Rada
Európskej únie

V Bruseli 20. apríla 2023
(OR. en)

8512/23

Medziinštitucionálny spis:
2023/0109(COD)

CYBER 92
TELECOM 108
CADREFIN 51
FIN 448
BUDGET 6
IND 181
JAI 471
MI 314
DATAPROTECT 110
RELEX 481
CODEC 662

NÁVRH

Od:	Martine DEPREZOVÁ, riaditeľka, v zastúpení generálnej tajomníčky Európskej komisie
Dátum doručenia:	19. apríla 2023
Komu:	Thérèse BLANCHETOVÁ, generálna tajomníčka Rady Európskej únie
Č. dok. Kom.:	COM(2023) 209 final
Predmet:	Návrh NARIADENIA EURÓPSKEHO PARLAMENTU A RADY, ktorým sa stanovujú opatrenia na posilnenie solidarity a kapacít v Únii na odhaľovanie kybernetických hrozieb a incidentov, prípravu a reakciu na ne

Delegáciám v prílohe zasielame dokument COM(2023) 209 final.

Príloha: COM(2023) 209 final

EURÓPSKA
KOMISIA

V Štrasburgu 18. 4. 2023
COM(2023) 209 final

2023/0109 (COD)

Návrh

NARIADENIE EURÓPSKEHO PARLAMENTU A RADY,

ktorým sa stanovujú opatrenia na posilnenie solidarity a kapacít v Únii na odhaľovanie kybernetických hrozieb a incidentov, prípravu a reakciu na ne

DÔVODOVÁ SPRÁVA

1. KONTEXT NÁVRHU

• Dôvody a ciele návrhu

Táto dôvodová správa dopĺňa návrh aktu o kybernetickej solidarite. So zvyšovaním miery prepojenia a vzájomnej závislosti našich verejných správ, podnikov, ako aj občanov bez ohľadu na hranice a odvetvia hospodárstva stúpa význam používania informačných a komunikačných technológií a závislosti od nich vo všetkých odvetviach hospodárskej činnosti. Zvýšená miera zavádzania digitálnych technológií zvyšuje riziko kybernetických bezpečnostných incidentov a ich možných vplyvov. Členské štáty zároveň čelia čoraz väčším kybernetickobezpečnostným rizikám a celkovo komplexnému prostrediu hrozieb s jasným rizikom rýchleho presahu kybernetických incidentov z jedného členského štátu do iných členských štátov.

Kybernetické operácie sa okrem toho čoraz väčšmi stávajú súčasťou hybridných stratégií a stratégií vedenia vojny s významným dosahom na cieľ. Ruskej vojenskej agresii voči Ukrajine konkrétne predchádzala stratégia nepriateľských kybernetických operácií, ktoré pokračujú aj počas samotnej agresie, čo podstatne zmenilo vnímanie a hodnotenie spoločnej pripravenosti EÚ v oblasti riadenia kybernetických kríz a spôsobilo volanie po prijatí naliehavých opatrení. Hrozba možného rozsiahleho incidentu, ktorým by sa významne narušili a poškodili kritické infraštruktúry, si vyžaduje vyššiu mieru pripravenosti na všetkých úrovniach ekosystému kybernetickej bezpečnosti v EÚ. Táto hrozba nevyplýva len z ruskej vojenskej agresie voči Ukrajine a zahŕňa nepretržité kybernetické hrozby zo strany štátnych a neštátnych subjektov, ktoré vzhľadom na veľký počet kriminálnych a haktivistických aktérov napojených na štát, ktorí sa podieľajú na aktuálnom geopolitickom napätí, môžu pretrvávať. Počet kybernetických útokov sa za posledné roky dramaticky zvýšil, pričom išlo aj o útoky na dodávateľský reťazec zamerané na kybernetickú špionáž, ransomware alebo narušenie. Útok na dodávateľský reťazec spoločnosti SolarWinds v roku 2020 zasiahol viac ako 18 000 organizácií na celom svete vrátane vládnych agentúr a veľkých spoločností. Rozvratný účinok významných kybernetických incidentov môže byť príliš silný na to, aby ich dokázal samostatne zvládnuť jeden alebo viacero zasiahnutých členských štátov. Z tohto dôvodu je potrebné posilniť solidaritu na úrovni Únie, aby bolo možné zlepšiť odhaľovanie kybernetických hrozieb a incidentov, prípravu a reakciu na ne.

V súvislosti s odhaľovaním kybernetických hrozieb a incidentov je naliehavo potrebné posilniť výmenu informácií a zlepšiť naše kolektívne kapacity s cieľom radikálne skrátiť čas potrebný na odhalenie kybernetických hrozieb skôr, ako môžu spôsobiť rozsiahle škody a vysoké náklady[1]. Veľa kybernetických hrozieb a incidentov má z dôvodu prepojenosti

[1] Podľa správy spoločností Ponemon Institute a IBM Security trvala identifikácia narušenia v roku 2022 v priemere 207 dní a ďalších 70 dní trvalo, kým sa zabránilo jeho šíreniu. Priemerné náklady súvisiace s porušením ochrany údajov so životnosťou vyše 200 dní zároveň v roku 2022 predstavovali 4,86 milióna EUR v porovnaní s nákladmi na úrovni 3,74 milióna EUR v prípade porušení, ktoré trvali menej ako 200 dní. [*Cost of a data breach 2022* (Náklady porušenia ochrany údajov v roku 2022), https://www.ibm.com/reports/data-breach].

digitálnych infraštruktúr potenciálne cezhraničný rozmer, výmena relevantných informácií medzi členskými štátmi je však naďalej obmedzená. Vybudovanie siete cezhraničných centier bezpečnostných operácií na zlepšenie spôsobilostí týkajúcich sa odhaľovania a reakcie má za cieľ pomôcť pri riešení tohto problému.

Pokiaľ ide o pripravenosť a reakciu na kybernetické incidenty, v súčasnosti existuje len nízka miera podpory na úrovni Únie a solidarity medzi členskými štátmi. Rada vo svojich záveroch z októbra 2021 poukázala na potrebu riešiť tieto nedostatky, pričom vyzvala Komisiu, aby predložila návrh nového Fondu pre reakcie na núdzové situácie v oblasti kybernetickej bezpečnosti[2].

Týmto nariadením sa takisto vykonáva stratégia kybernetickej bezpečnosti EÚ prijatá v decembri 2020[3], ktorou sa oznámilo vytvorenie európskeho kybernetického štítu, ktorým sa posilňujú spôsobilosti Európskej únie týkajúce sa odhaľovania kybernetických hrozieb a výmeny informácií o nich prostredníctvom združenia vnútroštátnych a cezhraničných centier bezpečnostných operácií.

Toto nariadenie vychádza z prvých krokov, ktoré sa už spravili v úzkej spolupráci s hlavnými zainteresovanými stranami a ktoré boli podporené v rámci programu Digitálna Európa. Konkrétne v prípade centier bezpečnostných operácií sa v rámci pracovného programu pre kybernetickú bezpečnosť programu Digitálna Európa na roky 2021 – 2022 uskutočnila výzva na vyjadrenie záujmu na spoločné obstarávanie nástrojov a infraštruktúry na zriadenie cezhraničných centier bezpečnostných operácií a výzva na granty s cieľom umožniť budovanie kapacít centier bezpečnostných operácií slúžiacich verejným a súkromným organizáciám. Pokiaľ ide o pripravenosť a reakciu na incidenty, Komisia pripravila krátkodobý program na podporu členských štátov prostredníctvom dodatočného financovania prideleného Agentúre Európskej únie pre kybernetickú bezpečnosť (ENISA) s cieľom okamžite zvýšiť pripravenosť na závažné kybernetické incidenty a posilniť kapacity reakcie na ne. Obidve opatrenia sa pripravujú v úzkej koordinácii s členskými štátmi. Týmto nariadením sa odstraňujú nedostatky a začleňujú sa poznatky získané z týchto opatrení.

V neposlednom rade sa týmto návrhom plní záväzok v súlade so spoločným oznámením o kybernetickej obrane[4] prijatým 10. novembra, ktorým je vypracovanie návrhu iniciatívy EÚ v oblasti kybernetickej solidarity s týmito cieľmi: posilniť spoločné spôsobilosti EÚ týkajúce sa odhaľovania, situačnej informovanosti a reakcie, postupne vybudovať kybernetické rezervy na úrovni EÚ so službami od dôveryhodných súkromných poskytovateľov a podporovať testovanie kritických subjektov.

---

2 Závery Rady o vývoji prístupu Európskej únie ku kybernetickej bezpečnosti, ktoré Rada schválila na zasadnutí 23. mája 2022 (9364/22).

3 Spoločné oznámenie Európskemu parlamentu a Rade, Stratégia kybernetickej bezpečnosti EÚ v digitálnej dekáde [JOIN(2020) 18 final].

4 Spoločné oznámenie Európskemu parlamentu a Rade, Politika EÚ v oblasti kybernetickej obrany [JOIN(2022) 49 final].

V tejto súvislosti Komisia predkladá tento akt o kybernetickej solidarite s cieľom posilniť solidaritu na úrovni Únie, aby bolo možné lepšie odhaľovať kybernetické hrozby a incidenty, pripraviť sa a reagovať na ne, a to prostredníctvom týchto špecifických cieľov:

- posilniť spoločné odhaľovanie kybernetických hrozieb a incidentov a situačnú informovanosť o nich v EÚ, a tak prispievať k európskej technologickej suverenite v oblasti kybernetickej bezpečnosti,
- posilniť pripravenosť kritických subjektov z celej EÚ a posilniť solidaritu rozvíjaním kapacít spoločnej reakcie na významné alebo rozsiahle kybernetické incidenty, a to aj sprístupnením podpory reakcie na incidenty tretím krajinám pridruženým k programu Digitálna Európa,
- zvýšiť odolnosť Únie a prispieť k účinnej reakcii prostredníctvom skúmania a posudzovania významných alebo rozsiahlych incidentov vrátane získavania poznatkov a prípadne odporúčaní.

Tieto ciele sa vykonávajú prostredníctvom týchto opatrení:

- zavedenie celoeurópskej infraštruktúry centier bezpečnostných operácií (európsky kybernetický štít) s cieľom vybudovať a posilniť spoločné spôsobilosti týkajúce sa odhaľovania a situačnej informovanosti,
- vytvorenie mechanizmu na riešenie kybernetických núdzových situácií s cieľom podporiť členské štáty pri príprave na významné a rozsiahle kybernetické incidenty, pri reakcii na ne a pri okamžitom zotavení sa z nich. Podpora pri reakcii na incidenty sa sprístupní aj európskym inštitúciám, orgánom, úradom a agentúram Únie,
- vytvorenie európskeho mechanizmu preskúmania kybernetických incidentov, ktorý bude slúžiť na skúmanie a posudzovanie konkrétnych významných alebo rozsiahlych incidentov.

Finančná podpora európskeho kybernetického štítu a mechanizmu na riešenie kybernetických núdzových situácií bude pochádzať z programu Digitálna Európa, ktorý sa týmto legislatívnym nástrojom zmení s cieľom vytvoriť uvedené opatrenia, zabezpečiť finančnú podporu na ich rozvoj a objasniť podmienky na jej čerpanie.

• Súlad s existujúcimi ustanoveniami v tejto oblasti politiky

Rámec EÚ tvorí niekoľko právnych predpisov, ktoré už na úrovni Únie existujú alebo sa navrhujú, týkajúcich sa obmedzenia zraniteľností, zvýšenia odolnosti kritických subjektov voči kybernetickobezpečnostným rizikám a podpory koordinovaného zvládania rozsiahlych kybernetických incidentov a kríz, predovšetkým smernica o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sieťových a informačných systémov v Únii (smernica NIS 2)[5], akt o kybernetickej bezpečnosti[6], smernica o útokoch na informačné systémy[7],

[5] Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (smernica NIS 2).

odporúčanie Komisie (EÚ) 2017/1584 o koordinovanej reakcii na kybernetické incidenty a krízy veľkého rozsahu[8].

Opatrenia navrhované v rámci aktu o kybernetickej solidarite sa týkajú situačnej informovanosti, výmeny informácií, ako aj podpory pripravenosti na kybernetické incidenty a reakcií na ne. Tieto opatrenia sú v súlade s cieľmi regulačného rámca, ktorý existuje na úrovni Únie, predovšetkým s cieľmi podľa smernice (EÚ) 2022/2555 (ďalej len „smernica NIS 2“), a podporujú tieto ciele. Akt o kybernetickej solidarite bude vychádzať predovšetkým z existujúceho rámca operačnej spolupráce v oblasti kybernetickej bezpečnosti a rámca pre riadenie kybernetických kríz, najmä pokiaľ ide o Európsku sieť styčných organizácií pre kybernetické krízy (EU-CyCLONe) a sieť jednotiek pre riešenie počítačových bezpečnostných incidentov (jednotky CSIRT), a bude tieto rámce podporovať.

Platformy cezhraničných centier bezpečnostných operácií by mali predstavovať novú kapacitu, ktorá bude dopĺňať sieť jednotiek CSIRT tým, že budú zhromažďovať údaje o kybernetickobezpečnostných hrozbách od verejných a súkromných subjektov a zabezpečovať spoločné využívanie týchto údajov, zvyšovať ich hodnotu prostredníctvom odborných analýz a najmodernejších nástrojov a prispievať k rozvoju spôsobilostí a technologickej suverenity Únie.

Tento návrh je napokon v súlade s odporúčaním Rady o celoúnijnom koordinovanom prístupe k posilneniu odolnosti kritickej infraštruktúry[9], v ktorom sa členské štáty vyzývajú, aby bezodkladne prijali účinné opatrenia a aby v duchu solidarity zabezpečili lojálnu, účinnú a koordinovanú spoluprácu medzi sebou, s Komisiou a inými príslušnými verejnými orgánmi, ako aj dotknutými subjektmi, a zvýšili tak odolnosť kritickej infraštruktúry, ktorá sa využíva pri poskytovaní základných služieb na vnútornom trhu.

- **Súlad s ostatnými politikami Únie**

Návrh je v súlade s ostatnými mechanizmami a protokolmi riešenia krízových situácií, ako je mechanizmus integrovanej politickej reakcie na krízu. Akt o kybernetickej solidarite bude dopĺňať tieto rámce a protokoly krízového riadenia, a to poskytovaním osobitnej podpory pripravenosti na kybernetické incidenty a reakcií na ne. Návrh bude v súlade aj s vonkajšou činnosťou EÚ v oblasti reakcie na rozsiahle incidenty v rámci spoločnej zahraničnej

---

6 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).

7 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.

8 Návrh nariadenia Európskeho parlamentu a Rady o horizontálnych požiadavkách kybernetickej bezpečnosti pre produkty s digitálnymi prvkami a o zmene nariadenia (EÚ) 2019/1020 [COM(2022) 454 final].

9 Odporúčanie Rady z 8. decembra 2022 o celoúnijnom koordinovanom prístupe k posilneniu odolnosti kritickej infraštruktúry (Text s významom pre EHP), 2023/C 20/01.

a bezpečnostnej politiky (SZBP), a to aj prostredníctvom súboru nástrojov EÚ v oblasti kybernetickej diplomacie. Návrh bude dopĺňať opatrenia vykonávané v kontexte článku 42 ods. 7 Zmluvy o Európskej únii alebo v situáciách vymedzených v článku 222 Zmluvy o fungovaní Európskej únie.

Návrh takisto dopĺňa mechanizmus Únie v oblasti civilnej ochrany[10] zriadený v decembri 2013 a dokončený novým právnym predpisom prijatým v máji 2021[11], ktorým sa posilňuje prevencia, pripravenosť a reakcia ako piliere mechanizmu Únie v oblasti civilnej ochrany a vytvárajú dodatočné kapacity EÚ týkajúce sa reakcie na nové riziká v Európe a na svete a zvyšuje rezerva v systéme rescEU.

2. PRÁVNY ZÁKLAD, SUBSIDIARITA A PROPORCIONALITA

• Právny základ

Právnym základom tohto návrhu je článok 173 ods. 3 a článok 322 ods. 1 písm. a) Zmluvy o fungovaní Európskej únie (ZFEÚ). V článku 173 ZFEÚ sa stanovuje, že Únia a členské štáty zabezpečia podmienky potrebné na existenciu konkurencieschopnosti priemyslu Únie. Cieľom tohto nariadenia je posilnenie konkurenčnej pozície priemyslu a odvetvia služieb v Európe v rámci celého digitalizovaného hospodárstva a podpora ich digitálnej transformácie, a to posilnením úrovne kybernetickej bezpečnosti na digitálnom jednotnom trhu. Jeho cieľom je konkrétne zvýšenie odolnosti občanov, podnikov a subjektov pôsobiacich v kritických odvetviach a v odvetviach s vysokou úrovňou kritickosti voči čoraz väčším kybernetickobezpečnostným hrozbám, ktoré môžu mať zničujúce spoločenské a hospodárske dôsledky.

Návrh takisto vychádza z článku 322 ods. 1 písm. a) ZFEÚ, pretože obsahuje osobitné pravidlá prenosu, ktoré sa odchyľujú od zásady ročnej platnosti stanovenej v nariadení Európskeho parlamentu a Rady (EÚ, Euratom) 2018/1046 (ďalej len „nariadenie o rozpočtových pravidlách“)[12]. Na účely správneho finančného riadenia a berúc do úvahy nepredvídateľnú, výnimočnú a špecifickú povahu prostredia kybernetickej bezpečnosti a kybernetických hrozieb by mechanizmus na riešenie kybernetickobezpečnostných núdzových situácií mal mať určitú mieru pružnosti vo vzťahu k rozpočtovému riadeniu, a to najmä tým, že nevyužité viazané a platobné rozpočtové prostriedky určené na opatrenia zamerané na plnenie cieľov uvedených v nariadení by bolo možné automaticky preniesť do ďalšieho rozpočtového roka. Keďže v dôsledku tohto nového pravidla vzniknú problémy v súvislosti s nariadením o rozpočtových pravidlách, táto otázka by sa mohla riešiť v rámci súčasných rokovaní o prepracovaní nariadenia o rozpočtových pravidlách.

---

[10] Rozhodnutie Európskeho parlamentu a Rady č. 1313/2013/EÚ zo 17. decembra 2013 o mechanizme Únie v oblasti civilnej ochrany (Text s významom pre EHP).

[11] Nariadenie Európskeho parlamentu a Rady (EÚ) 2021/836 z 20. mája 2021, ktorým sa mení rozhodnutie č. 1313/2013/EÚ o mechanizme Únie v oblasti civilnej ochrany (Text s významom pre EHP).

[12] Nariadenie Európskeho parlamentu a Rady (EÚ, Euratom) 2018/1046 z 18. júla 2018 o rozpočtových pravidlách, ktoré sa vzťahujú na všeobecný rozpočet Únie (Ú. v. EÚ L 193, 30.7.2018, s. 1).

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

Z výrazného cezhraničného charakteru kybernetických hrozieb a rastúceho počtu rizík a incidentov s účinkami, ktoré presahujú hranice, odvetvia a produkty, vyplýva, že ciele tejto intervencie nemožno účinne dosiahnuť len na úrovni samotných členských štátov a že si vyžadujú spoločný postup a solidaritu na úrovni Únie.

Skúsenosti z boja proti kybernetickým hrozbám vyplývajúcim z vojny proti Ukrajine spoločne s poznatkami získanými z cvičenia v oblasti kybernetickej bezpečnosti, ktoré sa uskutočnilo v rámci francúzskeho predsedníctva (EU CyCLES), ukázali, že by sa mali vypracovať konkrétne mechanizmy vzájomnej podpory, najmä spolupráce so súkromným sektorom, aby sa dosiahla solidarita na úrovni EÚ. V tejto súvislosti sa v záveroch Rady z 23. mája 2022 o vývoji prístupu Európskej únie ku kybernetickej bezpečnosti Komisia vyzýva, aby predložila návrh nového Fondu pre reakcie na núdzové situácie v oblasti kybernetickej bezpečnosti.

Podpora a opatrenia na úrovni Únie na lepšie odhaľovanie kybernetickobezpečnostných hrozieb a na zvýšenie kapacít v oblasti pripravenosti a reakcie poskytujú pridanú hodnotu, pretože predchádzajú duplicite úsilia v Únii a členských štátoch. Viedli by k lepšiemu využívaniu existujúcich aktív a k väčšej koordinácii a výmene informácií o získaných poznatkoch. V rámci mechanizmu na riešenie kybernetických núdzových situácií sa takisto uvažuje o poskytovaní podpory z rezervy EÚ na účely kybernetickej bezpečnosti tretím krajinám pridruženým k programu Digitálna Európa.

Podpora poskytovaná prostredníctvom rôznych iniciatív, ktoré sa majú zriadiť a financovať na úrovni Únie, bude dopĺňať, ale nie zdvojovať vnútroštátne spôsobilosti týkajúce sa odhaľovania kybernetických hrozieb a incidentov, situačnej informovanosti o nich a pripravenosti a reakcie na ne.

- **Proporcionalita**

Opatrenia neprekračujú rámec toho, čo je nevyhnutné na dosiahnutie všeobecných a špecifických cieľov nariadenia. Opatrenia v tomto nariadení nemajú vplyv na povinnosti členských štátov týkajúce sa národnej a verejnej bezpečnosti, prevencie, vyšetrovania, odhaľovania a stíhania trestných činov. Nemajú vplyv ani na právne záväzky subjektov pôsobiacich v kritických odvetviach a v odvetviach s vysokou úrovňou kritickosti týkajúce sa prijímania kybernetickobezpečnostných opatrení v súlade so smernicou NIS 2.

Opatrenia uvedené v tomto nariadení dopĺňajú toto úsilie a opatrenia prostredníctvom podpory vytvárania infraštruktúr na lepšie odhaľovanie a analýzu hrozieb a prostredníctvom poskytovania podpory pre opatrenia v oblasti pripravenosti a reakcie v prípade významných alebo rozsiahlych incidentov.

- **Výber nástroja**

Návrh má formu nariadenia Európskeho parlamentu a Rady. Ide o najvhodnejší právny nástroj, keďže iba nariadenie so svojimi priamo uplatniteľnými právnymi ustanoveniami

môže poskytnúť nevyhnutný stupeň jednotnosti potrebný na zriadenie a prevádzkovanie európskeho kybernetického štítu a mechanizmu na riešenie kybernetických núdzových situácií zabezpečením podpory z programu Digitálna Európa na ich zriadenie, ako aj stanovením jasných podmienok využívania a prideľovania tejto podpory.

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

- **Konzultácie so zainteresovanými stranami**

Opatrenia stanovené v tomto nariadení sa podporia z programu Digitálna Európa, čo bolo predmetom rozsiahlych konzultácií. Ďalej budú vychádzať z prvých krokov, ktoré sa pripravovali v úzkej spolupráci s hlavnými zainteresovanými stranami. Čo sa týka centier bezpečnostných operácií, Komisia v úzkej spolupráci s členskými štátmi v rámci Európskeho centra priemyselných, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti (kompetenčné centrum) vypracovala koncepčný dokument o rozvoji platforiem cezhraničných centier bezpečnostných operácií a pripravila výzvu na vyjadrenie záujmu. V tejto súvislosti sa uskutočnil prieskum kapacít vnútroštátnych centier bezpečnostných operácií a v technickej pracovnej skupine kompetenčného centra, v ktorej sa stretli zástupcovia členských štátov, sa diskutovalo o spoločných prístupoch a technických požiadavkách. Okrem toho sa uskutočnila výmena názorov s príslušným odvetvím, predovšetkým prostredníctvom skupiny odborníkov pre centrá bezpečnostných operácií vytvorenej agentúrou ENISA a prostredníctvom Európskej organizácie kybernetickej bezpečnosti (ECSO).

Po druhé, pokiaľ ide o pripravenosť a reakciu na incidenty, Komisia pripravila krátkodobý program na podporu členských štátov prostredníctvom dodatočného financovania prideleného agentúre ENISA z programu Digitálna Európa s cieľom okamžite zvýšiť pripravenosť na závažné kybernetické incidenty a posilniť kapacity reakcie na ne. Spätná väzba členských štátov a príslušného odvetvia získaná počas vykonávania tohto krátkodobého programu už poskytuje cenné poznatky, ktoré sa používajú pri príprave navrhovaného nariadenia v záujme riešenia zistených nedostatkov. Toto bol prvý krok v súlade so závermi Rady o prístupe ku kybernetickej bezpečnosti, v ktorých sa Komisia vyzýva, aby predložila návrh nového Fondu pre reakcie na núdzové situácie v oblasti kybernetickej bezpečnosti.

Okrem toho sa 16. februára 2023 na základe diskusného dokumentu konal seminár s odborníkmi členských štátov týkajúci sa mechanizmu na riešenie kybernetických núdzových situácií. Na tomto seminári sa zúčastnili všetky členské štáty a jedenásť z nich písomne poskytlo ďalšie príspevky.

- **Posúdenie vplyvu**

Vzhľadom na naliehavý charakter návrhu nebolo vykonané žiadne posúdenie vplyvu. Opatrenia stanovené v tomto nariadení sa podporia z programu Digitálna Európa a sú v súlade

s opatreniami uvedenými v nariadení o programe Digitálna Európa, ktoré bolo predmetom osobitného posúdenia vplyvu. Toto nariadenie nebude mať žiadne významné administratívne alebo environmentálne vplyvy, ktoré by presahovali vplyvy, ktoré sa posúdili už v posúdení vplyvu k nariadeniu o programe Digitálna Európa.

Ďalej vychádza z prvých opatrení vypracovaných v úzkej spolupráci s hlavnými zainteresovanými stranami, ako sa uvádza v predchádzajúcom texte, a nadväzuje na výzvu členských štátov Komisii, aby do konca tretieho štvrťroku 2022 predložila návrh nového Fondu pre reakcie na núdzové situácie v oblasti kybernetickej bezpečnosti.

Konkrétne v súvislosti so situačnou informovanosťou a s odhaľovaním v rámci európskeho kybernetického štítu sa v rámci pracovného programu pre kybernetickú bezpečnosť programu Digitálna Európa na roky 2021 – 2022 uskutočnila výzva na vyjadrenie záujmu na spoločné obstarávanie nástrojov a infraštruktúry na zriadenie cezhraničných centier bezpečnostných operácií a výzva na granty s cieľom umožniť budovanie kapacít centier bezpečnostných operácií slúžiacich verejným a súkromným organizáciám.

Ako sa už uviedlo, v oblasti pripravenosti a reakcie na incidenty Komisia pripravila krátkodobý program na podporu členských štátov z programu Digitálna Európa, ktorý vykonáva agentúra ENISA. Služby, ktorých sa program týka, zahŕňajú opatrenia v oblasti pripravenosti, ako je penetračné testovanie kritických subjektov s cieľom identifikovať zraniteľnosti. Posilňujú sa aj možnosti pomoci členským štátom v prípade závažného incidentu s vplyvom na kritické subjekty. Vykonávanie tohto krátkodobého programu agentúrou ENISA v súčasnosti prebieha a už poskytlo významné poznatky, ktoré sa zohľadnili pri vypracúvaní tohto nariadenia.

- **Základné práva**

Tým, že tento návrh prispieva k bezpečnosti digitálnych informácií, prispeje k ochrane práva na slobodu a bezpečnosť v súlade s článkom 6 Charty základných práv Európskej únie a práva na rešpektovanie súkromného a rodinného života v súlade s článkom 7 Charty základných práv Európskej únie. Ochranou podnikov pred kybernetickými útokmi spôsobujúcimi ekonomické škody návrh prispieva aj k slobode podnikania v súlade s článkom 16 Charty základných práv Európskej únie a k právu vlastniť majetok v súlade s článkom 17 Charty základných práv Európskej únie. Ochranou integrity kritickej infraštruktúry proti kybernetickým útokom návrh napokon prispeje k právu na zdravotnú starostlivosť v súlade s článkom 35 Charty základných práv Európskej únie a k právu na prístup k službám všeobecného hospodárskeho záujmu v súlade s článkom 36 Charty základných práv Európskej únie.

4. VPLYV NA ROZPOČET

Opatrenia tohto nariadenia sa podporia finančnými prostriedkami strategického cieľa Kybernetická bezpečnosť programu Digitálna Európa.

Celkový rozpočet obsahuje zvýšenie o 100 miliónov EUR, ktoré sa podľa návrhu v tomto nariadení majú prerozdeliť z iných strategických cieľov programu Digitálna Európa. Tým sa nová celková suma dostupná na opatrenia v oblasti kybernetickej bezpečnosti v rámci programu Digitálna Európa zvýši na 842,8 milióna EUR.

Časťou dodatočnej sumy 100 miliónov EUR sa podporí rozpočet spravovaný kompetenčným centrom na vykonávanie opatrení týkajúcich sa centier bezpečnostných operácií a pripravenosti v rámci ich pracovného(-ých) programu(-ov). Dodatočné finančné prostriedky okrem toho poslúžia na podporu vytvorenia rezervy EÚ na účely kybernetickej bezpečnosti.

Tieto prostriedky dopĺňajú rozpočet, ktorý už bol stanovený na podobné opatrenia v rámci pracovného programu hlavného programu Digitálna Európa a cieľa Kybernetická bezpečnosť programu Digitálna Európa na roky 2023 – 2027, čím by sa celková suma na roky 2023 – 2027 mohla zvýšiť na 551 miliónov EUR, pričom 115 miliónov EUR už bolo vyčlenených vo forme pilotných projektov na roky 2021 – 2022. Spoločne s príspevkami členských štátov by celkový rozpočet mohol dosiahnuť až 1,109 miliardy EUR.

Prehľad súvisiacich nákladov je uvedený v legislatívnom finančnom výkaze, ktorý je pripojený k tomuto návrhu.

5. ĎALŠIE PRVKY

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

Komisia bude monitorovať vykonávanie a uplatňovanie týchto nových ustanovení, ako aj dosahovanie súladu s nimi na účely posúdenia ich účinnosti. Komisia do štyroch rokov od dátumu uplatňovania tohto nariadenia predloží Európskemu parlamentu a Rade správu o jeho hodnotení a preskúmaní.

- **Podrobné vysvetlenie konkrétnych ustanovení návrhu**

Všeobecné ciele, predmet úpravy a vymedzenie pojmov (kapitola I)

V kapitole I sa uvádzajú ciele nariadenia, ktorými je posilnenie solidarity na úrovni Únie, aby bolo možné lepšie odhaľovať kybernetické hrozby a incidenty, pripraviť sa a reagovať na ne, a najmä posilnenie spoločného odhaľovania kybernetických hrozieb a incidentov a situačnej informovanosti o nich v Únii, posilnenie pripravenosti subjektov pôsobiacich v kritických odvetviach a v odvetviach s vysokou úrovňou kritickosti z celej Únie a posilnenie solidarity rozvíjaním kapacít spoločnej reakcie na významné alebo rozsiahle kybernetické incidenty a zvýšenie odolnosti Únie prostredníctvom skúmania a posudzovania významných alebo rozsiahlych incidentov. V tejto kapitole sa takisto uvádzajú opatrenia na dosiahnutie týchto cieľov: zavedenie európskeho kybernetického štítu, vytvorenie mechanizmu na riešenie kybernetických núdzových situácií a zriadenie mechanizmu preskúmania kybernetických incidentov. V tejto kapitole sa vymedzujú aj pojmy, ktoré sa používajú v celom nástroji.

Európsky kybernetický štít (kapitola II)

Kapitolou II sa zriaďuje európsky kybernetický štít a uvádzajú sa jeho rôzne prvky a podmienky účasti. Po prvé sa v tejto kapitole uvádza celkový cieľ európskeho kybernetického štítu, ktorým je rozvíjať vyspelé spôsobilosti Únie týkajúce sa odhaľovania, analýzy a spracovania údajov o kybernetických hrozbách a incidentoch v Únii, ako aj špecifické operačné ciele. Stanovuje sa v nej, že financovanie z prostriedkov Únie určené na európsky kybernetický štít sa bude realizovať v súlade s nariadením o programe Digitálna Európa.

V kapitole sa ďalej opisuje druh subjektov, ktoré tvoria európsky kybernetický štít. Štít tvoria vnútroštátne centrá bezpečnostných operácií a cezhraničné centrá bezpečnostných operácií. Každý zúčastnený členský štát určí vnútroštátne centrum bezpečnostných operácií. Centrum funguje ako referenčné miesto a brána pre ostatné verejné a súkromné organizácie na vnútroštátnej úrovni na zber a analýzu informácií o kybernetických hrozbách a incidentoch, pričom má pomáhať cezhraničnému centru bezpečnostných operácií. Kompetenčné centrum môže na základe výzvy na vyjadrenie záujmu vybrať vnútroštátne centrum bezpečnostných operácií, aby sa spolu s kompetenčným centrom podieľalo na spoločnom obstarávaní nástrojov a infraštruktúr a aby získalo grant na ich prevádzku. Ak vnútroštátne centrum bezpečnostných operácií dostáva podporu z Únie, musí sa zaviazať, že do dvoch rokov požiada o účasť na cezhraničnom centre bezpečnostných operácií.

Cezhraničné centrá bezpečnostných operácií tvorí konzorcium aspoň troch členských štátov zastupovaných vnútroštátnymi centrami bezpečnostných operácií, ktoré sa zaviazali, že budú spolupracovať s cieľom koordinovať svoje činnosti v oblasti odhaľovania a monitorovania kybernetických hrozieb. Kompetenčné centrum môže na základe počiatočnej výzvy na vyjadrenie záujmu vybrať hostiteľské konzorcium, aby sa spolu s kompetenčným centrom podieľalo na spoločnom obstarávaní nástrojov a infraštruktúr a aby získalo grant na ich prevádzku. Členovia hostiteľského konzorcia uzatvárajú písomnú dohodu o konzorciu, v ktorej sa stanovujú jeho vnútorné mechanizmy. V tejto kapitole sa následne podrobne opisujú požiadavky na výmenu informácií medzi účastníkmi v cezhraničných centrách bezpečnostných operácií a na výmenu informácií medzi cezhraničným centrom bezpečnostných operácií a ostatnými cezhraničnými centrami bezpečnostných operácií, ako aj s príslušnými subjektmi EÚ. Vnútroštátne centrá bezpečnostných operácií, ktoré sú členmi cezhraničného centra bezpečnostných operácií, si navzájom vymieňajú príslušné informácie súvisiace s kybernetickými hrozbami a podrobnosti vrátane záväzku zabezpečiť výmenu značného objemu údajov a podmienok tejto výmeny údajov by sa mali vymedziť v dohode o konzorciu. Cezhraničné centrá bezpečnostných operácií zabezpečujú vysokú úroveň vzájomnej interoperability. Cezhraničné centrá bezpečnostných operácií by takisto mali uzatvoriť dohody o spolupráci s inými cezhraničnými centrami bezpečnostných operácií a v týchto dohodách by mali stanoviť zásady výmeny informácií. Ak cezhraničné centrá bezpečnostných operácií získajú informácie týkajúce sa potenciálneho alebo prebiehajúceho rozsiahleho kybernetického incidentu, poskytnú relevantné informácie sieti EU-CyCLONe, sieti jednotiek CSIRT a Komisii s ohľadom na ich príslušné úlohy v oblasti krízového riadenia v súlade so smernicou (EÚ) 2022/2555. Na konci kapitoly II sa uvádzajú bezpečnostné podmienky účasti na európskom kybernetickom štíte.

Mechanizmus na riešenie kybernetickobezpečnostných núdzových situácií (kapitola III)

Kapitolou III sa zriaďuje mechanizmus na riešenie kybernetických núdzových situácií s cieľom zvýšiť odolnosť Únie voči závažným kybernetickým hrozbám a pripraviť sa na krátkodobý vplyv významných a rozsiahlych kybernetických incidentov alebo kríz a v duchu solidarity ho zmierňovať. Opatrenia na vykonávanie mechanizmu na riešenie kybernetických núdzových situácií sa podporujú finančnými prostriedkami z programu Digitálna Európa. Mechanizmus umožňuje opatrenia na podporu pripravenosti na významné alebo rozsiahle kybernetické incidenty vrátane koordinovaného testovania subjektov pôsobiacich v odvetviach s vysokou úrovňou kritickosti, na reakciu na tieto incidenty a okamžité zotavenie sa z nich alebo na zmierňovanie významných kybernetických hrozieb, ako aj opatrenia vzájomnej pomoci.

Medzi opatrenia mechanizmu na riešenie kybernetických núdzových situácií v oblasti pripravenosti patrí koordinované testovanie subjektov pôsobiacich v odvetviach s vysokou úrovňou kritickosti z hľadiska pripravenosti. Komisia by po konzultáciách s agentúrou ENISA a so skupinou pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti mala pravidelne určovať relevantné odvetvia alebo pododvetvia z odvetví s vysokou úrovňou kritickosti uvedených v prílohe I k smernici (EÚ) 2022/2555, ktorých subjekty môžu byť predmetom koordinovaného testovania pripravenosti na úrovni EÚ.

Na účely vykonávania navrhovaných opatrení reakcie na incidenty sa v tomto nariadení stanovuje rezerva EÚ na účely kybernetickej bezpečnosti, ktorú tvoria služby reakcie na incidenty poskytované dôveryhodnými poskytovateľmi vybraté v súlade s kritériami stanovenými v tomto nariadení. Medzi používateľov služieb rezervy EÚ na účely kybernetickej bezpečnosti patria orgány pre riadenie kybernetických kríz a jednotky CSIRT členských štátov a inštitúcie, orgány a agentúry Únie. Celkovú zodpovednosť za vykonávanie rezervy EÚ na účely kybernetickej bezpečnosti má Komisia, ktorá môže prevádzkou a správou rezervy EÚ na účely kybernetickej bezpečnosti v plnom rozsahu alebo čiastočne poveriť agentúru ENISA.

Na získanie podpory z rezervy EÚ na účely kybernetickej bezpečnosti by používatelia mali prijať vlastné opatrenia na zmiernenie účinkov incidentu, v prípade ktorého sa požaduje podpora. Žiadosti o podporu z rezervy EÚ na účely kybernetickej bezpečnosti by mali zahŕňať nevyhnutné relevantné informácie o incidente a opatreniach, ktoré už používatelia prijali. Kapitola obsahuje aj opis spôsobov vykonávania vrátane posudzovania žiadostí o podporu z rezervy EÚ na účely kybernetickej bezpečnosti.

V nariadení sa stanovujú aj zásady obstarávania a podmienky účasti týkajúce sa dôveryhodných poskytovateľov rezervy EÚ na účely kybernetickej bezpečnosti.

Tretie krajiny môžu požiadať o podporu z rezervy EÚ na účely kybernetickej bezpečnosti, ak sa to umožňuje v dohodách o pridružení uzatvorených v súvislosti s účasťou týchto krajín na programe Digitálna Európa. V tejto kapitole sa opisujú ďalšie podmienky a spôsoby takejto účasti.

Mechanizmus preskúmania kybernetických incidentov (kapitola IV)

Na žiadosť Komisie, siete EU-CyCLONe alebo siete jednotiek CSIRT by agentúra ENISA mala preskúmať a posúdiť hrozby, zraniteľnosti a zmierňujúce opatrenia s ohľadom na konkrétny významný alebo rozsiahly kybernetický incident. Výsledky preskúmania a posúdenia vo forme správy o preskúmaní incidentu by agentúra ENISA mala predložiť sieti jednotiek CSIRT, sieti EU-CyCLONe a Komisii s cieľom podporiť ich pri plnení si úloh. Ak incident súvisí s treťou krajinou, Komisia by správu mala poskytnúť vysokému predstaviteľovi. Správa by mala obsahovať získané poznatky a v prípade potreby odporúčania na zlepšenie prístupu Únie ku kybernetickej bezpečnosti.

Záverečné ustanovenia (kapitola V)

Kapitola V obsahuje zmeny nariadenia o programe Digitálna Európa a stanovuje sa v nej povinnosť Komisie pripravovať pre Európsky parlament a Radu pravidelné správy na hodnotenie a preskúmanie nariadenia. Komisia sa splnomocňuje prijímať vykonávacie akty v súlade s postupom preskúmania uvedeným v článku 21 s cieľom: spresniť podmienky interoperability medzi cezhraničnými centrami bezpečnostných operácií; určiť procesné opatrenia na výmenu informácií medzi cezhraničnými centrami bezpečnostných operácií a subjektmi Únie v súvislosti s potenciálnym alebo prebiehajúcim rozsiahlym kybernetickým incidentom; stanoviť technické požiadavky na zabezpečenie vysokej úrovne bezpečnosti údajov a fyzickej bezpečnosti infraštruktúry a na ochranu bezpečnostných záujmov Únie pri výmene informácií so subjektmi, ktoré nie sú verejnými subjektmi členských štátov; spresniť druhy a počet služieb reakcie potrebných pre rezervu EÚ na účely kybernetickej bezpečnosti a ďalej spresniť podrobné pravidlá prideľovania podporných služieb rezervy EÚ na účely kybernetickej bezpečnosti.

2023/0109 (COD)

Návrh

NARIADENIE EURÓPSKEHO PARLAMENTU A RADY,

ktorým sa stanovujú opatrenia na posilnenie solidarity a kapacít v Únii na odhaľovanie kybernetických hrozieb a incidentov, prípravu a reakciu na ne

EURÓPSKY PARLAMENT A RADA EURÓPSKEJ ÚNIE,

so zreteľom na Zmluvu o fungovaní Európskej únie, a najmä na jej článok 173 ods. 3 a článok 322 ods. 1 písm. a),

so zreteľom na návrh Európskej komisie,

po postúpení návrhu legislatívneho aktu národným parlamentom,

so zreteľom na stanovisko Dvora audítorov[1],

so zreteľom na stanovisko Európskeho hospodárskeho a sociálneho výboru[2],

so zreteľom na stanovisko Výboru regiónov[3],

konajúc v súlade s riadnym legislatívnym postupom,

keďže:

(1) So zvyšovaním miery prepojenia a vzájomnej závislosti našich verejných správ, podnikov, ako aj občanov bez ohľadu na hranice a odvetvia hospodárstva stúpa význam používania informačných a komunikačných technológií a závislosti od nich vo všetkých odvetviach hospodárskej činnosti.

(2) Rozsah, frekvencia a dosah kybernetických incidentov sa zvyšujú, pričom ide aj útoky na dodávateľský reťazec zamerané na kybernetickú špionáž, ransomware alebo narušenie. Tieto incidenty predstavujú závažnú hrozbu pre fungovanie sietí a informačných systémov. Hrozba možných rozsiahlych incidentov, ktoré by mohli významne narušiť alebo poškodiť kritické infraštruktúry, si vzhľadom na rýchly vývoj situácie v oblasti hrozieb vyžaduje vyššiu mieru pripravenosti na všetkých úrovniach rámca kybernetickej bezpečnosti v Únii. Táto hrozba nevyplýva len z ruskej vojenskej agresie voči Ukrajine a vzhľadom na veľký počet kriminálnych a haktivistických aktérov napojených na štát, ktorí sa podieľajú na aktuálnom geopolitickom napätí, môže pretrvávať. Takéto incidenty môžu zabraňovať poskytovaniu verejných služieb a realizácii hospodárskych činností, a to aj v kritických odvetviach alebo v odvetviach s vysokou úrovňou kritickosti, spôsobovať značné finančné straty, narúšať dôveru používateľa, spôsobovať značné škody hospodárstvu Únie a dokonca by mohli mať zdravie alebo život ohrozujúce dôsledky. Kybernetické incidenty sú navyše nepredvídateľné, keďže často vznikajú a vyvíjajú sa vo veľmi krátkom časovom intervale, nie sú obmedzené na konkrétnu geografickú oblasť a vyskytujú sa súčasne v mnohých krajinách alebo sa v nich ihneď rozširujú.

---

1 Ú. v. EÚ C […], […], s. […].
2 Ú. v. EÚ C , , s. .
3 Ú. v. EÚ C , , s. .

(3) Je nevyhnutné posilniť konkurenčnú pozíciu odvetví priemyslu a služieb v Únii v rámci celého digitalizovaného hospodárstva a podporiť ich digitálnu transformáciu, a to posilnením úrovne kybernetickej bezpečnosti na digitálnom jednotnom trhu. Podľa odporúčaní v troch rôznych návrhoch Konferencie o budúcnosti Európy[4] je nevyhnutné zvýšiť odolnosť občanov, podnikov a subjektov pôsobiacich v kritických infraštruktúrach voči čoraz väčším kybernetickým hrozbám, ktoré môžu mať zničujúce spoločenské a hospodárske dôsledky. Sú preto potrebné investície do infraštruktúr a služieb, ktorými sa podporí rýchlejšie odhaľovanie kybernetických hrozieb a incidentov a reakcia na ne, a členské štáty potrebujú pomoc, aby sa mohli lepšie pripraviť na významné a rozsiahle kybernetické incidenty a aby na ne mohli lepšie reagovať. Únia by takisto mala zvýšiť svoje kapacity v týchto oblastiach, predovšetkým v súvislosti so zberom a analýzou údajov o kybernetických hrozbách a incidentoch.

(4) Únia už prijala niekoľko opatrení na zníženie zraniteľnosti a zvýšenie odolnosti kritických infraštruktúr a subjektov voči kybernetickobezpečnostným rizikám, najmä smernicu Európskeho parlamentu a Rady (EÚ) 2022/2555[5], odporúčanie Komisie (EÚ) 2017/1584[6], smernicu Európskeho parlamentu a Rady 2013/40/EÚ[7] a nariadenie Európskeho parlamentu a Rady (EÚ) 2019/881[8]. V odporúčaní Rady o celoúnijnom koordinovanom prístupe k posilneniu odolnosti kritickej infraštruktúry sa členské štáty navyše vyzývajú, aby bezodkladne prijali účinné opatrenia a aby v duchu solidarity zabezpečili lojálnu, účinnú a koordinovanú spoluprácu medzi sebou, s Komisiou a inými príslušnými verejnými orgánmi, ako aj dotknutými subjektmi, a zvýšili tak odolnosť kritickej infraštruktúry, ktorá sa využíva pri poskytovaní základných služieb na vnútornom trhu.

(5) Čoraz väčšie kybernetickobezpečnostné riziká a celkové prostredie komplexných hrozieb s jasným rizikom rýchleho presahu kybernetických incidentov z jedného členského štátu do iných členských štátov a z tretích krajín do Únie si v záujme lepšieho odhaľovania kybernetických hrozieb a incidentov, prípravy a reakcie na ne vyžadujú silnejšiu solidaritu na úrovni Únie. Členské štáty takisto v záveroch Rady o vývoji prístupu EÚ ku kybernetickej bezpečnosti vyzvali Komisiu, aby predložila návrh nového Fondu pre reakcie na núdzové situácie v oblasti kybernetickej bezpečnosti[9].

---

4 https://futureu.europa.eu/sk/.

5 Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (Ú. v. EÚ L 333, 27.12.2022, s. 80).

6 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).

7 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).

8 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).

9 Závery Rady o vývoji prístupu Európskej únie ku kybernetickej bezpečnosti, ktoré Rada schválila na zasadnutí 23. mája 2022 (9364/22).

(6) V spoločnom oznámení o politike EÚ v oblasti kybernetickej obrany[10] prijatom 10. novembra 2022 bola oznámená iniciatíva na podporu kybernetickej solidarity EÚ, ktorá má tieto ciele: posilniť spoločné spôsobilosti EÚ týkajúce sa odhaľovania, situačnej informovanosti a reakcie presadzovaním zavádzania infraštruktúry centier bezpečnostných operácií v EÚ, podporovať postupné vybudovanie kybernetických rezerv na úrovni EÚ so službami od dôveryhodných súkromných poskytovateľov a podporovať testovanie možných zraniteľností kritických subjektov na základe posúdení rizika na úrovni EÚ.

(7) Je nevyhnutné posilniť odhaľovanie kybernetických hrozieb a incidentov a situačnú informovanosť o nich v celej Únii a posilniť solidaritu zvýšením pripravenosti členských štátov a Únie na významné a rozsiahle kybernetické incidenty a ich spôsobilostí reagovať na tieto incidenty. Mala by sa preto zaviesť celoeurópska infraštruktúra centier bezpečnostných operácií (európsky kybernetický štít) s cieľom vybudovať a posilniť spoločné spôsobilosti týkajúce sa odhaľovania a situačnej informovanosti; mal by sa zriadiť mechanizmus na riešenie kybernetickobezpečnostných núdzových situácií s cieľom podporiť členské štáty pri príprave na významné a rozsiahle kybernetické incidenty, pri reakcii na ne a pri okamžitom zotavení sa z nich; mal by sa vytvoriť mechanizmus preskúmania kybernetických incidentov, ktorý bude slúžiť na skúmanie a posudzovanie konkrétnych významných alebo rozsiahlych incidentov. Týmito opatreniami nie sú dotknuté články 107 a 108 Zmluvy o fungovaní Európskej únie (ďalej len „ZFEÚ“).

(8) Na dosiahnutie týchto cieľov je takisto nevyhnutné v určitých oblastiach zmeniť nariadenie Európskeho parlamentu a Rady (EÚ) 2021/694[11]. Konkrétne by sa nariadenie (EÚ) 2021/694 malo týmto nariadením zmeniť v súvislosti s doplnením nových operačných cieľov týkajúcich sa európskeho kybernetického štítu a mechanizmu na riešenie kybernetických núdzových situácií v rámci špecifického cieľa 3 programu Digitálna Európa, ktorý je zameraný na zaručenie odolnosti, integrity a dôveryhodnosti digitálneho jednotného trhu, na posilnenie kapacít na monitorovanie kybernetických útokov a hrozieb a reakcie na ne a na posilnenie cezhraničnej spolupráce v oblasti kybernetickej bezpečnosti. Tieto ciele sa doplnia osobitnými podmienkami, za ktorých možno na tieto opatrenia prideliť finančnú podporu, a mali by sa stanoviť mechanizmy riadenia a koordinácie potrebné na dosiahnutie zamýšľaných cieľov. Medzi ďalšie zmeny nariadenia (EÚ) 2021/694 by mal patriť opis navrhovaných opatrení v rámci nových operačných cieľov, ako aj merateľné ukazovatele na monitorovanie vykonávania týchto nových operačných cieľov.

(9) Financovanie opatrení v rámci tohto nariadenia by sa malo stanoviť v nariadení (EÚ) 2021/694, ktoré by malo zostať príslušným základným aktom pre tieto opatrenia zakotvené v špecifickom cieli 3 programu Digitálna Európa. Osobitné podmienky účasti týkajúce sa každého opatrenia sa stanovia v príslušných pracovných programoch v súlade s platným ustanovením nariadenia (EÚ) 2021/694.

(10) Na toto nariadenie sa vzťahujú horizontálne rozpočtové pravidlá prijaté Európskym parlamentom a Radou na základe článku 322 ZFEÚ. Uvedené pravidlá sú stanovené

[10] Spoločné oznámenie Európskemu parlamentu a Rade Politika EÚ v oblasti kybernetickej obrany [JOIN(2022) 49 final].

[11] Nariadenie Európskeho parlamentu a Rady (EÚ) 2021/694 z 29. apríla 2021, ktorým sa zriaďuje program Digitálna Európa a zrušuje rozhodnutie (EÚ) 2015/2240 (Ú. v. EÚ L 166, 11.5.2021, s. 1).

v nariadení o rozpočtových pravidlách a určujú najmä postup stanovovania a plnenia rozpočtu Únie a stanovujú kontroly zodpovednosti účastníkov finančných operácií. Pravidlá prijaté na základe článku 322 ZFEÚ zahŕňajú aj všeobecný režim podmienenosti na ochranu rozpočtu Únie, ako sa stanovuje v nariadení Európskeho parlamentu a Rady (EÚ, Euratom) 2020/2092.

(11) Na účely správneho finančného riadenia by sa mali stanoviť osobitné pravidlá pre prenos nepoužitých viazaných a platobných rozpočtových prostriedkov. Pri dodržiavaní zásady, že rozpočet Únie sa stanovuje ročne, by sa týmto nariadením s ohľadom na nepredvídateľný, neobyčajný a špecifický charakter prostredia kybernetickej bezpečnosti mala nad rámec možností stanovených v nariadení o rozpočtových pravidlách stanoviť možnosť preniesť nepoužité finančné prostriedky, a tak maximalizovať kapacitu mechanizmu na riešenie kybernetickobezpečnostných núdzových situácií podporovať členské štáty v účinnom boji proti kybernetickým hrozbám.

(12) S cieľom účinnejšie predchádzať kybernetickým hrozbám a incidentom, posudzovať ich a reagovať na ne sa musia vybudovať komplexnejšie znalosti o hrozbách pre kritické aktíva a infraštruktúry na území Únie vrátane ich geografického rozloženia, vzájomného prepojenia a potenciálnych účinkov v prípade kybernetických útokov, ktoré by zasiahli tieto infraštruktúry. Zaviesť by sa mala rozsiahla infraštruktúra centier bezpečnostných operácií Únie (tzv. európsky kybernetický štít), ktorú by tvorilo niekoľko spolupracujúcich cezhraničných platforiem, z ktorých každá by združovala niekoľko vnútroštátnych centier bezpečnostných operácií. Táto infraštruktúra by mala slúžiť záujmom a potrebám v oblasti kybernetickej bezpečnosti na vnútroštátnej úrovni a na úrovni Únie, pričom by mala v plnej miere využívať najmodernejšie technológie vyspelých nástrojov na zber a analýzu údajov, čím by sa zlepšili spôsobilosti týkajúce sa odhaľovania a zvládania kybernetických hrozieb a poskytovanie situačnej informovanosti v reálnom čase. Táto infraštruktúra by mala slúžiť na zlepšenie odhaľovania kybernetických hrozieb a incidentov, a tak dopĺňať a podporovať subjekty a siete Únie zodpovedné za krízové riadenie v Únii, predovšetkým Európsku sieť styčných organizácií pre kybernetické krízy (ďalej len „EU-CyCLONe“), ako je vymedzená v smernici Európskeho parlamentu a Rady (EÚ) 2022/2555[12].

(13) Každý členský štát by mal na vnútroštátnej úrovni určiť verejný subjekt poverený v danom členskom štáte koordináciou činností v oblasti odhaľovania kybernetických hrozieb. Tieto vnútroštátne centrá bezpečnostných operácií by mali fungovať ako referenčné miesto a brána na vnútroštátnej úrovni, pokiaľ ide o účasť na európskom kybernetickom štíte, a mali by zabezpečiť na vnútroštátnej úrovni účinnú a efektívnu výmenu a zber informácií o kybernetických hrozbách od verejných a súkromných subjektov.

(14) V rámci európskeho kybernetického štítu by sa malo zriadiť viacero cezhraničných centier bezpečnostných operácií. V nich by sa mali združovať vnútroštátne centrá bezpečnostných operácií aspoň z troch členských štátov, aby bolo možné v plnej miere dosiahnuť prínos z cezhraničného odhaľovania hrozieb a výmeny a riadenia

[12] Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (smernica NIS 2) (Ú. v. EÚ L 333, 27.12.2022, s. 80).

informácií. Všeobecným cieľom cezhraničných centier bezpečnostných operácií by malo byť posilnenie kapacít týkajúcich sa analýzy kybernetickobezpečnostných hrozieb, predchádzania týmto hrozbám a ich odhaľovania a podpora získavania kvalitných spravodajských informácií o kybernetickobezpečnostných hrozbách, predovšetkým prostredníctvom spoločného využívania údajov z rozličných zdrojov, verejných či súkromných, ako aj prostredníctvom výmeny a spoločného využívania najmodernejších nástrojov a spoločného rozvoja spôsobilostí týkajúcich sa odhaľovania, analýzy a prevencie v dôveryhodnom prostredí. Centrá by mali vytvárať nové dodatočné kapacity, ktoré by vychádzali z existujúcich centier bezpečnostných operácií a jednotiek pre riešenie počítačových bezpečnostných incidentov (ďalej len „jednotky CSIRT“) a iných príslušných aktérov a dopĺňali ich.

(15) Na vnútroštátnej úrovni zabezpečujú monitorovanie, odhaľovanie a analýzu kybernetických hrozieb zvyčajne centrá bezpečnostných operácií verejných a súkromných subjektov v kombinácii s jednotkami CSIRT. Jednotky CSIRT si okrem toho v súlade so smernicou (EÚ) 2022/2555 vymieňajú informácie v rámci siete jednotiek CSIRT. Cezhraničné centrá bezpečnostných operácií by mali predstavovať novú kapacitu, ktorá bude dopĺňať sieť jednotiek CSIRT tým, že budú zhromažďovať údaje o kybernetickobezpečnostných hrozbách od verejných a súkromných subjektov a zabezpečovať spoločné využívanie týchto údajov, zvyšovať ich hodnotu prostredníctvom odborných analýz, spoločne nadobudnutých infraštruktúr a najmodernejších nástrojov a prispievať k rozvoju spôsobilostí a technologickej suverenity Únie.

(16) Cezhraničné centrá bezpečnostných operácií by mali fungovať ako ústredné kontaktné miesto umožňujúce rozsiahle zhromažďovanie relevantných údajov a spravodajských informácií o kybernetických hrozbách, ktoré umožňuje rozširovanie informácií o hrozbách rozsiahlemu a rozmanitému súboru aktérov [napr. tímom reakcie na núdzové počítačové situácie (ďalej len „CERT“), jednotkám CSIRT, strediskám pre výmenu a analýzu informácií, prevádzkovateľom kritických infraštruktúr]. Medzi informácie, ktoré sú predmetom výmeny medzi účastníkmi cezhraničného centra bezpečnostných operácií, by mohli patriť údaje zo sietí a senzorov, z informačných kanálov pre spravodajské informácie o hrozbách, z indikátorov ohrozenia a z kontextualizované informácie o incidentoch, hrozbách a zraniteľnostiach. Navyše by cezhraničné centrá bezpečnostných operácií mali takisto uzatvárať dohody o spolupráci s inými cezhraničnými centrami bezpečnostných operácií.

(17) Spoločná situačná informovanosť relevantných orgánov je nevyhnutnou podmienkou pripravenosti a koordinácie celej Únie, pokiaľ ide o významné a rozsiahle kybernetické incidenty. Smernicou (EÚ) 2022/2555 sa zriaďuje sieť EU-CyCLONe s cieľom podporiť koordinované riadenie rozsiahlych kybernetických incidentov a kríz na operačnej úrovni a zabezpečiť pravidelnú výmenu relevantných informácií medzi členskými štátmi a inštitúciami, orgánmi a agentúrami Únie. Odporúčanie (EÚ) 2017/1584 o koordinovanej reakcii na kybernetické incidenty a krízy veľkého rozsahu sa zaoberá úlohou všetkých príslušných aktérov. V smernici (EÚ) 2022/2555 sa takisto pripomína zodpovednosť Komisie v rámci mechanizmu Únie v oblasti civilnej ochrany zriadeného rozhodnutím Európskeho parlamentu a Rady č. 1313/2013/EÚ, ako aj jej zodpovednosť za poskytovanie analytických správ týkajúcich sa dojednaní mechanizmu integrovanej politickej reakcie na krízu podľa vykonávacieho rozhodnutia (EÚ) 2018/1993. Cezhraničné centrá bezpečnostných operácií by preto v situáciách, keď získajú informácie týkajúce sa potenciálneho alebo prebiehajúceho rozsiahleho kybernetického incidentu, mali poskytnúť relevantné informácie sieti EU-

CyCLONe, sieti jednotiek CSIRT a Komisii. V závislosti od situácie by medzi informácie určené na spoločné využívanie mohli patriť najmä technické informácie, informácie o povahe a motívoch útočníka alebo potenciálneho útočníka a netechnické informácie vyššej úrovne o potenciálnom alebo prebiehajúcom rozsiahlom kybernetickom incidente. V tejto súvislosti by sa mala náležitá pozornosť venovať zásade potreby poznať a potenciálne citlivej povahe vymieňaných informácií.

(18) Subjekty zúčastňujúce sa na európskom kybernetickom štíte by mali zabezpečiť vysokú úroveň interoperability medzi sebou, a to v prípade potreby aj v súvislosti s formátmi údajov, taxonómiou, nástrojmi na spracovanie a analýzu údajov, a bezpečné komunikačné kanály, minimálnu úroveň bezpečnosti aplikačnej vrstvy, prehľad situačnej informovanosti a ukazovatele. Pri prijímaní spoločnej taxonómie a vypracovaní vzorov u situačných správ, ktoré slúžia na opis technických príčin a účinkov kybernetických incidentov, by sa mali zohľadniť prebiehajúce práce na oznamovaní incidentov v kontexte vykonávania smernice (EÚ) 2022/2555.

(19) S cieľom umožniť výmenu údajov o kybernetickobezpečnostných hrozbách z rôznych zdrojov, v širokom meradle a v dôveryhodnom prostredí by subjekty zúčastnené na európskom kybernetickom štíte mali byť vybavené najmodernejšími a mimoriadne bezpečnými nástrojmi, vybavením a infraštruktúrami. To by malo umožniť zlepšenie kapacít kolektívneho odhaľovania a včasného varovania pre orgány a príslušné subjekty, predovšetkým prostredníctvom používania najnovších technológií umelej inteligencie a analýzy údajov.

(20) Vďaka zberu, spoločnému využívaniu a výmene údajov by európsky kybernetický štít mal posilniť technologickú suverenitu Únie. Zhromažďovanie vybratých údajov vysokej kvality by malo takisto prispieť k rozvoju vyspelých technológií umelej inteligencie a analýzy údajov. To by sa malo uľahčiť prepojením európskeho kybernetického štítu s celoeurópskou infraštruktúrou vysokovýkonnej výpočtovej techniky zriadenou nariadením Rady (EÚ) 2021/1173[13].

(21) Hoci je európsky kybernetický štít civilný projekt, komunita kybernetickej obrany by mohla ťažiť zo silnejších civilných spôsobilostí týkajúcich sa odhaľovania a situačnej informovanosti vyvinutých na ochranu kritickej infraštruktúry. Cezhraničné centrá bezpečnostných operácií s podporou Komisie a Európskeho centra priemyselných, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti (ďalej len „kompetenčné centrum“) a v spolupráci s vysokým predstaviteľom Únie pre zahraničné veci a bezpečnostnú politiku (ďalej len „vysoký predstaviteľ“) by mali postupne vypracovať osobitné protokoly a normy umožňujúce spoluprácu s komunitou kybernetickej obrany vrátane podmienok preverovania a bezpečnostných podmienok. Vývoj európskeho kybernetického štítu by mali sprevádzať úvahy umožňujúce v úzkej kooperácii s vysokým predstaviteľom budúcu spoluprácu so sieťami a s platformami zodpovednými za výmenu informácií v komunite kybernetickej obrany.

(22) Výmena informácií medzi účastníkmi európskeho kybernetického štítu by mala prebiehať v súlade s existujúcimi právnymi požiadavkami, a najmä s právom Únie a vnútroštátnym právom v oblasti ochrany údajov, ako aj s pravidlami Únie v oblasti hospodárskej súťaže, ktorými sa riadi výmena informácií. Pokiaľ je nevyhnutne potrebné spracovávanie osobných údajov, príjemca informácií by mal zaviesť

[13] Nariadenie Rady (EÚ) 2021/1173 z 13. júla 2021 o zriadení spoločného podniku pre európsku vysokovýkonnú výpočtovú techniku a o zrušení nariadenia (EÚ) 2018/1488 (Ú. v. EÚ L 256, 19.7.2021, s. 3).

technické a organizačné opatrenia, ktorými sa zaručia práva a slobody dotknutých osôb, a údaje by mal zničiť hneď, keď už nie sú potrebné na uvedený účel, a o ich zničení by mal informovať subjekt, ktorý údaje sprístupnil.

(23) Bez toho, aby bol dotknutý článok 346 ZFEÚ, výmena informácií, ktoré sú dôverné podľa predpisov Únie alebo vnútroštátnych predpisov, by sa mala zúžiť na informácie, ktoré sú relevantné a primerané účelu tejto výmeny. Pri výmene týchto informácií by sa mala zachovávať ich dôvernosť a chrániť bezpečnostné a komerčné záujmy dotknutých subjektov, a to plne v súlade s obchodným a podnikovým tajomstvom.

(24) So zreteľom na zvyšujúce sa riziká a čoraz väčší počet kybernetických incidentov postihujúcich členské štáty je nevyhnutné zriadiť nástroj krízovej podpory s cieľom zvýšiť odolnosť Únie voči významným a rozsiahlym kybernetickým incidentom a doplniť opatrenia členských štátov prostredníctvom núdzovej finančnej podpory určenej na pripravenosť, reakciu a okamžité zotavenie sa základných služieb. Tento nástroj by mal umožňovať rýchle nasadenie pomoci vo vymedzených situáciách a za jasných podmienok a mal by umožniť dôkladné monitorovanie a hodnotenie spôsobu využívania zdrojov. Zatiaľ čo primárnu zodpovednosť za predchádzanie kybernetickým incidentom a krízam, za prípravu a reakciu na ne majú členské štáty, mechanizmus na riešenie kybernetických núdzových situácií podporuje solidaritu medzi členskými štátmi v súlade s článkom 3 ods. 3 Zmluvy o Európskej únii (ďalej len „ZEÚ“).

(25) Mechanizmus na riešenie kybernetických núdzových situácií by mal poskytovať podporu členským štátom, ktorá bude dopĺňať ich vlastné opatrenia a zdroje a ďalšie existujúce možnosti podpory v prípade reakcie na významné a rozsiahle kybernetické incidenty a okamžitého zotavenia sa z nich, ako sú služby poskytované Agentúrou Európskej únie pre kybernetickú bezpečnosť (ďalej len „ENISA“) v súlade s jej mandátom, koordinovaná reakcia a pomoc siete jednotiek CSIRT, podpora na zmierňovanie od siete EU-CyCLONe, ako aj vzájomná pomoc medzi členskými štátmi aj v súvislosti s článkom 42 ods. 7 ZEÚ, tímy rýchlej kybernetickej reakcie stálej štruktúrovanej spolupráce (PESCO)[14] a tímy rýchlej reakcie na hybridné hrozby. Týmto mechanizmom by sa mala riešiť potreba zabezpečiť, aby na účely podpory pripravenosti na kybernetické incidenty a reakcie na ne v celej Únii a v tretích krajinách boli k dispozícii špecializované prostriedky.

(26) Týmto nástrojom nie sú dotknuté postupy a rámce na koordináciu reakcie na krízu na úrovni Únie, najmä mechanizmus Únie v oblasti civilnej ochrany[15], mechanizmus integrovanej politickej reakcie na krízu[16,] a smernica (EÚ) 2022/2555. Nástroj môže prispievať k opatreniam vykonávaným v kontexte článku 42 ods. 7 ZEÚ alebo v situáciách vymedzených v článku 222 ZFEÚ alebo ich môže dopĺňať. Využívanie tohto nástroja by sa malo v prípade potreby koordinovať s vykonávaním opatrení súboru nástrojov kybernetickej diplomacie.

(27) Pomoc poskytovaná podľa tohto nariadenia by mala slúžiť na podporu opatrení, ktoré prijali členské štáty na vnútroštátnej úrovni, a mala by ich dopĺňať. Na tento účel treba

---

14 ROZHODNUTIE RADY (SZBP) 2017/2315 z 11. decembra 2017 o nadviazaní stálej štruktúrovanej spolupráce (PESCO) a stanovení zoznamu zúčastnených členských štátov.

15 Rozhodnutie Európskeho parlamentu a Rady č. 1313/2013/EÚ zo 17. decembra 2013 o mechanizme Únie v oblasti civilnej ochrany (Ú. v. EÚ L 347, 20.12.2013, s. 924).

16 Mechanizmus integrovanej politickej reakcie na krízu a v súlade s odporúčaním Komisie (EÚ) 2017/1584 z 13. septembra 2017 o koordinovanej reakcii na kybernetické incidenty a krízy veľkého rozsahu.

zabezpečiť úzku spoluprácu a konzultácie medzi Komisiou a zasiahnutým členským štátom. Keď bude členský štát žiadať o podporu v rámci mechanizmu na riešenie kybernetických núdzových situácií, mal by poskytnúť relevantné informácie odôvodňujúce potrebu podpory.

(28) Podľa smernice (EÚ) 2022/2555 musia členské štáty určiť alebo zriadiť aspoň jeden orgán pre riadenie kybernetických kríz a musia zabezpečiť, aby tieto orgány mali primerané zdroje na účinné a efektívne vykonávanie svojich úloh. Členské štáty podľa nej musia ďalej určiť spôsobilosti, aktíva a postupy, ktoré možno použiť v prípade krízy, a musia prijať národný plán reakcie na rozsiahle kybernetické incidenty a krízy, v ktorom sa stanovia ciele a spôsoby riadenia rozsiahlych kybernetických incidentov a kríz. Členské štáty takisto musia zriadiť jednu alebo viacero jednotiek CSIRT poverených zodpovednosťou za riešenie incidentov podľa presne stanoveného postupu, ktoré sa budú zaoberať prinajmenšom odvetviami, pododvetviami a druhmi subjektov, ktoré patria do rozsahu pôsobnosti uvedenej smernice, a musia zabezpečiť, aby tieto jednotky mali primerané zdroje na účinné plnenie svojich úloh. Týmto nariadením nie je dotknutá úloha Komisie pri zabezpečovaní dodržiavania povinností vyplývajúcich zo smernice (EÚ) 2022/2555 členskými štátmi. Mechanizmus na riešenie kybernetických núdzových situácií by mal poskytovať pomoc pri opatreniach zameraných na posilňovanie pripravenosti, ako aj pri opatreniach reakcie na incidenty s cieľom zmierniť vplyv významných a rozsiahlych kybernetických incidentov, podporovať okamžité zotavenie sa a/alebo obnoviť fungovanie základných služieb.

(29) V rámci opatrení v oblasti pripravenosti a v záujme presadzovania jednotného prístupu a zvýšenia bezpečnosti v celej Únii a na jej vnútornom trhu by sa mala poskytovať koordinovaná podpora na testovanie a posudzovanie kybernetickej bezpečnosti subjektov pôsobiacich v odvetviach s vysokou úrovňou kritickosti určených v súlade so smernicou (EÚ) 2022/2555. Na tento účel by Komisia s podporou agentúry ENISA a v spolupráci so skupinou pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti zriadenou na základe smernice (EÚ) 2022/2555 mala pravidelne určovať relevantné odvetvia alebo pododvetvia, ktoré by mali byť oprávnené prijímať finančnú podporu na koordinované testovanie na úrovni Únie. Odvetvia alebo pododvetvia by sa mali vyberať z prílohy I k smernici (EÚ) 2022/2555 (ďalej len „odvetvia s vysokou úrovňou kritickosti“). Výkon koordinovaného testovania by mal vychádzať zo spoločných scenárov rizika a metodík. Aj vzhľadom na potrebu zabrániť duplicite by sa pri výbere odvetví a vypracúvaní scenárov rizika mali zohľadniť relevantné posúdenia rizík a scenáre rizika pre celú Úniu, ako sú napríklad hodnotenia rizík a scenáre rizika požadované v záveroch Rady o vývoji prístupu Európskej únie ku kybernetickej bezpečnosti, ktoré má vykonávať Komisia, vysoký predstaviteľ a skupina pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti v spolupráci s príslušnými civilnými a vojenskými orgánmi a agentúrami a vytvorenými sieťami vrátane siete EU-CyCLONe, ako aj posúdenie rizika komunikačných sietí a infraštruktúr požadované v spoločnej ministerskej výzve z Nevers, ktoré vykonáva skupina pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti s podporou Komisie a agentúry ENISA a v spolupráci s Orgánom európskych regulátorov pre elektronické komunikácie, koordinované posúdenia rizík, ktoré sa majú vykonávať podľa článku 22 smernice (EÚ) 2022/2555, a testovanie digitálnej prevádzkovej

odolnosti stanovené v nariadení Európskeho parlamentu a Rady (EÚ) 2022/2554[17]. Pri výbere odvetví by sa malo zohľadniť aj odporúčanie Rady o celoúnijnom koordinovanom prístupe k posilneniu odolnosti kritickej infraštruktúry.

(30) Mechanizmus na riešenie kybernetických núdzových situácií by mal navyše ponúkať podporu na ďalšie opatrenia v oblasti pripravenosti a podporovať pripravenosť v iných odvetviach, na ktoré sa nevzťahuje koordinované testovanie subjektov pôsobiacich v odvetviach s vysokou úrovňou kritickosti. Tieto opatrenia by mohli zahŕňať rozličné druhy vnútroštátnych činností zameraných na pripravenosť.

(31) Mechanizmus na riešenie kybernetických núdzových situácií by mal poskytovať aj podporu na opatrenia reakcie na incidenty s cieľom zmierniť vplyv významných a rozsiahlych kybernetických incidentov, podporovať okamžité zotavenie sa alebo obnoviť fungovanie základných služieb. V prípade potreby by mal dopĺňať mechanizmus Únie v oblasti civilnej ochrany s cieľom zabezpečiť komplexný prístup k reakcii na vplyvy kybernetických incidentov na občanov.

(32) Mechanizmus na riešenie kybernetických núdzových situácií by mal podporovať pomoc, ktorú poskytujú členské štáty členskému štátu, ktorý čelí významnému alebo rozsiahlemu kybernetickému incidentu, vrátane pomoci poskytovanej sieťou jednotiek CSIRT stanovenou v článku 15 smernice (EÚ) 2022/2555. Členským štátom poskytujúcim pomoc by sa malo umožniť predkladať žiadosti na pokrytie nákladov súvisiacich s vysielaním tímov odborníkov v rámci vzájomnej pomoci. Oprávnené náklady by mohli zahŕňať príspevky na cestovné výdavky, na ubytovanie a diéty odborníkov na kybernetickú bezpečnosť.

(33) Postupne by sa mala vytvoriť rezerva na úrovni Únie na účely kybernetickej bezpečnosti, ktorú by mali tvoriť služby súkromných poskytovateľov riadených bezpečnostných služieb na podporu opatrení reakcie a okamžitého zotavenia sa v prípadoch významných alebo rozsiahlych kybernetických incidentov. Rezerva EÚ na účely kybernetickej bezpečnosti by mala zabezpečovať dostupnosť a pripravenosť služieb. Služby rezervy EÚ na účely kybernetickej bezpečnosti by mali slúžiť na podporu vnútroštátnych orgánov pri poskytovaní pomoci zasiahnutým subjektom pôsobiacim v kritických odvetviach alebo v odvetviach s vysokou úrovňou kritickosti ako doplnok k ich vlastným opatreniam na vnútroštátnej úrovni. Keď členské štáty žiadajú o podporu z rezervy EÚ na účely kybernetickej bezpečnosti, mali by výslovne uviesť podporu poskytovanú zasiahnutému subjektu na vnútroštátnej úrovni, ktorá by sa mala zohľadniť pri posudzovaní žiadosti členského štátu. Služby rezervy EÚ na účely kybernetickej bezpečnosti sa za podobných podmienok môžu používať aj na podporu inštitúcií, orgánov a agentúr Únie.

(34) Na účely výberu súkromných poskytovateľov služieb na poskytovanie služieb v kontexte rezervy EÚ na účely kybernetickej bezpečnosti je nevyhnutné stanoviť súbor minimálnych kritérií, ktoré by sa mali uviesť vo výzve na predkladanie ponúk, na základe ktorej sa vyberú títo poskytovatelia, aby sa zabezpečilo, že budú splnené potreby orgánov členských štátov a subjektov pôsobiacich v kritických odvetviach alebo v odvetviach s vysokou úrovňou kritickosti.

[17] Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554 zo 14. decembra 2022 o digitálnej prevádzkovej odolnosti finančného sektora a o zmene nariadení (ES) č. 1060/2009, (EÚ) č. 648/2012, (EÚ) č. 600/2014, (EÚ) č. 909/2014 a (EÚ) 2016/1011.

(35) Na podporu vytvorenia rezervy EÚ na účely kybernetickej bezpečnosti by Komisia mohla zvážiť, že požiada agentúru ENISA o vypracovanie kandidátskeho systému certifikácie podľa nariadenia (EÚ) 2019/881 pre riadené bezpečnostné služby v oblastiach, na ktoré sa vzťahuje mechanizmus na riešenie kybernetických núdzových situácií.

(36) V záujme podpory cieľov tohto nariadenia týkajúcich sa presadzovania spoločnej situačnej informovanosti, zvyšovania odolnosti Únie a umožnenia účinnej reakcie na významné a rozsiahle kybernetické incidenty by sieť EU-CyCLONe, sieť jednotiek CSIRT alebo Komisia mali mať možnosť požiadať agentúru ENISA o preskúmanie a posúdenie hrozieb, zraniteľností a zmierňujúcich opatrení s ohľadom na konkrétny významný alebo rozsiahly kybernetický incident. Po dokončení preskúmania a posúdenia incidentu by agentúra ENISA mala vypracovať správu o preskúmaní incidentu, a to v spolupráci s príslušnými zainteresovanými stranami vrátane zástupcov súkromného sektora, členských štátov, Komisie a iných relevantných inštitúcií, orgánov a agentúr EÚ. Pokiaľ ide o súkromný sektor, agentúra ENISA vyvíja spôsoby výmeny informácií so špecializovanými poskytovateľmi vrátane poskytovateľov riadených bezpečnostných riešení a predajcov s cieľom prispieť k poslaniu agentúry ENISA dosiahnuť vysokú spoločnú úroveň kybernetickej bezpečnosti v celej Únii. Vychádzajúc zo spolupráce so zainteresovanými stranami vrátane súkromného sektora by sa správa o preskúmaní konkrétnych incidentov mala zamerať na posúdenie príčin, vplyvov incidentu a krokov na jeho zmiernenie po jeho výskyte. Osobitnú pozornosť by bolo treba venovať vstupným informáciám a poznatkom, ktoré poskytujú poskytovatelia riadených bezpečnostných služieb, ktorí spĺňajú podmienky najvyššej úrovne odbornej integrity, nestrannosti a nevyhnutných technických odborných znalostí vyžadovaných týmto nariadením. Správa by sa mala doručiť sieti EU-CyCLONe, sieti jednotiek CSIRT a Komisii a mala by sa premietnuť do ich činností. Ak incident súvisí s treťou krajinou, Komisia správu poskytne aj vysokému predstaviteľovi.

(37) S ohľadom na nepredvídateľnosť útokov na kybernetickú bezpečnosť a na skutočnosť, že tieto útoky často nie sú obmedzené na konkrétnu geografickú oblasť a predstavujú vysoké riziko presahu, prispieva k ochrane celej Únie zvýšenie odolnosti susedných krajín a posilnenie ich kapacity účinne reagovať na významné a rozsiahle kybernetické incidenty. Tretie krajiny pridružené k programu Digitálna Európa sa preto môžu podporovať z rezervy EÚ na účely kybernetickej bezpečnosti, ak je to možné podľa príslušnej dohody o pridružení k programu Digitálna Európa. Financovanie určené pre pridružené tretie krajiny by mala podporiť Únia v rámci príslušných partnerstiev a nástrojov financovania týchto krajín. Podpora by sa mala vzťahovať na služby v oblasti reakcie na významné a rozsiahle kybernetické incidenty a v oblasti okamžitého zotavenia sa z nich. Pri poskytovaní podpory tretím krajinám pridruženým k programu Digitálna Európa by sa mali uplatňovať podmienky stanovené v tomto nariadení pre rezervu EÚ na účely kybernetickej bezpečnosti a dôveryhodných poskytovateľov.

(38) V záujme zabezpečenia jednotných podmienok vykonávania tohto nariadenia by sa mali na Komisiu preniesť vykonávacie právomoci s cieľom stanoviť podmienky interoperability medzi cezhraničnými centrami bezpečnostných operácií; určiť procesné opatrenia na výmenu informácií medzi cezhraničnými centrami bezpečnostných operácií a subjektmi Únie v súvislosti s potenciálnym alebo prebiehajúcim rozsiahlym kybernetickým incidentom; stanoviť technické požiadavky na zaistenie bezpečnosti európskeho kybernetického štítu; spresniť druhy a počet

služieb reakcie potrebných pre rezervu EÚ na účely kybernetickej bezpečnosti a ďalej spresniť podrobné pravidlá prideľovania podporných služieb rezervy EÚ na účely kybernetickej bezpečnosti. Tieto právomoci by sa mali vykonávať v súlade s nariadením Európskeho parlamentu a Rady (EÚ) č. 182/2011.

(39) Cieľ tohto nariadenia možno lepšie dosiahnuť na úrovni Únie než na úrovni členských štátov. Únia preto môže prijať opatrenia v súlade so zásadou subsidiarity a zásadou proporcionality stanovenými v článku 5 Zmluvy o Európskej únii. Toto nariadenie neprekračuje rámec nevyhnutný na dosiahnutie uvedeného cieľa,

PRIJALI TOTO NARIADENIE:

Kapitola I

VŠEOBECNÉ CIELE, PREDMET ÚPRAVY A VYMEDZENIE POJMOV

Článok 1

Predmet úpravy a ciele

1. Týmto nariadením sa stanovujú opatrenia na posilnenie kapacít v Únii na odhaľovanie kybernetických hrozieb a incidentov, prípravu a reakciu na ne, najmä prostredníctvom týchto opatrení:

a) zavedenie celoeurópskej infraštruktúry centier bezpečnostných operácií („európsky kybernetický štít“) s cieľom vybudovať a posilniť spoločné spôsobilosti týkajúce sa odhaľovania a situačnej informovanosti;

b) vytvorenie mechanizmu na riešenie kybernetickobezpečnostných núdzových situácií s cieľom podporiť členské štáty pri príprave na významné a rozsiahle kybernetické incidenty, pri reakcii na ne a pri okamžitom zotavení sa z nich;

c) vytvorenie európskeho mechanizmu preskúmania kybernetických incidentov, ktorý bude slúžiť na skúmanie a posudzovanie významných alebo rozsiahlych incidentov.

2. Toto nariadenie má za cieľ posilniť solidaritu na úrovni Únie prostredníctvom týchto špecifických cieľov:

a) posilniť spoločné odhaľovanie kybernetických hrozieb a incidentov a situačnú informovanosť o nich v Únii, v dôsledku čoho bude možné posilniť konkurenčnú pozíciu odvetví priemyslu a služieb v Únii v rámci celého digitálneho hospodárstva a prispievať k technologickej suverenite Únie v oblasti kybernetickej bezpečnosti;

b) posilniť pripravenosť subjektov pôsobiacich v kritických odvetviach a v odvetviach s vysokou úrovňou kritickosti z celej Únie a posilniť solidaritu rozvíjaním kapacít spoločnej reakcie na významné alebo rozsiahle kybernetické incidenty, a to aj sprístupnením podpory Únie týkajúcej sa reakcie na kybernetické incidenty tretím krajinám pridruženým k programu Digitálna Európa;

c) zvýšiť odolnosť Únie a prispieť k účinnej reakcii prostredníctvom skúmania a posudzovania významných alebo rozsiahlych incidentov vrátane získavania poznatkov a prípadne odporúčaní.

3. Týmto nariadením nie je dotknutá primárna zodpovednosť členských štátov za národnú a verejnú bezpečnosť a za prevenciu, vyšetrovanie, odhaľovanie a stíhanie trestných činov.

Článok 2

Vymedzenie pojmov

Na účely tohto nariadenia sa uplatňuje toto vymedzenie pojmov:

1. **„cezhraničné centrum bezpečnostných operácií“** je platforma s účasťou viacerých krajín, ktorou sa do koordinovanej sieťovej štruktúry spájajú vnútroštátne centrá bezpečnostných operácií aspoň z troch členských štátov, ktoré tvoria hostiteľské konzorcium, a ktorá je určená na predchádzanie kybernetickým hrozbám a incidentom a na podporu tvorby spravodajských informácií vysokej kvality, najmä prostredníctvom výmeny údajov z rôznych zdrojov, verejných a súkromných, ako aj prostredníctvom spoločného využívania najmodernejších nástrojov a spoločného vývoja spôsobilostí v oblasti odhaľovania kybernetických hrozieb a incidentov, ich analýzy, prevencie a ochrany pred nimi v dôveryhodnom prostredí;
2. **„verejný subjekt“** je verejnoprávna inštitúcia v zmysle vymedzenia v článku 2 ods. 1 bode 4 smernice Európskeho parlamentu a Rady 2014/24/EÚ[18];
3. **„hostiteľské konzorcium“** je konzorcium zložené zo zúčastnených štátov zastúpených vnútroštátnymi centrami bezpečnostných operácií, ktoré súhlasili so zriadením cezhraničného centra bezpečnostných operácií a s prispievaním na účely nadobudnutia nástrojov a infraštruktúry pre cezhraničné centrum bezpečnostných operácií a na jeho prevádzku;
4. **„subjekt“** je subjekt v zmysle vymedzenia v článku 6 bode 38 smernice (EÚ) 2022/2555;
5. **„subjekty pôsobiace v kritických odvetviach a v odvetviach s vysokou úrovňou kritickosti“** sú druh subjektov, ktoré sa uvádzajú v prílohe I a II k smernici (EÚ) 2022/2555;
6. **„kybernetická hrozba“** je kybernetická hrozba v zmysle vymedzenia v článku 2 bode 8 nariadenia (EÚ) 2019/881;
7. **„významný kybernetický incident“** je kybernetický incident, ktorý spĺňa kritériá stanovené v článku 23 ods. 3 smernice (EÚ) 2022/2555;
8. **„rozsiahly kybernetický incident“** je incident v zmysle vymedzenia v článku 6 bode 7 smernice (EÚ) 2022/2555;

[18] Smernica Európskeho parlamentu a Rady 2014/24/EÚ z 26. februára 2014 o verejnom obstarávaní a o zrušení smernice 2004/18/ES (Ú. v. EÚ L 94, 28.3.2014, s. 65).

9. **„pripravenosť“** je stav pohotovosti a spôsobilosti zabezpečiť účinnú rýchlu reakciu na významný alebo rozsiahly kybernetický incident, ktorý sa dosahuje v dôsledku vopred uskutočnených opatrení posúdenia rizika a monitorovacích opatrení;

10. **„reakcia“** je opatrenie v prípade významného alebo rozsiahleho kybernetického incidentu, prípadne počas neho alebo po ňom s cieľom riešiť jeho okamžité alebo krátkodobé nepriaznivé následky;

11. **„dôveryhodní poskytovatelia“** sú poskytovatelia riadených bezpečnostných služieb v zmysle vymedzenia v článku 6 bode 40 smernice (EÚ) 2022/2555, ktorí sú vybratí v súlade s článkom 16 tohto nariadenia.

Kapitola II

EURÓPSKY KYBERNETICKÝ ŠTÍT

Článok 3

Zriadenie európskeho kybernetického štítu

1. Zriadi sa prepojená celoeurópska infraštruktúra centier bezpečnostných operácií (ďalej len „európsky kybernetický štít“) s cieľom rozvíjať pokročilé spôsobilosti Únie odhaľovať kybernetické hrozby a incidenty v Únii, analyzovať ich a spracovávať o nich údaje. Tvoria ju všetky vnútroštátne centrá bezpečnostných operácií a cezhraničné centrá bezpečnostných operácií.

Opatrenia, ktorými sa vykonáva európsky kybernetický štít, sa podporia financovaním z programu Digitálna Európa a vykonávajú sa v súlade s nariadením (EÚ) 2021/694, a najmä s jeho špecifickým cieľom 3.

2. Európsky kybernetický štít:

a) združuje údaje o kybernetických hrozbách a incidentoch z rôznych zdrojov prostredníctvom cezhraničných centier bezpečnostných operácií a zabezpečuje ich výmenu;

b) vytvára kvalitné, využiteľné informácie a spravodajské informácie o kybernetických hrozbách, pričom používa najmodernejšie nástroje, najmä technológie umelej inteligencie a analýzy údajov;

c) prispieva k lepšej ochrane a reakcii na kybernetické hrozby;

d) prispieva k rýchlejšiemu odhaľovaniu kybernetických hrozieb a situačnej informovanosti v celej Únii;

e) poskytuje služby a činnosti pre komunitu v oblasti kybernetickej bezpečnosti v Únii vrátane prispievania k rozvoju pokročilých nástrojov v oblasti umelej inteligencie a analýzy údajov.

Vyvíja sa v spolupráci s celoeurópskou infraštruktúrou vysokovýkonnej výpočtovej techniky zriadenou na základe nariadenia (EÚ) 2021/1173.

Článok 4

Vnútroštátne centrá bezpečnostných operácií

1. Na účely účasti v európskom kybernetickom štíte každý členský štát určí aspoň jedno vnútroštátne centrum bezpečnostných operácií. Toto vnútroštátne centrum bezpečnostných operácií je verejný subjekt.

Má spôsobilosť konať ako referenčný bod a brána pre ďalšie verejné a súkromné organizácie na vnútroštátnej úrovni na účely zhromažďovania a analyzovania informácií o kybernetických hrozbách a incidentoch a prispievania k cezhraničnému centru bezpečnostných operácií. Je vybavené najmodernejšími technológiami, ktoré sú schopné odhaľovať, agregovať a analyzovať údaje relevantné z hľadiska kybernetických hrozieb a incidentov.

2. V nadväznosti na výzvu na vyjadrenie záujmu vyberá Európske centrum priemyselných, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti (ďalej len „kompetenčné centrum“) vnútroštátne centrá bezpečnostných operácií na účely účasti na spoločnom obstarávaní nástrojov a infraštruktúr s kompetenčným centrom. Vybratým vnútroštátnym centrám bezpečnostných operácií môže kompetenčné centrum udeľovať granty na financovanie prevádzky týchto nástrojov a infraštruktúr. Až 50 % obstarávacích nákladov na nástroje a infraštruktúry a až 50 % prevádzkových nákladov pokrýva finančný príspevok Únie, pričom zvyšné náklady pokrývajú členské štáty. Pred spustením postupu nadobudnutia nástrojov a infraštruktúr kompetenčné centrum a vnútroštátne centrá bezpečnostných operácií uzavrú dohodu o poskytovaní hostiteľských služieb a o používaní, ktorou sa upravuje používanie nástrojov a infraštruktúr.

3. Vnútroštátne centrum bezpečnostných operácií vybrané podľa odseku 2 sa zaväzuje požiadať o účasť v cezhraničnom centre bezpečnostných operácií do dvoch rokov od dátumu nadobudnutia nástrojov a infraštruktúr alebo dátumu prijatia grantového financovania, podľa toho, čo nastane skôr. Ak sa vnútroštátne centrum bezpečnostných operácií do uvedeného času nestane účastníkom cezhraničného centra bezpečnostných operácií, nemá nárok na dodatočnú podporu Únie na základe tohto nariadenia.

Článok 5

Cezhraničné centrá bezpečnostných operácií

1. Hostiteľské konzorcium zložené aspoň z troch členských štátov zastúpených vnútroštátnymi centrami bezpečnostných operácií, ktoré sa zaviazali spolupracovať na koordinácii svojich činností v oblasti odhaľovania kybernetických incidentov a monitorovania hrozieb, je oprávnené zúčastňovať sa na úkonoch s cieľom zriadiť cezhraničné centrum bezpečnostných operácií.

2. V nadväznosti na výzvu na vyjadrenie záujmu kompetenčné centrum vyberie hostiteľské konzorcium na účely účasti na spoločnom obstarávaní nástrojov a infraštruktúr s kompetenčným centrom. Na financovanie prevádzky týchto nástrojov a infraštruktúr môže kompetenčné centrum udeliť hostiteľskému konzorciu grant. Až 75 % obstarávacích nákladov na nástroje a infraštruktúry a až 50 % prevádzkových nákladov pokrýva finančný príspevok

Únie, pričom zvyšné náklady pokryje hostiteľské konzorcium. Pred spustením postupu nadobudnutia nástrojov a infraštruktúr kompetenčné centrum a hostiteľské konzorcium uzavrú dohodu o poskytovaní hostiteľských služieb a o používaní, ktorou sa upravuje používanie nástrojov a infraštruktúr.

3. Členovia hostiteľského konzorcia uzavrú písomnú dohodu o konzorciu, v ktorej sa stanovujú ich vnútorné mechanizmy na vykonávanie dohody o poskytovaní hostiteľských služieb a o používaní.

4. Na právne účely je cezhraničné centrum bezpečnostných operácií zastupované vnútroštátnym centrom bezpečnostných operácií, ktoré koná ako koordinačné centrum bezpečnostných operácií, alebo hostiteľským konzorciom, ak má právnu subjektivitu. Za dodržiavanie požiadaviek dohody o poskytovaní hostiteľských služieb a o používaní a tohto nariadenia zodpovedá koordinačné centrum bezpečnostných operácií.

Článok 6

Spolupráca a výmena informácií v rámci cezhraničných centier bezpečnostných operácií a medzi nimi

1. Členovia hostiteľského konzorcia si medzi sebou v rámci cezhraničného centra bezpečnostných operácií vymieňajú relevantné informácie vrátane informácií o kybernetických hrozbách, udalostiach odvrátených v poslednej chvíli, o zraniteľnostiach, technikách a postupoch, indikátoroch kompromitácie, nepriateľských taktikách, informácií špecifických pre jednotlivé hrozby a aktérov, výstrah a odporúčaní týkajúcich sa konfigurácie kybernetických bezpečnostných nástrojov na odhaľovanie kybernetických útokov, ak takáto výmena informácií:

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

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

2. Písomnou dohodou o konzorciu uvedenou v článku 5 ods. 3 sa stanovuje:

a) záväzok zabezpečiť výmenu značného objemu údajov uvedených v odseku 1 a podmienky, na základe ktorých sa má výmena informácií uskutočňovať;

b) rámec riadenia, ktorým sa podnecuje výmena informácií všetkými účastníkmi;

c) ciele v súvislosti s prispievaním k vývoju pokročilých nástrojov v oblasti umelej inteligencie a analýzy údajov.

3. S cieľom podnecovať výmenu informácií medzi cezhraničnými centrami bezpečnostných operácií tieto centrá zaisťujú vysokú úroveň vzájomnej interoperability. Na uľahčenie interoperability medzi cezhraničnými centrami bezpečnostných operácií môže Komisia po

konzultácii s kompetenčným centrom prostredníctvom vykonávacích aktov určiť podmienky uvedenej interoperability. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 21 ods. 2 tohto nariadenia.

4. Cezhraničné centrá bezpečnostných operácií uzatvárajú medzi sebou dohody o spolupráci, v ktorých sa určia zásady výmeny informácií medzi cezhraničnými platformami.

Článok 7

Spolupráca a výmena informácií so subjektmi Únie

1. Ak cezhraničné centrá bezpečnostných operácií získajú informácie týkajúce sa potenciálneho alebo prebiehajúceho rozsiahleho kybernetického incidentu, poskytnú bez zbytočného odkladu relevantné informácie sieti EU-CyCLONe, sieti jednotiek CSIRT a Komisii s ohľadom na ich príslušné úlohy v oblasti krízového riadenia v súlade so smernicou (EÚ) 2022/2555.

2. Procesné opatrenia na výmenu informácií podľa odseku 1 môže určiť Komisia prostredníctvom vykonávacích aktov. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 21 ods. 2 tohto nariadenia.

Článok 8

Bezpečnosť

1. Členské štáty, ktoré sa zúčastňujú na európskom kybernetickom štíte, zaistia vysokú úroveň bezpečnosti údajov a fyzickej bezpečnosti infraštruktúry európskeho kybernetického štítu a zaistia primerané spravovanie a kontrolu infraštruktúry takým spôsobom, aby bola chránená pred hrozbami a aby bola zaistená jej bezpečnosť a bezpečnosť systémov vrátane bezpečnosti údajov, ktoré sa vymieňajú prostredníctvom infraštruktúry.

2. Členské štáty, ktoré sa zúčastňujú na európskom kybernetickom štíte, zaistia, aby výmena informácií v rámci európskeho kybernetického štítu so subjektmi, ktoré nie sú verejnými subjektmi členských štátov, negatívne neovplyvnila bezpečnostné záujmy Únie.

3. Komisia môže prijať vykonávacie akty, v ktorých sa stanovia technické požiadavky pre členské štáty, aby si splnili povinnosť podľa odseku 1 a 2. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 21 ods. 2 tohto nariadenia. S cieľom uľahčiť spoluprácu s vojenskými aktérmi pritom Komisia s podporou vysokého predstaviteľa zohľadňuje relevantné bezpečnostné normy na úrovni obrany.

Kapitola III

MECHANIZMUS NA RIEŠENIE KYBERNETICKÝCH NÚDZOVÝCH SITUÁCIÍ

Článok 9

Zriadenie mechanizmu na riešenie kybernetických núdzových situácií

1. Zriaďuje sa mechanizmus na riešenie kybernetických núdzových situácií (ďalej len „mechanizmus“) s cieľom zvýšiť odolnosť Únie voči závažným kybernetickým hrozbám a pripraviť sa na krátkodobý vplyv významných a rozsiahlych kybernetických incidentov a v duchu solidarity ho zmierňovať.

2. Opatrenia, ktorými sa mechanizmus na riešenie kybernetických núdzových situácií vykonáva, sa podporia financovaním z programu Digitálna Európa a vykonávajú sa v súlade s nariadením (EÚ) 2021/694, a najmä s jeho špecifickým cieľom 3.

Článok 10

Druhy opatrení

1. Mechanizmom sa podporujú tieto druhy opatrení:

a) opatrenia v oblasti pripravenosti vrátane koordinovaného testovania pripravenosti subjektov pôsobiacich v odvetviach s vysokou úrovňou kritickosti v celej Únii;

b) opatrenia reakcie, ktorými sa podporuje reakcia na významné alebo rozsiahle kybernetické incidenty a okamžité zotavenie sa z nich a ktoré majú poskytovať dôveryhodní poskytovatelia, ktorí sa zúčastňujú na rezerve EÚ na účely kybernetickej bezpečnosti zriadenej podľa článku 12;

c) opatrenia vzájomnej pomoci, ktoré zahŕňajú poskytovanie pomoci vnútroštátnymi orgánmi jedného členského štátu druhému členskému štátu, najmä podľa článku 11 ods. 3 písm. f) smernice (EÚ) 2022/2555.

Článok 11

Koordinované testovanie pripravenosti subjektov

1. Komisia na účely podpory koordinovaného testovania pripravenosti subjektov uvedeného v článku 10 ods. 1 písm. a) v celej Únii po konzultácii so skupinou pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti a s agentúrou ENISA identifikuje spomedzi odvetví s vysokou úrovňou kritickosti uvedených v prílohe I k smernici (EÚ) 2022/2555 dotknuté odvetvia alebo pododvetvia, z ktorých môžu byť subjekty podrobné koordinovanému testovaniu pripravenosti, pričom sa zohľadnia existujúce a plánované koordinované posúdenia rizík a testovanie odolnosti na úrovni Únie.

2. Skupina pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti v spolupráci s Komisiou, agentúrou ENISA a vysokým predstaviteľom vypracováva spoločné scenáre rizika a metodiky na vykonávanie koordinovaného testovania.

Článok 12

Vytvorenie rezervy EÚ na účely kybernetickej bezpečnosti

1. Vytvára sa rezerva EÚ na účely kybernetickej bezpečnosti s cieľom pomáhať používateľom uvedeným v odseku 3 pri reakcii na významné alebo rozsiahle kybernetické incidenty alebo pri poskytovaní podpory pri takejto reakcii, a pri okamžitom zotavení sa z takýchto incidentov.

2. Rezerva EÚ na účely kybernetickej bezpečnosti sa pozostáva zo služieb reakcie na incidenty poskytovaných dôveryhodnými poskytovateľmi vybratými v súlade s kritériami stanovenými v článku 16. Súčasťou rezervy sú vopred vyčlenené služby. Tieto služby sú nasaditeľné vo všetkých členských štátoch.

3. Medzi používateľov služieb z rezervy EÚ na účely kybernetickej bezpečnosti patria:

a) orgány pre riadenie kybernetických kríz a jednotky CSIRT členských štátov, ako sa uvádza v článku 9 ods. 1 a 2, resp. v článku 10 smernice (EÚ) 2022/2555;

b) inštitúcie, orgány a agentúry Únie.

4. Používatelia uvedení v odseku 3 písm. a) využívajú služby z rezervy EÚ na účely kybernetickej bezpečnosti s cieľom reagovať alebo podporovať reakciu na významné alebo rozsiahle kybernetické incidenty, ktoré zasahujú subjekty pôsobiace v kritických odvetviach alebo v odvetviach s vysokou úrovňou kritickosti, a okamžité zotavenie sa z nich.

5. Celkovú zodpovednosť za vykonávanie rezervy EÚ na účely kybernetickej bezpečnosti nesie Komisia. Komisia určuje priority a vývoj rezervy EÚ na účely kybernetickej bezpečnosti v súlade požiadavkami používateľov uvedených v odseku 3 a dohliada na jej vykonávanie a zaisťuje komplementárnosť, súdržnosť, synergie a prepojenia s ďalšími podpornými opatreniami na základe tohto nariadenia, ako aj s ďalšími opatreniami a programami Únie.

6. Prostredníctvom dohôd o príspevku môže Komisia prevádzkou a správou rezervy EÚ na účely kybernetickej bezpečnosti úplne alebo sčasti poveriť agentúru ENISA.

7. S cieľom podporiť Komisiu pri vytváraní rezervy EÚ na účely kybernetickej bezpečnosti agentúra ENISA vypracuje po konzultáciách s členskými štátmi a Komisiou mapovanie potrebných služieb. Po konzultácii s Komisiou vypracuje agentúra ENISA podobné mapovanie s cieľom identifikovať potreby tretích krajín, ktoré majú podľa článku 17 nárok na podporu z rezervy EÚ na účely kybernetickej bezpečnosti. Komisia v prípade potreby uskutoční konzultácie s vysokým predstaviteľom.

8. Druhy a počet služieb reakcie potrebných pre rezervu EÚ na účely kybernetickej bezpečnosti môže Komisia spresniť prostredníctvom vykonávacích aktov. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 21 ods. 2.

Článok 13

Žiadosti o podporu z rezervy EÚ na účely kybernetickej bezpečnosti

1. Používatelia uvedení v článku 12 ods. 3 môžu požiadať o služby z rezervy EÚ na účely kybernetickej bezpečnosti na podporu reakcie na významné alebo rozsiahle kybernetické incidenty a okamžitého zotavenia sa z nich.

2. Aby mohli používatelia uvedení v článku 12 ods. 3 prijímať podporu z rezervy EÚ na účely kybernetickej bezpečnosti, prijmú opatrenia na zmiernenie účinkov incidentu, v prípade ktorého sa požaduje podpora, vrátane poskytnutia priamej technickej pomoci a ďalších zdrojov s cieľom pomôcť pri reakcii na incident a pri úsilí o okamžité zotavenie sa.

3. Žiadosti o podporu od používateľov uvedených v článku 12 ods. 3 písm. a) tohto nariadenia sa predkladajú Komisii a agentúre ENISA prostredníctvom jednotného kontaktného miesta určeného alebo zriadeného členským štátom v súlade s článkom 8 ods. 3 smernice (EÚ) 2022/2555.

4. O svojich žiadostiach o podporu pri reakcii na incidenty a pri okamžitom zotavení sa z nich podľa tohto článku informujú členské štáty informujú sieť jednotiek CSIRT a v prípade potreby sieť EU-CyCLONe.

5. Žiadosti o podporu pri reakcii na incidenty a okamžitom zotavení sa z nich musia obsahovať:

a) náležité informácie týkajúce sa zasiahnutého subjektu a potenciálnych vplyvov incidentu a plánovaného použitia požadovanej podpory vrátane uvedenia odhadovaných potrieb;

b) informácie o opatreniach prijatých na zmiernenie incidentu, v prípade ktorého sa požaduje podpora, ako sa uvádza v odseku 2;

c) informácie o ďalších formách podpory dostupnej pre zasiahnutý subjekt vrátane existujúcich zmluvných dohôd o službách reakcie na incidenty a okamžitého zotavenia sa z nich, ako aj poistných zmlúv, ktoré sa potenciálne vzťahujú na takýto druh incidentu.

6. Na uľahčenie predkladania žiadostí o podporu z rezervy EÚ na účely kybernetickej bezpečnosti vypracuje agentúra ENISA v spolupráci s Komisiou a skupinou pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti vzor.

7. Podrobné opatrenia týkajúce sa prideľovania služieb podpory z rezervy EÚ na účely kybernetickej bezpečnosti môže Komisia ďalej upresniť prostredníctvom vykonávacích aktov. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 21 ods. 2.

Článok 14

Vykonávanie podpory z rezervy EÚ na účely kybernetickej bezpečnosti

1. Žiadosti o podporu z rezervy EÚ na účely kybernetickej bezpečnosti posudzuje Komisia s podporou agentúry ENISA alebo podľa vymedzenia v dohodách o príspevku na základe článku 12 ods. 6 a odpoveď sa bezodkladne zašle používateľom uvedeným v článku 12 ods. 3.

2. Na určenie priority žiadostí v prípade viacerých súčasných žiadostí sa podľa potreby zohľadňujú tieto kritériá:

a) závažnosť kybernetického incidentu;

b) druh zasiahnutého subjektu, pričom vyššia priorita sa priraďuje incidentom, ktorými sú zasiahnuté kľúčové subjekty v zmysle vymedzenia v článku 3 ods. 1 smernice (EÚ) 2022/2555;

c) potenciálny vplyv na zasiahnutý členský štát (zasiahnuté členské štáty) alebo používateľov;

d) potenciálny cezhraničný charakter incidentu a riziko presahovania na ďalšie členské štáty alebo používateľov;

e) opatrenia prijaté používateľom s cieľom pomôcť pri reakcii na incident a pri úsilí o okamžité zotavenie sa, ako sa uvádza v článku 13 ods. 2 a v článku 13 ods. 5) písm. b).

3. Služby rezervy EÚ na účely kybernetickej bezpečnosti sa poskytujú v súlade s osobitnými dohodami medzi poskytovateľom služieb a používateľom, ktorému sa poskytuje podpora v rámci rezervy EÚ na účely kybernetickej bezpečnosti. Súčasťou dohôd sú podmienky upravujúce zodpovednosť.

4. Dohody uvedené v odseku 3 môžu vychádzať zo vzorov vypracovaných agentúrou ENISA po konzultácii s členskými štátmi.

5. Komisia a agentúra ENISA nenesú zmluvnú zodpovednosť za škody spôsobené tretím stranám v dôsledku služieb poskytnutých v rámci vykonávania rezervy EÚ na účely kybernetickej bezpečnosti.

6. Do jedného mesiaca od skončenia podporného opatrenia poskytnú používatelia Komisii a agentúre ENISA súhrnnú správu o poskytnutých službách, dosiahnutých výsledkoch a získaných poznatkoch. Keď je používateľ z tretej krajiny, ako sa stanovuje v článku 17, takáto správa sa poskytne aj vysokému predstaviteľovi.

7. O využívaní a výsledkoch podpory predkladá Komisia pravidelne správy skupine pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti.

Článok 15

Koordinácia s mechanizmami krízového riadenia

1. V prípadoch, keď sú významné alebo rozsiahle kybernetické incidenty spôsobené katastrofami v zmysle vymedzenia v rozhodnutí 1313/2013/EÚ[19] alebo majú za následok takéto katastrofy, podporou podľa tohto nariadenia pri reakcii na takéto incidenty sa dopĺňajú opatrenia podľa rozhodnutia 1313/2013/EÚ, pričom toto rozhodnutie ňou nie je dotknuté.

2. V prípade rozsiahleho, cezhraničného kybernetického incidentu, keď sa aktivuje mechanizmus integrovanej politickej reakcie na krízu, sa podpora podľa tohto nariadenia pri reakcii na takýto incident vykonáva v súlade s príslušnými protokolmi a postupmi v rámci mechanizmu integrovanej politickej reakcie na krízu.

[19] Rozhodnutie Európskeho parlamentu a Rady č. 1313/2013/EÚ zo 17. decembra 2013 o mechanizme Únie v oblasti civilnej ochrany (Ú. v. EÚ L 347, 20.12.2013, s. 924).

3. Podporou v rámci mechanizmu na riešenie kybernetických núdzových situácií sa na základe konzultácie s vysokým predstaviteľom môže dopĺňať pomoc poskytnutá v kontexte spoločnej zahraničnej a bezpečnostnej politiky a spoločnej bezpečnostnej a obrannej politiky, a to aj prostredníctvom tímov rýchlej kybernetickej reakcie. Môže sa ňou dopĺňať aj pomoc poskytnutá jedným členským štátom inému členskému štátu v kontexte článku 42 ods. 7 Zmluvy o Európskej únii alebo môže k takejto pomoci prispievať.

4. Podpora v rámci mechanizmu na riešenie kybernetických núdzových situácií môže tvoriť súčasť spoločnej reakcie medzi Úniou a členskými štátmi v situáciách uvedených v článku 222 Zmluvy o fungovaní Európskej únie.

Článok 16

Dôveryhodní poskytovatelia

1. V postupoch obstarávania na účely vytvorenia rezervy EÚ na účely kybernetickej bezpečnosti koná verejný obstarávateľ v súlade so zásadami stanovenými v nariadení (EÚ, Euratom) 2018/1046 a v súlade s týmito zásadami:

a) zaistiť, aby súčasťou rezervy EÚ na účely kybernetickej bezpečnosti boli služby, ktoré môžu byť nasadené vo všetkých členských štátoch, pričom sa zohľadňujú najmä vnútroštátne požiadavky na poskytovanie takýchto služieb vrátane certifikácie alebo akreditácie;

b) zaistiť ochranu základných bezpečnostných záujmov Únie a jej členských štátov;

c) zaistiť, aby rezerva EÚ na účely kybernetickej bezpečnosti prinášala pridanú hodnotu EÚ tým, že bude prispievať k cieľom stanoveným v článku 3 nariadenia (EÚ) 2021/694 vrátane podpory rozvíjania zručností v oblasti kybernetickej bezpečnosti v EÚ.

2. Pri obstarávaní služieb pre rezervu EÚ na účely kybernetickej bezpečnosti verejný obstarávateľ zahŕňa do súťažných podkladov tieto podmienky účasti:

a) poskytovateľ preukáže, že jeho zamestnanci spĺňajú najvyššiu úroveň profesijnej bezúhonnosti, nezávislosti a zodpovednosti a majú nevyhnutné technické odborné spôsobilosti na vykonávanie činností v svojej osobitnej oblasti, a zaistí trvalosť/kontinuitu odborných znalostí, ako aj požadované technické zdroje;

b) poskytovateľ, jeho dcérske spoločnosti a subdodávatelia majú zavedený rámec na ochranu citlivých informácií týkajúcich sa služby, a najmä dôkazov, zistení a správ, a dodržiavajú predpisy Únie v oblasti bezpečnosti týkajúce sa ochrany utajovaných skutočností EÚ;

c) poskytovateľ poskytne dostatočný dôkaz o tom, že jeho štruktúra riadenia je transparentná a že nie je pravdepodobné, že ohrozí jeho nestrannosť a kvalitu jeho služieb ani že spôsobí konflikty záujmov;

d) poskytovateľ musí mať príslušnú bezpečnostnú previerku prinajmenšom v prípade zamestnancov určených na nasadenie služby;

e) poskytovateľ musí mať príslušnú úroveň bezpečnosti svojich informačných systémov;

f) poskytovateľ disponuje hardvérovým a softvérovým technickým vybavením potrebným na podporu požadovanej služby;

g) poskytovateľ vie preukázať, že má skúsenosti s poskytovaním podobných služieb príslušným vnútroštátnym orgánom alebo subjektom pôsobiacim v kritických odvetviach alebo v odvetviach s vysokou úrovňou kritickosti;

h) poskytovateľ je schopný poskytnúť službu v krátkom čase v členskom(-ých) štáte(-och), v ktorom(-ých) môže službu poskytovať;

i) poskytovateľ je schopný poskytovať službu v miestnom jazyku členského(-ých) štátu(-ov), v ktorom(-ých) môže službu poskytovať;

j) po zavedení systému certifikácie EÚ pre riadené bezpečnostné služby podľa nariadenia (EÚ) 2019/881 musí byť poskytovateľ certifikovaný v súlade s uvedeným systémom.

Článok 17

Podpora pre tretie krajiny

1. Tretie krajiny môžu požiadať o podporu z rezervy EÚ na účely kybernetickej bezpečnosti, ak sa to umožňuje v dohodách o pridružení uzatvorených v súvislosti s účasťou týchto krajín na programe Digitálna Európa.

2. Podpora z rezervy EÚ na účely kybernetickej bezpečnosti musí byť v súlade s týmto nariadením a so všetkými osobitnými podmienkami stanovenými v dohodách o pridružení uvedených v odseku 1.

3. Medzi používateľov z pridružených tretích krajín oprávnených prijímať služby z rezervy EÚ na účely kybernetickej bezpečnosti patria príslušné orgány, napríklad jednotky CSIRT a orgány pre riadenie kybernetických kríz.

4. Každá tretia krajina, ktorá je oprávnená prijímať podporu z rezervy EÚ na účely kybernetickej bezpečnosti, určí orgán, ktorý má konať ako jednotné kontaktné miesto na účely tohto nariadenia.

5. Pred prijatím akejkoľvek podpory z rezervy EÚ na účely kybernetickej bezpečnosti tretie krajiny poskytujú Komisii a vysokému predstaviteľovi informácie o svojej kybernetickej odolnosti a spôsobilostiach v oblasti riadenia rizík, a to prinajmenšom vrátane informácií o vnútroštátnych opatreniach prijatých s cieľom pripraviť sa na významné alebo rozsiahle kybernetické incidenty, ako aj informácií o zodpovedných vnútroštátnych subjektoch vrátane jednotiek CSIRT alebo rovnocenných subjektov, o ich spôsobilostiach a zdrojoch, ktoré sú im pridelené. V prípadoch, keď sa ustanovenia článkov 13 a 14 tohto nariadenia vzťahujú na členské štáty, uplatňujú sa na tretie krajiny, ako sa stanovuje v odseku 1.

6. Pokiaľ ide o prijaté žiadosti a vykonávanie podpory priznanej tretím krajinám z rezervy EÚ na účely kybernetickej bezpečnosti, postupuje Komisia v koordinácii s vysokým predstaviteľom.

Kapitola IV

MECHANIZMUS PRESKÚMANIA KYBERNETICKÝCH INCIDENTOV

Článok 18

Mechanizmus preskúmania kybernetických incidentov

1. Na žiadosť Komisie, siete EU-CyCLONe alebo siete jednotiek CSIRT agentúra ENISA preskúma a posúdi hrozby, zraniteľnosti a zmierňujúce opatrenia, pokiaľ ide o konkrétny významný alebo rozsiahly kybernetický incident. Po dokončení preskúmania a posúdenia incidentu predloží agentúra ENISA správu o preskúmaní incidentu sieti jednotiek CSIRT, sieti EU-CyCLONe a Komisii s cieľom podporiť ich pri plnení ich úloh, najmä so zreteľom na úlohy stanovené v článkoch 15 a 16 smernice (EÚ) 2022/2555. V prípade potreby Komisia správu poskytne vysokému predstaviteľovi.

2. S cieľom vypracovať správu o preskúmaní incidentu uvedenú v odseku 1 agentúra ENISA spolupracuje so všetkými príslušnými zainteresovanými stranami vrátane zástupcov členských štátov, Komisie a iných relevantných inštitúcií, orgánov a agentúr EÚ, poskytovateľov riadených bezpečnostných služieb a používateľov služieb v oblasti kybernetickej bezpečnosti. V prípade potreby agentúra ENISA spolupracuje aj so subjektmi zasiahnutými významnými alebo rozsiahlymi kybernetickými incidentmi. Na podporu preskúmania môže agentúra ENISA uskutočniť konzultácie aj s ďalšími druhmi zainteresovaných strán. Zástupcovia, s ktorými sa uskutočňujú konzultácie, oznámia každý potenciálny konflikt záujmov.

3. Súčasťou správy je preskúmanie a analýza konkrétneho významného alebo rozsiahleho kybernetického incidentu vrátane hlavných príčin, zraniteľností a získaných poznatkov. Dôverné informácie sa v nej chránia v súlade s právom Únie alebo vnútroštátnym právom v oblasti ochrany citlivých alebo utajovaných skutočností.

4. Podľa potreby sa v správe uvádzajú odporúčania na zlepšenie prístupu Únie ku kybernetickej bezpečnosti.

5. Ak je to možné, zverejní sa verzia tejto správy. Táto verzia obsahuje len verejné informácie.

Kapitola V

ZÁVEREČNÉ USTANOVENIA

Článok 19

Zmeny nariadenia (EÚ) 2021/694

Nariadenie (EÚ) 2021/694 sa mení takto:

1. Článok 6 sa mení takto:

a) Odsek 1 sa mení takto:

1. Vkladá sa toto písmeno aa):

„aa) podpora rozvoja kybernetického štítu EÚ vrátane rozvoja, nasadenia a prevádzky platforiem vnútroštátnych a cezhraničných centier bezpečnostných operácií, ktoré prispievajú k situačnej informovanosti v Únii a k zlepšovaniu spôsobilostí Únie v oblasti spravodajských informácií o kybernetických hrozbách;“;

2. Dopĺňa sa toto písmeno g):

„g) zriadenie a prevádzkovanie mechanizmu na riešenie kybernetických núdzových situácií s cieľom podporovať členské štáty pri príprave na významné kybernetické incidenty a pri reakcii na ne, a to doplnkovo k vnútroštátnym zdrojom a spôsobilostiam a ďalším formám podpory dostupným na úrovni Únie vrátane vytvorenia rezervy EÚ na účely kybernetickej bezpečnosti.“;

a) Odsek 2 sa nahrádza takto:

„2. Akcie v rámci špecifického cieľa 3 sa vykonávajú v prvom rade prostredníctvom Európskeho centra priemyselných, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti a siete národných koordinačných centier v súlade s nariadením Európskeho parlamentu a Rady (EÚ) 2021/887[20] s výnimkou akcií, ktorými sa vykonáva rezerva EÚ na účely kybernetickej bezpečnosti, ktoré vykonáva Komisia a agentúra ENISA.“

2. Článok 9 sa mení takto:

a) V odseku 2 sa písmená b), c) a d) nahrádzajú takto:

„b) 1 776 956 000 EUR na špecifický cieľ 2 – Umelá inteligencia;

c) 1 629 566 000 EUR na špecifický cieľ 3 – Kybernetická bezpečnosť a dôvera;

d) 482 347 000 EUR na špecifický cieľ 4 – Pokročilé digitálne zručnosti;“;

b) Dopĺňa sa tento odsek 8:

„8. Odchylne od článku 12 ods. 4 nariadenia (EÚ, Euratom) 2018/1046 sa nepoužité viazané a platobné rozpočtové prostriedky na akcie, ktorými sa sledujú ciele stanovené v článku 6 ods. 1 písm. g) tohto nariadenia, automaticky prenesú a môžu sa viazať a vyplatiť do 31. decembra nasledujúceho rozpočtového roka.“

3. V článku 14 sa odsek 2 nahrádza takto:

[20] Nariadenie Európskeho parlamentu a Rady (EÚ) 2021/887 z 20. mája 2021, ktorým sa zriaďuje Európske centrum priemyselných, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti a sieť národných koordinačných centier (Ú. v. EÚ L 202, 8.6.2021, s. 1 – 31).

„2. Z programu sa môže poskytovať financovanie v akejkoľvek forme stanovenej v nariadení o rozpočtových pravidlách, primárne najmä prostredníctvom verejného obstarávania alebo formou grantov a cien.

Ak si dosiahnutie cieľa akcie vyžaduje obstarávanie inovačného tovaru a služieb, granty sa môžu udeliť len prijímateľom, ktorí sú verejnými obstarávateľmi alebo obstarávateľmi, ako sa vymedzujú v smerniciach Európskeho parlamentu a Rady 2014/24/EÚ[27] a 2014/25/EÚ[28].

Ak je na dosiahnutie cieľov akcie potrebné dodanie inovačného tovaru alebo služieb, ktoré ešte nie sú vo veľkom rozsahu dostupné na komerčnom základe, verejný obstarávateľ alebo obstarávateľ môže povoliť zadanie viacerých zákaziek v rámci toho istého postupu verejného obstarávania.

Z riadne odôvodnených dôvodov verejnej bezpečnosti môže verejný obstarávateľ alebo obstarávateľ požadovať, aby sa miesto vykonávania zmluvy nachádzalo na území Únie.

Pri vykonávaní postupov obstarávania pre rezervu EÚ na účely kybernetickej bezpečnosti, ktorá bola vytvorená na základe článku 12 nariadenia (EÚ) 2023/XX, môžu Komisia a agentúra ENISA konať ako centrálna obstarávacia organizácia s cieľom vykonávať obstarávanie na účet alebo v mene tretích krajín pridružených k programu v súlade s článkom 10. Komisia a agentúra ENISA môžu konať aj ako veľkoobchodník tak, že nakupujú, skladujú a opätovne predávajú alebo darujú či prenajímajú tovar a služby uvedeným tretím krajinám. Odchylne od článku 169 ods. 3 nariadenia (EÚ) XXX/XXXX [prepracované znenie nariadenia o rozpočtových pravidlách] postačuje na udelenie mandátu konať Komisii alebo agentúre ENISA žiadosť jednej tretej krajiny.

Pri vykonávaní postupov obstarávania pre rezervu EÚ na účely kybernetickej bezpečnosti, ktorá bola vytvorená na základe článku 12 nariadenia (EÚ) 2023/XX, môžu Komisia a agentúra ENISA konať ako centrálna obstarávacia organizácia s cieľom vykonávať obstarávanie na účet alebo v mene inštitúcií, orgánov a agentúr Únie. Komisia a agentúra ENISA môžu konať aj ako veľkoobchodník tak, že nakupujú, skladujú a opätovne predávajú alebo darujú či prenajímajú tovar a služby inštitúciám, orgánom a agentúram Únie. Odchylne od článku 169 ods. 3 nariadenia (EÚ) XXX/XXXX [prepracované znenie nariadenia o rozpočtových pravidlách] postačuje na udelenie mandátu konať Komisii alebo agentúre ENISA žiadosť jednej inštitúcie, orgánu alebo agentúry Únie.

Z programu sa môže poskytovať financovanie aj vo forme finančných nástrojov v rámci operácií kombinovaného financovania.“

4. Dopĺňa sa tento článok 16a:

„V prípade akcií, ktorými sa vykonáva európsky kybernetický štít zriadený na základe článku 3 nariadenia (EÚ) 2023/XX, sa uplatňujú pravidlá stanovené v článkoch 4 a 5

nariadenia (EÚ) 2023/XX. V prípade rozporu medzi ustanoveniami tohto nariadenia a článkami 4 a 5 nariadenia (EÚ) 2023/XX majú prednosť uvedené články a uplatňujú sa na uvedené osobitné akcie.“

5. Článok 19 sa nahrádza takto:

„Granty v rámci programu sa udeľujú a riadia v súlade s hlavou VIII nariadenia o rozpočtových pravidlách a môžu pokrývať až 100 % oprávnených nákladov bez toho, aby tým bola dotknutá zásada spolufinancovania stanovená v článku 190 nariadenia o rozpočtových pravidlách. Takéto granty sa udeľujú a riadia, ako je bližšie stanovené pre každý špecifický cieľ.

Podporu vo forme grantov môže Európske centrum priemyselných, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti (ďalej len „kompetenčné centrum“) v súlade s článkom 195 ods. 1 písm. d) nariadenia o rozpočtových pravidlách udeliť vnútroštátnym centrám bezpečnostných operácií uvedeným v článku 4 nariadenia XXXX a hostiteľskému konzorciu uvedenému v článku 5 nariadenia XXXX priamo bez výzvy na predkladanie návrhov.

Podporu vo forme grantov pre mechanizmus na riešenie kybernetických núdzových situácií, ako sa stanovuje v článku 10 nariadenia XXXX, môže kompetenčné centrum v súlade s článkom 195 ods. 1 písm. d) nariadenia o rozpočtových pravidlách udeliť členským štátom priamo bez výzvy na predkladanie návrhov.

V prípade akcií uvedených v článku 10 ods. 1 písm. c) nariadenia 202X/XXXX informuje kompetenčné centrum o žiadostiach členských štátov o priame granty bez výzvy na predkladanie návrhov Komisiu a agentúru ENISA.

Na podporu vzájomnej pomoci pri reakcii na významný alebo rozsiahly kybernetický incident v zmysle vymedzenia v článku 10 písm. c) nariadenia XXXX a v súlade s článkom 193 ods. 2 druhým pododsekom písm. a) nariadenia o rozpočtových pravidlách sa v riadne odôvodnených prípadoch môžu náklady považovať za oprávnené, aj keď vznikli pred podaním žiadosti o grant.“

6. Prílohy I a II sa menia v súlade s prílohou k tomuto nariadeniu.

Článok 20

Hodnotenie

Komisia do [štyri roky od dátumu začatia uplatňovania tohto nariadenia] predloží Európskemu parlamentu a Rade správu o hodnotení a preskúmaní tohto nariadenia.

Článok 21

Postup výboru

1. Komisii pomáha koordinačný výbor programu Digitálna Európa zriadený nariadením (EÚ) 2021/694. Tento 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.

Článok 22

Nadobudnutie účinnosti

Toto nariadenie nadobúda účinnosť dvadsiatym dňom po jeho uverejnení v *Úradnom vestníku Európskej únie*.

Toto nariadenie je záväzné v celom rozsahu a priamo uplatniteľné vo všetkých členských štátoch.

V Štrasburgu

Za Európsky parlament	*Za Radu*
predsedníčka	*predseda/predsedníčka*

LEGISLATÍVNY FINANČNÝ VÝKAZ

1. RÁMEC NÁVRHU/INICIATÍVY

1.1. Názov návrhu/iniciatívy

1.2. Príslušné oblasti politiky

1.3. Návrh/iniciatíva sa týka:

1.4. Ciele

1.4.1. Všeobecné ciele

1.4.2. Špecifické ciele

1.4.3. Očakávané výsledky a vplyv

1.4.4. Ukazovatele výkonnosti

1.5. Dôvody návrhu/iniciatívy

1.5.1. Požiadavky, ktoré sa majú splniť v krátkodobom alebo dlhodobom horizonte vrátane podrobného harmonogramu prvotnej fázy vykonávania iniciatívy.

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 Únie“ hodnota vyplývajúca zo zásahu Únie, ktorá dopĺňa hodnotu, ktorú by inak vytvorili len samotné členské štáty.

1.5.3. Poznatky získané z podobných skúseností v minulosti

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

1.5.5. Posúdenie rôznych disponibilných možností financovania vrátane možnosti prerozdelenia

1.6. Trvanie a finančný vplyv návrhu/iniciatívy

1.7. Plánované metódy plnenia rozpočtu

2. OPATRENIA V OBLASTI RIADENIA

2.1. Zásady monitorovania a predkladania správ

2.2. Systémy riadenia a kontroly

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

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

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)

2.3. Opatrenia na predchádzanie podvodom a nezrovnalostiam

3. ODHADOVANÝ FINANČNÝ VPLYV NÁVRHU/INICIATÍVY

3.1. Príslušné okruhy viacročného finančného rámca a rozpočtové riadky výdavkov

3.2. Odhadovaný finančný vplyv návrhu na rozpočtové prostriedky

3.2.1. Zhrnutie odhadovaného vplyvu na operačné rozpočtové prostriedky

3.2.2. Odhadované výsledky financované z operačných rozpočtových prostriedkov

3.2.3. Zhrnutie odhadovaného vplyvu na administratívne rozpočtové prostriedky

3.2.3.1. Odhadované potreby ľudských zdrojov

3.2.4. Súlad s platným viacročným finančným rámcom

3.2.5. Príspevky od tretích strán

3.3. Odhadovaný vplyv na príjmy

1. RÁMEC NÁVRHU/INICIATÍVY

1.1. Názov návrhu/iniciatívy

Nariadenie Európskeho parlamentu a Rady, ktorým sa stanovujú opatrenia na posilnenie solidarity a kapacít v Únii na odhaľovanie kybernetických hrozieb a incidentov, prípravu a reakciu na ne

1.2. Príslušné oblasti politiky

Európa pripravená na digitálny vek

Európske strategické investície

Činnosť: Formovanie digitálnej budúcnosti Európy.

1.3. Návrh/iniciatíva sa týka:

☒ **novej akcie**

☐ **novej akcie, ktorá nadväzuje na pilotný projekt/prípravnú akciu**[33]

☐ **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. Ciele

1.4.1. Všeobecné ciele

Aktom o kybernetickej solidarite sa posilní solidarita na úrovni Únie, aby bolo možné lepšie odhaľovať kybernetické hrozby a incidenty, pripraviť sa a reagovať na ne. Jeho cieľom je:

a) posilniť spoločné odhaľovanie kybernetických hrozieb a incidentov a situačnú informovanosť o nich v EÚ;

b) posilniť pripravenosť kritických subjektov z celej EÚ a posilniť solidaritu rozvíjaním kapacít spoločnej reakcie na významné alebo rozsiahle kybernetické incidenty, a to aj sprístupnením podpory reakcie na incidenty tretím krajinám pridruženým k programu Digitálna Európa;

c) zvýšiť odolnosť Únie a prispieť k účinnej reakcii prostredníctvom skúmania a posudzovania významných alebo rozsiahlych incidentov vrátane získavania poznatkov a prípadne odporúčaní.

1.4.2. Špecifické ciele

Aktom o kybernetickej solidarite sa dosiahne súbor cieľov prostredníctvom:

a) zavedenia celoeurópskej infraštruktúry centier bezpečnostných operácií (európsky kybernetický štít) s cieľom vybudovať a posilniť spoločné spôsobilosti týkajúce sa odhaľovania a situačnej informovanosti;

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

b) vytvorenia mechanizmu na riešenie kybernetických núdzových situácií s cieľom podporiť členské štáty pri príprave na významné a rozsiahle kybernetické incidenty, pri reakcii na ne a pri okamžitom zotavení sa z nich. Podpora pri reakcii na incidenty sa sprístupní aj európskym inštitúciám, orgánom, úradom a agentúram Únie.

Finančná podpora pre tieto opatrenia bude pochádzať z programu Digitálna Európa, ktorý sa týmto legislatívnym nástrojom zmení s cieľom vytvoriť uvedené opatrenia, zabezpečiť finančnú podporu na ich rozvoj a objasniť podmienky na jej čerpanie;

c) vytvorenia európskeho mechanizmu preskúmania kybernetických incidentov na skúmanie a posudzovanie významných alebo rozsiahlych incidentov.

1.4.3. Očakávané výsledky a vplyv

Uveďte, aký vplyv by mal mať návrh/iniciatíva na prijímateľov/cieľové skupiny.

Návrh by priniesol značné prínosy rôznym zainteresovaným stranám. Európskym kybernetickým štítom sa zlepšia spôsobilosti členských štátov v oblasti odhaľovania kybernetických hrozieb. Mechanizmom na riešenie kybernetických núdzových situácií sa doplnia opatrenia členských štátov prostredníctvom núdzovej podpory určenej na pripravenosť, reakciu a okamžité zotavenie sa/obnovenie fungovania základných služieb.

Týmito opatreniami sa posilní konkurenčná pozícia priemyslu a podnikov v Európe v rámci celého digitalizovaného hospodárstva a podporí ich digitálna transformácia, a to posilnením úrovne kybernetickej bezpečnosti na digitálnom jednotnom trhu. Jeho cieľom je konkrétne zvýšenie odolnosti občanov, podnikov a subjektov pôsobiacich v kritických odvetviach alebo v odvetviach s vysokou úrovňou kritickosti voči čoraz väčším kybernetickobezpečnostným hrozbám, ktoré môžu mať zničujúce spoločenské a hospodárske dôsledky. Dosiahne sa to investíciami do nástrojov, ktorými sa podporí rýchlejšie odhaľovanie kybernetických hrozieb a incidentov a reakcia na ne, a členským štátom sa poskytne pomoc, aby sa mohli lepšie pripraviť na významné a rozsiahle kybernetické incidenty a aby na ne mohli lepšie reagovať. Podporiť by sa malo aj to, aby Európa získala silnejšie kapacity v týchto oblastiach, predovšetkým v súvislosti so zberom a analýzou údajov o kybernetických hrozbách a incidentoch.

1.4.4. Ukazovatele výkonnosti

Uveďte ukazovatele na monitorovanie pokroku a dosiahnutých výsledkov.

Na účely podpory solidarity na úrovni Únie by sa mohlo zohľadniť viacero ukazovateľov:

1. počet infraštruktúr alebo nástrojov kybernetickej bezpečnosti alebo oboje, získaných prostredníctvom spoločného verejného obstarávania;
2. počet opatrení, ktorými sa podporuje pripravenosť na kybernetické incidenty a reakcia na ne v rámci mechanizmu na riešenie kybernetických núdzových situácií.

1.5. Dôvody návrhu/iniciatívy

1.5.1. Požiadavky, ktoré sa majú splniť v krátkodobom alebo dlhodobom horizonte vrátane podrobného harmonogramu prvotnej fázy vykonávania iniciatívy.

Toto nariadenie by malo byť v plnej miere uplatniteľné krátko po prijatí, t. j dvadsiatym dňom po jeho uverejnení v *Úradnom vestníku Európskej únie*.

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 Únie“ hodnota vyplývajúca zo zásahu Únie, ktorá dopĺňa hodnotu, ktorú by inak vytvorili len samotné členské štáty.

Z výrazného cezhraničného charakteru kybernetických hrozieb vo všeobecnosti a rastúceho počtu rizík a incidentov s účinkami, ktoré presahujú hranice, odvetvia a produkty, vyplýva, že ciele tejto intervencie nemožno účinne dosiahnuť len na úrovni členských štátov a vyžaduje sa spoločný postup a solidarita na úrovni Únie. Skúsenosti z boja proti kybernetickým hrozbám vyplývajúcim z vojny proti Ukrajine spoločne s poznatkami získanými z cvičenia v oblasti kybernetickej bezpečnosti, ktoré sa uskutočnilo v rámci francúzskeho predsedníctva (EU CyCLES), ukázali, že by sa mali vypracovať konkrétne mechanizmy vzájomnej podpory, najmä spolupráce so súkromným sektorom, aby sa dosiahla solidarita na úrovni EÚ. V tejto súvislosti sa v záveroch Rady z 23. mája 2022 o vývoji prístupu Európskej únie ku kybernetickej bezpečnosti Komisia vyzýva, aby predložila návrh nového Fondu pre reakcie na núdzové situácie v oblasti kybernetickej bezpečnosti. Podpora a opatrenia na úrovni Únie na lepšie odhaľovanie kybernetickobezpečnostných hrozieb a na zvýšenie kapacít v oblasti pripravenosti a reakcie poskytujú pridanú hodnotu, pretože predchádzajú duplicite úsilia v Únii a členských štátoch. Viedli by k lepšiemu využívaniu existujúcich aktív a k väčšej koordinácii a výmene informácií o získaných poznatkoch.

1.5.3. Poznatky získané z podobných skúseností v minulosti

V súvislosti so situačnou informovanosťou a s odhaľovaním v rámci európskeho kybernetického štítu sa v rámci pracovného programu pre kybernetickú bezpečnosť programu Digitálna Európa na roky 2021 – 2022 uskutočnila výzva na vyjadrenie záujmu na spoločné obstarávanie nástrojov a infraštruktúry na zriadenie cezhraničných centier bezpečnostných operácií a výzva na granty s cieľom umožniť budovanie kapacít centier bezpečnostných operácií slúžiacich verejným a súkromným organizáciám.

Pokiaľ ide o pripravenosť a reakciu na incidenty, Komisia pripravila krátkodobý program na podporu členských štátov prostredníctvom dodatočného financovania prideleného agentúre ENISA s cieľom okamžite zvýšiť pripravenosť na závažné kybernetické incidenty a posilniť kapacity reakcie na ne. Služby, ktorých sa program týka, zahŕňajú opatrenia v oblasti pripravenosti, ako je penetračné testovanie kritických subjektov s cieľom identifikovať zraniteľnosti. Posilňujú sa aj možnosti pomoci členským štátom v prípade závažného incidentu s vplyvom na kritické subjekty. Vykonávanie tohto krátkodobého programu agentúrou ENISA v súčasnosti prebieha a už poskytlo hodnotné relevantné poznatky, ktoré sa zohľadnili pri vypracúvaní tohto nariadenia.

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

Akt o kybernetickej solidarite bude vychádzať z opatrení, ktoré v súčasnosti podporuje Únia a členské štáty, a to s cieľom zlepšiť situačnú informovanosť a odhaľovanie kybernetických hrozieb a reagovať na rozsiahle a cezhraničné kybernetické incidenty. Nástroj je navyše v súlade s ďalšími rámcami krízového riadenia vrátane mechanizmu integrovanej politickej reakcie na krízu, spoločnej bezpečnostnej a obrannej politiky vrátane tímov rýchlej kybernetickej reakcie, ako aj s pomocou poskytnutou jedným členským štátom inému členskému štátu v kontexte článku 42 ods. 7 Zmluvy o Európskej únii. Novým návrhom sa takisto dopĺňajú a podporujú štruktúry vytvorené v rámci ďalších nástrojov v oblasti kybernetickej bezpečnosti, napríklad smernice (EÚ) 2022/2555 (smernica NIS 2) alebo nariadenia 2019/881 (akt o kybernetickej bezpečnosti).

1.5.5. Posúdenie rôznych disponibilných možností financovania vrátane možnosti prerozdelenia

Riadenie oblastí činnosti pridelených agentúre ENISA sa zhoduje s jej existujúcim mandátom a všeobecnými úlohami. Tieto oblasti činnosti si môžu vyžadovať osobitné profily alebo nové úlohy, ktoré sa však dajú zvládnuť s existujúcimi zdrojmi agentúry ENISA a vyriešiť presunom alebo prepojením rôznych úloh. Agentúra ENISA v súčasnosti vykonáva krátkodobý program, ktorý Komisia zriadila v roku 2022 s cieľom okamžite zvýšiť pripravenosť na závažné kybernetické incidenty a posilniť kapacity reakcie na ne. Medzi služby, ktorých sa program týka, patria možnosti pomoci členským štátom v prípade závažného incidentu s vplyvom na kritické subjekty. Vykonávanie tohto krátkodobého programu agentúrou ENISA v súčasnosti prebieha a už poskytlo hodnotné relevantné poznatky, ktoré sa zohľadnili pri vypracúvaní tohto nariadenia. Zdroje pridelené na tento krátkodobý program by sa mohli použiť aj v kontexte tohto nariadenia.

1.6. Trvanie a finančný vplyv návrhu/iniciatívy

☒ **Obmedzené trvanie**

– ☒ S účinnosťou od dátumu prijatia návrhu nariadenia Európskeho parlamentu a Rady, ktorým sa stanovujú opatrenia na posilnenie solidarity a kapacít v Únii na odhaľovanie kybernetických hrozieb a incidentov, prípravu a reakciu na ne (ďalej len „akt o kybernetickej solidarite“),

– ☒ finančný vplyv na viazané rozpočtové prostriedky od roku 2023 do roku 2027 a na platobné rozpočtové prostriedky od roku 2023 do roku 2031[34].

☐ **Neobmedzené trvanie**

– Počiatočná fáza vykonávania bude trvať od RRRR do RRRR,

– potom bude implementácia pokračovať v plnom rozsahu.

1.7. Plánované metódy plnenia rozpočtu[35]

☒ **Priame riadenie** na úrovni Komisie

– ☒ prostredníctvom jej útvarov vrátane zamestnancov v delegáciách Únie,

– ☐ prostredníctvom výkonných agentúr.

☐ **Zdieľané riadenie** s členskými štátmi

☒ **Nepriame riadenie**, pri ktorom sa plnením rozpočtu poveria:

– ☐ tretie krajiny alebo subjekty, ktoré tieto krajiny určili,

– ☐ medzinárodné organizácie a ich agentúry (uveďte),

– ☐ Európska investičná banka (EIB) a Európsky investičný fond,

– ☒ subjekty uvedené v článkoch 70 a 71 nariadenia o rozpočtových pravidlách,

– ☐ verejnoprávne subjekty,

– ☐ súkromnoprávne subjekty poverené vykonávaním verejnej služby, pokiaľ sú im poskytnuté primerané finančné záruky,

– ☐ súkromnoprávne subjekty spravované právom členského štátu, ktoré sú poverené vykonávaním verejno-súkromného partnerstva a ktorým sú poskytnuté primerané finančné záruky,

– ☐ subjekty alebo osoby poverené vykonávaním osobitných akcií v oblasti SZBP podľa hlavy V Zmluvy o Európskej únii a určené v príslušnom základnom akte.

– *V prípade viacerých spôsobov riadenia uveďte v oddiele „Poznámky“ presnejšie vysvetlenie.*

Poznámky

Opatrenia týkajúce sa európskeho kybernetického štítu bude vykonávať kompetenčné centrum. Kým bude mať kompetenčné centrum kapacity na plnenie svojho vlastného rozpočtu, opatrenia bude v mene kompetenčného centra vykonávať Európska komisia v rámci priameho riadenia. Kompetenčné centrum môže na základe výziev na vyjadrenie záujmu

[34] Opatrenia v akte by sa mali podporiť v nasledujúcom viacročnom finančnom rámci.

[35] Vysvetlenie metód plnenia rozpočtu a odkazy na nariadenie o rozpočtových pravidlách sú k dispozícii na webovom sídle BUDGpedia: https://myintracomm.ec.europa.eu/corp/budget/financial-rules/budget-implementation/Pages/implementation-methods.aspx.

vybrať subjekty, aby sa zúčastnili na spoločnom obstarávaní nástrojov. Kompetenčné centrum môže udeľovať granty na prevádzku týchto nástrojov.

Kompetenčné centrum môže okrem toho udeľovať granty na opatrenia v oblasti pripravenosti v rámci mechanizmu na riešenie kybernetických núdzových situácií.

Celkovú zodpovednosť za vykonávanie rezervy EÚ na účely kybernetickej bezpečnosti nesie Komisia. Komisia môže prevádzku a správu rezervy EÚ na účely kybernetickej bezpečnosti úplne alebo sčasti zveriť agentúre ENISA, a to prostredníctvom dohôd o príspevku. Opatrenia tohto nariadenia zverené agentúre ENISA sú v súlade s jej existujúcim mandátom. Medzi tieto opatrenia patrí: i) podpora skupiny pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti pri vývoji opatrení v oblasti pripravenosti podľa posúdení rizík; ii) podpora Komisie pri vytváraní rezervy EÚ na účely kybernetickej bezpečnosti a pri dohľade nad jej vykonávaním vrátane prijímania a spracúvania žiadostí o podporu; iii) vypracovanie vzorov na uľahčenie predkladania žiadostí o podporu a osobitných dohôd uzatváraných medzi poskytovateľom služieb a používateľom, ktorému sa podpora v rámci rezervy EÚ na účely kybernetickej bezpečnosti poskytuje; iv) preskúmanie a posúdenie hrozieb, zraniteľností a zmierňujúcich opatrení vzhľadom na konkrétny významný alebo rozsiahly kybernetický incident a vypracovanie súvisiacich správ.

Na všetky tieto úlohy sa odhaduje potreba siedmich ekvivalentov plného pracovného času z existujúcich zdrojov agentúry ENISA, pričom sa už vychádza z odborných znalostí a prípravných prác, ktoré agentúra ENISA v súčasnosti vykonáva v rámci pilotného projektu núdzovej podpory na účely pripravenosti a reakcie na incidenty.

2. OPATRENIA V OBLASTI RIADENIA

2.1. Zásady monitorovania a predkladania správ

Uveďte frekvenciu a podmienky, ktoré sa vzťahujú na tieto opatrenia.

Na účely posúdenia účinnosti týchto nových ustanovení bude Komisia monitorovať ich vykonávanie, uplatňovanie a dodržiavanie. Komisia do štyroch rokov od dátumu uplatňovania tohto nariadenia predloží Európskemu parlamentu a Rade správu o jeho hodnotení a preskúmaní.

2.2. Systémy riadenia a kontroly

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

Nariadením sa zavádza rámec na vykonávanie financovania z prostriedkov EÚ s cieľom zvýšiť odolnosť v oblasti kybernetickej bezpečnosti prostredníctvom opatrení, ktorými sa zlepšujú spôsobilosti v oblasti odhaľovania, reakcie a zotavenia sa v prípade významných a rozsiahlych kybernetických incidentov. Vykonávanie tejto smernice budú riadiť oddelenia v rámci GR CNECT, ktoré sú zodpovedné za danú oblasť politiky.

Na tieto nové úlohy je potrebné vybaviť útvary Komisie primeranými zdrojmi. Odhaduje sa, že presadzovanie nového nariadenia si vyžiada šesť ekvivalentov plného pracovného času (traja administrátori a traja zmluvní zamestnanci) na plnenie týchto úloh:

- určenie opatrení v oblasti pripravenosti podľa posúdení rizík,
- zaistenie interoperability medzi platformami cezhraničných centier bezpečnostných operácií,
- vypracovanie potenciálnych vykonávacích aktov (dvoch pre centrá bezpečnostných operácií a dvoch pre mechanizmus na riešenie kybernetických núdzových situácií),
- spravovanie dohôd o poskytovaní hostiteľských služieb a o používaní pre centrá bezpečnostných operácií,
- vytvorenie a spravovanie rezervy EÚ na účely kybernetickej bezpečnosti priamo alebo prostredníctvom dohody o príspevku pre agentúru ENISA. V prípade dohody o príspevku pre agentúru ENISA vypracovanie dohody o príspevku a dohľad nad jej plnením v súvislosti s úlohami, ktoré sú zverené agentúre ENISA,
- účasť v konzultačných skupinách zriadených agentúrou ENISA s cieľom preskúmať a posúdiť významné a rozsiahle kybernetické incidenty a príprava správ.

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

V súvislosti s európskym kybernetickým štítom je identifikované riziko, že členské štáty si nevymieňajú dostatočné množstvo relevantných informácií o kybernetických hrozbách buď v rámci platforiem cezhraničných centier bezpečnostných operácií, alebo medzi platformami cezhraničných centier bezpečnostných operácií a ďalšími

príslušnými subjektmi na úrovni EÚ. S cieľom zmierniť tieto riziká bude pridelenie finančného krytia nasledovať po výzve na vyjadrenie záujmu, v ktorej sa členské štáty zaviažu zdieľať určité množstvo informácií s úrovňou EÚ. Tento záväzok sa ďalej formalizuje v dohode o poskytovaní hostiteľských služieb a o používaní, ktorou sa kompetenčnému centru udelia právomoci vykonávať audity s cieľom uistiť sa, že sa spoločne obstarané nástroje a infraštruktúra používajú v súlade s uvedenou dohodou. Záväzky k vysokej úrovni výmeny informácií v rámci cezhraničných centier bezpečnostných operácií sa sformalizujú v dohode o konzorciu.

V súvislosti s mechanizmom na riešenie kybernetických núdzových situácií je identifikované riziko, že používatelia, ktorí sa na mechanizme zúčastňujú, neprijímajú dostatočné opatrenia na zaistenie pripravenosti voči kybernetickým útokom. Preto musia používatelia takéto opatrenia v oblasti pripravenosti prijať, aby mohli dostať podporu z rezervy EÚ na účely kybernetickej bezpečnosti. Pri predkladaní žiadostí o podporu z rezervy EÚ na účely kybernetickej bezpečnosti musia používatelia vysvetliť, aké opatrenia už prijali v rámci reakcie na incident, a toto vysvetlenie sa zohľadní pri posudzovaní žiadostí o podporu z rezervy EÚ na účely kybernetickej bezpečnosti.

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)

Pretože pravidlá účasti na programe Digitálna Európa platné pre podporu podľa aktu o kybernetickej solidarite sú podobné ako pravidlá, ktoré bude používať Komisia vo svojich pracovných programoch, a súbor prijímateľov má podobný rizikový profil ako súbor prijímateľov programov v rámci priameho riadenia, možno predpokladať, že chybovosť bude podobná ako chybovosť predpokladaná Komisiou pre program Digitálna Európa, teda že existuje primeraná istota, že riziko chyby bude v priebehu viacročného výdavkového obdobia v rozpätí 2 % – 5 % ročne, pričom konečným cieľom je dosiahnuť na záver viacročných programov zvyškovú chybovosť po zohľadnení finančného vplyvu všetkých auditov a opatrení na účely nápravy a vymáhania čo najbližšie k úrovni 2 %.

2.3. Opatrenia na predchádzanie podvodom a nezrovnalostiam

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

V prípade európskeho kybernetického štítu bude mať kompetenčné centrum v súlade s dohodou o poskytovaní hostiteľských služieb a o používaní, ktorá sa má podpísať medzi hostiteľským konzorciom a kompetenčným centrom, právomoc vykonávať audit spoločne obstaraných nástrojov a infraštruktúr, a to na základe prístupu k informáciám a kontrol na mieste.

Na dodatočné rozpočtové prostriedky potrebné pre toto nariadenie sa budú vzťahovať existujúce opatrenia na predchádzanie podvodom uplatniteľné na inštitúcie, orgány a agentúry Únie.

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[36]	krajín EZVO[37]	kandidátskych krajín a potenciálnych kandidátov[38]	iných tretích krajín	iné pripísané príjmy
1	02 04 01 10 – Program Digitálna Európa – Kybernetická bezpečnosť	DRP	ÁNO	ÁNO	NIE	NIE
1	02 04 01 11 – Program Digitálna Európa – Európske centrum priemyselných, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti	DRP	ÁNO	ÁNO	NIE	NIE
1	02 04 03 – Program Digitálna Európa – Umelá inteligencia	DRP	ÁNO	ÁNO	NIE	NIE
1	02 04 04 – Program Digitálna Európa – Zručnosti	DRP	ÁNO	ÁNO	NIE	NIE
1	02 01 30 – Výdavky na podporu programu Digitálna Európa	NRP	ÁNO	ÁNO	NIE	NIE

[36] DRP = diferencované rozpočtové prostriedky/NRP = nediferencované rozpočtové prostriedky.
[37] EZVO: Európske združenie voľného obchodu.
[38] Kandidátske krajiny a prípadne potenciálne kandidátske krajiny.

3.2. Odhadovaný finančný vplyv návrhu na rozpočtové prostriedky

3.2.1. Zhrnutie odhadovaného vplyvu na operačné rozpočtové prostriedky

– ☐ Návrh/iniciatíva si nevyžaduje použitie operačných rozpočtových prostriedkov.

– ☒ Návrh/iniciatíva si vyžaduje použitie operačných rozpočtových prostriedkov, ako je uvedené v tejto tabuľke:

v mil. EUR (zaokrúhlené na tri desatinné miesta)

Okruh viacročného finančného rámca	Číslo	1 **Jednotný trh, inovácie a digitálna ekonomika**

Návrhom sa nezvýši celková úroveň záväzkov na základe programu Digitálna Európa. Príspevok k tejto iniciatíve v skutočnosti predstavuje prerozdelenie záväzkov zo špecifických cieľov 2 a 4 na posilnenie rozpočtu špecifického cieľa 3 a kompetenčného centra. Na účely tejto iniciatívy by sa mohlo použiť každé zvýšenie záväzkov na základe programu Digitálna Európa vyplývajúce z revízie VFR.

GR CONNECT			Rok **2025**	Rok **2026**	Rok **2027**	Rok **2028+**	Uveďte všetky roky, počas ktorých vplyv trvá (pozri bod 1.6)			**SPOLU**
○ Operačné rozpočtové prostriedky										
Rozpočtový riadok[39] 02.040110 (prerozdelenie z riadku 02.0403 a 02.0404)	Záväzky	1a	15,000	15,000	6,000	p.m.				**36,000**
	Platby	2a	15,000	15,000	6,000					**36,000**
Rozpočtový riadok 02.040111.02 (prerozdelenie z riadku 02.0403 a 02.0404)	Záväzky	1b	13,000	23,000	28,000	p.m.				**64,000**
	Platby	2b	8,450	18,200	25,250	12,100				**64,000**
Administratívne rozpočtové prostriedky financované z finančného krytia na vykonávanie osobitných programov[40]										
Rozpočtový riadok 02.0130		3	0,150	0,150	0,150	p.m.				0,450

[39] Podľa oficiálnej rozpočtovej nomenklatúry.

[40] Technická a/alebo administratívna pomoc a výdavky na podporu vykonávania programov a/alebo akcií Európskej únie (pôvodné rozpočtové riadky „BA“), nepriamy výskum, priamy výskum.

Rozpočtové prostriedky za GR pre komunikačné siete, obsah a technológie SPOLU	Záväzky	= 1a + 1b + 3	**28,150**	**38,150**	**34,150**	**p.m.**				**100,450**
	Platby	= 2a + 2b + 3	**23,600**	**33,350**	**31,400**	**12,100**				**100,450**

○Operačné rozpočtové prostriedky SPOLU	Záväzky	4	28,000	38,000	34,000	p.m.				**100,000**
	Platby	5	23,450	33,200	31,250	12,100				**100,000**
○ Administratívne rozpočtové prostriedky financované z finančného krytia na vykonávanie osobitných programov SPOLU		6	0,150	0,150	0,150	p.m.				**0,450**
Rozpočtové prostriedky OKRUHU 1 viacročného finančného rámca **SPOLU**	Záväzky	= 4 + 6	**28,150**	**38,150**	**34,150**	**p.m.**				**100,450**
	Platby	= 5 + 6	**23,600**	**33,350**	**31,400**	**12,100**				**100,450**

Ak má návrh/iniciatíva vplyv na viaceré operačné okruhy, zopakujte oddiel uvedený vyššie:

○ Operačné rozpočtové prostriedky SPOLU (všetky operačné okruhy)	Záväzky	4	28,000	38,000	34,000	p.m.				**100,000**
	Platby	5	23,450	33,200	31,250	12,100				**100,000**
Administratívne rozpočtové prostriedky financované z finančného krytia na vykonávanie osobitných programov SPOLU (všetky operačné okruhy)		6	0,150	0,150	0,150					**0,450**
Rozpočtové prostriedky OKRUHOV 1 až 6 viacročného finančného rámca **SPOLU** (referenčná suma)	Záväzky	= 4 + 6	**28,150**	**38,150**	**34,150**	**p.m.**				**100,450**
	Platby	= 5 + 6	**23,600**	**33,350**	**31,400**	**12,100**				**100,450**

Okruh viacročného finančného rámca	7	„Administratívne výdavky“

Tento oddiel treba vyplniť s použitím rozpočtových údajov administratívnej povahy, ktoré sa najprv uvedú v prílohe k legislatívnemu finančnému výkazu (príloha 5 k rozhodnutiu Komisie o interných pravidlách plnenia oddielu všeobecného rozpočtu Európskej únie týkajúceho sa Komisie), ktorá sa na účely medziútvarovej konzultácie nahrá do aplikácie DECIDE.

v mil. EUR (zaokrúhlené na tri desatinné miesta)

		Rok **2025**	Rok **2026**	Rok **2027**	Rok **2028+**	Uveďte všetky roky, počas ktorých vplyv trvá (pozri bod 1.6)			**SPOLU**
GR: Generálne riaditeľstvo pre komunikačné siete, obsah a technológie									
○ Ľudské zdroje		0,786	0,786	0,786	p.m.				**2,358**
○ Ostatné administratívne výdavky		0,035	0,035	0,035	p.m.				**0,105**
GENERÁLNE RIADITEĽSTVO PRE KOMUNIKAČNÉ SIETE, OBSAH A TECHNOLÓGIE SPOLU	Rozpočtové prostriedky	**0,821**	**0,821**	**0,821**					**2,463**

Rozpočtové prostriedky OKRUHU 7 viacročného finančného rámca **SPOLU**	(Záväzky spolu = Platby spolu)	**0,821**	**0,821**	**0,821**					**2,463**

v mil. EUR (zaokrúhlené na tri desatinné miesta)

		Rok **2025**	Rok **2026**	Rok **2027**	Rok **2028+**	Uveďte všetky roky, počas ktorých vplyv trvá (pozri bod 1.6)			**SPOLU**
Rozpočtové prostriedky OKRUHOV 1 až 7	Záväzky	**28,971**	**38,971**	**34,971**	**p.m.**				**102,913**
	Platby	**24,421**	**34,171**	**32,221**	**12,100**				**102,913**

viacročného finančného rámca **SPOLU**										

3.2.2. Odhadované výsledky financované z operačných rozpočtových prostriedkov

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

Uveďte ciele a výstupy			Rok **N**		Rok **N + 1**		Rok **N + 2**		Rok **N + 3**		Uveďte všetky roky, počas ktorých vplyv trvá (pozri bod 1.6)						**SPOLU**	
	VÝSTUPY																	
⇩	Druh[41]	Priemerné náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet spolu	Náklady spolu
ŠPECIFICKÝ CIEĽ č. 1[42]…																		
– Výstup																		
– Výstup																		
– Výstup																		
Špecifický cieľ č. 1 medzisúčet																		
ŠPECIFICKÝ CIEĽ č. 2 …																		
– Výstup																		
Špecifický cieľ č. 2 medzisúčet																		
SPOLU																		

[41] Výstupy sú produkty, ktoré sa majú dodať, a služby, ktoré sa majú poskytnúť (napr.: počet financovaných výmen študentov, vybudované cesty v km atď.).

[42] Ako je uvedené v bode 1.4.2. „Špecifické ciele…“

3.2.3. 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 tri desatinné miesta)

	Rok 2025	Rok r 2026	Rok 2027	Rok N + 3	Uveďte všetky roky, počas ktorých vplyv trvá (pozri bod 1.6)			**SPOLU**
OKRUH 7 viacročného finančného rámca								
Ľudské zdroje	0,786	0,786	0,786					**2,358**
Ostatné administratívne výdavky	0,035	0,035	0,035					**0,105**
Medzisúčet OKRUHU 7 viacročného finančného rámca	**0,821**	**0,821**	**0,821**					**2,463**

Mimo OKRUHU 7[43] viacročného finančného rámca								
Ľudské zdroje								
Ostatné administratívne výdavky	0,150	0,150	0,150					**0,450**
Medzisúčet mimo OKRUHU 7 viacročného finančného rámca	**0,150**	**0,150**	**0,150**					**0,450**

SPOLU	**0,971**	**0,971**	**0,971**					**2,913**

Rozpočtové prostriedky potrebné na ľudské zdroje a 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 prideľovania zdrojov a v závislosti od rozpočtových obmedzení.

[43] Technická a/alebo administratívna pomoc a výdavky na podporu vykonávania programov a/alebo akcií Európskej únie (pôvodné rozpočtové riadky „BA“), nepriamy výskum, priamy výskum.

3.2.3.1. Odhadované potreby ľudských zdrojov

– ☐ Návrh/iniciatíva si nevyžaduje použitie ľudských zdrojov.

– ☒ Návrh/iniciatíva si vyžaduje použitie týchto ľudských zdrojov:

odhady sa vyjadrujú v jednotkách ekvivalentu plného pracovného času

		Rok **2025**	Rok **2026**	Rok 2027	Rok **N + 3**	Uveďte všetky roky, počas ktorých vplyv trvá (pozri bod 1.6)		
O Plán pracovných miest (úradníci a dočasní zamestnanci)								
20 01 02 01 (ústredie a zastúpenia Komisie)		3	3	3				
20 01 02 03 (delegácie)								
01 01 01 01 (nepriamy výskum)								
01 01 01 11 (priamy výskum)								
Iné rozpočtové riadky (uveďte)								
O Externí zamestnanci (ekvivalent plného pracovného času)[44]								
20 02 01 (ZZ, VNE, DAZ z celkového finančného krytia)		3	3	3				
20 02 03 (ZZ, MZ, VNE, DAZ, PED v delegáciách)								
XX 01 xx **yy zz**[45]	– ústredie							
	– delegácie							
01 01 01 02 (ZZ, DAZ, VNE – nepriamy výskum)								
01 01 01 12 (ZZ, VNE, DAZ – priamy výskum)								
Iné rozpočtové riadky (uveďte)								
SPOLU		**6**	**6**	**6**				

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 prerozdelení v rámci GR, a v prípade potreby budú doplnené zdrojmi, ktoré sa môžu prideliť riadiacemu GR v rámci ročného postupu prideľovania zdrojov a v závislosti od rozpočtových obmedzení.

Opis úloh, ktoré sa majú vykonať:

Úradníci a dočasní zamestnanci	– určenie opatrení v oblasti pripravenosti podľa posúdení rizík (článok 11), – vypracovanie potenciálnych vykonávacích aktov (dvoch pre centrá bezpečnostných operácií a dvoch pre mechanizmus na riešenie kybernetických núdzových situácií), – spravovanie dohôd o poskytovaní hostiteľských služieb a o používaní pre centrá bezpečnostných operácií, – vytvorenie a spravovanie rezervy EÚ na účely kybernetickej bezpečnosti priamo alebo prostredníctvom dohody o príspevku pre agentúru ENISA.
Externí zamestnanci	Pod dohľadom úradníka – určenie opatrení v oblasti pripravenosti podľa posúdení rizík (článok 11), – vypracovanie potenciálnych vykonávacích aktov (dvoch pre centrá bezpečnostných operácií a dvoch pre mechanizmus na riešenie kybernetických núdzových situácií), – spravovanie dohôd o poskytovaní hostiteľských služieb a o používaní pre

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

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

	centrá bezpečnostných operácií, – vytvorenie a spravovanie rezervy EÚ na účely kybernetickej bezpečnosti priamo alebo prostredníctvom dohody o príspevku pre agentúru ENISA.

3.2.4. *Súlad s platným viacročným finančným rámcom*

Návrh/iniciatíva:

– [X] môže byť v plnej miere financovaná prerozdelením v rámci príslušného okruhu viacročného finančného rámca (VFR).

Vysvetlite požadované preprogramovanie a uveďte príslušné rozpočtové riadky a zodpovedajúce sumy. V prípade väčšieho preprogramovania poskytnite tabuľku vo formáte Excel.

	23	24	25	26	27	spolu
ŠC 1	16 232 897	20 528 765	17 406 899	16 223 464	10 022 366	80 414 391
Počiatočný stav ŠC 2	226 316 819	295 067 000	195 649 000	221 809 000	246 608 000	1 185 449 819
Na iniciatívu CYBER			18 000 000	28 000 000	19 000 000	65 000 000
NOVÝ ŠC 2	**226 316 819**	**295 067 000**	**177 649 000**	**193 809 000**	**227 608 000**	**1 120 449 819**
ŠC 3 DB 24	24 361 553	35 596 172	3 638 000	3 638 000	11 175 000	78 408 725
Zo ŠC 2 – ŠC 4			15 000 000	15 000 000	6 000 000	36 000 000
NOVÝ ŠC 3	**24 361 553**	**35 596 172**	**18 638 000**	**18 638 000**	**17 175 000**	**114 408 725**
Počiatočný stav – kompetenčné centrum	176 222 303	208 374 879	104 228 130	90 704 986	84 851 497	664 381 795
Zo ŠC 2 – ŠC 4			13 000 000	23 000 000	28 000 000	64 000 000
Nové – kompetenčné centrum	**176 222 303**	**208 374 879**	**117 228 130**	**113 704 986**	**112 851 497**	**728 381 795**
Počiatočný stav ŠC 4	66 902 708	64 892 032	56 577 977	70 477 245	72 107 201	330 957 163
Na iniciatívu CYBER			10 000 000	10 000 000	15 000 000	35 000 000
NOVÝ ŠC 4	**66 902 708**	**64 892 032**	**46 577 977**	**60 477 245**	**57 107 201**	**295 957 163**

– [ ] si vyžaduje použitie nepridelenej rezervy v rámci príslušného okruhu VFR a/alebo použitie osobitných nástrojov vymedzených v nariadení o VFR.

Vysvetlite potrebu a uveďte príslušné okruhy, rozpočtové riadky, zodpovedajúce sumy a nástroje, ktorých použitie sa navrhuje.

– [ ] si vyžaduje revíziu VFR.

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

3.2.5. *Príspevky od tretích strán*

Návrh/iniciatíva:

– [X] nezahŕňa spolufinancovanie tretími stranami,

– [ ] zahŕňa spolufinancovanie tretími stranami, ako je odhadnuté v nasledujúcej tabuľke:

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

	Rok **N**[46]	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								

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

3.3. Odhadovaný vplyv na príjmy

– ☒ Návrh/iniciatíva nemá finančný vplyv na príjmy.

– ☐ Návrh/iniciatíva má tento finančný vplyv:

  – ☐ vplyv na vlastné zdroje,

  – ☐ vplyv na iné príjmy,

  – uveďte, či sú príjmy pripísané rozpočtovým riadkom výdavkov.

v mil. EUR (zaokrúhlené na tri desatinné miesta)

Rozpočtový riadok príjmov:	Rozpočtové prostriedky k dispozícii v bežnom rozpočtovom roku	Vplyv návrhu/iniciatívy[47]						
		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 pripísaných príjmov uveďte ovplyvnené rozpočtové riadky výdavkov.

[…]

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

[…]

[47] 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.