi príslušnými orgánmi podľa tejto smernice a smernice Európskeho parlamentu a Rady (EÚ) XXXX/XXXX³⁸ [smernica o odolnosti kritických subjektov] na účely výmeny informácií o incidentoch a kybernetických hrozbách a vykonávania úloh dohľadu.
2. Členské štáty v rámci národnej stratégie kybernetickej bezpečnosti prijímajú najmä tieto politiky:

³⁸

[vložte celý názov a odkaz na uverejnenie v ú. v., keď budú známe]

- a) politiku zameranú na kybernetickú bezpečnosť v dodávateľskom reťazci produktov a služieb IKT, ktoré kľúčové a dôležité subjekty používajú na poskytovanie svojich služieb;
 - b) usmernenia týkajúce sa zahrnutia a špecifikácie požiadaviek týkajúcich sa kybernetickej bezpečnosti produktov a služieb IKT vo verejnom obstarávaní;
 - c) politiku na podporu a uľahčenie koordinovaného zverejňovania informácií o zraniteľnosti v zmysle článku 6;
 - d) politiku súvisiacu s udrжанím všeobecnej dostupnosti a integrity verejného jadra otvoreného internetu;
 - e) politiku podporovania a rozvíjania zručností v oblasti kybernetickej bezpečnosti, iniciatívy na zvyšovanie povedomia, ako aj v oblasti výskumu a vývoja;
 - f) politiku podporovania akademických a výskumných inštitúcií pri vývoji nástrojov kybernetickej bezpečnosti a bezpečnej sieťovej infraštruktúry;
 - g) politiku, príslušné postupy a vhodné nástroje na zdieľanie informácií s cieľom podporovať dobrovoľné zdieľanie informácií o kybernetickej bezpečnosti medzi spoločnosťami v súlade s právom Únie;
 - h) politiku zameranú na špecifické potreby MSP, najmä tých MSP, ktoré sú vylúčené z rozsahu pôsobnosti tejto smernice, v súvislosti s usmerneniami a podporou pri zlepšovaní ich odolnosti voči kybernetickobezpečnostným hrozbám.
3. Členské štáty oznámia Komisii svoje národné stratégie kybernetickej bezpečnosti do troch mesiacov od ich prijatia. Z oznámenia môžu vylúčiť špecifické informácie, a to v takom prípade a takom rozsahu, v akom je to nevyhnutne potrebné na zachovanie národnej bezpečnosti.
4. Členské štáty posúdia svoje národné stratégie kybernetickej bezpečnosti aspoň každé štyri roky na základe kľúčových ukazovateľov výkonnosti a v prípade potreby ich zmenia. Agentúra Európskej únie pre kybernetickú bezpečnosť (ENISA) členským štátom na ich žiadosť pomáha pri vypracúvaní národnej stratégie a kľúčových ukazovateľov výkonnosti na posúdenie stratégie.

Článok 6

Koordinované zverejňovanie informácií o zraniteľnosti a európsky register zraniteľností

1. Každý členský štát určí jednu zo svojich jednotiek CSIRT v zmysle článku 9 za koordinátora na účely koordinovaného zverejňovania informácií o zraniteľnosti. Určená jednotka CSIRT koná ako dôveryhodný sprostredkovateľ, ktorý v prípade potreby uľahčuje interakciu medzi oznamujúcim subjektom a výrobcom alebo poskytovateľom produktov IKT alebo služieb IKT. Ak sa oznámená zraniteľnosť týka viacerých výrobcov alebo poskytovateľov produktov IKT alebo služieb IKT v celej Únii, určená jednotka CSIRT každého dotknutého členského štátu spolupracuje so sieťou jednotiek CSIRT.
2. Agentúra ENISA vytvorí a vedie európsky register zraniteľnosti. Na tento účel agentúra ENISA zriadi a udržiava vhodné informačné systémy, politiky a postupy, najmä s cieľom umožniť dôležitým a kľúčovým subjektom a ich dodávateľom sietí a

informačných systémov zverejňovať a registrovať zraniteľnosti v produktoch IKT alebo službách IKT, ako aj poskytovať prístup k informáciám o zraniteľnosti nachádzajúcich sa v registri všetkým zainteresovaným stranám. Register obsahuje najmä informácie opisujúce zraniteľnosť, zasiahnuté produkty IKT alebo služby IKT a závažnosť zraniteľnosti z hľadiska okolností, za ktorých ju možno zneužiť, dostupnosť súvisiacich bezpečnostných záplat a v prípade, že žiadne nie sú k dispozícii, usmernenie pre používateľov zraniteľných produktov a služieb o tom, ako možno zmierniť riziká vyplývajúce zo zverejnených zraniteľností.

Článok 7

Národné rámce krízového riadenia kybernetickej bezpečnosti

1. Každý členský štát určí jeden alebo viac príslušných orgánov zodpovedných za riadenie incidentov a kríz veľkého rozsahu. Členské štáty zabezpečia, aby príslušné orgány mali primerané zdroje na účinné a efektívne vykonávanie zverených úloh.
2. Každý členský štát určí kapacity, prostriedky a postupy, ktoré možno použiť v prípade krízy na účely tejto smernice.
3. Každý členský štát prijme národný plán reakcie na kybernetickobezpečnostné incidenty a krízy, v ktorom sú stanovené ciele a spôsoby riadenia kybernetickobezpečnostných incidentov a kríz veľkého rozsahu. V pláne sa stanovia najmä tieto prvky:
 - a) ciele vnútroštátnych opatrení a činností v oblasti pripravenosti;
 - b) úlohy a zodpovednosti vnútroštátnych príslušných orgánov;
 - c) postupy krízového riadenia a kanály na výmenu informácií;
 - d) opatrenia v oblasti pripravenosti vrátane cvičení a činností odbornej prípravy;
 - e) príslušné verejné a súkromné zainteresované strany a použitá infraštruktúra;
 - f) vnútroštátne postupy a dojednania medzi príslušnými vnútroštátnymi orgánmi a inštitúciami s cieľom zabezpečiť účinnú účasť členského štátu na koordinovanom riadení kybernetickobezpečnostných incidentov a kríz veľkého rozsahu na úrovni Únie, ako aj jeho podporu tohto riadenia.
4. Členské štáty oznámia Komisii určenie svojich príslušných orgánov uvedených v odseku 1 a predložia svoje vnútroštátne plány reakcie na kybernetickobezpečnostné incidenty a krízy uvedené v odseku 3 do troch mesiacov od tohto určenia a prijatia týchto plánov. Členské štáty môžu z plánu vylúčiť špecifické informácie, a to v takom prípade a takom rozsahu, v akom je to nevyhnutne potrebné pre ich národnú bezpečnosť.

Článok 8

Vnútroštátne príslušné orgány a jednotné kontaktné miesta

1. Každý členský štát určí jeden alebo viacero príslušných orgánov zodpovedných za kybernetickú bezpečnosť a za úlohy dohľadu uvedené v kapitole VI tejto smernice. Členské štáty môžu na tento účel určiť už existujúci orgán alebo existujúce orgány.

2. Príslušné orgány uvedené v odseku 1 monitorujú uplatňovanie tejto smernice na vnútroštátnej úrovni.
3. Každý členský štát určí jedno vnútroštátne jednotné kontaktné miesto pre kybernetickú bezpečnosť (ďalej len „jednotné kontaktné miesto“). Ak členský štát určí iba jeden príslušný orgán, tento 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 v iných členských štátoch, ako aj zabezpečiť medziodvetvovú spoluprácu s inými príslušnými vnútroštátnymi orgánmi v rámci daného členského štátu.
5. Členské štáty zabezpečia, aby príslušné orgány uvedené v odseku 1 a jednotné kontaktné miesta mali primerané zdroje na účinné a efektívne vykonávanie zverených úloh, a teda na plnenie cieľov tejto smernice. Členské štáty zabezpečia účinnú, efektívnu a bezpečnú spoluprácu určených zástupcov v rámci skupiny pre spoluprácu uvedenej v článku 12.
6. Každý členský štát bez zbytočného odkladu oznámi Komisii určenie príslušného orgánu uvedeného v odseku 1 a jednotného kontaktného miesta uvedeného v odseku 3, ich úlohy a akékoľvek následné zmeny. Každý členský štát svoje určenie uverejní. Komisia uverejní zoznam určených jednotných kontaktných miest.

Článok 9

Jednotky pre riešenie počítačových bezpečnostných incidentov (jednotky CSIRT)

1. Každý členský štát určí jednu alebo viac jednotiek CSIRT, ktoré spĺňajú požiadavky stanovené v článku 10 ods. 1, pokrývajú aspoň odvetvia, pododvetvia alebo subjekty uvedené v prílohách I a II a zodpovedajú za riešenie incidentov podľa presne stanoveného postupu. Jednotku CSIRT možno zriadiť v rámci príslušného orgánu uvedeného v článku 8.
2. Členské štáty zabezpečia, aby každá jednotka CSIRT mala primerané zdroje na účinné plnenie svojich úloh stanovených v článku 10 ods. 2.
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 inými relevantnými zainteresovanými stranami. Členské štáty na tento účel zabezpečia, aby jednotky CSIRT prispievali k zavádzaniu bezpečných nástrojov na výmenu informácií.
4. Jednotky CSIRT spolupracujú a v prípade potreby si vymieňajú relevantné informácie v súlade s článkom 26 s dôveryhodnými odvetvovými alebo medziodvetvovými komunitami kľúčových a dôležitých subjektov.
5. Jednotky CSIRT sa zúčastňujú na partnerských preskúmaniach organizovaných v súlade s článkom 16.
6. Členské štáty zabezpečia účinnú, efektívnu a bezpečnú spoluprácu svojich jednotiek CSIRT v rámci siete jednotiek CSIRT uvedenej v článku 13.
7. Členské štáty bez zbytočného odkladu oznámia Komisii jednotky CSIRT určené v súlade s odsekom 1, koordinátora jednotiek CSIRT určeného v súlade s článkom 6

ods. 1 a ich príslušné úlohy stanovené vo vzťahu k subjektom uvedeným v prílohách I a II.

8. Členské štáty môžu pri zriaďovaní vnútroštátnych jednotiek CSIRT požiadať o pomoc agentúru ENISA.

Článok 10

Požiadavky na jednotky CSIRT a ich úlohy

1. Jednotky CSIRT musia spĺňať tieto požiadavky:
 - a) jednotky CSIRT musia zabezpečovať vysokú úroveň dostupnosti svojich komunikačných služieb, a to tak, že predchádzajú tomu, aby zlyhali ako celok, ak zlyhá ich ľubovoľný jediný bod, a musia mať k dispozícii niekoľko spôsobov, ktorými ich možno kedykoľvek kontaktovať a ktorými môžu tieto jednotky kontaktovať iných. Jednotky CSIRT musia jasne špecifikovať komunikačné kanály a oboznámiť s nimi zainteresované strany a spolupracujúcich partnerov;
 - b) pracoviská jednotiek CSIRT a podporné informačné systémy musia byť umiestnené na zabezpečených miestach;
 - c) jednotky CSIRT musia mať zavedený vhodný systém riadenia a zasielania žiadostí, a to najmä s cieľom uľahčiť ich účinné a efektívne odovzdávanie;
 - d) jednotky CSIRT musia byť primerane personálne vybavené, aby sa zabezpečila stála dostupnosť ich služieb;
 - e) jednotky CSIRT musia byť vybavené redundantnými systémami a záložným pracovným priestorom na zabezpečenie kontinuity svojich služieb;
 - f) jednotky CSIRT musia mať možnosť zapojiť sa do sietí medzinárodnej spolupráce.
2. Jednotky CSIRT plnia tieto úlohy:
 - a) monitorujú kybernetické hrozby, zraniteľnosti a incidenty na vnútroštátnej úrovni;
 - b) poskytujú kľúčovým a dôležitým subjektom, ako aj iným relevantným zainteresovaným stranám včasné varovanie, výstrahy, hlásenia a šíria informácie o kybernetických hrozbách, zraniteľnostiach a incidentoch;
 - c) reagujú na incidenty;
 - d) pripravujú dynamickú analýzu rizík a incidentov a poskytujú situačný prehľad o kybernetickej bezpečnosti;
 - e) na žiadosť subjektu proaktívne kontrolujú siete a informačné systémy používané na poskytovanie jeho služieb;
 - f) zapájajú sa do siete jednotiek CSIRT a poskytujú vzájomnú pomoc ostatným členom siete na ich žiadosť.
3. Jednotky CSIRT nadviažu spoluprácu s príslušnými aktérmi v súkromnom sektore s cieľom lepšie dosiahnuť ciele smernice.

4. Jednotky CSIRT v záujme uľahčenia spolupráce podporujú prijímanie a využívanie spoločných alebo normalizovaných postupov, režimov utajenia a taxonómie v súvislosti s týmito prvkami:
- a) postupy riešenia incidentov;
 - b) krízové riadenie kybernetickej bezpečnosti;
 - c) koordinované zverejňovanie informácií o zraniteľnosti.

Článok 11

Spolupráca na vnútroštátnej úrovni

1. Ak príslušné orgány uvedené v článku 8, jednotné kontaktné miesto a jednotky CSIRT jedného členského štátu sú samostatnými subjektmi, pri plnení povinností stanovených v tejto smernici vzájomne spolupracujú.
2. Členské štáty zabezpečia, aby ich príslušné orgány alebo jednotky CSIRT dostávali oznámenia o incidentoch, závažných kybernetických hrozbách a udalostiach odvrátených v poslednej chvíli predkladané podľa tejto smernice. Ak členský štát rozhodne, že jeho jednotky CSIRT nemajú dostávať tieto oznámenia, jednotkám CSIRT sa v rozsahu potrebnom na plnenie ich úloh poskytne prístup k údajom o incidentoch, ktoré oznámili kľúčové alebo dôležité subjekty podľa článku 20.
3. Členské štáty zabezpečia, aby ich príslušné orgány alebo jednotky CSIRT informovali jednotné kontaktné miesto o oznámeniach o incidentoch, závažných kybernetických hrozbách a udalostiach odvrátených v poslednej chvíli predkladaných podľa tejto smernice.
4. Členské štáty v rozsahu potrebnom na účinné plnenie úloh a povinností stanovených v tejto smernici zabezpečia primeranú spoluprácu medzi príslušnými orgánmi a jednotnými kontaktnými miestami, ako aj orgánmi presadzovania práva, orgánmi na ochranu údajov a orgánmi zodpovednými za kritickú infraštruktúru podľa smernice (EÚ) XXXX/XXXX [smernica o odolnosti kritických subjektov] a vnútroštátnymi finančnými orgánmi určenými v súlade s nariadením Európskeho parlamentu a Rady (EÚ) XXXX/XXXX³⁹ [nariadenie DORA] v rámci daného členského štátu.
5. Členské štáty zabezpečia, aby ich príslušné orgány pravidelne poskytovali príslušným orgánom určeným podľa smernice (EÚ) XXXX/XXXX [smernica o odolnosti kritických subjektov] informácie o kybernetickobezpečnostných rizikách, kybernetických hrozbách a incidentoch, ktoré zasiahli kľúčové subjekty identifikované ako kritické alebo rovnocenné s kritickými subjektmi podľa smernice (EÚ) XXXX/XXXX [smernica o odolnosti kritických subjektov], ako aj opatrenia prijaté príslušnými orgánmi v reakcii na tieto riziká a incidenty.

³⁹

[vložte celý názov a odkaz na uverejnenie v ú. v., keď budú známe]

KAPITOLA III

Spolupráca

Článok 12

Skupina pre spoluprácu

1. S cieľom podporiť a uľahčiť strategickú spoluprácu a výmenu informácií medzi členskými štátmi v oblasti uplatňovania tejto smernice sa zriaďuje skupina pre spoluprácu.
2. Skupina pre spoluprácu si plní úlohy na základe dvojročných pracovných programov uvedených v odseku 6.
3. Skupina pre spoluprácu sa skladá zo zástupcov členských štátov, Komisie a agentúry ENISA. Na činnostiach skupiny pre spoluprácu sa ako pozorovateľ zúčastňuje Európska služba pre vonkajšiu činnosť. Na činnostiach skupiny pre spoluprácu sa môžu zúčastňovať európske orgány dohľadu (ESA) v súlade s článkom 17 ods. 5 písm. c) nariadenia (EÚ) XXXX/XXXX [nariadenie DORA].

Vo vhodných prípadoch môže skupina pre spoluprácu prizvať k svojej práci zástupcov príslušných zainteresovaných strán.

Sekretariát zabezpečuje Komisia.

4. Skupina pre spoluprácu plní tieto úlohy:
 - a) poskytovanie usmernení príslušným orgánom v súvislosti s transpozíciou a vykonávaním tejto smernice;
 - b) výmena najlepších postupov a informácií v súvislosti s vykonávaním tejto smernice, a to aj pokiaľ ide o kybernetické hrozby, incidenty, zraniteľnosti, udalosti odvrátené v poslednej chvíli, iniciatívy na zvyšovanie povedomia, odbornú prípravu, cvičenia a zručnosti, budovanie kapacít, ako aj normy a technické špecifikácie;
 - c) vzájomné poradenstvo a spolupráca s Komisiou v súvislosti s novými politickými iniciatívami v oblasti kybernetickej bezpečnosti;
 - d) vzájomné poradenstvo a spolupráca s Komisiou v súvislosti s návrhom vykonávacích alebo delegovaných aktov Komisie prijatých podľa tejto smernice;
 - e) výmena najlepších postupov a informácií s príslušnými inštitúciami, orgánmi, úradmi a agentúrami Únie;
 - f) prediskutovanie správ o partnerskom preskúmaní uvedených v článku 16 ods. 7;
 - g) prediskutovanie výsledkov spoločných činností dohľadu v cezhraničných prípadoch, ako sa uvádza v článku 34;
 - h) poskytovanie strategických usmernení sieti jednotiek CSIRT v súvislosti s konkrétnymi vznikajúcimi otázkami;
 - i) prispievanie ku kybernetickobezpečnostným schopnostiam v celej Únii uľahčovaním výmeny vnútroštátnych úradníkov prostredníctvom

programu budovania kapacít, do ktorého sú zapojení zamestnanci z príslušných orgánov členských štátov alebo jednotiek CSIRT;

- j) organizovanie pravidelných spoločných stretnutí s príslušnými súkromnými zainteresovanými stranami z celej Únie s cieľom prediskutovať činnosti skupiny a zhromažďovať informácie o nových politických výzvach;
 - k) prediskutovanie práce vykonanej v súvislosti s kybernetickobezpečnostnými cvičeniami vrátane práce agentúry ENISA.
- 5. Skupina pre spoluprácu môže od siete jednotiek CSIRT požadovať technickú správu na vybrané témy.
 - 6. Do ... [24 mesiacov po nadobudnutí účinnosti tejto smernice] a potom každé dva roky skupina pre spoluprácu zostavuje pracovný program týkajúci sa činností, ktoré sa majú vykonávať v rámci plnenia jej cieľov a úloh. Časový rámec prvého programu prijatého podľa tejto smernice sa zosúladí s časovým rámcom posledného programu prijatého podľa smernice (EÚ) 2016/1148.
 - 7. Komisia môže prijať vykonávacie akty stanovujúce procesné opatrenia potrebné na fungovanie skupiny pre spoluprácu. Uvedené vykonávacie akty sa prijímú v súlade s postupom preskúmania, na ktorý sa odkazuje v článku 37 ods. 2.
 - 8. Skupina pre spoluprácu sa pravidelne a aspoň raz ročne stretáva so skupinou pre odolnosť kritických subjektov zriadenou podľa smernice (EÚ) XXXX/XXXX [smernica o odolnosti kritických subjektov] s cieľom podporovať strategickú spoluprácu a výmenu informácií.

Článok 13

Sieť jednotiek CSIRT

- 1. S cieľom prispieť k zvyšovaniu dôvery a podporiť rýchlu a účinnú operačnú spoluprácu medzi členskými štátmi sa zriaďuje sieť vnútroštátnych jednotiek CSIRT.
- 2. Sieť jednotiek CSIRT sa skladá zo zástupcov jednotiek CSIRT členských štátov a jednotky CERT-EU. Komisia sa zúčastňuje na práci siete jednotiek CSIRT ako pozorovateľ. Agentúra ENISA zabezpečuje sekretariát a aktívne podporuje spoluprácu medzi jednotkami CSIRT.
- 3. Sieť jednotiek CSIRT plní tieto úlohy:
 - a) výmena informácií o schopnostiach jednotiek CSIRT;
 - b) výmena relevantných informácií o incidentoch, udalostiach odvrátených v poslednej chvíli, kybernetických hrozbách, rizikách a zraniteľnostiach;
 - c) na žiadosť zástupcu siete jednotiek CSIRT potenciálne zasiahnutej incidentom výmena a prediskutovanie informácií o danom incidente a súvisiacich kybernetických hrozbách, rizikách a zraniteľnostiach;
 - d) na žiadosť zástupcu siete jednotiek CSIRT prediskutovanie a pokiaľ možno vykonanie koordinovanej reakcie na incident, ktorý bol identifikovaný v jurisdikcii daného členského štátu;

- e) poskytovanie podpory členským štátom pri riešení cezhraničných incidentov podľa tejto smernice;
 - f) spolupráca a poskytovanie pomoci určeným jednotkám CSIRT uvedeným v článku 6, pokiaľ ide o riadenie viacstranného koordinovaného zverejňovania informácií o zraniteľnostiach, ktoré zasiahli viacerých výrobcov alebo poskytovateľov produktov IKT, služieb IKT a procesov IKT, ktorí majú sídlo v rôznych členských štátoch;
 - g) 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 spôsobmi koordinácie pri reakcii na cezhraničné riziká a incidenty;
 - v) s príspevkom k národnému plánu reakcie na kybernetickobezpečnostné incidenty a krízy uvedeného v článku 7 ods. 3;
 - h) informovanie skupiny pre spoluprácu o svojej činnosti a o ďalších formách operačnej spolupráce prediskutovaných podľa písmena g), v prípade potreby požadovanie usmernení v tomto ohľade;
 - i) bilancia kybernetickobezpečnostných cvičení vrátane cvičení organizovaných agentúrou ENISA;
 - j) na žiadosť niektorej jednotky CSIRT prediskutovanie schopností a pripravenosti tejto jednotky CSIRT;
 - k) spolupráca a výmena informácií s regionálnymi a únijnými centrami bezpečnostných operácií (SOC) s cieľom zlepšiť spoločné situačné povedomie o incidentoch a hrozbách v celej Únii;
 - l) prediskutovanie správ o partnerskom preskúmaní uvedených v článku 16 ods. 7;
 - m) vydávanie usmernení s cieľom uľahčiť zblížovanie operačných postupov so zreteľom na uplatňovanie ustanovení tohto článku, pokiaľ ide o operačnú spoluprácu.
4. Na účely preskúmania uvedeného v článku 35 sieť jednotiek CSIRT do [24 mesiacov odo dňa nadobudnutia účinnosti tejto smernice] a potom každé dva roky posúdi pokrok dosiahnutý v rámci operačnej spolupráce a vypracuje správu. V správe sa predovšetkým vyvodí závery o výsledkoch partnerských preskúmaní uvedených v článku 16 a vykonaných v súvislosti s vnútroštátnymi jednotkami CSIRT vrátane záverov a odporúčaní, ktoré sa vykonávajú podľa tohto článku. Táto správa sa predloží aj skupine pre spoluprácu.
5. Sieť jednotiek CSIRT prijme vlastný rokovací poriadok.

Článok 14

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

1. S cieľom podporiť koordinované riadenie kybernetickobezpečnostných incidentov a kríz veľkého rozsahu na operačnej úrovni a zabezpečiť pravidelnú výmenu informácií medzi členskými štátmi a inštitúciami, orgánmi a agentúrami Únie sa týmto zriaďuje Európska sieť styčných organizácií pre kybernetické krízy (EU-CyCLONE).
2. Sieť EU-CyCLONE tvoria zástupcovia orgánov krízového riadenia členských štátov určených v súlade s článkom 7, Komisia a agentúra ENISA. Agentúra ENISA zabezpečuje sekretariát siete a podporuje bezpečnú výmenu informácií.
3. Sieť EU-CyCLONE plní tieto úlohy:
 - a) zvyšovanie úrovne pripravenosti na riadenie incidentov a kríz veľkého rozsahu;
 - b) vytváranie spoločného situačného povedomia o relevantných kybernetickobezpečnostných udalostiach;
 - c) koordinácia riadenia incidentov a kríz veľkého rozsahu, ako aj podpora rozhodovania na politickej úrovni v súvislosti s takýmito incidentmi a krízami;
 - d) prediskutovanie národných plánov podľa článku 7 ods. 2 týkajúcich sa kybernetickobezpečnostných incidentov a reakcie na ne.
4. Sieť EU-CyCLONE prijme svoj rokovací poriadok.
5. Sieť EU-CyCLONE pravidelne podáva skupine pre spoluprácu správy o kybernetických hrozbách, incidentoch a trendoch, pričom sa zameriava najmä na ich vplyv na kľúčové a dôležité subjekty.
6. Sieť EU-CyCLONE spolupracuje so sieťou jednotiek CSIRT na základe dohodnutých procedurálnych opatrení.

Článok 15

Správa o stave kybernetickej bezpečnosti v Únii

1. Agentúra ENISA v spolupráci s Komisiou vydáva každé dva roky správu o stave kybernetickej bezpečnosti v Únii. Správa obsahuje najmä posúdenie týchto aspektov:
 - a) rozvoj kybernetickobezpečnostných schopností v celej Únii;
 - b) technické, finančné a ľudské zdroje, ktoré majú príslušné orgány k dispozícii, a politiky kybernetickej bezpečnosti, ako aj vykonávanie opatrení v oblasti dohľadu a opatrení na presadzovanie práva na základe výsledkov partnerských preskúmaní uvedených v článku 16;
 - c) index kybernetickej bezpečnosti poskytujúci súhrnné posúdenie úrovne vyspelosti kybernetickobezpečnostných schopností.
2. Správa obsahuje konkrétne politické odporúčania na zvýšenie úrovne kybernetickej bezpečnosti v celej Únii a zhrnutie zistení za konkrétne obdobie z technických

situačných správ EÚ o kybernetickej bezpečnosti, ktoré vydala agentúra ENISA v súlade s článkom 7 ods. 6 nariadenia (EÚ) 2019/881.

Článok 16

Partnerské preskúmania

1. Komisia po konzultácii so skupinou pre spoluprácu a agentúrou ENISA a najneskôr 18 mesiacov od nadobudnutia účinnosti tejto smernice stanoví metodiku a obsah systému partnerského preskúmania na posúdenie účinnosti politík členských štátov v oblasti kybernetickej bezpečnosti. Preskúmania vykonávajú technickí experti v oblasti kybernetickej bezpečnosti vybraní z iných členských štátov, než je skúmaný členský štát, a zameriavajú sa aspoň na:
 - i) účinnosť vykonávania požiadaviek na riadenie kybernetickobezpečnostných rizík a oznamovacích povinností uvedených v článkoch 18 a 20;
 - ii) úroveň schopností vrátane dostupných finančných, technických a ľudských zdrojov a účinnosť plnenia úloh príslušných vnútroštátnych orgánov;
 - iii) operačné schopnosti a účinnosť jednotiek CSIRT;
 - iv) účinnosť vzájomnej pomoci uvedenej v článku 34;
 - v) účinnosť rámca na zdieľanie informácií uvedeného v článku 26 tejto smernice.
2. Metodika zahŕňa objektívne, nediskriminačné, spravodlivé a transparentné kritériá, na základe ktorých členské štáty určia expertov oprávnených vykonávať partnerské preskúmania. Agentúra ENISA a Komisia určia expertov, ktorí sa ako pozorovatelia zúčastňujú na partnerských preskúmaniach. Komisia s podporou agentúry ENISA vytvorí v rámci metodiky uvedenej v odseku 1 objektívny, nediskriminačný, spravodlivý a transparentný systém výberu a náhodného pridelovania expertov pre každé partnerské preskúmanie.
3. O organizačných aspektoch partnerských preskúmaní rozhoduje Komisia s podporou agentúry ENISA a po konzultácii so skupinou pre spoluprácu tieto aspekty vychádzajú z kritérií vymedzených v metodike uvedenej v odseku 1. V partnerských preskúmaniach sa posudzujú aspekty uvedené v odseku 1 pre všetky členské štáty a odvetvia vrátane vybraných problémov špecifických pre jeden alebo viacero členských štátov alebo pre jedno alebo viacero odvetví.
4. Partnerské preskúmania zahŕňajú skutočné alebo virtuálne návštevy na mieste a výmenu informácií na diaľku. Vzhľadom na zásadu dobrej spolupráce členské štáty, ktoré sú predmetom preskúmania, poskytnú určeným expertom požadované informácie potrebné na posúdenie skúmaných aspektov. Všetky informácie získané v procese partnerského preskúmania sa použijú výlučne na uvedený účel. Experti, ktorí sa zúčastňujú na partnerskom preskúmaní, nesmú sprístupniť tretím stranám žiadne citlivé alebo dôverné informácie získané v priebehu tohto preskúmania.
5. Tie isté aspekty po preskúmaní v určitom členskom štáte nepodliehajú ďalšiemu partnerskému preskúmaniu v rámci tohto členského štátu počas dvoch rokov od ukončenia partnerského preskúmania, pokiaľ Komisia po konzultácii s agentúrou ENISA a skupinou pre spoluprácu nerozhodne inak.

6. Členský štát zabezpečí, aby sa akékoľvek riziko konfliktu záujmov týkajúce sa určených expertov bez zbytočného odkladu oznámilo ostatným členským štátom, Komisii a agentúre ENISA.
7. Experti zúčastňujúci sa na partnerských preskúmaniach vypracujú správy o zisteniach a záveroch preskúmaní. Správy sa predkladajú Komisii, skupine pre spoluprácu, sieti jednotiek CSIRT a agentúre ENISA. Prediskutujú sa v skupine pre spoluprácu a v sieti jednotiek CSIRT. Správy možno uverejniť na vyhradenom webovom sídle skupiny pre spoluprácu.

KAPITOLA IV

Povinnosti týkajúce sa riadenia kybernetickobezpečnostných rizík a oznamovania

ODDIEL I

Riadenie kybernetickobezpečnostných rizík a oznamovanie

Článok 17

Riadenie

1. Členské štáty zabezpečia, aby riadiace orgány kľúčových a dôležitých subjektov schválili opatrenia na riadenie kybernetickobezpečnostných rizík, ktoré tieto subjekty prijali s cieľom dosiahnuť súlad s článkom 18, dohliadali na jeho vykonávanie a zodpovedali sa za to, ak subjekty nedodržiavajú povinnosti podľa tohto článku.
2. Členské štáty zabezpečia, aby členovia riadiaceho orgánu pravidelne absolvovali osobitnú odbornú prípravu s cieľom získať dostatočné znalosti a zručnosti s cieľom zachytiť a posúdiť riziká a postupy riadenia v oblasti kybernetickej bezpečnosti a ich vplyv na činnosť subjektu.

Článok 18

Opatrenia na riadenie kybernetickobezpečnostných rizík

1. Členské štáty zabezpečia, aby kľúčové a dôležité subjekty prijali vhodné a primerané technické a organizačné opatrenia na riadenie rizík súvisiacich s bezpečnosťou sietí a informačných systémov, ktoré tieto subjekty využívajú pri poskytovaní svojich služieb. S ohľadom na najnovší technický vývoj tieto opatrenia zabezpečujú takú úroveň bezpečnosti sietí a informačných systémov, ktorá zodpovedá miere daného rizika.
2. Opatrenia uvedené v odseku 1 obsahujú aspoň:
 - a) analýzu rizika a bezpečnostné politiky informačného systému;
 - b) riešenie incidentov (predchádzanie incidentom, ich odhaľovanie a reakcia na ne);

- c) kontinuita činností a krízové riadenie;
 - d) bezpečnosť dodávateľského reťazca vrátane bezpečnostných aspektov týkajúcich sa vzťahov medzi každým subjektom a jeho dodávateľmi alebo poskytovateľmi služieb, ako sú napríklad poskytovatelia služieb ukladania a spracúvania dát alebo riadených bezpečnostných služieb;
 - e) bezpečnosť pri nadobúdaní, vývoji a údržbe sietí a informačných systémov vrátane riešenia zraniteľností a zverejňovania informácií o zraniteľnostiach;
 - f) politiky a postupy (testovanie a audit) na posúdenie účinnosti opatrení na riadenie kybernetickobezpečnostných rizík;
 - g) používanie kryptografie a šifrovania.
3. Členské štáty zabezpečia, aby subjekty pri zvažovaní vhodných opatrení uvedených v odseku 2 písm. d) zohľadňovali zraniteľnosti špecifické pre každého dodávateľa a poskytovateľa služieb a celkovú kvalitu produktov a prax ich dodávateľov a poskytovateľov služieb v oblasti kybernetickej bezpečnosti vrátane ich postupov bezpečného vývoja.
 4. Členské štáty zabezpečia, aby subjekt po zistení, že jeho služby alebo úlohy nie sú v súlade s požiadavkami stanovenými v odseku 2, prijal bez zbytočného odkladu všetky potrebné nápravné opatrenia a danú službu s týmito požiadavkami zosúladiť.
 5. Komisia môže prijať vykonávacie akty s cieľom stanoviť technické a metodické špecifikácie prvkov uvedených v odseku 2. Pri vypracúvaní týchto aktov Komisia postupuje v súlade s postupom preskúmania, na ktorý sa odkazuje v článku 37 ods. 2, a v čo najväčšej možnej miere dodržiava medzinárodné a európske normy, ako aj príslušné technické špecifikácie.
 6. Komisia je splnomocnená prijímať delegované akty v súlade s článkom 36 s cieľom doplniť prvky stanovené v odseku 2 na zohľadnenie nových kybernetických hrozieb, technologického vývoja alebo odvetvových špecifik.

Článok 19

Koordinované posúdenia rizika kritických dodávateľských reťazcov na úrovni EÚ

1. Skupina pre spoluprácu môže v spolupráci s Komisiou a agentúrou ENISA vykonávať koordinované posúdenia bezpečnostného rizika dodávateľských reťazcov konkrétnych kritických služieb, systémov alebo produktov IKT, pričom zohľadní technické a prípadne aj netechnické faktory rizík.
2. Komisia po konzultácii so skupinou pre spoluprácu a agentúrou ENISA určí konkrétne kritické služby, systémy alebo produkty IKT, ktoré môžu podliehať koordinovanému posúdeniu rizika uvedenému v odseku 1.

Článok 20

Oznamovacie povinnosti

1. Členské štáty zabezpečia, aby kľúčové a dôležité subjekty bez zbytočného odkladu oznámili príslušným orgánom alebo jednotke CSIRT v súlade s odsekmi 3 a 4 každý

incident so závažným vplyvom na poskytovanie ich služieb. V prípade potreby tieto subjekty bez zbytočného odkladu oznámia príjemcom svojich služieb incidenty, ktoré by mohli nepriaznivo ovplyvniť ich poskytovanie. Členské štáty zabezpečia, aby tieto subjekty oznamovali okrem iného informácie umožňujúce príslušným orgánom alebo jednotke CSIRT určiť prípadný cezhraničný vplyv incidentu.

2. Členské štáty zabezpečia, aby kľúčové a dôležité subjekty bez zbytočného odkladu oznámili príslušným orgánom alebo jednotke CSIRT každú závažnú kybernetickú hrozbu, ktorú tieto subjekty zistia a ktorá by mohla potenciálne viesť k závažnému incidentu.

Uvedené subjekty v príslušných prípadoch bez zbytočného odkladu oznámia príjemcom svojich služieb, ktorých potenciálne zasiahla závažná kybernetická hrozba, všetky opatrenia alebo nápravné kroky, ktoré títo príjemcovia môžu v reakcii na danú hrozbu prijať. Subjekty v prípade potreby týmto príjemcom oznámia aj informáciu o samotnej hrozbe. Oznámenie nesmie mať pre oznamujúci subjekt za následok vyššiu zodpovednosť.

3. Incident sa považuje za závažný, ak:
 - a) dotknutému subjektu spôsobil alebo môže spôsobiť podstatné narušenie prevádzky alebo finančné straty;
 - b) zasiahol alebo môže zasiahnuť iné fyzické alebo právnické osoby spôsobením značných hmotných alebo nehmotných strát.
4. Členské štáty zabezpečia, aby dotknuté subjekty na účely oznámenia podľa odseku 1 predložili príslušným orgánom alebo jednotke CSIRT:
 - a) bez zbytočného odkladu a v každom prípade do 24 hodín od zistenia incidentu prvotné oznámenie, v ktorom sa prípadne uvedie, či incident pravdepodobne spôsobilo nezákonné alebo zlomyseľné konanie;
 - b) na žiadosť príslušného orgánu alebo jednotky CSIRT priebežnú správu o relevantných aktualizáciách daného stavu;
 - c) najneskôr jeden mesiac po predložení oznámenia podľa písmena a) konečnú správu, ktorá obsahuje aspoň tieto informácie:
 - i) podrobný opis incidentu, jeho závažnosť a vplyv;
 - ii) druh hrozby alebo základnú príčinu, ktorá pravdepodobne incident spôsobila;
 - iii) uplatnené a prebiehajúce zmierňujúce opatrenia.

Členské štáty zabezpečia, aby sa v riadne odôvodnených prípadoch a po dohode s príslušnými orgánmi alebo jednotkou CSIRT mohol príslušný subjekt odchýliť od lehôt stanovených v písmenách a) a c).

5. Príslušné vnútroštátne orgány alebo jednotka CSIRT poskytnú oznamujúcemu subjektu do 24 hodín od prijatia prvotného oznámenia uvedeného v odseku 4 písm. a) odpoveď vrátane počiatočnej spätnej väzby k incidentu a na žiadosť subjektu usmernenia k vykonávaniu možných zmierňujúcich opatrení. Ak jednotka CSIRT nedostala oznámenie uvedené v odseku 1, usmernenie poskytne príslušný orgán v spolupráci s jednotkou CSIRT. Jednotka CSIRT poskytne doplňujúcu technickú podporu, ak o to príslušný subjekt požiada. Ak existuje podozrenie, že incident má

trestnoprávnu povahu, príslušné vnútroštátne orgány alebo jednotka CSIRT poskytnú aj usmernenia týkajúce sa oznamovania incidentu orgánom presadzovania práva.

6. V prípade potreby, a najmä ak sa incident uvedený v odseku 1 týka dvoch alebo viacerých členských štátov, príslušný orgán alebo jednotka CSIRT informuje o incidente ostatné zasiahnuté členské štáty a agentúru ENISA. Príslušné orgány, jednotky CSIRT a jednotné kontaktné miesta pri tom v súlade s právom Únie alebo vnútroštátnymi právnymi predpismi, ktoré sú v súlade s právom Únie, chránia bezpečnosť a obchodné záujmy subjektu, ako aj dôvernosť poskytnutých informácií.
7. Po porade s dotknutým subjektom môže príslušný orgán alebo jednotka CSIRT a prípadne orgány alebo jednotky CSIRT ďalších dotknutých členských štátov informovať o incidente verejnosť alebo požiadať o to daný subjekt, ak je informovanosť verejnosti potrebná na zabránenie incidentu alebo riešenie prebiehajúceho incidentu alebo ak je zverejnenie incidentu vo verejnom záujme z iného dôvodu.
8. Na žiadosť príslušného orgánu alebo jednotky CSIRT jednotné kontaktné miesto postúpi doručené oznámenia podľa odsekov 1 a 2 jednotným kontaktným miestam ostatných zasiahnutých členských štátov.
9. Jednotné kontaktné miesto predkladá agentúre ENISA každý mesiac súhrnnú správu s anonymizovanými a agregovanými údajmi o incidentoch, závažných kybernetických hrozbách a udalostiach odvrátených v poslednej chvíli oznámených v súlade s odsekmi 1 a 2 a v súlade s článkom 27. S cieľom prispieť k poskytovaniu porovnateľných informácií môže agentúra ENISA vydať technické usmernenia týkajúce sa parametrov informácií uvedených v súhrnnej správe.
10. Príslušné orgány poskytnú príslušným orgánom určeným podľa smernice (EÚ) XXXX/XXXX [smernica o odolnosti kritických subjektov] informácie o incidentoch a kybernetických hrozbách, ktoré v súlade s odsekmi 1 a 2 oznámili kľúčové subjekty identifikované ako kritické subjekty alebo ako subjekty rovnocenné s kritickými subjektmi podľa smernice (EÚ) XXXX/XXXX [smernica o odolnosti kritických subjektov].
11. Komisia môže prijať vykonávacie akty, v ktorých bližšie určí druh informácií, formát a postup oznámenia predkladaného podľa odsekov 1 a 2. Komisia môže prijať aj vykonávacie akty s cieľom ďalej konkretizovať prípady, v ktorých sa incident považuje za závažný, ako sa uvádza v odseku 3. Uvedené vykonávacie akty sa prijímú v súlade s postupom preskúmania, na ktorý sa odkazuje v článku 37 ods. 2.

Článok 21

Použitie európskych systémov certifikácie kybernetickej bezpečnosti

1. S cieľom preukázať súlad s určitými požiadavkami článku 18 môžu členské štáty vyžadovať, aby kľúčové a dôležité subjekty certifikovali určité produkty IKT, služby IKT a procesy IKT v rámci osobitných európskych systémov certifikácie kybernetickej bezpečnosti prijatých podľa článku 49 nariadenia (EÚ) 2019/881. Produkty, služby a procesy, ktoré podliehajú certifikácii, môže vytvoriť kľúčový alebo dôležitý subjekt alebo sa môžu obstať od tretích strán.
2. Komisia je splnomocnená prijímať delegované akty, v ktorých bližšie určí, od ktorých kategórií kľúčových subjektov sa vyžaduje získanie certifikátu a v rámci

ktorých konkrétnych európskych systémov certifikácie kybernetickej bezpečnosti podľa odseku 1. Delegované akty sa prijímajú v súlade s článkom 36.

3. Komisia môže požiadať agentúru ENISA, aby vypracovala kandidátsky systém podľa článku 48 ods. 2 nariadenia (EÚ) 2019/881 v prípadoch, keď nie je k dispozícii žiadny európsky systém certifikácie kybernetickej bezpečnosti na účely odseku 2.

Článok 22 **Normalizácia**

1. Členské štáty v záujme harmonizovaného vykonávania článku 18 ods. 1 a 2 a bez toho, aby ukladali povinnosť využívať určitý typ technológie alebo diskriminovali v prospech takéhoto využívania, podporujú využívanie európskych alebo medzinárodne uznávaných noriem a špecifikácií, ktoré sú relevantné pre bezpečnosť sietí a informačných systémov.
2. Agentúra ENISA v spolupráci s členskými štátmi vypracúva odporúčania a usmernenia týkajúce sa technických oblastí, ktoré sa majú zväziť v súvislosti s odsekom 1, ako aj odporúčania a usmernenia týkajúce sa už existujúcich noriem vrátane vnútroštátnych noriem členských štátov, ktoré by sa mohli vzťahovať na uvedené oblasti.

Článok 23 **Databázy doménových mien a registračných údajov**

1. S cieľom prispieť k bezpečnosti, stabilite a odolnosti DNS členské štáty zabezpečia, aby správcovia TLD a subjekty poskytujúce služby registrácie doménových mien pre TLD zbierali a uchovávali presné a úplné registračné údaje o doménových menách vo vyhradenom databázovom zariadení s náležitou starostlivosťou, na ktoré sa vzťahujú právne predpisy Únie o ochrane údajov, pokiaľ ide o údaje, ktoré sú osobnými údajmi.
2. Členské štáty zabezpečia, aby databázy s registračnými údajmi o doménových menách uvedené v odseku 1 obsahovali relevantné informácie na identifikáciu a kontaktovanie držiteľov doménových mien a kontaktných miest spravujúcich doménové mená v rámci TLD.
3. Členské štáty zabezpečia, aby správcovia TLD a subjekty poskytujúce služby registrácie doménových mien pre TLD mali zavedené politiky a postupy s cieľom zabezpečiť, aby databázy obsahovali presné a úplné informácie. Členské štáty zabezpečia, aby takéto politiky a postupy boli verejne dostupné.
4. Členské štáty zabezpečia, aby správcovia TLD a subjekty poskytujúce služby registrácie doménových mien pre TLD bez zbytočného odkladu po registrácii mena domény uverejnili registračné údaje domény, ktoré nie sú osobnými údajmi.
5. Členské štáty zabezpečia, aby registre TLD a subjekty poskytujúce služby registrácie doménových mien pre TLD poskytovali prístup k špecifickým registračným údajom o doménových menách na základe zákonných a riadne odôvodnených žiadostí oprávnených záujemcov o prístup v súlade s právnymi predpismi Únie o ochrane

údajov. Členské štáty zabezpečia, aby správcovia TLD a subjekty poskytujúce služby registrácie doménových mien pre TLD odpovedali bez zbytočného odkladu na všetky žiadosti o prístup. Členské štáty zabezpečia, aby politiky a postupy zverejňovania takýchto údajov boli verejne dostupné.

Oddiel II

Jurisdikcia a registrácia

Článok 24

Jurisdikcia a teritorialita

1. Predpokladá sa, že poskytovatelia služieb DNS, správcovia mien TLD, poskytovatelia služieb cloud computingu, poskytovatelia služieb dátového centra a poskytovatelia sietí na sprístupňovanie obsahu uvedení v bode 8 prílohy I, ako aj poskytovatelia digitálnych služieb uvedení v bode 6 prílohy II sú v jurisdikcii členského štátu, v ktorom majú hlavné miesto podnikateľskej činnosti v Únii.
2. Na účely tejto smernice sa predpokladá, že subjekty uvedené v odseku 1 majú hlavné miesto podnikateľskej činnosti v Únii v členskom štáte, v ktorom sa prijímajú rozhodnutia týkajúce sa opatrení na riadenie kybernetickobezpečnostných rizík. Ak sa takéto rozhodnutia neprijímajú v žiadnom mieste podnikateľskej činnosti v Únii, predpokladá sa, že hlavné miesto podnikateľskej činnosti je v členskom štáte, v ktorom majú subjekty miesto podnikateľskej činnosti s najvyšším počtom zamestnancov v Únii.
3. Ak subjekt uvedený v odseku 1 nie je usadený v Únii, ale ponúka služby v rámci Únie, určí zástupcu v Únii. Zástupca musí byť usadený v jednom z členských štátov, v ktorých ponúka služby. Predpokladá sa, že takýto subjekt podlieha jurisdikcii toho členského štátu, v ktorom je usadený jeho zástupca. Ak v zmysle tohto článku nie je v Únii určený zástupca, ktorýkoľvek členský štát, v ktorom subjekt poskytuje služby, môže proti tomuto subjektu podniknúť právne kroky pre nedodržanie povinností podľa tejto smernice.
4. Ak subjekt určí zástupcu v zmysle odseku 1, nie sú tým dotknuté právne kroky, ktoré by mohli byť podniknuté proti samotnému subjektu.

Článok 25

Register kľúčových a dôležitých subjektov

1. Agentúra ENISA vytvorí a vedie register kľúčových a dôležitých subjektov uvedených v článku 24 ods. 1. Subjekty predložia agentúre ENISA najneskôr [12 mesiacov od nadobudnutia účinnosti tejto smernice] tieto informácie:
 - a) názov subjektu;
 - b) adresu svojho hlavného miesta podnikateľskej činnosti a iných zákonných miest podnikateľskej činnosti v Únii, alebo ak nie sú usadené v Únii, adresu svojho zástupcu určeného podľa článku 24 ods. 3;
 - c) aktuálne kontaktné údaje vrátane e-mailových adries a telefónnych čísel subjektov.

2. Subjekty uvedené v odseku 1 oznámia agentúre ENISA všetky zmeny údajov, ktoré predložili podľa odseku 1, a to bezodkladne a v každom prípade do troch mesiacov odo dňa, keď zmena nadobudla účinnosť.
3. Agentúra ENISA postúpi informácie získané podľa odseku 1 jednotným kontaktným miestam v závislosti od uvedenej lokality hlavného miesta podnikateľskej činnosti každého subjektu alebo jeho určeného zástupcu, ak subjekt nie je usadený v Únii. Ak má subjekt uvedený v odseku 1 okrem svojho hlavného miesta podnikateľskej činnosti v Únii ďalšie miesta podnikateľskej činnosti v iných členských štátoch, agentúra ENISA informuje aj jednotné kontaktné miesta v týchto členských štátoch.
4. Ak subjekt nezaregistruje svoju činnosť alebo neposkytne relevantné informácie v lehote stanovenej v odseku 1, každý členský štát, v ktorom subjekt poskytuje služby, je príslušný zabezpečiť, aby tento subjekt dodržiaval povinnosti stanovené v tejto smernici.

KAPITOLA V

Zdieľanie informácií

Článok 26

Dojednania o zdieľaní informácií o kybernetickej bezpečnosti

1. Bez toho, aby bolo dotknuté nariadenie (EÚ) 2016/679, členské štáty zabezpečia, aby si kľúčové a dôležité subjekty mohli medzi sebou vymieňať relevantné informácie o kybernetickej bezpečnosti vrátane informácií o kybernetických hrozbách, zraniteľnostiach, ukazovateľoch kompromitácie, taktikách, technikách a postupoch, kybernetickobezpečnostných varovaniach a konfiguračných nástrojoch, ak takáto výmena informácií:
 - a) má za cieľ predchádzať incidentom, odhaľovať ich, reagovať na ne alebo ich zmierňovať;
 - b) zvyšuje úroveň kybernetickej bezpečnosti, najmä zvyšovaním povedomia o kybernetických hrozbách, obmedzovaním alebo zabráňovaním možnosti šírenia takýchto hrozieb, podporou celej škály obranných kapacít, zverejňovaním informácií o zraniteľnosti a jej nápravou, technikami odhaľovania hrozieb, stratégiami zmierňovania, alebo fázami reakcie a obnovy.
2. Členské štáty zabezpečia, aby sa výmena informácií uskutočňovala v rámci dôveryhodných komunit kľúčových a dôležitých subjektov. Takáto výmena sa uskutočňuje prostredníctvom mechanizmov spoločného využívania informácií vzhľadom na potenciálne citlivú povahu vymieňaných informácií a v súlade s pravidlami práva Únie uvedenými v odseku 1.
3. Členské štáty stanovia pravidlá, v ktorých sa konkretizuje postup, operačné prvky (vrátane využívania špecializovaných platforiem IKT), obsah a podmienky dohôd o výmene informácií uvedených v odseku 2. V týchto pravidlách sa stanovia aj podrobnosti o zapojení orgánov verejnej moci do takýchto dohôd, ako aj operačné prvky vrátane využívania špecializovaných IT platforiem. Členské štáty poskytnú pri

uplatňovaní takýchto opatrení podporu v súlade so svojimi politikami uvedenými v článku 5 ods. 2 písm. g).

4. Kľúčové a dôležité subjekty oznámia príslušným orgánom svoju účasť na dohodách o výmene informácií uvedených v odseku 2 pri uzatváraní takýchto dohôd alebo prípadne ich odstúpení od takýchto dohôd, keď odstúpenie nadobudne účinnosť.
5. Agentúra ENISA podporuje v súlade s právom Únie uzavretie dohôd o výmene informácií o kybernetickej bezpečnosti uvedených v odseku 2 poskytovaním najlepších postupov a usmernení.

Článok 27

Dobrovoľné oznámenie relevantných informácií

Členské štáty zabezpečia, aby subjekty, ktoré nepatria do rozsahu pôsobnosti tejto smernice, mohli dobrovoľne podávať oznámenia o závažných incidentoch, kybernetických hrozbách alebo udalostiach odvrátených v poslednej chvíli, a to bez toho, aby bol dotknutý článok 3. Členské štáty pri spracúvaní oznámení konajú v súlade s postupom stanoveným v článku 20. Členské štáty môžu uprednostniť spracúvanie povinných oznámení pred dobrovoľnými oznámeniami. V dôsledku dobrovoľného oznámenia nevznikajú oznamujúcemu subjektu žiadne ďalšie povinnosti, ktoré by sa naň neboli vzťahovali, ak by oznámenie nepodal.

KAPITOLA VI

Dohľad a presadzovanie práva

Článok 28

Všeobecné aspekty týkajúce sa dohľadu a presadzovania práva

1. Členské štáty zabezpečia, aby príslušné orgány účinne monitorovali a prijímali opatrenia potrebné na zabezpečenie súladu s touto smernicou, najmä s povinnosťami stanovenými v článkoch 18 a 20.
2. Príslušné orgány pri riešení incidentov, ktoré majú za následok porušenie ochrany osobných údajov, úzko spolupracujú s orgánmi na ochranu údajov.

Článok 29

Dohľad a presadzovanie práva v prípade 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, pričom zohľadnia okolnosti každého jednotlivého prípadu.
2. Členské štáty zabezpečia, aby príslušné orgány mali pri vykonávaní svojich úloh dohľadu nad kľúčovými subjektmi právomoc podrobiť tieto subjekty:
 - a) kontrolám na mieste a dohľadu na diaľku vrátane náhodných kontrol;

- b) pravidelným auditom;
 - c) cieleným bezpečnostným auditom založeným na posúdeniach rizika alebo dostupných informáciách súvisiacich s rizikom;
 - d) bezpečnostným kontrolám založeným na objektívnych, nediskriminačných, spravodlivých a transparentných kritériách posúdenia rizika;
 - e) žiadostiam o informácie potrebné na posúdenie opatrení v oblasti kybernetickej bezpečnosti, ktoré subjekt prijal, vrátane zdokumentovaných politík v oblasti kybernetickej bezpečnosti, ako aj dodržiavania povinnosti informovať agentúru ENISA podľa článku 25 ods. 1 a 2;
 - f) žiadostiam o prístup k údajom, dokumentom alebo akýmkoľvek informáciám potrebným na plnenie ich úloh dohľadu;
 - g) žiadostiam o dôkazy vykonávania politík v oblasti kybernetickej bezpečnosti, ako sú výsledky bezpečnostných auditov uskutočnených kvalifikovaným audítorom a príslušné podkladové dôkazy.
3. Príslušné orgány pri vykonávaní svojich právomocí podľa odseku 2 písm. e) až g) uvedú účel žiadosti a konkretizujú požadované informácie.
4. Členské štáty zabezpečia, aby príslušné orgány pri vykonávaní svojich právomocí na presadzovanie práva v súvislosti s kľúčovými subjektmi mali právomoc:
- a) vydávať varovania, že subjekty nedodržiavajú povinnosti stanovené v tejto smernici;
 - b) vydávať záväzné pokyny alebo príkazy, ktorými sa od týchto subjektov vyžaduje napraviť zistené nedostatky alebo porušenia povinností stanovených v tejto smernici;
 - c) nariadiť týmto subjektom, aby upustili od konania, ktoré nie je v súlade s povinnosťami stanovenými v tejto smernici, a zdržať sa opakovania takého konania;
 - d) nariadiť týmto subjektom, aby svoje opatrenia na riadenie rizík a/alebo oznamovacie povinnosti zosúlادili s povinnosťami stanovenými v článkoch 18 a 20 určeným spôsobom a v určenej lehote;
 - e) nariadiť týmto subjektom, aby informovali fyzické alebo právnické osoby, ktorým poskytujú služby alebo činnosti, ktoré sú potenciálne zasiahnuté závažnou kybernetickou hrozbou, o akýchkoľvek možných ochranných alebo nápravných opatreniach, ktoré môžu tieto fyzické alebo právnické osoby prijať v reakcii na túto hrozbu;
 - f) nariadiť týmto subjektom, aby v primeranej lehote vykonali odporúčania poskytnuté na základe bezpečnostného auditu;
 - g) určiť monitorujúceho úradníka s presne vymedzenými úlohami na určené obdobie s cieľom dohliadať na dodržiavanie ich povinností stanovených v článkoch 18 a 20;
 - h) nariadiť týmto subjektom, aby určeným spôsobom zverejnili aspekty nedodržiavania povinností stanovených v tejto smernici;
 - i) vydať verejné vyhlásenie, v ktorom sa uvedie právnická a fyzická osoba alebo osoby zodpovedné za porušenie povinnosti stanovenej v tejto smernici a povaha tohto porušenia;

- j) uložiť správnu sankciu alebo požiadať o jej uloženie podľa článku 31 príslušné orgány alebo súdy podľa vnútroštátnych zákonov, a to popri opatreniach uvedených v písmenách a) až i) tohto odseku alebo namiesto týchto opatrení, v závislosti od okolností každého jednotlivého prípadu.
5. Ak sa opatrenia na presadzovanie práva prijaté podľa odseku 4 písm. a) až d) a f) ukážu ako neúčinné, členské štáty zabezpečia, aby príslušné orgány mali právomoc stanoviť lehotu, v 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 príslušné orgány mali právomoc:
- a) pozastaviť certifikáciu alebo povoľovanie alebo požiadať certifikačný alebo povoľujúci subjekt, aby pozastavil certifikáciu alebo povoľovanie týkajúce sa časti alebo všetkých služieb alebo činností, ktoré poskytuje kľúčový subjekt;
 - b) uložiť dočasný zákaz alebo od príslušných orgánov alebo súdov podľa vnútroštátnych zákonov požadovať uloženie dočasného zákazu vykonávať riadiace funkcie v tomto kľúčovom subjekte, a to každej osobe vykonávajúcej riadiace úlohy na úrovni výkonného riaditeľa alebo právneho zástupcu v tomto kľúčovom subjekte a akejkoľvek inej fyzickej osobe zodpovednej za porušenie.
- Tieto sankcie sa uplatňujú len dovtedy, kým subjekt neprijme potrebné opatrenia na nápravu nedostatkov alebo nesplní požiadavky príslušného orgánu, ktorý takéto sankcie uplatnil.
6. Členské štáty zabezpečia, aby každá fyzická osoba zodpovedná za kľúčový subjekt alebo konajúca ako jeho zástupca na základe právomoci zastupovať ho, prijímať rozhodnutia v jeho mene alebo vykonávať kontrolu nad ním mala právomoc zabezpečiť dodržiavanie povinností stanovených v tejto smernici. Členské štáty zabezpečia, aby tieto fyzické osoby mohli niesť zodpovednosť za porušenie svojich úloh zabezpečovať dodržiavanie povinností stanovených v tejto smernici.
7. Príslušné orgány pri prijímaní opatrení na presadzovanie práva alebo uplatňovaní sankcií podľa odsekov 4 a 5 dodržiavajú právo na obhajobu a zohľadňujú okolnosti každého jednotlivého prípadu a prinajmenšom náležite zohľadňujú:
- a) závažnosť porušenia a dôležitosť porušených ustanovení. Medzi porušenia, ktoré by sa mali považovať za závažné, patria: opakované porušenia, neoznámenie incidentov so závažným účinkom narušenia alebo nevykonanie ich nápravy, nevykonanie nápravy nedostatkov na základe záväzných pokynov príslušných orgánov, marenie auditov alebo monitorovacích činností nariadených príslušným orgánom na základe zistenia porušenia, poskytovanie nepravdivých alebo hrubo nepresných informácií týkajúcich sa požiadaviek na riadenie rizík alebo oznamovacích povinností stanovených v článkoch 18 a 20;
 - b) trvanie porušenia vrátane opakovaného porušovania;
 - c) skutočné spôsobené škody alebo vzniknuté straty alebo potenciálne škody alebo straty, ktoré mohli vzniknúť, pokiaľ ich možno určiť. Pri hodnotení tohto aspektu sa okrem iného zohľadnia skutočné alebo potenciálne finančné alebo hospodárske straty, účinky na iné služby, počet dotknutých alebo potenciálne dotknutých používateľov;
 - d) úmyselný alebo nedbanlivostný charakter porušenia;

- e) opatrenia, ktoré subjekt prijal na zabránenie alebo zmiernenie škôd a/alebo strát;
 - f) dodržiavanie schválených kódexov správania alebo schválených mechanizmov certifikácie;
 - g) úroveň spolupráce zodpovednej fyzickej alebo právnickej osoby (osôb) s príslušnými orgánmi.
8. Príslušné orgány uvedú podrobné odôvodnenie svojich rozhodnutí na presadzovanie práva. Pred prijatím takýchto rozhodnutí oznámia dotknutým subjektom svoje predbežné zistenia a poskytnú im primeraný čas na predloženie pripomienok.
9. Členské štáty zabezpečia, aby ich príslušné orgány informovali relevantné príslušné orgány dotknutého členského štátu určené podľa smernice (EÚ) XXXX/XXXX [smernica o odolnosti kritických subjektov], keď vykonávajú svoje právomoci v oblasti dohľadu a presadzovania práva zamerané na zabezpečenie dodržiavania povinností podľa tejto smernice zo strany kľúčového subjektu identifikovaného ako kritický alebo ako rovnocenný s kritickým subjektom podľa smernice (EÚ) XXXX/XXXX [smernica o odolnosti kritických subjektov]. Príslušné orgány môžu na žiadosť príslušných orgánov podľa smernice (EÚ) XXXX/XXXX [smernica o odolnosti kritických subjektov] vykonávať svoje právomoci v oblasti dohľadu a presadzovania práva vo vzťahu ku kľúčovému subjektu identifikovanému ako kritický alebo ako rovnocenný subjekt.

Článok 30

Dohľad a presadzovanie práva v prípade dôležitých subjektov

1. Ak členské štáty dostanú dôkaz alebo indíciu, že dôležitý subjekt nedodržiava povinnosti stanovené v tejto smernici, a najmä v článkoch 18 a 20, zabezpečia, aby príslušné orgány konali v prípade potreby prostredníctvom opatrení dohľadu *ex post*.
2. Členské štáty zabezpečia, aby príslušné orgány mali pri vykonávaní svojich úloh dohľadu nad dôležitými subjektmi právomoc podrobiť tieto subjekty:
 - a) kontrolám na mieste a dohľadu *ex post* na diaľku;
 - b) cieleným bezpečnostným auditom založeným na posúdeniach rizika alebo dostupných informáciách súvisiacich s rizikom;
 - c) bezpečnostným kontrolám založeným na objektívnych, spravodlivých a transparentných kritériách posúdenia rizika;
 - d) žiadostiam o informácie potrebné na posúdenie *ex post* týkajúce sa opatrení v oblasti kybernetickej bezpečnosti vrátane zdokumentovaných politík v oblasti kybernetickej bezpečnosti, ako aj dodržiavania povinnosti informovať agentúru ENISA podľa článku 25 ods. 1 a 2;
 - e) žiadostiam o prístup k údajom, dokumentom a/alebo akýmkoľvek informáciám potrebným na plnenie úloh dohľadu.
3. Príslušné orgány pri vykonávaní svojich právomocí podľa odseku 2 písm. d) alebo e) uvedú účel žiadosti a konkretizujú požadované informácie.
4. Členské štáty zabezpečia, aby príslušné orgány pri vykonávaní svojich právomocí na presadzovanie práva v súvislosti s dôležitými subjektmi mali právomoc:

- a) vydávať varovania, že subjekty nedodržiavajú povinnosti stanovené v tejto smernici;
 - b) vydávať záväzné pokyny alebo príkazy, ktorými sa od týchto subjektov vyžaduje napraviť zistené nedostatky alebo porušenie povinností stanovených v tejto smernici;
 - c) nariadiť týmto subjektom, aby upustili od konania, ktoré nie je v súlade s povinnosťami stanovenými v tejto smernici, a zdržať sa opakovania takého konania;
 - d) nariadiť týmto subjektom, aby svoje opatrenia na riadenie rizík alebo oznamovacie povinnosti zosúlادili s povinnosťami stanovenými v článkoch 18 a 20 určeným spôsobom a v určenej lehote;
 - e) nariadiť týmto subjektom, aby informovali fyzické alebo právnické osoby, ktorým poskytujú služby alebo činnosti, ktoré sú potenciálne zasiahnuté závažnou kybernetickou hrozbou, o akýchkoľvek možných ochranných alebo nápravných opatreniach, ktoré môžu tieto fyzické alebo právnické osoby prijať v reakcii na túto hrozbu;
 - f) nariadiť týmto subjektom, aby v primeranej lehote vykonali odporúčania poskytnuté na základe bezpečnostného auditu;
 - g) nariadiť týmto subjektom, aby určeným spôsobom zverejnili aspekty nedodržiavania svojich povinností stanovených v tejto smernici;
 - h) vydať verejné vyhlásenie, v ktorom sa uvedie právnická a fyzická osoba alebo osoby zodpovedné za porušenie povinností stanovenej v tejto smernici a povaha tohto porušenia;
 - i) uložiť správnu sankciu alebo požiadať o jej uloženie podľa článku 31 príslušné orgány alebo súdy podľa vnútroštátnych zákonov, a to popri opatreniach uvedených v písmenách a) až h) tohto odseku alebo namiesto týchto opatrení, v závislosti od okolností každého jednotlivého prípadu.
5. Článok 29 ods. 6 až 8 sa uplatňuje aj na opatrenia dohľadu a presadzovania práva stanovené v tomto článku v prípade dôležitých subjektov uvedených v prílohe II.

Článok 31

Všeobecné podmienky ukladania správnych sankcií kľúčovým a dôležitým subjektom

1. Členské štáty zabezpečia, aby uloženie správnych sankcií kľúčovým a dôležitým subjektom podľa tohto článku za porušenie povinností stanovených v tejto smernici bolo v každom jednotlivom prípade účinné, primerané a odrádzajúce.
2. Správne sankcie sa v závislosti od okolností každého jednotlivého prípadu ukladajú popri opatreniach uvedených v článku 29 ods. 4 písm. a) až i), článku 29 ods. 5 a článku 30 ods. 4 písm. a) až h) a j) alebo namiesto týchto opatrení.
3. Pri rozhodovaní o uložení správnej sankcie, ako aj pri rozhodovaní o jej výške v každom jednotlivom prípade sa náležite zohľadnia aspoň prvky stanovené v článku 29 ods. 7.
4. Členské štáty zabezpečia, aby sa za porušenia povinností stanovených v článku 18 alebo článku 20 v súlade s odsekmi 2 a 3 tohto článku ukladali správne pokuty v

maximálnej výške aspoň 10 000 000 EUR alebo najviac 2 % celkového svetového ročného obratu podniku, ku ktorému kľúčový alebo dôležitý subjekt patrí, v predchádzajúcom účtovnom období, podľa toho, ktorá suma je vyššia.

5. Členské štáty môžu v súlade s predchádzajúcim rozhodnutím príslušného orgánu stanoviť právomoc ukladať pravidelné peňažné pokuty s cieľom prinútiť kľúčový alebo dôležitý subjekt, aby prestal porušovať predpisy.
6. Bez toho, aby boli dotknuté právomoci príslušných orgánov podľa článkov 29 a 30, každý členský štát môže stanoviť pravidlá, či a v akom rozsahu sa môžu správne sankcie uložiť subjektom verejnej správy uvedeným v článku 4 bode 23 s prihliadnutím na povinnosti stanovené v tejto smernici.

Článok 32

Porušenia povinností, pri ktorých došlo k porušeniu ochrany osobných údajov

1. Ak majú príslušné orgány indície, že kľúčový alebo dôležitý subjekt pri porušení povinností stanovených v článkoch 18 a 20 porušil aj ochranu osobných údajov, ako sa vymedzuje v článku 4 bode 12 nariadenia (EÚ) 2016/679, pričom takéto porušenie sa oznamuje podľa článku 33 uvedeného nariadenia, v primeranej lehote o tom informujú príslušné dozorné orgány podľa článkov 55 a 56 uvedeného nariadenia.
2. Ak sa dozorné orgány, ktoré sú príslušné v súlade s článkami 55 a 56 nariadenia (EÚ) 2016/679, rozhodnú uplatniť svoje právomoci podľa článku 58 písm. i) uvedeného nariadenia a uložiť správnu sankciu, príslušné orgány neuložia správnu sankciu za to isté porušenie podľa článku 31 tejto smernice. Príslušné orgány však môžu uplatňovať opatrenia na presadzovanie práva alebo vykonávať sankčné právomoci stanovené v článku 29 ods. 4 písm. a) až i), článku 29 ods. 5 a článku 30 ods. 4 písm. a) až h) tejto smernice.
3. Ak je dozorný orgán, príslušný podľa nariadenia (EÚ) 2016/679, usadený v inom členskom štáte než príslušný orgán, príslušný orgán môže informovať dozorný orgán usadený v tom istom členskom štáte.

Článok 33

Sankcie

1. Členské štáty stanovujú pravidlá ukladania sankcií za porušenie vnútroštátnych predpisov prijatých podľa tejto smernice a prijímajú všetky opatrenia potrebné na zabezpečenie ich uplatňovania. Stanovené sankcie musia byť účinné, primerané a odrádzajúce.
2. Členské štáty najneskôr do [dvoch] rokov od nadobudnutia účinnosti tejto smernice oznámia tieto pravidlá a opatrenia Komisii a bez zbytočného odkladu jej oznámia všetky následné zmeny, ktoré sa ich týkajú.

Článok 34

Vzájomná pomoc

1. Ak kľúčový alebo dôležitý subjekt poskytuje služby vo viac ako jednom členskom štáte, alebo sa jeho hlavné miesto podnikateľskej činnosti alebo zástupca nachádzajú v jednom členskom štáte, ale jeho siete a informačné systémy sú umiestnené v niektorom inom alebo vo viacerých iných členských štátoch, príslušný orgán členského štátu, v ktorom sa nachádza hlavné alebo iné miesto podnikateľskej činnosti alebo zástupca, a príslušné orgány týchto iných členských štátov spolupracujú a v prípade potreby si navzájom pomáhajú. Táto spolupráca zahŕňa aspoň tieto prvky:
 - a) príslušné orgány, ktoré uplatňujú opatrenia v oblasti 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 v oblasti dohľadu a presadzovania práva a následné opatrenia v súlade s článkami 29 a 30;
 - b) príslušný orgán môže požiadať iný príslušný orgán, aby prijal opatrenia dohľadu alebo presadzovania práva uvedené v článkoch 29 a 30;
 - c) príslušný orgán po prijatí odôvodnenej žiadosti od iného príslušného orgánu poskytne tomuto inému príslušnému orgánu pomoc, aby sa opatrenia dohľadu alebo presadzovania práva uvedené v článkoch 29 a 30 mohli vykonávať účinným, efektívnym a konzistentným spôsobom. Takáto vzájomná pomoc sa môže vzťahovať na žiadosti o informácie a opatrenia dohľadu vrátane žiadostí o vykonanie kontrol na mieste alebo dohľadu na diaľku alebo cielených bezpečnostných auditov. Príslušný orgán, ktorému je žiadosť o pomoc určená, nesmie túto žiadosť zamietnuť, pokiaľ sa po výmene názorov s ostatnými dotknutými orgánmi, agentúrou ENISA a Komisiou nestanoví, že buď daný orgán nie je príslušný poskytnúť požadovanú pomoc, alebo že požadovaná pomoc nie je primeraná úlohám príslušného orgánu v oblasti dohľadu vykonávaným v súlade s článkom 29 alebo článkom 30.
2. V prípade potreby a po vzájomnej dohode môžu príslušné orgány z rôznych členských štátov vykonávať spoločné opatrenia dohľadu uvedené v článkoch 29 a 30.

KAPITOLA VII

Prechodné a záverečné ustanovenia

Článok 35

Preskúmanie

Komisia pravidelne preskúmava fungovanie tejto smernice a podáva o tom správu Európskemu parlamentu a Rade. V správe sa posúdi najmä relevantnosť odvetví, pododvetví, veľkosti a typu subjektov 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. Prvá správa sa predloží do ... [54 mesiacov po dátume nadobudnutia účinnosti tejto smernice].

Článok 36

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 18 ods. 6 a článku 21 ods. 2 sa Komisii udeľuje na obdobie piatich rokov od [...].
3. Delegovanie právomoci uvedené v článku 18 ods. 6 a článku 21 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 odborníkmi 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 18 ods. 6 a článku 21 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 37

Postup výboru

1. Komisii pomáha výbor. Uvedený výbor je výborom v zmysle nariadenia (EÚ) č. 182/2011.
2. Ak sa odkazuje na tento odsek, uplatňuje sa článok 5 nariadenia (EÚ) č. 182/2011.
3. Ak sa má stanovisko výboru získať písomným postupom, tento postup sa ukončí bez výsledku, ak tak v rámci lehoty na vydanie stanoviska rozhodne predseda výboru alebo ak o to požiada člen výboru.

Článok 38

Transpozícia

1. Členské štáty prijímú a zverejnia [do 18 mesiacov po nadobudnutí účinnosti tejto smernice] zákony, iné právne predpisy a správne opatrenia potrebné na dosiahnutie súladu s touto smernicou. Bezodkladne o tom informujú Komisiu. Tieto ustanovenia sa uplatňujú od ... [jeden deň po dátume uvedenom v prvom pododseku].
2. Členské štáty uvedú priamo v prijatých ustanoveniach alebo pri ich úradnom uverejnení odkaz na túto smernicu. Podrobnosti o odkaze upravia členské štáty.

Článok 39

Zmena nariadenia (EÚ) č. 910/2014

Článok 19 nariadenia (EÚ) č. 910/2014 sa vypúšťa.

Článok 40

Zmena smernice (EÚ) 2018/1972

Články 40 a 41 smernice (EÚ) 2018/1972 sa vypúšťajú.

Článok 41

Zrušenie

Smernica (EÚ) 2016/1148 sa zrušuje s účinnosťou od ... [dátum lehoty na transpozíciu smernice].

Odkazy na smernicu (EÚ) 2016/1148 sa považujú za odkazy na túto smernicu a znejú v súlade s tabuľkou zhody uvedenou v prílohe III.

Článok 42

Nadobudnutie účinnosti

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

Článok 43

Adresáti

Táto smernica je určená členským štátom.

V Bruseli

*Za Európsky parlament
predseda*

*Za Radu
predseda*

LEGISLATÍVNY FINANČNÝ VÝKAZ

Obsah

1.	RÁMEC NÁVRHU/INICIATÍVY	4
1.1.	Názov návrhu/iniciatívy	4
1.2.	Príslušné oblasti politiky (<i>programové zoskupenie</i>)	4
1.3.	Návrh/iniciatíva sa týka:	4
1.4.	Dôvody návrhu/iniciatívy.....	4
1.4.1.	Potreby, ktoré sa majú uspokojiť v krátkodobom alebo dlhodobom horizonte vrátane podrobného harmonogramu prvej fázy vykonávania iniciatívy	4
1.4.2.	Prínos zapojenia Únie (môže byť výsledkom rôznych faktorov, napr. lepšej koordinácie, právnej istoty, väčšej účinnosti alebo komplementárnosti). Na účely tohto bodu je „prínos zapojenia Európskej únie“ hodnota vyplývajúca zo zásahu Únie, ktorá dopĺňa hodnotu, ktorú by inak vytvorili len samotné členské štáty.	4
1.4.3.	Poznatky získané z podobných skúseností v minulosti.....	5
1.4.4.	Zlučiteľnosť a možná synergia s inými vhodnými nástrojmi	5
1.5.	Trvanie a finančný vplyv	6
1.6.	Plánovaný spôsob riadenia.....	6
2.	OPATRENIA V OBLASTI RIADENIA	8
2.1.	Opatrenia týkajúce sa monitorovania a predkladania správ.....	8
2.2.	Systémy riadenia a kontroly	8
2.2.1.	Opodstatnenie navrhovaných spôsobov riadenia, mechanizmov vykonávania financovania, spôsobov platby a stratégie kontroly	8
2.2.2.	Informácie o zistených rizikách a systémoch vnútornej kontroly zavedených na ich zmierňovanie	8
2.2.3.	Odhad a opodstatnenie nákladovej účinnosti kontrol (pomer medzi nákladmi na kontroly a hodnotou súvisiacich riadených finančných prostriedkov) a posúdenie očakávaných úrovní rizika chyby (pri platbe a uzavretí)	8
2.3.	Opatrenia na predchádzanie podvodom a nezrovnalostiam.....	8
3.	ODHADOVANÝ FINANČNÝ VPLYV NÁVRHU/INICIATÍVY	9
3.1.	Okruh viacročného finančného rámca a nové navrhované rozpočtové riadky výdavkov	9
3.2.	Odhadovaný vplyv na výdavky.....	10
3.2.1.	Zhrnutie odhadovaného vplyvu na výdavky	10
3.2.2.	Zhrnutie odhadovaného vplyvu na administratívne rozpočtové prostriedky	13
3.2.3.	Príspevky od tretích strán.....	15
3.3.	Odhadovaný vplyv na príjmy	15

1. RÁMEC NÁVRHU/INICIATÍVY

1.1. Názov návrhu/iniciatívy

Návrh smernice o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii a o zrušení smernice (EÚ) 2016/1148.

1.2. Príslušné oblasti politiky (*programové zoskupenie*)

Komunikačné siete, obsah a technológie
--

1.3. Návrh/iniciatíva sa týka:

☐ novej akcie

☐ novej akcie, ktorá nadväzuje na pilotný projekt/prípravnú akciu⁴⁰

☒ predĺženia trvania existujúcej akcie

☐ zlúčenia jednej alebo viacerých akcií do ďalšej/novej akcie alebo presmerovania jednej alebo viacerých akcií na ďalšiu/novú akciu

1.4. Dôvody návrhu/iniciatívy

1.4.1. *Potreby, ktoré sa majú uspokojiť v krátkodobom alebo dlhodobom horizonte vrátane podrobného harmonogramu prvotnej fázy vykonávania iniciatívy*

Cieľom revízie je zvýšiť úroveň kybernetickej odolnosti komplexného súboru podnikov pôsobiacich v Európskej únii vo všetkých príslušných odvetviach, znížiť mieru nezrovnalostí, pokiaľ ide o odolnosť na vnútornom trhu v odvetviach, na ktoré sa už smernica vzťahuje, a zlepšiť úroveň spoločnej situačnej informovanosti a spoločnej schopnosti prípravy a reakcie.

1.4.2. *Prínos zapojenia Únie (môže byť výsledkom rôznych faktorov, napr. lepšej koordinácie, právnej istoty, väčšej účinnosti alebo komplementárnosti). Na účely tohto bodu je „prínos zapojenia Európskej únie“ hodnota vyplývajúca zo zásahu Únie, ktorá dopĺňa hodnotu, ktorú by inak vytvorili len samotné členské štáty.*

Kybernetická odolnosť v rámci Únie nemôže byť účinná, ak sa k nej prostredníctvom vnútroštátnych alebo regionálnych dátových síl pristupuje odlišným spôsobom. Cieľom smernice NIS bolo napraviť tento nedostatok stanovením rámca pre bezpečnosť sietí a informačných systémov na vnútroštátnej úrovni a úrovni Únie. Prvé pravidelné preskúmanie smernice NIS však poukázalo na istý počet charakteristických nedostatkov, ktoré napokon viedli k výrazným rozdielom v členských štátoch, a to pokiaľ ide o spôsobilosti, plánovanie a úroveň ochrany, čo má zároveň vplyv na rovnaké podmienky pre podobné spoločnosti na vnútornom trhu.
--

Intervenciu EÚ nad rámec súčasných opatrení smernice NIS možno odôvodniť najmä týmito skutočnosťami: i) cezhraničný charakter problému; ii) potenciál opatrenia EÚ zlepšiť a uľahčiť účinné vnútroštátne politiky; iii) príspevok zosúladeného postupu založeného na spolupráci v oblasti politických opatrení NIS k účinnej ochrane údajov a súkromia.

⁴⁰

Podľa článku 58 ods. 2 písm. a) alebo b) nariadenia o rozpočtových pravidlách.

Uvedené ciele možno preto lepšie dosiahnuť prostredníctvom opatrení na úrovni EÚ ako zo strany samotných členských štátov.

1.4.3. Poznatky získané z podobných skúseností v minulosti

Smernica NIS je prvým horizontálnym nástrojom vnútorného trhu, ktorého cieľom je zlepšiť odolnosť sietí a systémov v Únii proti kybernetickým rizikám. Smernica NIS už významne prispela k zvýšeniu spoločnej úrovne kybernetickej bezpečnosti medzi členskými štátmi. Preskúmanie fungovania a vykonávania tejto smernice však poukázalo na viacero nedostatkov, ktoré sa, okrem rastúcej digitalizácie a potreby aktualizovanejšej reakcie, musia riešiť v revidovanom právnom akte.

1.4.4. Zlučiteľnosť a možná synergia s inými vhodnými nástrojmi

Nový návrh je úplne konzistentný a zosúladený s inými súvisiacimi iniciatívami, ako je návrh nariadenia o digitálnej prevádzkovej odolnosti finančného sektora a návrh smernice o odolnosti kritických prevádzkovateľov základných služieb. Je takisto zosúladený s európskym kódexom elektronických komunikácií, všeobecným nariadením o ochrane údajov a nariadením eIDAS.

Návrh je podstatnou časťou stratégie EÚ pre bezpečnostnú úniu.

1.5. Trvanie a finančný vplyv

☐ obmedzené trvanie

- ☐ v platnosti od [DD/MM]RRRR do [DD/MM]RRRR
- ☐ Finančný vplyv na viazané rozpočtové prostriedky od RRRR do RRRR a na platobné rozpočtové prostriedky od RRRR do RRRR.

☒ neobmedzené trvanie

- Počiatočná fáza vykonávania bude trvať od roku 2022 do roku 2025
- a potom bude vykonávanie pokračovať v plnom rozsahu.

1.6. Plánovaný spôsob riadenia⁴¹

Priame riadenie na úrovni Komisie

- ☒ prostredníctvom jej útvarov vrátane zamestnancov v delegáciách Únie,
- ☐ prostredníctvom výkonných agentúr
- ☐ Zdieľané riadenie s členskými štátmi
- ☐ Nepriame hospodárenie so zverení úloh súvisiacich s plnením rozpočtu:
 - ☐ tretím krajinám alebo subjektom, ktoré tieto krajiny určili,
 - ☐ medzinárodným organizáciám a ich agentúram (uvedie sa),
 - ☐ Európskej investičnej banke (EIB) a Európskemu investičnému fondu,
 - ☒ subjektom uvedeným v článkoch 70 a 71 nariadenia o rozpočtových pravidlách,
 - ☐ verejnoprávnym subjektom,
 - ☐ súkromnoprávnym subjektom povereným vykonávaním verejnej služby, pokiaľ tieto subjekty poskytujú dostatočné finančné záruky,
 - ☐ súkromnoprávnym subjektom spravovaným právom členského štátu, ktoré sú poverené vykonávaním verejno-súkromného partnerstva a ktoré poskytujú dostatočné finančné záruky,
 - ☐ osobám povereným vykonávaním osobitných činností v oblasti SZBP podľa hlavy V Zmluvy o Európskej únii a určeným v príslušnom základnom akte.
- *V prípade viacerých spôsobov riadenia uveďte v oddiele „Poznámky“ presnejšie vysvetlenie.*

Poznámky:

Agentúra Európskej únie pre kybernetickú bezpečnosť, ENISA, ktorej bol aktom o kybernetickej bezpečnosti udelený nový trvalý mandát, bude pomáhať členským štátom a Komisii pri vykonávaní revidovanej smernice NIS.

Agentúra ENISA bude mať na základe revidovanej smernice NIS od obdobia 2022/2023 dodatočné oblasti opatrení. Keďže tieto oblasti opatrení by boli podľa mandátu agentúry ENISA zahrnuté medzi jej všeobecné úlohy, budú pre agentúru predstavovať dodatočné pracovné zaťaženie. Podľa návrhu Komisie na revidovanú smernicu NIS sa bude od agentúry

⁴¹

Vysvetlenie spôsobov riadenia a odkazy na nariadenie o rozpočtových pravidlách sú k dispozícii na webovom sídle BudgWeb:
<https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx>.

ENISA okrem jej súčasných oblastí opatrení vyžadovať, aby do svojho pracovného programu osobitne zahrnula okrem iných aj tieto opatrenia: i) vyvinúť a spravovať európsky register zraniteľnosti (článok 6 ods. 2 návrhu); ii) zabezpečiť sekretariát Európskej siete styčných organizácií pre kybernetické krízy (CyCLONe) (článok 14 návrhu) a vydať výročnú správu o stave kybernetickej bezpečnosti v EÚ (článok 15 návrhu); iii) podporovať organizáciu partnerského preskúmania medzi členskými štátmi (článok 16 návrhu); iv) zhromažďovať súhrnné údaje o incidentoch od členských štátov a vydávať technické usmernenia (článok 20 ods. 9 návrhu); v) vytvoriť a spravovať register subjektov poskytujúcich cezhraničné služby (článok 25 návrhu).

Preto sa predloží žiadosť o päť doplňujúcich FTE od roku 2022 so zodpovedajúcim rozpočtom vo výške približne 0,61 milióna EUR ročne na pokrytie týchto nových pracovných miest (pozri samostatný finančný výkaz pre agentúry).

2. OPATRENIA V OBLASTI RIADENIA

2.1. Opatrenia týkajúce sa monitorovania a predkladania správ

Uved'te časový interval a podmienky, ktoré sa vzťahujú na tieto opatrenia.

Komisia pravidelne preskúma fungovanie tejto smernice a podá o tom správu Európskemu parlamentu a Rade, pričom prvýkrát tak urobí tri roky od nadobudnutia jej účinnosti.

Komisia takisto posúdi správnu transpozíciu smernice členskými štátmi.

2.2. Systémy riadenia a kontroly

2.2.1. *Opodstatnenie navrhovaných spôsobov riadenia, mechanizmov vykonávania financovania, spôsobov platby a stratégie kontroly*

Oddelenie v rámci GR CNECT, ktoré je zodpovedné za oblasť politiky, bude riadiť vykonávanie tejto smernice.

2.2.2. *Informácie o zistených rizikách a systémoch vnútornej kontroly zavedených na ich zmierňovanie*

Veľmi nízke riziko, keďže ekosystém smernice NIS je už zavedený.

2.2.3. *Odhad a opodstatnenie nákladovej účinnosti kontrol (pomer medzi nákladmi na kontroly a hodnotou súvisiacich riadených finančných prostriedkov) a posúdenie očakávaných úrovni rizika chyby (pri platbe a uzavretí)*

Neuplatňuje sa. Iba používanie administratívneho rozpočtu („celkový balík prostriedkov“).

2.3. Opatrenia na predchádzanie podvodom a nezrovnalostiam

Uved'te existujúce a plánované preventívne a ochranné opatrenia, napr. zo stratégie na boj proti podvodom.

Neuplatňuje sa. Iba používanie administratívneho rozpočtu („celkový balík prostriedkov“).

3. ODHADOVANÝ FINANČNÝ VPLYV NÁVRHU/INICIATÍVY

3.1. Okruh viacročného finančného rámca a nové navrhované rozpočtové riadky výdavkov

Okruh viacročného finančného rámca	Rozpočtový riadok	Druh výdavkov	Príspevky			
	Číslo [okruh...7.....]	DRP/NRP ⁴²	krajín EZVO ⁴³	kandidátskych krajín ⁴⁴	tretích krajín	v zmysle článku [21 ods. 2 písm. b)] nariadenia o rozpočtových pravidlách
	20 02 06 výdavky na riadenie					
	20 02 06	NRP	NIE	NIE	NIE	NIE

⁴² DRP = diferencované rozpočtové prostriedky/NRP = nediferencované rozpočtové prostriedky.

⁴³ EZVO: Európske združenie voľného obchodu.

⁴⁴ Kandidátske krajiny a prípadne potenciálni kandidáti zo západného Balkánu.

3.2. Odhadovaný vplyv na výdavky

3.2.1. Zhrnutie odhadovaného vplyvu na výdavky

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

Okruh viacročného finančného rámca	<...>	[Okruh.....]
---	-------	--------------

			2021	2022	2023	2024	2025	2026	2027	Po roku 2027	SPOLU
Operačné rozpočtové prostriedky (rozdelené podľa rozpočtových riadkov uvedených v bode 3.1.)	Závazky	(1)									
	Platby	(2)									
Administratívne rozpočtové prostriedky financované z finančného krytia na vykonávanie programu ⁴⁵	Závazky = Platby	(3)									
Rozpočtové prostriedky na finančné krytie programu SPOLU	Závazky	= 1 + 3									
	Platby	= 2 + 3									

Okruh viacročného finančného rámca	7	„Administratívne výdavky“ Zasadnutia: Plenárne zasadnutia skupiny pre spoluprácu NIS sa zvyčajne konajú štyrikrát ročne. Komisia kryje náklady spojené s cateringom, ako aj cestovné náklady zástupcov 27 členských štátov (jeden zástupca na jeden členský štát). Náklady na jedno zasadnutie môžu predstavovať až 15 000 EUR. Služobné cesty: Služobné cesty súvisia s monitorovaním a vykonávaním smernice NIS. Príklad: V jednom roku (máj 2019 až júl 2020) sa mali organizovať tzv.
---	---	--

⁴⁵ Technická a/alebo administratívna pomoc a výdavky určené na financovanie vykonávania programov a/alebo akcií EÚ (pôvodné rozpočtové riadky „BA“), nepriamy výskum, priamy výskum.

		návštevy krajín NIS a malo sa navštíviť všetkých 27 členských štátov s cieľom diskutovať o vykonávaní smernice NIS v EÚ.
--	--	--

Tento oddiel sa vyplní s použitím rozpočtových údajov administratívnej povahy, ktoré budú po prvýkrát uvedené v [prílohe k legislatívnemu finančnému výkazu](#), ktorá je nahraná do aplikácie DECIDE na účely medziúťvarovej konzultácie.

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

		2021	2022	2023	2024	2025	2026	2027	Po roku 2027	SPOLU
Ľudské zdroje		1,14	1,14	1,14	1,14	1,14	1,14	1,14		7,98
Ostatné administratívne výdavky		0,09	0,09	0,09	0,09	0,09	0,09	0,09		0,63
Rozpočtové prostriedky OKRUHU 7 viacročného finančného rámca SPOLU	(Závázky spolu = Platby spolu)	1,23	1,23	1,23	1,23	1,23	1,23	1,23		8,61

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

		2021	2022	2023	2024	2025	2026	2027	Po roku 2027	SPOLU
Rozpočtové prostriedky OKRUHOV viacročného finančného rámca SPOLU	Závázky									
	Platby									

3.2.2. Zhrnutie odhadovaného vplyvu na administratívne rozpočtové prostriedky

- ☐ Návrh/iniciatíva si nevyžaduje použitie administratívnych rozpočtových prostriedkov
- ☒ Návrh/iniciatíva si vyžaduje použitie administratívnych rozpočtových prostriedkov, ako je uvedené v nasledujúcej tabuľke:

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

Roky	2021	2022	2023	2024	2025	2026	2027	SPOLU
------	------	------	------	------	------	------	------	-------

OKRUH 7 viacročného finančného rámca								
Ľudské zdroje	1,14	1,14	1,14	1,14	1,14	1,14	1,14	7,98
Ostatné administratívne výdavky	0,09	0,09	0,09	0,09	0,09	0,09	0,09	0,63
Medzisúčet OKRUHU 7 viacročného finančného rámca	1,23	1,23	1,23	1,23	1,23	1,23	1,23	8,61

Mimo OKRUHU 7⁴⁶ viacročného finančného rámca								
Ľudské zdroje								
Ostatné administratívne výdavky								
Medzisúčet mimo OKRUHU 7 viacročného finančného rámca								

SPOLU	1,23	1,23	1,23	1,23	1,23	1,23	1,23	8,61
--------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------	-------------

Rozpočtové prostriedky potrebné na ľudské zdroje a na ostatné administratívne výdavky budú pokryté rozpočtovými prostriedkami GR, ktoré už boli pridelené na riadenie akcie a/alebo boli prerozdelené v rámci GR, a v prípade potreby budú doplnené zdrojmi, ktoré sa môžu prideliť riadiacemu GR v rámci ročného postupu pridelovania zdrojov a v závislosti od rozpočtových obmedzení.

⁴⁶

Technická a/alebo administratívna pomoc a výdavky určené na financovanie vykonávania programov a/alebo akcií EÚ (pôvodné rozpočtové riadky „BA“), nepriamy výskum, priamy výskum.

3.2.2.1. Odhadované potreby ľudských zdrojov

- ☐ Návrh/iniciatíva si nevyžaduje použitie ľudských zdrojov.
- ☒ Návrh/iniciatíva si vyžaduje použitie ľudských zdrojov, ako je uvedené v nasledujúcej tabuľke:

odhady sa vyjadrujú v jednotkách ekvivalentu plného pracovného času

Roky		2021	2022	2023	2024	2025	2026	2027
• Plán pracovných miest (úradníci a dočasní zamestnanci)								
ústredie a zastúpenia Komisie		6	6	6	6	6	6	6
delegácie								
výskum								
• Externí zamestnanci (ekvivalent plného pracovného času) – ZZ, MZ, VNE, DAZ a PED ⁴⁷								
Okruh 7								
Financované z OKRUHU 7 viacročného finančného rámca	– ústredie	3	3	3	3	3	3	3
	– delegácie							
Financované z finančného krytia na vykonávanie programu ⁴⁸	– ústredie							
	– delegácie							
Výskum								
Iné (uved'te)								
SPOLU		9	9	9	9	9	9	9

Potreby ľudských zdrojov budú pokryté úradníkmi GR, ktorí už boli pridelení na riadenie akcie a/alebo boli interne prerozdelení v rámci GR, a v prípade potreby budú doplnené zdrojmi, ktoré sa môžu prideliť riadiacemu GR v rámci ročného postupu prideľovania zdrojov v závislosti od rozpočtových obmedzení.

Opis úloh, ktoré sa majú vykonať:

Úradníci a dočasní zamestnanci	• príprava delegovaných aktov podľa článku 18 ods. 6, článku 21 ods. 2, článku 36, • príprava vykonávacích aktov podľa článku 12 ods. 8, článku 18 ods. 5, článku 20 ods. 11, • poskytovanie sekretariátu pre skupinu pre spoluprácu NIS, • organizácia plenárnych zasadnutí skupiny pre spoluprácu NIS a zasadnutí pracovných okruhov, • koordinácia práce členských štátov v súvislosti s rôznymi dokumentmi (usmernenia, súbory nástrojov atď.), • spolupráca s ostatnými útvarmi Komisie, agentúrou ENISA a vnútroštátnymi orgánmi s cieľom vykonávať smernicu NIS, • analýza vnútroštátnych metód a najlepších postupov súvisiacich s vykonávaním smernice NIS.
Externí zamestnanci	Podpora všetkých uvedených úloh podľa potreby

⁴⁷ ZZ = zmluvný zamestnanec; MZ = miestny zamestnanec; VNE = vyslaný národný expert; DAZ = dočasný agentúrny zamestnanec; PED = pomocný expert v delegácii.

⁴⁸ Čiastkový strop pre externých zamestnancov financovaných z operačných rozpočtových prostriedkov (pôvodné rozpočtové riadky „BA“).

3.2.3. Príspevky od tretích strán

Návrh/iniciatíva:

- ☒ nezahŕňa spolufinancovanie tretími stranami
- ☐ zahŕňa spolufinancovanie tretími stranami, ako je odhadnuté v nasledujúcej tabuľke:

rozpočtové prostriedky v mil. EUR (zaokrúhlené na 3 desatinné miesta)

Roky	2021	2022	2023	2024	2025	2026	2027	SPOLU
Uved'te spolufinancujúci subjekt								
Prostriedky zo spolufinancovania SPOLU								

3.3. Odhadovaný vplyv na príjmy

- ☒ Návrh/iniciatíva nemá finančný vplyv na príjmy.
- ☐ Návrh/iniciatíva má finančný vplyv na príjmy, ako je uvedené v nasledujúcej tabuľke:
 - ☐ vplyv na vlastné zdroje
 - ☐ vplyv na iné príjmy

uved'te, či sú príjmy pripísané rozpočtovým riadkom výdavkov ☐

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

Rozpočtový riadok príjmov:	Vplyv návrhu/iniciatívy ⁴⁹						
	2021	2022	2023	2024	2025	2026	2027
Článok							

V prípade pripísaných príjmov uved'te príslušné rozpočtové riadky výdavkov.

Ďalšie poznámky (napr. spôsob/vzorec použitý na výpočet vplyvu na príjmy alebo akékoľvek ďalšie informácie).

⁴⁹

Pokiaľ ide o tradičné vlastné zdroje (clá, odvody z produkcie cukru), uvedené sumy musia predstavovať čisté sumy, t. j. hrubé sumy po odčítaní 20 % na náklady na výber.

PRÍLOHA **k LEGISLATÍVNEMU FINANČNÉMU VÝKAZU**

Názov návrhu/iniciatívy:

Návrh smernice, ktorou sa reviduje smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii

1. **POTREBNÉ ĽUDSKÉ ZDROJE a NEVYHNUTNÉ NÁKLADY NA TIETO ZDROJE**
2. **NÁKLADY na OSTATNÉ ADMINISTRATÍVNE VÝDAVKY**
3. **METÓDY VÝPOČTU POUŽITÉ na ODHAD NÁKLADOV**
 - 3.1. **Ľudské zdroje**
 - 3.2. **Ostatné administratívne výdavky**

Táto príloha, ktorú vyplnia všetky GR/útvary, ktoré sa zúčastňujú na návrhu/iniciatíve, musí byť súčasťou legislatívneho finančného výkazu po začatí konzultácie medzi zainteresovanými útvarmi.

Tabuľky s údajmi sú použité ako zdroj tabuliek nachádzajúcich sa v legislatívnom finančnom výkaze. Slúžia výlučne na vnútorné použitie v rámci Komisie.

1. Náklady na potrebné ľudské zdroje

☐ Návrh/iniciatíva si nevyžaduje použitie ľudských zdrojov

☒ Návrh/iniciatíva si vyžaduje použitie ľudských zdrojov, ako je uvedené v nasledujúcej tabuľke:

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

OKRUH 7 viacročného finančného ráмка		2021		2022		2023		2024		2025		2026		2027		SPOLU	
		FTE	Rozpočtové prostriedky	FTE	Rozpočtové prostriedky	FTE	Rozpočtové prostriedky	FTE	Rozpočtové prostriedky	FTE	Rozpočtové prostriedky	FTE	Rozpočtové prostriedky	FTE	Rozpočtové prostriedky	FTE	Rozpočtové prostriedky
• Plán pracovných miest (úradníci a dočasní zamestnanci)																	
ústredie a zastúpenia Komisie	AD	6	0,9	6	0,9	6	0,9	6	0,9	6	0,9	6	0,9	6	0,9	42	6,3
	AST																
delegácie Únie	AD																
	AST																
• Externí zamestnanci ⁵⁰ 0,24																	
Celkový prostriedkov balík	ZZ	3	0,24	3	0,24	3	0,24	3	0,24	3	0,24	3	0,24	3	0,24	21	1,68
	VNE																
	DAZ																
delegácie Únie	ZZ																
	MZ																
	VNE																

⁵⁰ ZZ = zmluvný zamestnanec; MZ = miestny zamestnanec; VNE = vyslaný národný expert; DAZ = dočasný agentúrny zamestnanec; PED = pomocný expert v delegácii.

	DAZ																
	PED																
iné rozpočtové riadky (uved'te)																	
Medzisúčet – OKRUH 7 viacročného finančného rámca		9	1,14	9	1,14	9	1,14	9	1,14	9	1,14	9	1,14	9	1,14	63	7,98

Potreby ľudských zdrojov budú pokryté úradníkmi GR, ktorí už boli pridelení na riadenie akcie a/alebo boli interne prerozdelení v rámci GR, a v prípade potreby budú doplnené zdrojmi, ktoré sa môžu prideliť riadiacemu GR v rámci ročného postupu prideľovania zdrojov v závislosti od rozpočtových obmedzení.

Mimo OKRUHU 7 viacročného finančného rámca		2021		2022		2023		2024		2025		2025		2025		SPOLU	
		FTE	Rozpočtové prostriedky	FTE	Rozpočtové prostriedky	FTE	Rozpočtové prostriedky	FTE	Rozpočtové prostriedky	FTE	Rozpočtové prostriedky	FTE	Rozpočtové prostriedky	FTE	Rozpočtové prostriedky	FTE	Rozpočtové prostriedky
• Plán pracovných miest (úradníci a dočasní zamestnanci)																	
výskum	AD																
	AST																
• Externí zamestnanci ⁵¹																	
Externí zamestnanci financovaní z operačných rozpočtových prostriedkov (pôvodné rozpočtové riadky „BA“)	– ústredie	ZZ															
		VNE															
		DAZ															
	– delegácie Únie	ZZ															
		MZ															
		VNE															
		DAZ															
		PED															
	výskum	ZZ															
		VNE															
		DAZ															

⁵¹ ZZ = zmluvný zamestnanec; MZ = miestny zamestnanec; VNE = vyslaný národný expert; DAZ = dočasný agentúrny zamestnanec; PED = pomocný expert v delegácii.

iné rozpočtové riadky (uved'te)																	
Medzisúčet – mimo OKRUHU 7 viacročného finančného rámca																	

Potreby ľudských zdrojov budú pokryté úradníkmi GR, ktorí už boli pridelení na riadenie akcie a/alebo boli interne prerozdelení v rámci GR, a v prípade potreby budú doplnené zdrojmi, ktoré sa môžu prideliť riadiacemu GR v rámci ročného postupu prideľovania zdrojov v závislosti od rozpočtových obmedzení.

Odhadovaný vplyv na ľudské zdroje agentúry ENISA

Agentúra Európskej únie pre kybernetickú bezpečnosť, ENISA, ktorej bol aktom o kybernetickej bezpečnosti udelený nový trvalý mandát, bude pomáhať členským štátom a Komisii pri vykonávaní revidovanej smernice NIS.

Agentúra ENISA bude mať na základe revidovanej smernice NIS od obdobia 2022/2023 dodatočné oblasti opatrení. Keďže tieto oblasti opatrení by boli podľa mandátu agentúry ENISA zahrnuté medzi jej všeobecné úlohy, budú pre agentúru predstavovať dodatočné pracovné zaťaženie. Podľa návrhu Komisie na revidovanú smernicu NIS sa bude od agentúry ENISA okrem jej súčasných oblastí opatrení vyžadovať, aby do svojho pracovného programu osobitne zahrnula okrem iných aj tieto opatrenia: i) vyvinúť a spravovať európsky register zraniteľnosti (článok 6 ods. 2 návrhu); ii) zabezpečiť sekretariát Európskej siete styčných organizácií pre kybernetické krízy (CyCLONE) (článok 14 návrhu) a vydať výročnú správu o stave kybernetickej bezpečnosti v EÚ (článok 15 návrhu); iii) podporovať organizáciu partnerského preskúmania medzi členskými štátmi (článok 16 návrhu); iv) zhromažďovať súhrnné údaje o incidentoch od členských štátov a vydávať technické usmernenia (článok 20 ods. 9 návrhu); v) vytvoriť a spravovať register subjektov poskytujúcich cezhraničné služby (článok 25 návrhu).

Preto sa predloží žiadosť o päť doplňujúcich FTE od roku 2022 so zodpovedajúcim rozpočtom vo výške približne 0,61 milióna EUR ročne na pokrytie týchto nových pracovných miest (pozri samostatný finančný výkaz pre agentúru).

Preto sa predloží žiadosť o päť doplňujúcich FTE od roku 2022 so zodpovedajúcim rozpočtom na pokrytie týchto nových pracovných miest.

- ☐ Návrh/iniciatíva si nevyžaduje použitie administratívnych rozpočtových prostriedkov
- ☒ Návrh/iniciatíva si vyžaduje použitie administratívnych rozpočtových prostriedkov, ako je uvedené v nasledujúcej tabuľke:

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

	Rok N ⁵² 2022	Rok N + 1 2023	Rok N + 2 2024	Rok N + 3 2025	Uveďte všetky roky, počas ktorých vplyv trvá (pozri bod 1.6)	SPOLU
--	--------------------------------	----------------------	----------------------	----------------------	---	-------

⁵² Rok N je rok, v ktorom sa návrh/iniciatíva začína uskutočňovať. Nahrad'te „N“ očakávaným prvým rokom vykonávania (napríklad: 2021). To isté urobte aj pri nasledujúcich rokoch.

Dočasní zamestnanci (platová trieda AD)	0,450	0,450	0,450	0,450	0,450	0,450		2,7
Dočasní zamestnanci (platová trieda AST)								
Zmluvní zamestnanci	0,160	0,160	0,160	0,160	0,160	0,160		
Vyslaní národní experti								0,96

SPOLU	0,61	0,61	0,61	0,61	0,61	0,61		3,66
--------------	-------------	-------------	-------------	-------------	-------------	-------------	--	-------------

Požiadavky na pracovníkov (FTE):

	Rok N ⁵³ 2022	Rok N + 1 2023	Rok N + 2 2024	Rok N + 3 2025	Uveďte všetky roky, počas ktorých vplyv trvá (pozri bod 1.6)	SPOLU
--	--------------------------------	----------------------	----------------------	----------------------	---	--------------

Dočasní zamestnanci (platová trieda AD)	3	3	3	3	3	3		18
Dočasní zamestnanci (platová trieda AST)								

⁵³ Rok N je rok, v ktorom sa návrh/iniciatíva začína uskutočňovať. Nahradzte „N“ očakávaným prvým rokom vykonávania (napríklad: 2021). To isté urobte aj pri nasledujúcich rokoch.

Zmluvní zamestnanci	2	2	2	2	2	2		12
Vyslaní národní experti								

SPOLU	5	5	5	5	5	5		30
--------------	---	---	---	---	---	---	--	-----------

2. Náklady na ostatné administratívne výdavky

☐ Návrh/iniciatíva si nevyžaduje použitie administratívnych rozpočtových prostriedkov

☒ Návrh/iniciatíva si vyžaduje použitie administratívnych rozpočtových prostriedkov, ako je uvedené v nasledujúcej tabuľke:

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

OKRUH 7 viacročného finančného rámca	2021	2022	2023	2024	2025	2026	2027	Spolu
Ústredie:								
výdavky na služobné cesty a reprezentáciu	0,03	0,03	0,03	0,03	0,03	0,03	0,03	0,21
náklady na konferencie a zasadnutia	0,06	0,06	0,06	0,06	0,06	0,06	0,06	0,42
výbory ⁵⁴								

⁵⁴ Uved'te typ výboru a skupinu, do ktorej patrí.

štúdie a konzultácie								
informačné a riadiace systémy								
vybavenie a služby IKT ⁵⁵								
iné rozpočtové riadky (<i>ak je to potrebné, uveďte</i>)								
Delegácie Únie								
náklady na služobné cesty, konferencie a reprezentáciu								
ďalšie odborné vzdelávanie								
nadobudnutie, nájom a súvisiace výdavky								
zariadenie, nábytok, dodávky a služby								
Medzisúččet OKRUHU 7 viacročného finančného rámca	0,09	0,09	0,09	0,09	0,09	0,09	0,09	0,63

⁵⁵

IKT: Informačné a komunikačné technológie. Musí sa konzultovať DIGIT.

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

Mimo OKRUHU 7 viacročného finančného rámca	2021	2022	2023	2024	2025	2026	2027	Spolu
Výdavky na technickú a administratívnu pomoc (okrem externých zamestnancov) z operačných rozpočtových prostriedkov (pôvodné rozpočtové riadky „BA“)								
– ústredie								
– delegácie Únie								
Ostatné výdavky na riadenie v oblasti výskumu								
Iné rozpočtové riadky (ak je to potrebné, uveďte)								
Medzisúčet – mimo OKRUHU 7 viacročného finančného rámca								

SPOLU OKRUH 7 a mimo OKRUHU 7 viacročného finančného rámca	1,23	1,23	1,23	1,23	1,23	1,23	1,23	8,61
--	------	------	------	------	------	------	------	-------------

Požadované administratívne rozpočtové prostriedky budú pokryté rozpočtovými prostriedkami, ktoré už boli pridelené na riadenie akcie a/alebo boli prerozdelené, a v prípade potreby budú doplnené rozpočtovými prostriedkami, ktoré sa môžu prideliť riadiacemu GR v rámci ročného postupu prideľovania zdrojov v závislosti od rozpočtových obmedzení.

3. Metódy výpočtu použité na odhad nákladov

3.1. Ľudské zdroje

V tejto časti sa stanovuje metóda výpočtu použitá na odhad ľudských zdrojov považovaných za potrebné [predpokladané pracovné zaťaženie vrátane konkrétnych pracovných miest (pracovné profily Sysper 2), kategórií zamestnancov a zodpovedajúcich priemerných nákladov]

OKRUH 7 viacročného finančného rámca
<u>Pozn.:</u> Priemerné náklady na každú kategóriu zamestnancov v ústrediach sú k dispozícii na webovom sídle BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/pre/legalbasis/Pages/pre-040-020_preparation.aspx
• Úradníci a dočasní zamestnanci 6 úradníkov v prepočte na plný pracovný úväzok (priemerné náklady 0,150) = 0,9 za rok - príprava delegovaných aktov podľa článku 18 ods. 6, článku 21 ods. 2, článku 36, - príprava vykonávacích aktov podľa článku 12 ods. 8, článku 18 ods. 5, článku 20 ods. 11, - poskytovanie sekretariátu pre skupinu pre spoluprácu NIS, - organizácia plenárnych zasadnutí skupiny pre spoluprácu NIS a zasadnutí pracovných okruhov, - koordinácia práce členských štátov v súvislosti s rôznymi dokumentmi (usmernenia, súbory nástrojov atď.), - spolupráca s ostatnými útvarmi Komisie, agentúrou ENISA a vnútroštátnymi orgánmi s cieľom vykonávať smernicu NIS, - analýza vnútroštátnych metód a najlepších postupov súvisiacich s vykonávaním smernice NIS.
• Externí zamestnanci 3 ZZ (priemerné náklady 0,08) = 0,24 za rok - Podpora všetkých uvedených úloh podľa potreby

Mimo OKRUHU 7 viacročného finančného rámca
• Len miesta financované z rozpočtu na výskum
• Externí zamestnanci

3.2. Ostatné administratívne výdavky

Uved'te podrobnosti o metóde výpočtu použitej pri každom rozpočtovom riadku,

a najmä východiskové predpoklady (napr. počet zasadnutí za rok, priemerné náklady atď.)

OKRUH 7 viacročného finančného rámca

Zasadnutia: Plenárne zasadnutia skupiny pre spoluprácu NIS sa zvyčajne konajú štyrikrát ročne. Komisia kryje náklady spojené s cateringom, ako aj cestovné náklady zástupcov 27 členských štátov (jeden zástupca na jeden členský štát). Náklady jedného zasadnutia môžu predstavovať až 15 000 EUR, čo predstavuje 60 000 EUR ročne.

Služobné cesty: Služobné cesty súvisia s monitorovaním a vykonávaním smernice NIS. Príklad: V jednom roku (máj 2019 až júl 2020) sa mali organizovať tzv. návštevy krajín NIS a malo sa navštíviť všetkých 27 členských štátov s cieľom diskutovať o vykonávaní smernice NIS v EÚ.

Mimo OKRUHU 7 viacročného finančného rámca

PRÍLOHA 7

k

ROZHODNUTIU KOMISIE

**o interných pravidlách plnenia všeobecného rozpočtu Európskej únie
(oddielu Európskej komisie), určenému útvarom Komisie**

LEGISLATÍVNY FINANČNÝ VÝKAZ – „AGENTÚRY“

Tento legislatívny finančný výkaz sa vzťahuje na žiadosť zvýšiť počet zamestnancov agentúry ENISA o 5 FTE od roku 2022 s cieľom umožniť jej vykonávanie doplnkových činností súvisiacich s vykonávaním smernice NIS. Na tieto činnosti sa už vzťahuje mandát agentúry ENISA.

Obsah

1.	RÁMEC NÁVRHU/INICIATÍVY	16
1.1.	Názov návrhu/iniciatívy	16
1.2.	Príslušné oblasti politiky	16
1.3.	Návrh sa týka	16
1.4.	Ciele	16
1.4.1.	Všeobecné ciele.....	16
1.4.2.	Špecifické ciele	16
1.4.3.	Očakávané výsledky a vplyv.....	18
1.4.4.	Ukazovatele výkonnosti	18
1.5.	Dôvody návrhu/iniciatívy	19
1.5.1.	Potreby, ktoré sa majú uspokojiť v krátkodobom alebo dlhodobom horizonte vrátane podrobného harmonogramu prvej fázy vykonávania iniciatívy	19
1.5.2.	Prínos zapojenia Únie (môže byť výsledkom rôznych faktorov, napr. lepšej koordinácie, právnej istoty, väčšej účinnosti alebo komplementárnosti). Na účely tohto bodu je „prínos zapojenia Európskej únie“ hodnota vyplývajúca zo zásahu Únie, ktorá dopĺňa hodnotu, ktorú by inak vytvorili len samotné členské štáty.	20
1.5.3.	Poznatky získané z podobných skúseností v minulosti	20
1.5.4.	Zlučiteľnosť s viacročným finančným rámcom a možná synergie s inými vhodnými nástrojmi	20
1.5.5.	Posúdenie rôznych disponibilných možností financovania vrátane možnosti prerozdelenia	20
1.6.	Trvanie a finančný vplyv návrhu/iniciatívy	21
1.7.	Plánovaný spôsob riadenia	21
2.	OPATRENIA V OBLASTI RIADENIA	23
2.1.	Opatrenia týkajúce sa monitorovania a predkladania správ	23
2.2.	Systémy riadenia a kontroly	23
2.2.1.	Opodstatnenie navrhovaných spôsobov riadenia, mechanizmov vykonávania financovania, spôsobov platby a stratégie kontroly.....	23
2.2.2.	Informácie o zistených rizikách a systémoch vnútornej kontroly zavedených na ich zmiernenie	23
2.2.3.	Odhad a opodstatnenie nákladovej účinnosti kontrol (pomer medzi nákladmi na kontroly a hodnotou súvisiacich riadených finančných prostriedkov) a posúdenie očakávaných úrovní rizika chyby (pri platbe a uzavretí)	23
2.3.	Opatrenia na predchádzanie podvodom a nezrovnalostiam.....	24

3.	ODHADOVANÝ FINANČNÝ VPLYV NÁVRHU/INICIATÍVY	24
3.1.	Príslušné okruhy viacročného finančného rámca a rozpočtové riadky výdavkov	24
3.2.	Odhadovaný vplyv na výdavky.....	26
3.2.1.	Zhrnutie odhadovaného vplyvu na výdavky	26
3.2.2.	Odhadovaný vplyv na rozpočtové prostriedky [subjektu]	28
3.2.3.	Odhadovaný vplyv na ľudské zdroje agentúry ENISA.....	29
3.2.4.	Súlady s platným viacročným finančným rámcom.....	32
3.2.5.	Príspevky od tretích strán.....	32
3.3.	Odhadovaný vplyv na príjmy.....	33

1. RÁMEC NÁVRHU/INICIATÍVY

1.1. Názov návrhu/iniciatívy

Návrh smernice o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii a o zrušení smernice (EÚ) 2016/1148.

1.2. Príslušné oblasti politiky

Komunikačné siete, obsah a technológie

1.3. Návrh sa týka

- ☐ novej akcie
- ☐ novej akcie, ktorá nadväzuje na pilotný projekt/prípravnú akciu⁵⁶
- ☒ predĺženia trvania existujúcej akcie
- ☐ zlúčenia jednej alebo viacerých akcií do ďalšej/novej akcie

1.4. Ciele

1.4.1. Všeobecné ciele

Cieľom revízie je zvýšiť úroveň kybernetickej odolnosti komplexného súboru podnikov pôsobiacich v Európskej únii vo všetkých príslušných odvetviach, znížiť mieru nezrovnalostí, pokiaľ ide o odolnosť na vnútornom trhu v odvetviach, na ktoré sa už smernica vzťahuje, a zlepšiť úroveň spoločnej situačnej informovanosti a spoločnej schopnosti prípravy a reakcie.

1.4.2. Špecifické ciele

S cieľom vyriešiť problém nízkej úrovne kybernetickej odolnosti podnikov pôsobiacich v Európskej únii je špecifickým cieľom zabezpečiť, aby sa od subjektov vo všetkých odvetviach, ktoré sú závislé od sietí a informačných systémov a ktoré poskytujú kľúčové služby pre hospodárstvo a spoločnosť ako celok, vyžadovalo, aby prijali opatrenia v oblasti kybernetickej bezpečnosti a oznamovali incidenty s cieľom zvýšiť celkovú úroveň kybernetickej odolnosti na celom vnútornom trhu.

S cieľom vyriešiť problém nejednotnej úrovne odolnosti v členských štátoch a odvetviach je špecifickým cieľom zabezpečiť, aby všetky subjekty, ktoré sú aktívne v odvetviach, na ktoré sa vzťahuje právny rámec smernice NIS a ktoré sú podobnej veľkosti a majú porovnateľnú úlohu, podliehali rovnakému regulačnému režimu (a boli v rámci rozsahu pôsobnosti alebo mimo neho) bez ohľadu na to, do ktorej právomoci v rámci EÚ patria.

S cieľom zabezpečiť, aby sa od všetkých subjektov pôsobiacich v odvetviach, na ktoré sa vzťahuje právny rámec smernice NIS, vyžadovalo, aby plnili rovnaké povinnosti založené na princípe riadenia rizika, pokiaľ ide o bezpečnostné opatrenia, a aby museli oznamovať všetky incidenty na základe jednotného súboru kritérií, sa má v rámci špecifických cieľov zabezpečiť, aby príslušné orgány vynucovali účinnejšie dodržiavanie pravidiel stanovených právnym nástrojom, a to prostredníctvom zosúladených opatrení dohľadu a opatrení na presadzovanie, a aby zabezpečili porovnateľnú úroveň zdrojov v členských štátoch pridelených príslušným orgánom, ktoré by im umožnili splniť hlavné úlohy stanovené v rámci smernice NIS.

⁵⁶

Podľa článku 58 ods. 2 písm. a) alebo b) nariadenia o rozpočtových pravidlách.

S cieľom vyriešiť problém spoločnej situačnej informovanosti a nedostatočnej spoločnej reakcie na krízu, je špecifickým cieľom zabezpečiť, aby si členské štáty vymieňali zásadné informácie, a to zavedením jasných povinností pre príslušné orgány na výmenu informácií a spoluprácu, pokiaľ ide o kybernetické hrozby a incidenty, ako aj vyvinutím spoločnej operačnej kapacity Únie, pokiaľ ide o reakciu na krízy.

1.4.3. Očakávané výsledky a vplyv

Uved'te, aký vplyv by mal mať návrh/iniciatíva na príjemcov/cieľové skupiny.

Očakáva sa, že návrh prinesie významné výhody: odhady naznačujú, že môže viesť k zníženiu nákladov na kybernetické incidenty o 11,3 miliardy EUR. V rámci NIS by sa značne rozšíril odvetvový rozsah pôsobnosti, ale popri uvedených výhodách by sa pre nové subjekty, na ktoré sa má rámec vzťahovať, ako aj pre príslušné orgány vyvážilo zaťaženie, ktoré môže vzniknúť na základe požiadaviek smernice NIS, najmä z pohľadu dohľadu. Je to z toho dôvodu, že v novom rámci NIS by sa zriadil dvojúrovňový prístup s dôrazom na veľké a kľúčové subjekty a rozlišovanie režimu dohľadu, ktorý umožňuje len dohľad *ex post* pre veľký počet týchto subjektov, a to najmä pre tie, ktoré sa považujú za „dôležité“, ale nie „kľúčové“.

Návrh by celkovo viedol k efektívnym kompromisom a synergiám, pričom má najlepší potenciál zo všetkých analyzovaných možností politiky na zabezpečenie zvýšenej a konzistentnej úrovne kybernetickej odolnosti kľúčových subjektov v Únii, čo by v konečnom dôsledku viedlo k úspore nákladov pre podniky aj spoločnosť.

Návrh by takisto viedol k istým nákladom na zabezpečenie súladu a presadzovanie predpisov pre príslušné orgány členských štátov (odhadol sa celkový nárast o približne 20 – 30 % zdrojov). Nový rámec by však priniesol aj značné výhody, a to prostredníctvom lepšieho prehľadu o kľúčových podnikoch a lepšej interakcie s nimi, posilnenú cezhraničnú operačnú spoluprácu, ako aj vzájomnú pomoc a mechanizmy partnerského preskúmania. To by viedlo k celkovému posilneniu spôsobilostí v oblasti kybernetickej bezpečnosti v členských štátoch.

Pokiaľ ide o spoločnosti, ktoré by patrili do rozsahu pôsobnosti rámca NIS, odhaduje sa, že by potrebovali zvýšenie o maximálne 22 % svojich súčasných výdavkov v oblasti bezpečnosti IKT v prvých rokoch po zavedení nového rámca NIS (to predstavuje 12 % pre spoločnosti, ktoré už do rozsahu pôsobnosti súčasnej smernice NIS patria). Tento priemerný nárast výdavkov v oblasti bezpečnosti IKT by však viedol k pomernému úžitku z takých investícií, najmä z dôvodu výrazného zníženia nákladov na kybernetické incidenty (odhaduje sa 118 miliárd EUR za desať rokov).

Z rozsahu pôsobnosti rámca smernice NIS by boli vyňaté malé podniky a mikropodniky. Pokiaľ ide o stredné podniky, očakávať možno nárast úrovne výdavkov v oblasti bezpečnosti IKT v prvých rokoch po zavedení nového rámca NIS. Zvyšovanie úrovne bezpečnostných požiadaviek pre tieto subjekty by zároveň aj stimulovalo ich spôsobilosti v oblasti kybernetickej bezpečnosti a pomohlo im zlepšiť ich riadenie rizík v oblasti IKT.

Malo by to vplyv na štátne rozpočty a verejnú správu: v krátkodobom a strednodobom horizonte sa očakáva nárast približne o 20 – 30 % zdrojov.

Neočakávajú sa žiadne ďalšie významné negatívne vplyvy. Očakáva sa, že návrh bude viesť k stabilnejším spôsobilostiam v oblasti kybernetickej bezpečnosti a následne by mal významnejší zmierňujúci účinok na počet a závažnosť incidentov vrátane porušenia ochrany údajov. Takisto je pravdepodobné, že bude mať pozitívny vplyv na zabezpečenie rovnakých podmienok v členských štátoch pre všetky subjekty, ktoré patria do rozsahu pôsobnosti smernice NIS, a zníži informačné asymetrie v oblasti kybernetickej bezpečnosti.

1.4.4. Ukazovatele výkonnosti

Uved'te ukazovatele na monitorovanie pokroku a dosiahnutých výsledkov.

Posúdenie ukazovateľov vykoná Komisia za podpory agentúry ENISA a skupiny pre spoluprácu, a to tri roky od nadobudnutia účinnosti nového právneho aktu NIS. Niektoré

ukazovatele na monitorovanie, na základe ktorých sa vyhodnotí úspech preskúmania smernice NIS, sú:

- Zlepšené riešenie incidentov: Prijatím opatrení v oblasti kybernetickej bezpečnosti spoločnosti nielen zlepšujú svoju schopnosť úplne sa vyhnúť istým incidentom, ale aj svoju kapacitu reakcie na incidenty. Kritériá úspešnosti teda sú i) zníženie priemerného času na odhalenie incidentu; ii) priemerný čas, ktorý potrebujú organizácie na zotavenie po incidente a iii) priemerné náklady na škody spôsobené incidentom.
- Zvýšená informovanosť vrcholového manažmentu spoločností o kybernetických rizikách: Keďže sa od spoločností vyžaduje, aby prijali opatrenia, revidovaná smernica NIS prispeje k zvýšeniu informovanosti o rizikách spojených s kybernetickou bezpečnosťou medzi predstaviteľmi vrcholového manažmentu spoločností. To možno merať na základe štúdií toho, do akej miery spoločnosti v rámci rozsahu pôsobnosti smernice NIS uprednostňujú vo vnútorných politikách spoločnosti a jej postupoch kybernetickú bezpečnosť, ako je doložené v internej dokumentácii, príslušných programoch odborného vzdelávania a osvetových činnostiach pre zamestnancov a uprednostňovaním investícií v oblasti IKT súvisiacich s bezpečnosťou. Manažment všetkých kľúčových a dôležitých subjektov by mal takisto poznať pravidlá stanovené smernicou NIS.
- Vyrovnanie odvetvovo špecifických výdavkov: Výdavky na bezpečnosť IKT sa v rámci odvetví v EÚ výrazne líšia. Na základe požiadaviek, aby spoločnosti vo viacerých odvetviach prijali opatrenia, mali by sa odchýlky od priemerných odvetvovo špecifických výdavkov na bezpečnosť IKT ako percentuálny podiel celkových výdavkov na IKT znížiť medzi odvetviami a v členských štátoch.
- Silnejšie príslušné orgány a zvýšená spolupráca: Revidovaná smernica NIS by potenciálne mohla priniesť príslušným orgánom ďalšie úlohy. To by malo merateľný vplyv na finančné a ľudské zdroje vyčlenené pre agentúry kybernetickej bezpečnosti na vnútroštátnej úrovni, ako aj pozitívny vplyv na kapacitu príslušných orgánov na aktívnu spoluprácu a z nej vyplývajúce zvýšenie počtu prípadov, keď príslušné orgány spolupracujú na účely riešenia cezhraničných incidentov alebo vykonávania spoločných činností dohľadu.
- Intenzívnejšia výmena informácií: Revidovanou smernicou NIS by sa takisto zlepšila výmena informácií medzi spoločnosťami a s príslušnými orgánmi. Jedným z cieľov preskúmania by mohlo byť zvýšenie počtu subjektov zapojených do rôznych foriem výmeny informácií.

1.5. Dôvody návrhu/iniciatívy

1.5.1. *Potreby, ktoré sa majú uspokojiť v krátkodobom alebo dlhodobom horizonte vrátane podrobného harmonogramu prvej fázy vykonávania iniciatívy*

Cieľom návrhu je zvýšiť úroveň kybernetickej odolnosti komplexného súboru podnikov pôsobiach v Európskej únii vo všetkých príslušných odvetviach, pokiaľ ide o odolnosť na vnútornom trhu v odvetviach, na ktoré sa už smernica vzťahuje, a zlepšiť úroveň spoločnej situačnej informovanosti a spoločnej schopnosti prípravy a reakcie. Bude vychádzať z výsledkov dosiahnutých pri vykonávaní smernice (EÚ) 2016/1148 za posledné štyri roky.

- 1.5.2. *Prínos zapojenia Únie (môže byť výsledkom rôznych faktorov, napr. lepšej koordinácie, právnej istoty, väčšej účinnosti alebo komplementárnosti). Na účely tohto bodu je „prínos zapojenia Európskej únie“ hodnota vyplývajúca zo zásahu Únie, ktorá dopĺňa hodnotu, ktorú by inak vytvorili len samotné členské štáty.*

Kybernetická odolnosť v rámci Únie nemôže byť účinná, ak sa k nej prostredníctvom vnútroštátnych alebo regionálnych dátových síl pristupuje odlišným spôsobom. Cieľom smernice NIS bolo napraviť tento nedostatok stanovením rámca pre bezpečnosť sietí a informačných systémov na vnútroštátnej úrovni a úrovni Únie. Prvé pravidelné preskúmanie smernice NIS však poukázalo na istý počet charakteristických nedostatkov, ktoré napokon viedli k výrazným rozdielom v členských štátoch, a to pokiaľ ide o spôsobilosti, plánovanie a úroveň ochrany, čo má zároveň vplyv na rovnaké podmienky pre podobné spoločnosti na vnútornom trhu.

Intervenciu EÚ nad rámec súčasných opatrení smernice NIS možno odôvodniť najmä týmito skutočnosťami: i) cezhraničný charakter problému; ii) potenciál opatrenia EÚ zlepšiť a uľahčiť účinné vnútroštátne politiky; iii) príspevok zosúladeného postupu založeného na spolupráci v oblasti politických opatrení NIS k účinnej ochrane údajov a súkromia.

Uvedené ciele možno preto lepšie dosiahnuť prostredníctvom opatrení na úrovni EÚ ako zo strany samotných členských štátov.

- 1.5.3. *Poznatky získané z podobných skúseností v minulosti*

Smernica NIS je prvým horizontálnym nástrojom vnútorného trhu, ktorého cieľom je zlepšiť odolnosť sietí a systémov v Únii proti kybernetickým rizikám. Od nadobudnutia účinnosti v roku 2016 smernica už významne prispela k zvýšeniu spoločnej úrovne kybernetickej bezpečnosti medzi členskými štátmi. Preskúmanie fungovania a vykonávania tejto smernice však poukázalo na viacero nedostatkov, ktoré sa, okrem rastúcej digitalizácie a potreby aktualizovanejšej reakcie, musia riešiť v revidovanom právnom akte.

- 1.5.4. *Zlučiteľnosť s viacročným finančným rámcom a možná synergia s inými vhodnými nástrojmi*

Nový návrh je úplne konzistentný a zosúladený s inými súvisiacimi iniciatívami, ako je návrh nariadenia o digitálnej prevádzkovej odolnosti finančného sektora a návrh smernice o odolnosti kritických prevádzkovateľov základných služieb. Je takisto zosúladený s európskym kódexom elektronických komunikácií, všeobecným nariadením o ochrane údajov a nariadením eIDAS.

Návrh je podstatnou časťou stratégie EÚ pre bezpečnostnú úniu.

- 1.5.5. *Posúdenie rôznych disponibilných možností financovania vrátane možnosti prerozdelenia*

Riadenie týchto úloh agentúrou ENISA si vyžaduje špecifické profily a dodatočné pracovné zaťaženie, ktoré nemožno vykonať bez zvýšenia ľudských zdrojov.

1.6. Trvanie a finančný vplyv návrhu/iniciatívy

☐ obmedzené trvanie

- ☐ Návrh/iniciatíva je v platnosti od [DD/MM]RRRR do [DD/MM]RRRR
- ☐ Finančný vplyv trvá od RRRR do RRRR.

☒ neobmedzené trvanie

- Počiatočná fáza vykonávania bude trvať od roku 2022 do roku 2025,
- a potom bude vykonávanie pokračovať v plnom rozsahu.

1.7. Plánovaný spôsob riadenia⁵⁷

☒ Priame riadenie na úrovni Komisie

prostredníctvom

- ☐ výkonných agentúr
- ☐ Zdieľané riadenie s členskými štátmi
- ☐ **X Nepriame riadenie**, pri ktorom sa plnením rozpočtu poveria:
 - ☐ medzinárodné organizácie a ich agentúry (uved'te),
 - ☐ Európska investičná banka (EIB) a Európsky investičný fond,
 - ☒ subjekty uvedené v článkoch 70 a 71,
 - ☐ verejnoprávne subjekty,
 - ☐ súkromnoprávne subjekty poverené vykonávaním verejnej služby, pokiaľ tieto subjekty poskytujú dostatočné finančné záruky,
 - ☐ súkromnoprávne subjekty spravované právom členského štátu, ktoré sú poverené vykonávaním verejno-súkromného partnerstva a ktoré poskytujú dostatočné finančné záruky,
 - ☐ osoby poverené vykonávaním osobitných činností v oblasti SZBP podľa hlavy V Zmluvy o Európskej únii a určeným v príslušnom základnom akte.

Poznámky:

Agentúra Európskej únie pre kybernetickú bezpečnosť, ENISA, ktorej bol aktom o kybernetickej bezpečnosti udelený nový trvalý mandát, bude pomáhať členským štátom a Komisii pri vykonávaní revidovanej smernice NIS.

Agentúra ENISA bude mať na základe revidovanej smernice NIS od obdobia 2022/2023 dodatočné oblasti opatrení. Keďže tieto oblasti opatrení by boli podľa mandátu agentúry ENISA zahrnuté medzi jej všeobecné úlohy, budú pre agentúru predstavovať dodatočné pracovné zaťaženie. Podľa návrhu Komisie na revidovanú smernicu NIS sa bude od agentúry ENISA okrem jej súčasných oblastí opatrení vyžadovať, aby do svojho pracovného programu osobitne zahrnula okrem iných aj tieto opatrenia: i) vyvinúť a spravovať európsky register zraniteľnosti (článok 6 ods. 2 návrhu); ii) zabezpečiť sekretariát Európskej siete styčných organizácií pre kybernetické krízy (CyCLONe) (článok 14 návrhu) a vydať výročnú správu o stave kybernetickej bezpečnosti v EÚ (článok 15 návrhu); iii) podporovať

⁵⁷

Vysvetlenie spôsobov riadenia a odkazy na nariadenie o rozpočtových pravidlách sú k dispozícii na webovom sídle BudgWeb: <https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx>.

organizáciu partnerského preskúmania medzi členskými štátmi (článok 16 návrhu); iv) zhromažďovať súhrnné údaje o incidentoch od členských štátov a vydávať technické usmernenia (článok 20 ods. 9 návrhu); v) vytvoriť a spravovať register subjektov poskytujúcich cezhraničné služby (článok 25 návrhu).

Preto sa predloží žiadosť o päť doplňujúcich FTE od roku 2022 so zodpovedajúcim rozpočtom vo výške približne 0,61 milióna EUR ročne na pokrytie týchto nových pracovných miest.

2. OPATRENIA V OBLASTI RIADENIA

2.1. Opatrenia týkajúce sa monitorovania a predkladania správ

Uved'te časový interval a podmienky, ktoré sa vzťahujú na tieto opatrenia.

Komisia pravidelne preskúma fungovanie tejto smernice a podá o tom správu Európskemu parlamentu a Rade, pričom prvýkrát tak urobí tri roky od nadobudnutia jej účinnosti.

Komisia takisto posúdi správnu transpozíciu smernice členskými štátmi.

Monitorovanie a oznamovanie návrhu bude prebiehať podľa zásad uvedených v trvalom mandáte agentúry ENISA v súlade s NARIADENÍM (EÚ) 2019/881 (akt o kybernetickej bezpečnosti).

Údaje, ktoré sa používajú na plánované monitorovanie, by poskytovala hlavne agentúra ENISA, skupina pre spoluprácu, sieť jednotiek CSIRT a orgány členských štátov. Okrem údajov pochádzajúcich zo správ (vrátane výročných správ o činnosti) agentúry ENISA, skupiny pre spoluprácu a siete jednotiek CSIRT sa v prípade potreby použijú osobitné nástroje zberu údajov (napríklad prieskumy vnútroštátnych orgánov, Eurobarometer a správy z kampane Mesiac kybernetickej bezpečnosti a z celoeurópskych cvičení).

2.2. Systémy riadenia a kontroly

2.2.1. *Opodstatnenie navrhovaných spôsobov riadenia, mechanizmov vykonávania financovania, spôsobov platby a stratégie kontroly*

Oddelenie v rámci GR CNECT, ktoré je zodpovedné za oblasť politiky, bude riadiť vykonávanie tejto smernice.

Pokiaľ ide o riadenie agentúry ENISA, v článku 15 aktu o kybernetickej bezpečnosti sa stanovuje podrobný zoznam kontrolných funkcií správnej rady agentúry ENISA.

Podľa článku 31 aktu o kybernetickej bezpečnosti je výkonný riaditeľ agentúry ENISA zodpovedný za vykonávanie rozpočtu agentúry ENISA a vnútorný audítor Komisie má rovnaké právomoci nad agentúrou ENISA ako nad útvarmi Komisie. Správna rada agentúry ENISA vydáva stanovisko ku konečnej účtovnej závierke agentúry ENISA.

2.2.2. *Informácie o zistených rizikách a systémoch vnútornej kontroly zavedených na ich zmierňovanie*

Veľmi nízke riziko, keďže ekosystém smernice NIS je už zavedený a už sa vzťahuje aj na agentúru ENISA, ktorá má po nadobudnutí účinnosti aktu o kybernetickej bezpečnosti v roku 2019 trvalý mandát.

2.2.3. *Odhad a opodstatnenie nákladovej účinnosti kontrol (pomer medzi nákladmi na kontroly a hodnotou súvisiacich riadených finančných prostriedkov) a posúdenie očakávaných úrovní rizika chyby (pri platbe a uzavretí)*

Požadované zvýšenie rozpočtu uplatňuje hlavu 1 a je určené na financovanie miezd. To znamená, že riziko chyby na úrovni platieb je veľmi nízke.

2.3. Opatrenia na predchádzanie podvodom a nezrovnalostiam

Uveďte existujúce a plánované preventívne a ochranné opatrenia, napr. zo stratégie na boj proti podvodom.

Budú sa uplatňovať preventívne a ochranné opatrenia agentúry ENISA, a to:

– Platby za všetky požadované služby alebo štúdie kontrolujú zamestnanci agentúry pred zaplatením, berúc do úvahy všetky zmluvné náležitosti, hospodárske zásady a osvedčené finančné alebo riadiace postupy. Opatrenia proti podvodom (kontrola, požiadavky na hlásenie a pod.) sa zahrnú do všetkých dohôd a zmlúv uzavretých medzi agentúrou a príjemcami všetkých platieb.

– Na účely boja proti podvodu, korupcii a iným nezákonným činnostiam sa uplatňujú bez obmedzenia ustanovenia nariadenia (EÚ, Euratom) č. 883/2013 Európskeho parlamentu a Rady z 25. mája 1999, týkajúce sa vyšetrovaní vykonaných Európskym úradom proti podvodu (OLAF).

– Podľa článku 33 aktu o kybernetickej bezpečnosti pristúpila 28. decembra 2019 agentúra ENISA k medziinštitucionálnej dohode z 25. mája 1999 medzi Európskym parlamentom, Radou Európskej únie a Komisiou Európskych spoločenstiev týkajúcej sa vyšetrovaní Európskeho úradu pre boj proti podvodom (OLAF). Agentúra ENISA bezodkladne vydá príslušné predpisy uplatniteľné na všetkých jej zamestnancov.

3. ODHADOVANÝ FINANČNÝ VPLYV NÁVRHU/INICIATÍVY

3.1. Príslušné okruhy viacročného finančného rámca a rozpočtové riadky výdavkov

- Existujúce rozpočtové riadky

V poradí, v akom za sebou nasledujú okruhy viacročného finančného rámca a rozpočtové riadky.

Okruh viacročného finančného rámca	Rozpočtový riadok	Druh výdavkov	Príspevky			
	Číslo	DRP/NRP ⁵⁸	krajín EZVO ⁵⁹	kandidátskych krajín ⁶⁰	tretích krajín	v zmysle článku 21 ods. 2 písm. b) nariadenia o rozpočtových pravidlách
2	02 10 04	/NRP	ÁNO	NIE	NIE	/NIE

- Požadované nové rozpočtové riadky

V poradí, v akom za sebou nasledujú okruhy viacročného finančného rámca a rozpočtové riadky.

Okruh viacročného	Rozpočtový riadok	Druh výdavkov	Príspevky
-------------------	-------------------	---------------	-----------

⁵⁸ DRP = diferencované rozpočtové prostriedky/NRP = nediferencované rozpočtové prostriedky.

⁵⁹ EZVO: Európske združenie voľného obchodu.

⁶⁰ Kandidátske krajiny a prípadne potenciálni kandidáti zo západného Balkánu.

finančného rámca	Číslo	DRP/NRP	krajín EZVO	kandidátskych krajín	tretích krajín	v zmysle článku 21 ods. 2 písm. b) nariadenia o rozpočtových pravidlách
	[XX.YY.YY.YY]		ÁNO/ NIE	ÁNO/NIE	ÁNO/ NIE	ÁNO/NIE

3.2. Odhadovaný vplyv na výdavky

3.2.1. Zhrnutie odhadovaného vplyvu na výdavky

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

Okruh viacročného finančného rámca	Číslo	[Okruh...2 ekonomika.....]	Jednotný	trh,	inovácia	a digitálna
------------------------------------	-------	-------------------------------	----------	------	----------	-------------

[Subjekt]: <...ENISA....>			Rok N ⁶¹ 2022	Rok N + 1 2023	Rok N + 2 2024	Rok N + 3 2025	Uveďte všetky roky, počas ktorých vplyv trvá (pozri bod 1.6) 2026 2027			SPOLU
Hlava 1	Závazky	(1)	0,61	0,61	0,61	0,61	0,61	0,61		3,66
	Platby	(2)	0,61	0,61	0,61	0,61	0,61	0,61		3,66
Hlava 2	Závazky	(1a)								
	Platby	(2a)								
Hlava 3	Závazky	(3a)								
	Platby	(3b)								
Rozpočtové prostriedky pre [subjekt] <ENISA.....>SPOLU	Závazky	= 1 + 1a + 3a	0,61	0,61	0,61	0,61	0,61	0,61		3,66
	Platby	= 2 + 2a + 3b	0,61	0,61	0,61	0,61	0,61	0,61		3,66

⁶¹ Rok N je rok, v ktorom sa návrh/iniciatíva začína uskutočňovať. Nahradíte „N“ očakávaným prvým rokom vykonávania (napríklad: 2021). To isté urobte aj pri nasledujúcich rokoch.

Okruh viacročného finančného rámca	5	„Administratívne výdavky“
---	----------	---------------------------

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

		Rok N	Rok N + 1	Rok N + 2	Rok N + 3	Uveďte všetky roky, počas ktorých vplyv trvá (pozri bod 1.6)			SPOLU
GR: <.....>									
• Ľudské zdroje									
• Ostatné administratívne výdavky									
GR SPOLU <.....>		Rozpočtové prostriedky							

Rozpočtové prostriedky OKRUHU 5 viacročného finančného rámca SPOLU	(Závázky spolu = Platby spolu)								
---	--------------------------------	--	--	--	--	--	--	--	--

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

		Rok N ⁶² 2022	Rok N + 1 2023	Rok N + 2 2024	Rok N + 3 2025	Uveďte všetky roky, počas ktorých vplyv trvá (pozri bod 1.6)			SPOLU
						2026	2027		
Rozpočtové prostriedky OKRUHOV 1 až 5 viacročného finančného rámca SPOLU	Závázky	0,61	0,61	0,61	0,61	0,61	0,61		3,66
	Platby	0,61	0,61	0,61	0,61	0,61	0,61		3,66

⁶² Rok N je rok, v ktorom sa návrh/iniciatíva začína uskutočňovať. Nahradzte „N“ očakávaným prvým rokom vykonávania (napríklad: 2021). To isté urobte aj pri nasledujúcich rokoch.

3.2.2. Odhadovaný vplyv na rozpočtové prostriedky [subjektu]

- ☒ Návrh/iniciatíva si nevyžaduje použitie operačných rozpočtových prostriedkov
- ☐ Návrh/iniciatíva si vyžaduje použitie operačných rozpočtových prostriedkov, ako je uvedené v nasledujúcej tabuľke:

viazané rozpočtové prostriedky v mil. EUR (zaokrúhlené na 3 desatinné miesta)

Uved'te ciele a výstupy			Rok N		Rok N + 1		Rok N + 2		Rok N + 3		Uved'te všetky roky, počas ktorých vplyv trvá (pozri bod 1.6)						SPOLU	
	VÝSTUPY																	
	↓	Druh ⁶³	Priemerné náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Celkový počet
ŠPECIFICKÝ CIEĽ č. 1 ⁶⁴ ...																		
– Výstup																		
– Výstup																		
– Výstup																		
Špecifický cieľ č. 1 medzisúčet																		
ŠPECIFICKÝ CIEĽ č. 2...																		
– Výstup																		
Špecifický cieľ č. 2 medzisúčet																		
NÁKLADY SPOLU																		

⁶³ Výstupy znamenajú dodané produkty a služby (napr.: počet financovaných výmen študentov, vybudované cesty v km atď.).

⁶⁴ Ako je uvedené v bode 1.4.2. „Špecifické ciele...“.

3.2.3. Odhadovaný vplyv na ľudské zdroje agentúry ENISA

3.2.3.1. Zhrnutie

Agentúra ENISA bude mať na základe revidovanej smernice NIS od obdobia 2022/2023 dodatočné úlohy. Keďže tieto úlohy budú zahrnuté do mandátu agentúry ENISA, budú pre agentúru predstavovať dodatočné pracovné zaťaženie. Podľa návrhu Komisie na revidovanú smernicu NIS sa bude od agentúry ENISA okrem jej súčasných úloh vyžadovať, aby i) vyvinula a spravovala európsky register zraniteľnosti (článok 6 ods. 2); ii) zabezpečila sekretariát Európskej siete styčných organizácií pre kybernetické krízy (CyCLONe) (článok 14) a vydala výročnú správu o stave kybernetickej bezpečnosti v EÚ (článok 15); iii) podporovala organizáciu partnerského preskúmania medzi členskými štátmi (článok 16); iv) zhromažďovala súhrnné údaje o incidentoch od členských štátov a vydávala technické usmernenia (článok 20 ods. 9); v) vytvorila a spravovala register subjektov poskytujúcich cezhraničné služby (článok 25).

Preto sa predloží žiadosť o päť doplnujúcich FTE od roku 2022 so zodpovedajúcim rozpočtom na pokrytie týchto nových pracovných miest.

- ☐ Návrh/iniciatíva si nevyžaduje použitie administratívnych rozpočtových prostriedkov
- ☒ Návrh/iniciatíva si vyžaduje použitie administratívnych rozpočtových prostriedkov, ako je uvedené v nasledujúcej tabuľke:

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

	Rok N ⁶⁵ 2022	Rok N + 1 2023	Rok N + 2 2024	Rok N + 3 2025	Uveďte všetky roky, počas ktorých vplyv trvá (pozri bod 1.6)			SPOLU
	2022	2023	2024	2025	2026	2027		

Dočasní zamestnanci (platová trieda AD)	0,450	0,450	0,450	0,450	0,450	0,450		2,7
Dočasní zamestnanci (platová trieda AST)								
Zmluvní zamestnanci	0,160	0,160	0,160	0,160	0,160	0,160		0,96
Vyslaní národní experti								

SPOLU	0,61	0,61	0,61	0,61	0,61	0,61		3,66
-------	------	------	------	------	------	------	--	------

⁶⁵

Rok N je rok, v ktorom sa návrh/iniciatíva začína uskutočňovať. Nahraďte „N“ očakávaným prvým rokom vykonávania (napríklad: 2021). To isté urobte aj pri nasledujúcich rokoch.

Požiadavky na pracovníkov (FTE):

	Rok N ⁶⁶ 2022	Rok N + 1 2023	Rok N + 2 2024	Rok N + 3 2025	Uved'te všetky roky, počas ktorých vplyv trvá (pozri bod 1.6) 2026 2027		SPOLU
--	--------------------------------	----------------------	----------------------	----------------------	---	--	-------

Dočasní zamestnanci (platová trieda AD)	3	3	3	3	3	3	18
Dočasní zamestnanci (platová trieda AST)							
Zmluvní zamestnanci	2	2	2	2	2	2	12
Vyslaní národní experti							

SPOLU	5	5	5	5	5	5	30
-------	---	---	---	---	---	---	----

3.2.3.2. Odhadované potreby ľudských zdrojov pre príslušné GR

- ☐ Návrh/iniciatíva si nevyžaduje použitie ľudských zdrojov.
- ☐ Návrh/iniciatíva si vyžaduje použitie ľudských zdrojov, ako je uvedené v nasledujúcej tabuľke:

odhady sa zaokrúhľujú na celé čísla (alebo najviac na jedno desatinné miesto)

	Rok N	Rok N + 1	Rok N + 2	Rok N + 3	Uved'te všetky roky, počas ktorých vplyv trvá (pozri bod 1.6)		
• Plán pracovných miest (úradníci a dočasní zamestnanci)							
XX 01 01 01 (ústredie a zastúpenia Komisie)							
XX 01 01 02 (delegácie)							
XX 01 05 01 (nepriamy výskum)							
10 01 05 01 (priamy výskum)							
• Externí zamestnanci (ekvivalent plného pracovného času) ⁶⁷							

⁶⁶

Rok N je rok, v ktorom sa návrh/iniciatíva začína uskutočňovať. Nahrad'te „N“ očakávaným prvým rokom vykonávania (napríklad: 2021). To isté urobte aj pri nasledujúcich rokoch.

XX 01 02 01 (ZZ, VNE, DAZ z celkového balíka prostriedkov)							
XX 01 02 02 (ZZ, MZ, VNE, DAZ, PED v delegáciách)							
XX 01 04 yy ⁶⁸	– ústredie ⁶⁹						
	– delegácie						
XX 01 05 02 (ZZ, VNE, DAZ – nepriamy výskum)							
10 01 05 02 (ZZ, VNE, DAZ – priamy výskum)							
Iné rozpočtové riadky (uved'te)							
SPOLU							

XX predstavuje príslušnú oblasť politiky alebo rozpočtovú hlavu.

Potreby ľudských zdrojov budú pokryté úradníkmi GR, ktorí už boli pridelení na riadenie akcie a/alebo boli interne prerozdelení v rámci GR, a v prípade potreby budú doplnené zdrojmi, ktoré sa môžu pridelit' riadiacemu GR v rámci ročného postupu prideľovania zdrojov v závislosti od rozpočtových obmedzení.

Opis úloh, ktoré sa majú vykonať:

Úradníci a dočasní zamestnanci	
Externí zamestnanci	

Opis výpočtu nákladov na ekvivalent plného pracovného času by mal byť uvedený v oddiele 3 prílohy V.

⁶⁷ ZZ = zmluvný zamestnanec; MZ = miestny zamestnanec; VNE = vyslaný národný expert; DAZ = dočasný agentúrny zamestnanec; PED = pomocný expert v delegácii.

⁶⁸ Čiastkový strop pre externých zamestnancov financovaných z operačných rozpočtových prostriedkov (pôvodné rozpočtové riadky „BA“).

⁶⁹ Najmä pre štrukturálne fondy, Európsky poľnohospodársky fond pre rozvoj vidieka (EPFRV) a Európsky fond pre rybné hospodárstvo (EFRH).

3.2.4. Súlad s platným viacročným finančným rámcom

- ☒ Návrh/iniciatíva je v súlade s platným viacročným finančným rámcom.
- ☐ Návrh/iniciatíva si vyžaduje zmenu v plánovaní príslušného okruhu vo viacročnom finančnom rámci.

Vysvetlite požadovanú zmenu v plánovaní a uveďte príslušné rozpočtové riadky a zodpovedajúce sumy.

Návrh je zlučiteľný s VFR 2021 – 2027.

Vyrovnanie rozpočtu požadovaného na pokrytie navýšenia ľudských zdrojov v agentúre ENISA sa uskutoční znížením rovnakej sumy z rozpočtu pre program Digitálna Európa v rámci rovnakého okruhu.

- ☐ Návrh/iniciatíva si vyžaduje, aby sa použil nástroj flexibility alebo aby sa uskutočnila revízia viacročného finančného rámca⁷⁰.

Vysvetlite potrebu a uveďte príslušné okruhy, rozpočtové riadky a zodpovedajúce sumy.

3.2.5. Príspevky od tretích strán

- Návrh/iniciatíva nezahŕňa spolufinancovanie tretími stranami.
- Návrh/iniciatíva zahŕňa spolufinancovanie tretími stranami, ako je odhadnuté v nasledujúcej tabuľke:

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

	Rok N	Rok N + 1	Rok N + 2	Rok N + 3	Uveďte všetky roky, počas ktorých vplyv trvá (pozri bod 1.6)			Spolu
Uveďte spolufinancujúci subjekt								
Prostriedky zo spolufinancovania SPOLU								

⁷⁰

Pozri články 11 a 17 nariadenia Rady (EÚ, Euratom) č. 1311/2013, ktorým sa ustanovuje viacročný finančný rámec na roky 2014 – 2020.

3.3. Odhadovaný vplyv na príjmy

- ☐ Návrh/iniciatíva nemá finančný vplyv na príjmy.
- ☐ Návrh/iniciatíva má finančný vplyv na príjmy, ako je uvedené v nasledujúcej tabuľke:
 - ☐ vplyv na vlastné zdroje
 - ☐ vplyv na iné príjmy
 - ☐ uveďte, či sú príjmy pripísané rozpočtovým riadkom výdavkov

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

Rozpočtový príjmov:	riadok	Rozpočtové prostriedky k dispozícii v prebiehajúc om rozpočtovom roku	Vplyv návrhu/iniciatívy ⁷¹						
			Rok N	Rok N + 1	Rok N + 2	Rok N + 3	Uveďte všetky roky, počas ktorých vplyv trvá (pozri bod 1.6)		
Článok									

V prípade rôznych pripísaných príjmov uveďte príslušné rozpočtové riadky výdavkov.

--

Uveďte spôsob výpočtu vplyvu na príjmy.

--

⁷¹

Pokiaľ ide o tradičné vlastné zdroje (clá, odvody z produkcie cukru), uvedené sumy musia predstavovať čisté sumy, t. j. hrubé sumy po odčítaní 20 % na náklady na výber.