EURÓPSKA ÚNIA

EURÓPSKY PARLAMENT **RADA**

V Bruseli 19. decembra 2024
(OR. en)

2023/0109(COD)
LEX 2422

PE-CONS 94/1/24
REV 1

CYBER 208
TELECOM 218
CADREFIN 109
FIN 595
BUDGET 47
IND 328
JAI 1084
MI 633
DATAPROTECT 247
RELEX 881
CODEC 1588

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 A KTORÝM SA MENÍ NARIADENIE (EÚ) 2021/694 (AKT O KYBERNETICKEJ SOLIDARITE)

NARIADENIE EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2024/...

z 19. decembra 2024,

ktorým sa stanovujú opatrenia na posilnenie solidarity a kapacít v Únii na odhaľovanie kybernetických hrozieb a incidentov, prípravu a reakciu na ne a ktorým sa mení nariadenie (EÚ) 2021/694 (akt o kybernetickej solidarite)

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[4],

---

1 Stanovisko z 18. apríla 2023 (zatiaľ neuverejnené v úradnom vestníku).
2 Ú. v. EÚ C 349, 29.9.2023, s. 167.
3 Ú. v. EÚ C, C/2024/1049, 9.2.2024, ELI: http://data.europa.eu/eli/C/2024/1049/oj.
4 Pozícia Európskeho parlamentu z 24. apríla 2024 (zatiaľ neuverejnená v úradnom vestníku) a rozhodnutie Rady z 2. decembra 2024.

keďže:

(1) So zvyšovaním miery prepojenia a vzájomnej závislosti orgánov verejnej správy členského štátu, podnikov a občanov bez ohľadu na hranice a odvetvia hospodárstva stúpa význam používania informačných a komunikačných technológií a závislosti od nich vo všetkých odvetviach hospodárskej činnosti a spoločnosti, pričom zároveň vznikajú nové zraniteľnosti.

(2) Rozsah, frekvencia a dosah kybernetických bezpečnostných incidentov vrátane útokov na dodávateľský reťazec na účely kybernetickej špionáže, ransomware alebo narušenia sa v celej Únii, ako aj na globálnej úrovni, zvyšujú. Tieto incidenty predstavujú závažnú hrozbu pre fungovanie sietí a informačných systémov. Hrozba možných rozsiahlych kybernetických bezpečnostných incidentov, ktoré by mohli významne narušiť alebo poškodiť kritické infraštruktúry, si vzhľadom na rýchly vývoj situácie v oblasti hrozieb vyžaduje vyššiu mieru pripravenosti rámca kybernetickej bezpečnosti v Únii. Táto hrozba nevyplýva len z útočnej vojny Ruska proti Ukrajine a vzhľadom na veľký počet aktérov, ktorí sa podieľajú na aktuálnom geopolitickom napätí, môže pretrvávať. Takéto incidenty môžu zabraňovať poskytovaniu verejných služieb, keďže kybernetické útoky sú často zamerané na miestne, regionálne alebo vnútroštátne verejné služby a infraštruktúru, pričom miestne orgány sú obzvlášť zraniteľné, a to aj z dôvodu ich obmedzených zdrojov. Môžu taktiež zabraňovať realizácii hospodárskych činností v odvetviach s vysokou úrovňou kritickosti alebo v iných kritických odvetviach, spôsobovať značné finančné straty, narúšať dôveru používateľa, spôsobovať značné škody na hospodárstve a na demokratických systémoch Únie a dokonca by mohli mať zdravie alebo život ohrozujúce dôsledky. Kybernetické bezpečnostné incidenty sú navyše nepredvídateľné, keďže často vznikajú a vyvíjajú sa rýchlo, nie sú obmedzené na konkrétnu geografickú oblasť a vyskytujú sa súčasne v mnohých krajinách alebo sa v nich ihneď rozširujú. Je potrebná úzka spolupráca medzi verejným sektorom, súkromným sektorom, akademickou obcou, občianskou spoločnosťou a médiami.

(3) Je nevyhnutné posilniť konkurenčné postavenie priemyslu a služieb v Únii v rámci celého digitálneho 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. Je nevyhnutné zvýšiť odolnosť občanov, podnikov vrátane mikropodnikov, malých a stredných podnikov a startupov, a subjektov pôsobiacich v kritickej infraštruktúre voči rastúcim kybernetickým hrozbám, ktoré môžu mať zničujúci spoločenský a hospodársky dôsledok. Sú preto potrebné investície do infraštruktúry a služieb a do budovania spôsobilostí na rozvíjanie zručností v oblasti kybernetickej bezpečnosti, ktorými sa podporí rýchlejšie odhaľovanie kybernetických hrozieb a incidentov a rýchlejšia reakcia na ne. Členské štáty okrem toho potrebujú pomoc, aby sa mohli lepšie pripraviť na významné kybernetické bezpečnostné incidenty a rozsiahle kybernetické bezpečnostné incidenty a dokázali na ne lepšie reagovať, ako aj pomoc pri počiatočnom zotavení sa z nich. Stavajúc na existujúcich štruktúrach a v úzkej spolupráci s nimi by Únia by takisto mala zvýšiť svoje kapacity v týchto oblastiach, najmä pokiaľ ide o zber a analýzu údajov o kybernetických hrozbách a incidentoch.

(4) Únia už prijala niekoľko opatrení na zníženie zraniteľnosti a zvýšenie odolnosti kritickej infraštruktúry a subjektov voči rizikám, najmä nariadenie Európskeho parlamentu a Rady (EÚ) 2019/881[5], smernice Európskeho parlamentu a Rady 2013/40/EÚ[6] a (EÚ) 2022/2555[7] a odporúčanie Komisie (EÚ) 2017/1584[8]. Okrem toho sa v odporúčaní Rady z 8. decembra 2022 o celoúniovom koordinovanom prístupe k posilneniu odolnosti kritickej infraštruktúry členské štáty vyzývajú, aby prijali opatrenia a spolupracovali 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 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).

6 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).

7 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).

8 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).

(5) Čoraz väčšie kybernetickobezpečnostné riziká a celkové prostredie komplexných hrozieb s jasným rizikom rýchleho presahu incidentov z jedného členského štátu do iných členských štátov a z tretej krajiny do Únie si v záujme lepšieho odhaľovania kybernetických hrozieb a incidentov, prípravy, reakcie na ne a zotavenia sa z nich vyžadujú posilnenie solidarity na úrovni Únie, najmä posilnením spôsobilostí existujúcich štruktúr. Okrem toho sa v záveroch Rady z 23. mája 2022 o vývoji prístupu Európskej Únie ku kybernetickej bezpečnosti vyzvala Komisia, aby predložila návrh nového Fondu pre reakcie na núdzové situácie v oblasti kybernetickej bezpečnosti.

(6) V spoločnom oznámení Komisie a vysokého predstaviteľa Únie pre zahraničné veci a bezpečnostnú politiku z 10. novembra 2022 Európskemu parlamentu a Rade o politike EÚ v oblasti kybernetickej obrany bola oznámená iniciatíva na podporu kybernetickej solidarity EÚ s cieľmi posilniť spoločné spôsobilosti EÚ týkajúce sa odhaľovania, situačnej informovanosti a reakcie presadzovaním zavádzania infraštruktúry centier bezpečnostných operácií v EÚ, podporovať postupné vybudovanie rezervy EÚ na účely kybernetickej bezpečnosti 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 a spôsobilostí členských štátov a Únie predchádzať významným kybernetickým bezpečnostným incidentom a rozsiahlym kybernetickým bezpečnostným incidentom a reagovať na ne. Mala by sa preto zriadiť celoeurópska sieť kybernetických centier (ďalej len „európsky systém varovania pred kybernetickobezpečnostnými hrozbami“) s cieľom vybudovať koordinované spôsobilosti týkajúce sa odhaľovania a situačnej informovanosti, posilniť spôsobilosti Únie v oblasti odhaľovania hrozieb a zdieľania informácií; mal by sa zriadiť mechanizmus na riešenie kybernetickobezpečnostných núdzových situácií s cieľom podporiť členské štáty na ich žiadosť pri príprave na významné kybernetické bezpečnostné incidenty a rozsiahle kybernetické bezpečnostné incidenty, pri reakcii na ne, zmierňovaní ich vplyvu a pri začatí zotavenia sa po nich a podporovať ostatných používateľov pri reakcii na významné kybernetické bezpečnostné incidenty a rozsiahle rovnocenné kybernetické bezpečnostné incidenty; a mal by sa zriadiť európsky mechanizmus preskúmania kybernetických bezpečnostných incidentov s cieľom preskúmať a posúdiť konkrétne významné kybernetické bezpečnostné incidenty alebo rozsiahle kybernetické bezpečnostné incidenty. Opatrenia prijaté podľa tohto nariadenia by sa mali vykonávať s náležitým ohľadom na právomoci členských štátov a mali by dopĺňať, a nie duplikovať činnosti vykonávané sieťou jednotiek CSIRT, Európskou sieťou styčných organizácií pre kybernetické krízy (ďalej len „sieť EU-CyCLONe“) alebo skupinou pre spoluprácu (ďalej „skupina pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti“), ktoré boli všetky zriadené podľa smernice (EÚ) 2022/2555. Týmito opatreniami nie sú dotknuté články 107 a 108 Zmluvy o fungovaní Európskej únie (ďalej len „ZFEÚ“).

(8) Na dosiahnutie týchto cieľov je nevyhnutné v určitých oblastiach zmeniť nariadenie Európskeho parlamentu a Rady (EÚ) 2021/694[9]. Nariadenie (EÚ) 2021/694 malo týmto nariadením zmeniť najmä v súvislosti s doplnením nových operačných cieľov týkajúcich sa európskeho systému varovania pred kybernetickobezpečnostnými hrozbami 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 a koordinácie v oblasti kybernetickej bezpečnosti. Európsky systém varovania pred kybernetickobezpečnostnými hrozbami by mohol zohrávať dôležitú úlohu pri podpore členských štátov pri predvídaní kybernetických hrozieb a ochrane pred nimi, pričom rezerva EÚ na účely kybernetickej bezpečnosti by mohla zohrávať dôležitú úlohu pri podpore členských štátov, inštitúcií, orgánov, úradov a agentúr Únie a tretích krajín pridružených k programu Digitálna Európa pri reagovaní na významné kybernetické bezpečnostné incidenty, rozsiahle kybernetické bezpečnostné incidenty a rozsiahle rovnocenné kybernetické bezpečnostné incidenty a ich zmierňovaní. Tento vplyv by mohol zahŕňať značnú majetkovú alebo nemajetkovú ujmu a vážne riziká v oblasti verejnej bezpečnosti a ochrany. Vzhľadom na osobitné úlohy, ktoré by mohol zohrávať európsky systém varovania pred kybernetickobezpečnostnými hrozbami a rezerva EÚ na účely kybernetickej bezpečnosti, by sa týmto nariadením malo zmeniť nariadenie (EÚ) 2021/694, pokiaľ ide o účasť právnych subjektov, ktoré sú usadené v Únii, ale sú kontrolované z tretích krajín, keď existuje reálne riziko, že v Únii nie sú k dispozícii potrebné a dostatočné nástroje, infraštruktúra a služby alebo technológia, odborné znalosti a kapacity, a prínosy zapojenia takýchto subjektov prevyšujú bezpečnostné riziko. Mali by sa stanoviť osobitné podmienky za ktorých možno prideliť finančnú podporu opatreniam, ktorými sa vykonáva európsky systém varovania pred kybernetickobezpečnostnými hrozbami a rezerva EÚ na účely kybernetickej bezpečnosti, 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] 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).

(9) Na posilnenie reakcie Únie na kybernetické hrozby a incidenty je kľúčové koordinovať s medzinárodnými inštitúciami, ako aj s dôveryhodnými, podobne zmýšľajúcimi medzinárodnými partnermi. V tejto súvislosti by sa pod dôveryhodnými, podobne zmýšľajúcimi medzinárodnými partnermi mali rozumieť krajiny, ktoré majú spoločné zásady, ktoré inšpirovali vznik Únie, a to demokraciu, právny štát, univerzálnosť a nedeliteľnosť ľudských práv a základných slobôd, rešpektovanie ľudskej dôstojnosti, zásady rovnosti a solidarity a dodržiavanie zásad Charty Organizácie Spojených národov a medzinárodného práva, a ktoré neoslabujú základné bezpečnostné záujmy Únie alebo jej členských štátov. Takáto spolupráca by mohla byť prospešná aj pokiaľ ide o opatrenia prijaté podľa tohto nariadenia, najmä pokiaľ ide o európsky systém varovania pred kybernetickobezpečnostnými hrozbami a rezervu EÚ na účely kybernetickej bezpečnosti. V nariadení (EÚ) 2021/694 by sa za určitých podmienok dostupnosti a bezpečnosti malo stanoviť, že verejné súťaže pre európsky systém varovania pred kybernetickobezpečnostnými hrozbami a rezervu EÚ na účely kybernetickej bezpečnosti budú otvorené pre právne subjekty kontrolované z tretích krajín, pričom by podliehali bezpečnostným požiadavkám. Pri posudzovaní bezpečnostného rizika takéhoto otvorenia obstarávania je dôležité zohľadniť zásady a hodnoty, ktoré Únia zdieľa s podobne zmýšľajúcimi medzinárodnými partnermi, ak sa tieto zásady a hodnoty týkajú základných bezpečnostných záujmov Únie. Okrem toho, ak sa takéto bezpečnostné požiadavky posudzujú podľa nariadenia (EÚ) 2021/694, mohlo by sa zohľadniť niekoľko prvkov, ako je podniková štruktúra a rozhodovací proces subjektu, bezpečnosť údajov a utajovaných alebo citlivých informácií a zabezpečenie toho, aby výsledky opatrenia nepodliehali kontrole alebo obmedzeniam zo strany neoprávnených tretích krajín.

(10) 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 majú stanoviť v príslušných pracovných programoch v súlade s nariadením (EÚ) 2021/694.

(11) Na toto nariadenie sa vzťahujú horizontálne rozpočtové pravidlá prijaté Európskym parlamentom a Radou na základe článku 322 ZFEÚ. Uvedené pravidlá sú stanovené v nariadení Európskeho parlamentu a Rady (EÚ, Euratom) 2024/2509[10] 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].

---

[10] Nariadenie Európskeho parlamentu a Rady (EÚ, Euratom) 2024/2509 z 23. septembra 2024 o rozpočtových pravidlách, ktoré sa vzťahujú na všeobecný rozpočet Únie(Ú. v. EÚ L, 2024/2509, 26.9.2024, ELI: http://data.europa.eu/eli/reg/2024/2509/oj).

[11] Nariadenie Európskeho parlamentu a Rady (EÚ, Euratom) 2020/2092 zo 16. decembra 2020 o všeobecnom režime podmienenosti na ochranu rozpočtu Únie (Ú. v. EÚ L 433I, 22.12.2020, s. 1, ELI: http://data.europa.eu/eli/reg/2020/2092/oj).

(12) Hoci opatrenia v oblasti prevencie a pripravenosti sú nevyhnutné na zvýšenie odolnosti Únie pri riešení významných kybernetických bezpečnostných incidentov, rozsiahlych kybernetických bezpečnostných incidentov a rozsiahlych rovnocenných kybernetických bezpečnostných incidentov, výskyt, načasovanie a rozsah takýchto incidentov sú svojou povahou nepredvídateľné. Finančné zdroje potrebné na zabezpečenie primeranej reakcie sa môžu z roka na rok výrazne líšiť a mali by byť okamžite k dispozícii. Zosúladenie rozpočtovej zásady predvídateľnosti s nutnosťou rýchlej reakcie na nové potreby preto vyžaduje prispôsobiť finančné vykonávanie pracovných programov. Je teda vhodné povoliť prenos nepoužitých rozpočtových prostriedkov, ale len do nasledujúceho roka a len na kybernetickobezpečnostnú rezervu EÚ a na opatrenia podporujúce vzájomnú pomoc, a to navyše k prenosu rozpočtových prostriedkov schválených podľa článku 12 ods. 4 nariadenia (EÚ, Euratom) 2024/2509.

(13) S cieľom účinnejšie predchádzať kybernetickým hrozbám a incidentom, posudzovať ich, reagovať na ne a zotaviť sa z nich sa musia vybudovať komplexnejšie znalosti o hrozbách pre kritické aktíva a infraštruktúru na území Únie vrátane ich geografického rozloženia, vzájomného prepojenia a potenciálnych účinkov v prípade kybernetických útokov, ktoré by zasiahli túto infraštruktúru. Proaktívny prístup k identifikácii, zmierňovaniu a prevencii kybernetických hrozieb zahŕňa zvýšenú kapacitu pokročilých spôsobilostí odhaľovania. Európsky systém varovania pred kybernetickobezpečnostnými hrozbami by mal pozostávať z niekoľkých spolupracujúcich cezhraničných kybernetických centier, z ktorých každé zoskupuje tri alebo viac národných kybernetických centier. Táto infraštruktúra by mala slúžiť záujmom a potrebám v oblasti kybernetickej bezpečnosti na vnútroštátnej úrovni a na úrovni Únie, pričom by mala využívať najmodernejšie technológie pokročilého zberu relevantných údajov a informácií, vo vhodných prípadoch anonymizovaných, a analytické nástroje, čím by sa zlepšili koordinované spôsobilosti týkajúce sa odhaľovania a zvládania kybernetických hrozieb a poskytovanie situačnej informovanosti v reálnom čase. Táto infraštruktúra by mala slúžiť na zlepšenie prístupu ku kybernetickej bezpečnosti zvýšením odhaľovania, agregácie a analýzy údajov a informácií s cieľom predchádzať kybernetickým hrozbám a incidentov, a tak dopĺňať a podporovať subjekty a siete Únie zodpovedné za riadenie kybernetických kríz v Únii, najmä sieť EU-CyCLONe.

(14) Účasť na európskom systéme varovania pred kybernetickobezpečnostnými hrozbami je pre členské štáty dobrovoľná. Každý členský štát by mal na vnútroštátnej úrovni určiť jeden subjekt poverený v danom členskom štáte koordináciou činností v oblasti odhaľovania kybernetických hrozieb. Tieto národné kybernetické centrá by mali fungovať ako referenčné miesto a brána na vnútroštátnej úrovni, pokiaľ ide o účasť na európskom systéme varovania pred kybernetickobezpečnostnými hrozbami a mali by zabezpečiť, aby sa informácie o kybernetických hrozbách od verejných a súkromných subjektov zdieľali a zhromažďovali na vnútroštátnej úrovni účinným a efektívnym spôsobom. Národné kybernetické centrá by mohli posilniť spoluprácu a zdieľanie informácií medzi verejnými a súkromnými subjektmi a mohli by podporovať aj výmenu relevantných údajov a informácií s príslušnými odvetvovými a medziodvetvovými komunitami vrátane príslušných odvetvových stredísk pre výmenu a analýzu informácií (ďalej len „ISAC“). Úzka a koordinovaná spolupráca medzi verejnými a súkromnými subjektmi má zásadný význam pre posilnenie kybernetickej odolnosti Únie. Takáto spolupráca je obzvlášť cenná v kontexte zdieľania spravodajských informácií o kybernetických hrozbách s cieľom zlepšiť aktívnu kybernetickú ochranu. V rámci takejto spolupráce a zdieľania informácií by národné kybernetické centrá mohli žiadať a prijímať konkrétne informácie. Tieto národné kybernetické centrá nie sú podľa tohto nariadenia povinné ani oprávnené presadzovať takéto žiadosti. Vo vhodných prípadoch a v súlade s právom Únie a vnútroštátnym právom by vyžiadané alebo prijaté informácie mohli zahŕňať údaje z telemetrie, senzorov a logovania od subjektov, ako sú napríklad poskytovatelia riadených bezpečnostných služieb, ktorí pôsobia v odvetviach s vysokou úrovňou kritickosti alebo v iných kritických odvetviach v danom členskom štáte, s cieľom zlepšiť rýchle odhaľovanie potenciálnych kybernetických hrozieb a incidentov v skoršom štádiu, čím sa zlepší situačná informovanosť. Ak národné kybernetické centrum nie je príslušným orgánom určeným alebo zriadeným príslušným členským štátom podľa článku 8 ods. 1 smernice (EÚ) 2022/2555, je nevyhnutné, aby s týmto príslušným orgánom koordinovalo žiadosti o takéto údaje a ich prijímanie.

(15) V rámci európskeho systému varovania pred kybernetickobezpečnostnými hrozbami by sa malo zriadiť niekoľko cezhraničných kybernetických centier. Tieto cezhraničné kybernetické centrá by mali združovať vnútroštátne kybernetické centrá aspoň z troch členských štátov s cieľom zabezpečiť, aby bolo možné v plnej miere dosiahnuť prínos z cezhraničného odhaľovania hrozieb a zdieľania a riadenia informácií. Všeobecným cieľom cezhraničných kybernetických centier by malo byť posilnenie kapacít týkajúcich sa analýzy kybernetických hrozieb, predchádzania týmto hrozbám a ich odhaľovania a podpora získavania kvalitných spravodajských informácií o kybernetických hrozbách, najmä prostredníctvom zdieľania relevantných informácií, vo vhodných prípadoch anonymizovaných, v dôveryhodnom a bezpečnom prostredí, z rozličných zdrojov, verejných či súkromných, ako aj prostredníctvom zdieľania a spoločného využívania najmodernejších nástrojov a spoločného rozvoja spôsobilostí týkajúcich sa odhaľovania, analýzy a prevencie v dôveryhodnom a bezpečnom prostredí. Cezhraničné kybernetické centrá by mali vytvárať nové dodatočné kapacity, ktoré by vychádzali z existujúcich centier bezpečnostných operácií, jednotiek CSIRT a iných príslušných aktérov vrátane siete CSIRT a dopĺňali ich.

(16) Členský štát vybraný Európskym centrom priemyselných, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti (ďalej len „ECCC“) zriadeným nariadením Európskeho parlamentu a Rady (EÚ) 2021/887[12] na základe výzvy na vyjadrenie záujmu na zriadenie alebo posilnenie spôsobilostí národného kybernetického centra by mal spoločne s centrom ECCC nakúpiť príslušné nástroje, infraštruktúru a služby. Takýto členský štát by mal byť oprávnený získať grant na prevádzku nástrojov, infraštruktúry alebo služieb. Hostiteľské konzorcium pozostávajúce najmenej z troch členských štátov, ktoré bolo vybrané centrom ECCC na základe výzvy na vyjadrenie záujmu na zriadenie alebo posilnenie spôsobilostí cezhraničného kybernetického centra, by malo nakupovať príslušné nástroje, infraštruktúru alebo služby spoločne s centrom ECCC. Hostiteľské konzorcium by malo byť oprávnené získať grant na prevádzku nástrojov, infraštruktúry alebo služieb. Postup verejného obstarávania na nákup príslušných nástrojov, infraštruktúry alebo služieb by mali spoločne vykonávať centrum ECCC a príslušní verejní obstarávatelia z členských štátov vybraní na základe takýchto výziev na vyjadrenie záujmu. Takéto obstarávanie by malo byť v súlade s článkom 168 ods. 2 nariadenia (EÚ, Euratom) 2024/2509 a rozpočtovými pravidlami centra ECCC. Súkromné subjekty by preto nemali byť oprávnené zúčastňovať sa na výzvach na vyjadrenie záujmu o nákup nástrojov, infraštruktúry alebo služieb spolu s centrom ECCC, ani na získanie grantov na prevádzku týchto nástrojov, infraštruktúry alebo služieb. Členské štáty by však mali mať možnosť zapojiť súkromné subjekty do zriaďovania, zlepšovania a prevádzky svojich národných kybernetických centier a cezhraničných kybernetických centier inými spôsobmi, ktoré považujú za vhodné, v súlade s právom Únie a vnútroštátnym právom. Súkromné subjekty by mohli byť oprávnené aj na získanie finančných prostriedkov Únie podľa nariadenia (EÚ) 2021/887 na účely poskytovania podpory národným kybernetickým centrám.

---

[12] 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, ELI: http://data.europa.eu/eli/reg/2021/887/oj).

(17) S cieľom zlepšiť odhaľovanie kybernetických hrozieb a situačnú informovanosť v Únii by sa členský štát, ktorý je na základe výzvy na vyjadrenie záujmu vybraný na zriadenie alebo posilnenie spôsobilosti národného kybernetického centra, mal zaviazať, že požiada o účasť na cezhraničnom kybernetickom centre. Ak členský štát nie je účastníkom cezhraničného kybernetického centra do dvoch rokov odo dňa nadobudnutia nástrojov, infraštruktúry alebo služieb alebo od dátumu, keď dostane grantové financovanie, podľa toho, čo nastane skôr, nemal by byť oprávnený zúčastňovať sa na ďalších podporných opatreniach Únie v rámci Európskeho systému varovania v oblasti kybernetickej bezpečnosti na posilnenie spôsobilostí svojho národného kybernetického centra. V takýchto prípadoch by sa subjekty z členských štátov mohli stále zúčastniť na výzvach na predkladanie návrhov týkajúcich sa iných tém v rámci programu Digitálna Európa alebo iných programov financovania Únie vrátane výziev na kapacity na odhaľovanie kybernetických hrozieb a na zdieľanie informácií za predpokladu, že tieto subjekty spĺňajú kritériá oprávnenosti stanovené v uvedených programoch.

(18) Jednotky CSIRT si v súlade so smernicou (EÚ) 2022/2555 vymieňajú informácie v rámci siete jednotiek CSIRT. Európsky systém varovania pred kybernetickobezpečnostnými hrozbami by mal predstavovať novú spôsobilosť, ktorá bude dopĺňať sieť jednotiek CSIRT tým, že prispeje k budovaniu situačnej informovanosti Únie, ktorá umožní posilnenie spôsobilostí siete jednotiek CSIRT. Cezhraničné kybernetické centrá by mali koordinovať a úzko spolupracovať so sieťou jednotiek CSIRT. Mali by fungovať združovaním údajov a zdieľaním relevantných informácií, vo vhodných prípadoch anonymizovaných, o kybernetických hrozbách od verejných a súkromných subjektov, zvyšovať hodnotu takýchto údajov a informácií prostredníctvom odborných analýz, spoločne nadobudnutej infraštruktúry a najmodernejších nástrojov a prispievaním k technologickej suverenite Únie, jej otvorenej strategickej autonómii, konkurencieschopnosti a odolnosti a k rozvoju spôsobilostí Únie.

(19) Cezhraničné kybernetické centrá by mali fungovať ako ústredné kontaktné miesta umožňujúce rozsiahle zhromažďovanie relevantných údajov a spravodajských informácií o kybernetických hrozbách a umožňovať rozširovanie informácií o hrozbách rozsiahlemu a rozmanitému súboru zúčastnených strán, ako napríklad tímom reakcie na núdzové počítačové situácie (CERT), jednotkám CSIRT, strediskám ISAC a prevádzkovateľom kritických infraštruktúr. Členovia hostiteľského konzorcia by mali v dohode o konzorciu špecifikovať relevantné informácie, ktoré sa majú zdieľať medzi účastníkmi dotknutého cezhraničného kybernetického centra. Medzi informácie, ktoré sú predmetom výmeny medzi účastníkmi cezhraničného kybernetického centra, by mohli patriť napríklad údaje zo sietí a senzorov, informačné kanály pre spravodajské informácie o hrozbách, indikátory ohrozenia a kontextualizované informácie o incidentoch, kybernetických hrozbách, udalostiach odvrátených v poslednej chvíli, zraniteľnostiach, technikách a postupoch, nepriateľských taktikách, informácie špecifické pre jednotlivých aktérov hrozieb, kybernetickobezpečnostné varovania a odporúčania týkajúce sa konfigurácie nástrojov kybernetickej bezpečnosti na odhaľovanie kybernetických útokov. Navyše by cezhraničné kybernetické centrá mali medzi sebou takisto uzatvárať dohody o spolupráci. V takýchto dohodách o spolupráci by sa mali špecifikovať najmä zásady zdieľania informácií a interoperabilita. Ich ustanovenia týkajúce sa interoperability, najmä formátov a protokolov na zdieľanie informácií, by sa mali riadiť usmerneniami pre interoperabilitu vydanými Agentúrou Európskej únie pre kybernetickú bezpečnosť zriadenou nariadením (EÚ) 2019/881 (ďalej len „ENISA“) a preto by mali byť aj ich východiskovým bodom. Tieto usmernenia by sa mali vydať rýchlo, aby sa zabezpečilo, že cezhraničné kybernetické centrá ich budú môcť zohľadniť v počiatočnom štádiu. Mali by zohľadňovať medzinárodné normy a najlepšie postupy a fungovanie všetkých zriadených cezhraničných kybernetických centier.

(20) Cezhraničné kybernetické centrá a sieť jednotiek CSIRT by mali úzko spolupracovať s cieľom zabezpečiť synergie a komplementárnosť činností. Na tento účel by sa mali dohodnúť na procedurálnych dojednaniach týkajúcich sa spolupráce a zdieľania relevantných informácií. Mohlo by to zahŕňať zdieľanie relevantných informácií o kybernetických hrozbách a významných kybernetických bezpečnostných incidentoch a zabezpečenie toho, aby sa so sieťou jednotiek CSIRT zdieľali skúsenosti s najmodernejšími nástrojmi, najmä s umelou inteligenciou a technológiou analýzy údajov, ktoré sa používajú v rámci cezhraničných kybernetických centier.

(21) Spoločná situačná informovanosť relevantných orgánov je nevyhnutnou podmienkou pripravenosti a koordinácie celej Únie, pokiaľ ide o významné kybernetické bezpečnostné incidenty a rozsiahle kybernetické incidenty. Smernicou (EÚ) 2022/2555 sa zriadila sieť EU-CyCLONe s cieľom podporiť koordinované riadenie rozsiahlych kybernetických bezpečnostných incidentov a kríz na operačnej úrovni a zabezpečiť pravidelnú výmenu relevantných informácií medzi členskými štátmi a inštitúciami, orgánmi, úradmi a agentúrami Únie. Smernicou (EÚ) 2022/2555 sa taktiež zriadila sieť CSIRT, ktorá by mala podporovať rýchlu a účinnú operačnú spoluprácu medzi členskými štátmi. Na zabezpečenie situačnej informovanosti a posilnenie solidarity, v situáciách, keď cezhraničné kybernetické centrá získajú informácie týkajúce sa potenciálneho alebo prebiehajúceho rozsiahleho kybernetického bezpečnostného incidentu, by mali poskytnúť relevantné informácie sieti CSIRT a ako včasné varovanie informovať sieť EU-CyCLONe. V závislosti od situácie by medzi informácie určené na zdieľanie 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 bezpečnostnom incidente. V tejto súvislosti by sa mala náležitá pozornosť venovať zásade potreby poznať a potenciálne citlivej povahe zdieľaných informácií. V smernici (EÚ) 2022/2555 sa tiež opätovne potvrdzujú zodpovednosti Komisie v rámci mechanizmu Únie v oblasti civilnej ochrany zriadeného rozhodnutím Európskeho parlamentu a Rady č. 1313/2013/EÚ[13], a jej zodpovednosť za poskytovanie analytických správ týkajúcich sa dojednaní EÚ o integrovanej politickej reakcii na krízu (ďalej len „dojednania IPRK“) podľa vykonávacieho rozhodnutia (EÚ) 2018/1993[14].

---

13 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, ELI: http://data.europa.eu/eli/dec/2013/1313/oj).

14 Vykonávacie rozhodnutie Rady (EÚ) 2018/1993 z 11. decembra 2018 o dojednaniach EÚ o integrovanej politickej reakcii na krízu (Ú. v. EÚ L 320, 17.12.2018, s. 28, ELI: http://data.europa.eu/eli/dec_impl/2018/1993/oj).

Ak cezhraničné kybernetické centrá zdieľajú relevantné informácie a včasné varovania týkajúce sa potenciálneho alebo prebiehajúceho rozsiahleho kybernetického bezpečnostného incidentu so sieťou EU-CyCLONe a sieťou CSIRT, je nevyhnutné, aby sa tieto informácie zdieľali prostredníctvom týchto sietí s orgánmi členských štátov, ako aj s Komisiou. V tejto súvislosti sa v smernici (EÚ) 2022/2555 stanovuje, že účelom siete EU-CyCLONe je podporiť koordinované riadenie rozsiahlych kybernetických bezpečnostných incidentov a kríz na operačnej úrovni a zabezpečiť pravidelnú výmenu relevantných informácií medzi členskými štátmi a inštitúciami, orgánmi, úradmi a agentúrami Únie. Medzi úlohy siete EU-CyCLONe patrí rozvíjanie spoločnej situačnej informovanosti o takýchto incidentoch a krízach. Je mimoriadne dôležité, aby sieť EU-CyCLONe v súlade s týmto účelom a so svojimi úlohami zabezpečila, aby sa takéto informácie bezodkladne poskytli príslušným zástupcom členských štátov a Komisii. Na tento účel je veľmi dôležité, aby rokovací poriadok siete EU-CyCLONe obsahoval primerané ustanovenia.

(22) Subjekty zúčastňujúce sa na európskom systéme varovania pred kybernetickobezpečnostnými hrozbami by mali zabezpečiť vysokú úroveň interoperability medzi sebou, a to vo vhodných prípadoch aj v súvislosti s formátmi údajov, taxonómiou, nástrojmi na spracovanie a analýzu údajov. Mali by tiež zabezpečiť bezpečné komunikačné kanály, minimálnu úroveň bezpečnosti aplikačnej vrstvy, prehľad situačnej informovanosti a ukazovatele. Pri prijímaní spoločnej taxonómie a vypracovaní vzorov situačných správ, ktoré slúžia na opis príčin odhalených kybernetických hrozieb a rizík, by sa mala zohľadniť existujúca práca v kontexte vykonávania smernice (EÚ) 2022/2555.

(23) S cieľom umožniť výmenu podstatných údajov a informácií o kybernetických hrozbách z rôznych zdrojov, v širokom meradle a v dôveryhodnom a bezpečnom prostredí by subjekty zúčastnené na európskom systéme varovania pred kybernetickobezpečnostnými hrozbami mali byť vybavené najmodernejšími a mimoriadne bezpečnými nástrojmi, vybavením a infraštruktúrou a kvalifikovanými pracovníkmi. 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.

(24) Vďaka zberu, analýze, zdieľaniu a výmene relevantných údajov a informácií by európsky systém varovania pred kybernetickobezpečnostnými hrozbami mal posilniť technologickú suverenitu a otvorenú strategickú autonómiu v oblasti kybernetickej bezpečnosti, konkurencieschopnosť a odolnosť Únie. Zhromažďovanie vybratých údajov vysokej kvality by mohlo takisto prispieť k rozvoju vyspelých technológií umelej inteligencie a analýzy údajov. Na zhromažďovanie vysokokvalitných údajov je naďalej nevyhnutný ľudský dohľad, a teda kvalifikovaná pracovná sila.

(25) Hoci je európsky systém varovania pred kybernetickobezpečnostnými hrozbami civilný projekt, komunita kybernetickej obrany by mohla ťažiť zo silnejších civilných spôsobilostí týkajúcich sa odhaľovania a situačnej informovanosti vyvinutých na ochranu kritickej infraštruktúry.

(26) Zdieľanie informácií medzi účastníkmi európskeho systému varovania pred kybernetickobezpečnostnými hrozbami 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 spracúvanie osobných údajov, príjemca informácií by mal zaviesť 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.

(27) Zachovanie dôvernosti a informačnej bezpečnosti je mimoriadne dôležité pre všetky tri piliere tohto nariadenia, či už na podnecovanie zdieľania alebo výmeny informácií v kontexte európskeho systému varovania pred kybernetickobezpečnostnými hrozbami, ochranu záujmov subjektov žiadajúcich o podporu v rámci mechanizmu na riešenie kybernetickobezpečnostných núdzových situácií alebo na zabezpečenie toho, aby správy v rámci európskeho mechanizmu preskúmania kybernetických bezpečnostných incidentov mohli priniesť užitočné ponaučenia bez toho, aby to malo negatívny vplyv na subjekty postihnuté incidentmi. Účasť členských štátov a subjektov na týchto mechanizmoch závisí od vzťahu dôvery medzi ich zložkami. Ak sú informácie dôverné podľa pravidiel Únie alebo vnútroštátnych predpisov, ich zdieľanie alebo výmena podľa tohto nariadenia by sa mala obmedziť na tie, ktoré sú relevantné a primerané účelu zdieľania alebo výmeny. Uvedeným zdieľaním alebo výmenou by sa mala tiež zachovať dôvernosť uvedených informácií vrátane ochrany bezpečnostných a obchodných záujmov dotknutých subjektov. Zdieľanie alebo výmena informácií podľa tohto nariadenia by sa mohli uskutočňovať prostredníctvom dohôd o nezverejňovaní informácií alebo usmernení o distribúcii informácií, ako je semaforový protokol (Traffic Light Protocol – TLP). Semaforový protokol sa má chápať ako prostriedok na poskytovanie informácií o akýchkoľvek obmedzeniach, pokiaľ ide o ďalšie šírenie informácií. Používa sa takmer vo všetkých jednotkách CSIRT a v niektorých strediskách ISAC. Okrem týchto všeobecných požiadaviek, pokiaľ ide o európsky systém varovania pred kybernetickobezpečnostnými hrozbami, by sa v dohodách o hostiteľských konzorciách mali stanoviť osobitné pravidlá týkajúce sa podmienok zdieľania informácií v rámci dotknutého cezhraničného kybernetického centra. V týchto dohodách by sa mohlo najmä vyžadovať, aby sa informácie zdieľali len v súlade s právom Únie a vnútroštátnym právom.

(28) Pokiaľ ide o zavedenie rezervy EÚ na účely kybernetickej bezpečnosti, sú potrebné osobitné pravidlá dôvernosti. O podporu sa bude žiadať, bude sa posudzovať a poskytovať v kontexte krízy a vo vzťahu k subjektom pôsobiacim v citlivých odvetviach. Na účinné fungovanie rezervy EÚ na účely kybernetickej bezpečnosti je nevyhnutné, aby používatelia a subjekty mohli bezodkladne zdieľať všetky informácie, ktoré každý subjekt potrebuje na to, aby zohrával svoju úlohu pri posudzovaní žiadostí a zavádzaní podpory, a aby k nim mohli bezodkladne poskytnúť prístup. V tomto nariadení by sa preto malo stanoviť, že všetky takéto informácie sa používajú alebo zdieľajú len vtedy, ak je to potrebné na fungovanie rezervy EÚ na účely kybernetickej bezpečnosti, a že informácie, ktoré sú dôverné alebo utajované podľa práva Únie alebo vnútroštátneho práva, by sa mali používať a zdieľať len v súlade s uvedeným právom. Okrem toho by používatelia mali mať možnosť vo vhodných prípadoch používať protokoly na zdieľanie informácií, ako napríklad semaforový protokol, na ďalšie spresnenie obmedzení. Hoci používatelia majú v tejto súvislosti diskrečnú právomoc, je dôležité, aby pri uplatňovaní takýchto obmedzení zohľadnili možné dôsledky, najmä pokiaľ ide o oneskorené posúdenie alebo poskytnutie požadovaných služieb. V záujme efektívnej rezervy EÚ na účely kybernetickej bezpečnosti je dôležité, aby verejný obstarávateľ objasnil tieto dôsledky používateľovi pred podaním žiadosti. Tieto záruky sa obmedzujú na žiadosť a poskytovanie služieb rezervy EÚ na účely kybernetickej bezpečnosti a nemajú vplyv na výmenu informácií v iných kontextoch, napríklad pri obstarávaní rezervy EÚ na účely kybernetickej bezpečnosti.

(29) So zreteľom na zvyšujúce sa riziká a čoraz väčší počet incidentov postihujúcich členské štáty je nevyhnutné zriadiť nástroj krízovej podpory, a to mechanizmus na riešenie kybernetickobezpečnostných núdzových situácií, s cieľom zlepšiť odolnosť Únie voči významným kybernetickým bezpečnostným incidentom, rozsiahlym kybernetickým bezpečnostným incidentom a rozsiahlym rovnocenným kybernetickým bezpečnostným incidentom a doplniť opatrenia členských štátov prostredníctvom núdzovej finančnej podpory určenej na pripravenosť, reakciu na incidenty a počiatočné zotavenie sa základných služieb. Keďže úplné zotavenie sa z incidentu je komplexný proces obnovenia fungovania subjektu postihnutého incidentom do stavu pred incidentom a mohol by byť dlhým procesom, ktorý so sebou prinesie značné náklady, podpora z rezervy EÚ na účely kybernetickej bezpečnosti by sa mala obmedziť na počiatočnú fázu procesu obnovy, ktorá povedie k obnove základných funkcií systémov. Mechanizmus na riešenie kybernetickobezpečnostných núdzových situácií by mal umožňovať rýchle a efektívne 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 incidentom a krízam, za prípravu a reakciu na ne majú členské štáty, mechanizmus na riešenie kybernetickobezpečnostných núdzových situácií podporuje solidaritu medzi členskými štátmi v súlade s článkom 3 ods. 3 Zmluvy o Európskej únii (ďalej len „Zmluva o EÚ“).

(30) Mechanizmus na riešenie kybernetickobezpečnostných 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 kybernetické bezpečnostné incidenty, rozsiahle kybernetické bezpečnostné incidenty a rozsiahle rovnocenné kybernetické bezpečnostné incidenty a počiatočného zotavenia sa z nich, ako sú napríklad služby poskytované agentúrou 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 vrátane, v súvislosti s článkom 42 ods. 7 Zmluvy o EÚ a tímov rýchlej kybernetickej reakcie stálej štruktúrovanej spolupráce (PESCO) zriadenej podľa rozhodnutia Rady (SZBP) 2017/2315[15]. Mala by sa tým riešiť potreba zabezpečiť, aby na účely podpory pripravenosti, reakcie a zotavenia v prípade takýchto incidentov v celej Únii a v tretích krajinách pridružených k programu Digitálna Európa boli k dispozícii špecializované prostriedky.

[15] Rozhodnutie Rady (SZBP) 2017/2315 z 11. decembra 2017 o nadviazaní stálej štruktúrovanej spolupráce (PESCO) a stanovení zoznamu zúčastnených členských štátov (Ú. v. EÚ L 331, 14.12.2017, s. 57, ELI: http://data.europa.eu/eli/dec/2017/2315/2023-05-23).

(31) Týmto nariadením nie sú dotknuté postupy a rámce na koordináciu reakcie na krízu na úrovni Únie, najmä smernica (EÚ) 2022/2555, mechanizmus Únie v oblasti civilnej ochrany zriadený rozhodnutím Európskeho parlamentu a Rady č. 1313/2013/EÚ[16], dojednania IPRK a odporúčanie Komisie (EÚ) 2017/1584[17]. Podporou poskytovanou z mechanizmu na riešenie kybernetickobezpečnostných núdzových situácií sa 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, s ohľadom na civilnú povahu mechanizmu na riešenie kybernetickobezpečnostných núdzových situácií. Podpora poskytovaná v rámci mechanizmu na riešenie kybernetickobezpečnostných núdzových situácií môže dopĺňať opatrenia vykonávané v kontexte článku 42 ods. 7 Zmluvy o EÚ vrátane pomoci, ktorú jeden členský štát poskytuje inému členskému štátu, alebo môže byť súčasťou spoločnej reakcie Únie a členských štátov alebo v situáciách uvedených v článku 222 ZFEÚ. Vykonávanie tohto nariadenia by sa malo vo vhodných prípadoch koordinovať s vykonávaním opatrení v rámci súboru nástrojov kybernetickej diplomacie.

---

[16] 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).

[17] 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).

(32) 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 zabezpečiť úzku spoluprácu a konzultácie medzi Komisiou, agentúrou ENISA, členskými štátmi, a v relevantných prípadoch centrom ECCC. Keď bude členský štát žiadať o podporu v rámci mechanizmu na riešenie kybernetickobezpečnostných núdzových situácií núdzových situácií v oblasti kybernetickej bezpečnosti, mal by poskytnúť relevantné informácie odôvodňujúce potrebu podpory.

(33) 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 bezpečnostné incidenty a krízy, v ktorom sa stanovia ciele a spôsoby riadenia rozsiahlych kybernetických bezpečnostných 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 kybernetickobezpečnostných núdzových situácií by mal poskytovať pomoc pri opatreniach zameraných na posilňovanie pripravenosti, ako aj pri opatreniach reakcie na incidenty s cieľom zmierniť vplyv významných kybernetických bezpečnostných incidentov a rozsiahlych kybernetických bezpečnostných incidentov, podporovať počiatočné zotavenie a obnoviť základné funkcie služieb poskytovaných subjektmi pôsobiacimi v odvetviach s vysokou úrovňou kritickosti alebo subjektmi pôsobiacimi v iných kritických odvetviach.

(34) 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, a to aj prostredníctvom cvičení a školení. Na tento účel by Komisia po konzultácii s agentúrou ENISA , so skupinou pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti a so sieťou EU-CyCLONe mala pravidelne určovať relevantné odvetvia alebo pododvetvia, ktoré by mali byť oprávnené prijímať finančnú podporu na koordinované testovanie pripravenosti na úrovni Únie. Odvetvia alebo pododvetvia by sa mali vyberať z odvetví s vysokou úrovňou kritickosti uvedených v prílohe I k smernici (EÚ) 2022/2555. Koordinované testovanie pripravenosti by malo 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 Únie pre zahraničné veci a bezpečnostnú politiku (ďalej len „vysoký predstaviteľ“) a skupina pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti, v koordinácii s príslušnými civilnými a vojenskými orgánmi a agentúrami a vytvorenými sieťami vrátane siete EU-CyCLONe, ako aj posúdenie rizika komunikačných sietí a infraštruktúry 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 zriadeným nariadením Európskeho parlamentu a Rady (EÚ) 2018/1971[18], koordinované posúdenia bezpečnostných rizík kritických dodávateľských reťazcov na úrovni Únie, 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[19]. Pri výbere odvetví by sa malo zohľadniť aj odporúčanie Rady o celoúniovom koordinovanom prístupe k posilneniu odolnosti kritickej infraštruktúry.

---

[18] Nariadenie Európskeho parlamentu a Rady (EÚ) 2018/1971 z 11. decembra 2018, ktorým sa zriaďuje Orgán európskych regulátorov pre elektronické komunikácie (BEREC) a Agentúra na podporu orgánu BEREC (Úrad BEREC), ktorým sa mení nariadenie (EÚ) 2015/2120 a ktorým sa zrušuje nariadenie (ES) č. 1211/2009 (Ú. v. EÚ L 321, 17.12.2018, s. 1).

[19] 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 (Ú. v. EÚ L 333, 27.12.2022, s. 1).

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

(36) Keď členské štáty dostanú granty na podporu opatrení v oblasti pripravenosti, subjekty v odvetviach s vysokou úrovňou kritickosti sa môžu na týchto opatreniach dobrovoľne zúčastňovať. Osvedčeným postupom je, že po takýchto opatreniach zúčastnené subjekty vypracujú plán nápravy s cieľom vykonať všetky výsledné odporúčania konkrétnych opatrení s cieľom v čo najväčšej miere využiť opatrenie pripravenosti. Hoci je dôležité, aby členské štáty v rámci opatrení požadovali, aby zúčastnené subjekty vypracovali a vykonávali takéto plány nápravy, členské štáty nie sú podľa tohto nariadenia povinné ani oprávnené presadzovať takéto žiadosti. Takýmito žiadosťami nie sú dotknuté požiadavky na subjekty a právomoci príslušných orgánov v oblasti dohľadu v súlade so smernicou (EÚ) 2022/2555.

(37) Mechanizmus na riešenie kybernetickobezpečnostných núdzových situácií by mal poskytovať aj podporu na opatrenia reakcie na incidenty s cieľom zmierniť vplyv významných kybernetických bezpečnostných incidentov, rozsiahlych kybernetických bezpečnostných incidentov a rozsiahlych rovnocenných kybernetických bezpečnostných incidentov, podporovať počiatočné zotavenie alebo obnoviť fungovanie základných služieb. Vo vhodných prípadoch by mal dopĺňať mechanizmus Únie v oblasti civilnej ochrany s cieľom zabezpečiť komplexný prístup k reakcii na vplyv incidentov na občanov.

(38) Mechanizmus na riešenie kybernetickobezpečnostných núdzových situácií by mal podporovať technickú pomoc poskytovanú jedným členským štátom inému členskému štátu, ktorý je dotknutý významným kybernetickým bezpečnostným incidentom alebo rozsiahlym kybernetickým bezpečnostným incidentom, a to aj prostredníctvom jednotiek CSIRT, ako sa uvádza v článku 11 ods. 3 písm. f) smernice (EÚ) 2022/2555. Členským štátom poskytujúcim takúto pomoc by sa malo umožniť predkladať žiadosti na pokrytie nákladov súvisiacich s vysielaním tímov expertov v rámci vzájomnej pomoci. Oprávnené náklady by mohli zahŕňať príspevky na cestovné výdavky, na ubytovanie a diéty expertov na kybernetickú bezpečnosť.

(39) Vzhľadom na zásadnú úlohu, ktorú zohrávajú súkromné podniky pri odhaľovaní rozsiahlych kybernetických bezpečnostných incidentov a rozsiahlych rovnocenných kybernetických bezpečnostných incidentov, pripravenosti a reakcii na ne, je dôležité uznať hodnotu dobrovoľnej pro bono spolupráce s takýmito podnikmi, v rámci ktorej ponúkajú služby bezplatne v prípade rozsiahlych kybernetických bezpečnostných incidentov a kríz a rozsiahlych rovnocenných kybernetických bezpečnostných incidentov a kríz. Agentúra ENISA by v spolupráci s sieťou EU-CyCLONe mohla monitorovať vývoj takýchto iniciatív pro bono a podporovať ich súlad s kritériami uplatniteľnými na dôveryhodných poskytovateľov riadených bezpečnostných služieb podľa tohto nariadenia, a to aj pokiaľ ide o dôveryhodnosť súkromných podnikov, ich skúsenosti, ako aj schopnosť nakladať s citlivými informáciami bezpečným spôsobom.

(40) Ako súčasť mechanizmu na riešenie kybernetickobezpečnostných núdzových situácií by sa mala postupne zriadiť rezerva EÚ na účely kybernetickej bezpečnosti pozostávajúca zo služieb dôveryhodných poskytovateľov riadených bezpečnostných služieb na podporu reakcie a iniciovanie opatrení na zotavenie sa v prípadoch významných kybernetických bezpečnostných incidentov, rozsiahlych kybernetických bezpečnostných incidentov alebo rozsiahlych rovnocenných kybernetických bezpečnostných incidentov, ktoré majú vplyv na členské štáty, inštitúcie, orgány, úrady alebo agentúry Únie alebo tretie krajiny pridružené k programu Digitálna Európa. Rezerva EÚ na účely kybernetickej bezpečnosti by mala zabezpečovať dostupnosť a pripravenosť služieb. Mala by preto zahŕňať služby, ktoré sú viazané vopred, napríklad vrátane kapacít, ktoré sú v pohotovostnom režime a možno ich nasadiť v krátkom čase. Služby rezervy EÚ na účely kybernetickej bezpečnosti by mali slúžiť na podporu vnútroštátnych orgánov pri poskytovaní pomoci zasiahnutým subjektom pôsobiacim v odvetviach s vysokou úrovňou kritickosti alebo postihnutým subjektom pôsobiacim v iných kritických odvetviach ako doplnok k ich vlastným opatreniam na vnútroštátnej úrovni. Služby rezervy EÚ na účely kybernetickej bezpečnosti by mali byť za podobných podmienok schopné používať aj na podporu inštitúcií, orgánov, úradov a agentúr Únie. Rezerva EÚ na účely kybernetickej bezpečnosti by mohla prispieť aj k posilneniu konkurenčného postavenia priemyslu a služieb v Únii v celom digitálnom hospodárstve vrátane mikropodnikov a malých a stredných podnikov, ako aj startupov, a to aj poskytovaním stimulov na investície do výskumu a inovácií. Pri obstarávaní služieb pre rezervu EÚ na účely kybernetickej bezpečnosti je dôležité zohľadniť európsky rámec zručností v oblasti kybernetickej bezpečnosti agentúry ENISA. Keď používatelia žiadajú o podporu z rezervy EÚ na účely kybernetickej bezpečnosti, mali by do svojej žiadosti zahrnúť príslušné informácie týkajúce sa dotknutého subjektu a potenciálnych vplyvov, informácie o požadovanej službe z rezervy EÚ na účely kybernetickej bezpečnosti a podporu poskytovanú zasiahnutému subjektu na vnútroštátnej úrovni, ktorá by sa mala zohľadniť pri posudzovaní žiadosti žiadateľa. Na zabezpečenie komplementárnosti s inými formami podpory dostupnej pre zasiahnutý subjekt by mala žiadosť zahŕňať, ak sú dostupné, informácie o platných zmluvných dojednaniach o službách reakcie na incidenty a počiatočného zotavenia sa z nich, ako aj poistných zmlúv, ktoré sa potenciálne vzťahujú na takýto druh incidentu.

(41) S cieľom zabezpečiť účinné využívanie finančných prostriedkov Únie by sa vopred vyčlenené služby v rámci rezervy EÚ na účely kybernetickej bezpečnosti mali v súlade s príslušnou zmluvou zmeniť na služby pripravenosti súvisiace s predchádzaním incidentom a reakciou na ne v prípade, že sa tieto vopred vyčlenené služby nevyužijú na reakciu na incidenty v čase, na ktorý sú vopred vyčlenené. Tieto služby by mali byť doplnkové a nemali by zdvojovať opatrenia v oblasti pripravenosti, ktoré má riadiť centrum ECCC.

(42) Žiadosti o podporu z rezervy EÚ na účely kybernetickej bezpečnosti od orgánov pre riadenie kybernetických kríz a jednotiek CSIRT členských štátov alebo CERT-EU v mene inštitúcií, orgánov, úradov alebo agentúr Únie by mal posúdiť verejný obstarávateľ. Ak bola agentúra ENISA poverená správou a prevádzkou rezervy EÚ na účely kybernetickej bezpečnosti, týmto verejným obstarávateľom je agentúra ENISA. Žiadosti o podporu z tretích krajín pridružených k programu Digitálna Európa by mala posúdiť Komisia. S cieľom uľahčiť predkladanie a posudzovanie žiadostí o podporu by agentúra ENISA mohla zriadiť bezpečnú platformu.

(43) V prípade prijatia viacerých súbežných žiadostí by sa tieto žiadosti mali priorizovať v súlade s kritériami stanovenými v tomto nariadení. Vzhľadom na všeobecné ciele tohto nariadenia by tieto kritériá mali zahŕňať rozsah a závažnosť incidentu, typ zasiahnutého subjektu, potenciálny vplyv na zasiahnuté členské štáty a používateľov, potenciálny cezhraničný charakter incidentu a riziko presahu a opatrenia, ktoré už používateľ prijal na pomoc pri reakcii a počiatočnom zotavení. Vzhľadom na tieto ciele a vzhľadom na to, že žiadosti používateľov z členských štátov sú určené výlučne na podporu subjektov v celej Únii pôsobiacich v odvetviach s vysokou úrovňou kritickosti alebo subjektov pôsobiacich v iných kritických odvetviach, je vhodné uprednostniť žiadosti používateľov z členských štátov, kde tieto kritériá vedú k tomu, že sa dve alebo viaceré žiadosti posúdia ako rovnocenné. Týmto nie sú dotknuté žiadne povinnosti, ktoré môžu mať členské štáty podľa príslušných dohôd o hosťovaní, prijímať opatrenia na ochranu a pomoc inštitúciám, orgánom, úradom alebo agentúram Únie.

(44) Celkovú zodpovednosť za vykonávanie rezervy EÚ na účely kybernetickej bezpečnosti by mala niesť Komisia. Vzhľadom na rozsiahle skúsenosti, ktoré agentúra ENISA získala s opatreniami na podporu kybernetickej bezpečnosti, je agentúra ENISA najvhodnejšou agentúrou na vykonávanie rezervy EÚ na účely kybernetickej bezpečnosti. Preto by Komisia mala agentúru ENISA čiastočne alebo, ak to Komisia považuje za vhodné, úplne poveriť prevádzkou a správou rezervy EÚ na účely kybernetickej bezpečnosti. Poverenie by sa malo vykonať v súlade s príslušnými pravidlami podľa nariadenia (EÚ, Euratom) 2024/2509, a najmä by malo podliehať splneniu príslušných podmienok na podpísanie dohody o príspevku. Všetky aspekty prevádzky a správy rezervy EÚ na účely kybernetickej bezpečnosti, ktoré nie sú zverené agentúre ENISA, by mali podliehať priamemu riadeniu zo strany Komisie, a to aj pred podpísaním dohody o príspevku.

(45) Členské štáty by mali zohrávať kľúčovú úlohu pri vytváraní, nasadzovaní a po nasadení rezervy EÚ na účely kybernetickej bezpečnosti. Keďže nariadenie (EÚ) 2021/694 je príslušným základným aktom pre akcie, ktorými sa vykonáva rezerva EÚ na účely kybernetickej bezpečnosti, opatrenia v rámci rezervy EÚ na účely kybernetickej bezpečnosti by sa mali stanoviť v pracovných programoch uvedených v článku 24 nariadenia (EÚ) 2021/694. Podľa odseku 6 uvedeného článku má uvedené pracovné programy prijať Komisia prostredníctvom vykonávacích aktov v súlade s postupom preskúmania. Okrem toho by Komisia v koordinácii so skupinou pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti mala určiť priority a vývoj rezervy EÚ na účely kybernetickej bezpečnosti.

(46) Zmluvy uzavreté v rámci rezervy EÚ na účely kybernetickej bezpečnosti by nemali mať vplyv na vzťah medzi podnikmi a existujúce povinnosti medzi dotknutým subjektom alebo používateľmi a poskytovateľom služieb.

(47) Na účely výberu súkromných poskytovateľov služieb na poskytovanie služieb v kontexte rezervy EÚ na účely kybernetickej bezpečnosti je nevyhnutné stanoviť súbor minimálnych kritérií a požiadaviek, 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, subjektov pôsobiacich v odvetviach s vysokou úrovňou kritickosti alebo subjektov pôsobiacich iných kritických odvetviach. S cieľom riešiť osobitné potreby členských štátov by mal verejný obstarávateľ pri obstarávaní služieb pre rezervu EÚ na účely kybernetickej bezpečnosti vo vhodných prípadoch vypracovať dodatočné kritéria a požiadavky účasti popri kritériách a požiadavkách stanovených v tomto nariadení. Je dôležité podnecovať účasť menších poskytovateľov pôsobiacich na regionálnej a miestnej úrovni.

(48) Pri výbere poskytovateľov, ktorí sa majú zahrnúť do rezervy EÚ na účely kybernetickej bezpečnosti, by sa verejný obstarávateľ mal snažiť zabezpečiť, aby rezerva EÚ na účely kybernetickej bezpečnosti ako celok obsahovala poskytovateľov, ktorí sú schopní vyhovieť jazykovým požiadavkám používateľov. Na tento účel by mal verejný obstarávateľ pred vypracovaním špecifikácií ponuky zistiť, či potenciálni používatelia rezervy EÚ na účely kybernetickej bezpečnosti majú osobitné jazykové požiadavky, aby bolo možné poskytovať služby podpory z rezervy EÚ na účely kybernetickej bezpečnosti v jazyku spomedzi úradných jazykov inštitúcií Únie alebo členských štátov, ktorému bude používateľ alebo dotknutý subjekt pravdepodobne rozumieť. V prípade, že používateľ potrebuje na poskytovanie služieb podpory z rezervy EÚ na účely kybernetickej bezpečnosti viac ako jeden jazyk a tieto služby boli obstarané v týchto jazykoch pre uvedeného používateľa, používateľ by mal mať možnosť v žiadosti o podporu z rezervy EÚ na účely kybernetickej bezpečnosti uviesť, v ktorom z týchto jazykov by sa mali služby poskytovať v súvislosti s konkrétnym incidentom, ktorý viedol k podaniu žiadosti.

(49) Na podporu vytvorenia rezervy EÚ na účely kybernetickej bezpečnosti je dôležité, aby Komisia požiadala agentúru ENISA o vypracovanie kandidátskej schémy certifikácie kybernetickej bezpečnosti pre riadené bezpečnostné služby podľa nariadenia (EÚ) 2019/881 v oblastiach, na ktoré sa vzťahuje mechanizmus na riešenie kybernetickobezpečnostných núdzových situácií.

(50) V záujme podpory cieľov tohto nariadenia týkajúcich sa presadzovania spoločnej situačnej informovanosti, zvyšovania odolnosti Únie a umožnenia účinnej reakcie na významné kybernetické bezpečnostné incidenty a rozsiahle kybernetické bezpečnostné incidenty by Komisia alebo sieť EU-CyCLONe s podporou sieti jednotiek CSIRT a so súhlasom dotknutého členského štátu mali mať možnosť požiadať agentúru ENISA o preskúmanie a posúdenie kybernetických hrozieb, známych zneužiteľných zraniteľností a zmierňujúcich opatrení s ohľadom na konkrétny významný kybernetický bezpečnostný incident alebo rozsiahly kybernetický bezpečnostný incident. Po dokončení preskúmania a posúdenia incidentu by agentúra ENISA mala vypracovať správu o preskúmaní incidentu, a to v spolupráci s dotknutým členským štátom, príslušnými zainteresovanými stranami vrátane zástupcov súkromného sektora, Komisie a iných relevantných inštitúcií, orgánov, úradov a agentúr Únie. Vychádzajúc zo spolupráce so zainteresovanými stranami vrátane súkromného sektora by sa správa o preskúmaní konkrétnych incidentov mala zamerať na posúdenie príčin, vplyvu incidentu a krokov na jeho zmiernenie po jeho výskyte. Osobitnú pozornosť by bolo treba venovať vstupným informáciám a poznatkom, ktoré zdieľajú 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 slúžiť ako podklad pre ich prácu, ako aj prácu agentúry ENISA. Ak incident súvisí s treťou krajinou pridruženou k programu Digitálna Európa, Komisia by mala správu poskytnúť aj vysokému predstaviteľovi.

(51) S ohľadom na nepredvídateľnú povahu kybernetických útokov a na skutočnosť, že tieto útoky často nie sú obmedzené na konkrétnu geografickú oblasť a predstavujú vysoké riziko presahu, prispieva k ochrane celej Únie, a najmä jej vnútorného trhu a priemyslu ako celku, zvýšenie odolnosti susedných krajín a posilnenie ich kapacity účinne reagovať na významné kybernetické bezpečnostné incidenty a rozsiahle rovnocenné kybernetické bezpečnostné incidenty. Takéto činnosti by mohli ďalej prispievať ku kybernetickej diplomacii Únie. Tretie krajiny pridružené k programu Digitálna Európa by preto mali mať možnosť požiadať o podporu z rezervy EÚ na účely kybernetickej bezpečnosti na celom ich území alebo jeho časti, ak je to stanovené v dohode, prostredníctvom ktorej je tretia krajina pridružená k programu Digitálna Európa. Financovanie určené pre tretie krajiny pridružené k programu Digitálna Európa 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 kybernetické bezpečnostné incidenty a rozsiahle rovnocenné kybernetické bezpečnostné incidenty a v oblasti počiatočného zotavenia sa z nich.

(52) 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 riadených bezpečnostných služieb. Tretie krajiny pridružené k programu Digitálna Európa by mali mať možnosť požiadať o podporu z rezervy EÚ na účely kybernetickej bezpečnosti, ak sú cielené subjekty, pre ktoré žiadajú o podporu z rezervy EÚ na účely kybernetickej bezpečnosti, subjektmi pôsobiacimi v odvetviach s vysokou úrovňou kritickosti alebo subjektmi pôsobiacimi v iných kritických odvetviach a ak zistené incidenty vedú k závažným narušeniam prevádzky alebo by mohli mať účinky presahovania v Únii. Tretie krajiny pridružené k programu Digitálna Európa by mali byť oprávnené na získanie podpory len vtedy, ak sa takáto podpora výslovne stanovuje v dohode, prostredníctvom ktorej sú pridružené k programu Digitálna Európa. Okrem toho by takéto tretie krajiny mali zostať oprávnené len vtedy, ak sú splnené tri kritériá. Po prvé, tretia krajina by mala v plnej miere dodržiavať príslušné podmienky uvedenej dohody. Po druhé, vzhľadom na komplementárnu povahu rezervy EÚ na účely kybernetickej bezpečnosti tretia krajina mala prijať primerané kroky na prípravu na významné kybernetické bezpečnostné incidenty alebo rozsiahle rovnocenné kybernetické bezpečnostné incidenty. Po tretie, poskytovanie podpory z rezervy EÚ na účely kybernetickej bezpečnosti by malo byť v súlade s politikou Únie voči tejto krajine a celkovými vzťahmi s ňou, ako aj s inými politikami Únie v oblasti bezpečnosti. V kontexte posúdenia súladu s uvedením tretím kritériom by Komisia mala konzultovať s vysokým predstaviteľom o zosúladení poskytovania takejto podpory so spoločnou zahraničnou a bezpečnostnou politikou.

(53) Poskytovanie podpory tretím krajinám pridruženým k programu Digitálna Európa môže ovplyvniť vzťahy s tretími krajinami a bezpečnostnú politiku Únie, a to aj v kontexte spoločnej zahraničnej a bezpečnostnej politiky a spoločnej bezpečnostnej a obrannej politiky. Preto je vhodné, aby sa Rade udelili vykonávacie právomoci s cieľom povoliť a spresniť obdobie, počas ktorého sa môže poskytovať takáto podpora. Rada by mala konať na základe návrhu Komisie, pričom náležite zohľadní posúdenie týchto troch kritérií Komisiou. To isté by malo platiť pre obnovenia a návrhy na zmenu alebo zrušenie takýchto aktov. Ak sa Rada za výnimočných okolností domnieva, že došlo k významnej zmene okolností v súvislosti s tretím kritériom, Rada by mala mať možnosť konať z vlastnej iniciatívy a zmeniť alebo zrušiť vykonávací akt, bez čakania na návrh Komisie. Takéto významné zmeny si pravdepodobne vyžiadajú naliehavé opatrenia, budú mať pravdepodobne mimoriadne dôležité dôsledky na vzťahy s tretími krajinami a nebudú vopred vyžadovať podrobné posúdenie zo strany Komisie. Okrem toho by Komisia mala spolupracovať s vysokým predstaviteľom, pokiaľ ide o žiadosti a podporu z tretích krajín pridružených k programu Digitálna Európa a vykonávanie podpory poskytovanej takýmto tretím krajinám. Komisia by mala zohľadniť aj akékoľvek názory, ktoré poskytla agentúra ENISA v súvislosti s takýmito žiadosťami a podporou. Komisia by mala informovať Radu o výsledku posúdenia žiadostí vrátane príslušných úvah v tejto súvislosti a o nasadených službách.

(54) V oznámení Komisie z 18. apríla 2023 o Akadémii kybernetických zručností sa uznal nedostatok kvalifikovaných odborníkov. Takéto zručnosti sú potrebné na dosiahnutie cieľov tohto nariadenia. Únia naliehavo potrebuje odborníkov so zručnosťami a kompetenciami na predchádzanie kybernetickým útokom, ich odhaľovanie a odrádzanie od nich a na obranu Únie vrátane jej najkritickejšej infraštruktúry pred takýmito útokmi a na zabezpečenie jej odolnosti. Na tento účel je dôležité podporovať spoluprácu medzi zainteresovanými stranami vrátane súkromného sektora, akademickej obce a verejného sektora. Rovnako dôležité je vytvoriť synergie na všetkých územiach Únie, aby investície do vzdelávania a odbornej prípravy podporovali vytváranie záruk na zabránenie úniku mozgov alebo rozšíreniu nedostatku zručností v niektorých regiónoch viac ako v iných. Je naliehavo potrebné odstrániť nedostatok zručností v oblasti kybernetickej bezpečnosti s osobitným zameraním na zníženie rodových rozdielov v pracovnej sile v oblasti kybernetickej bezpečnosti s cieľom podporiť prítomnosť žien a ich účasť na navrhovaní digitálnej správy.

(55) V záujme podpory inovácií na digitálnom jednotnom trhu je dôležité posilniť výskum a inovácie v oblasti kybernetickej bezpečnosti, aby sa prispelo k zvýšeniu odolnosti členských štátov a otvorenej strategickej autonómie Únie, čo sú ciele tohto nariadenia. Synergie sú nevyhnutné na posilnenie spolupráce a koordinácie medzi rôznymi zainteresovanými stranami vrátane súkromného sektora, občianskej spoločnosti a akademickej obce.

(56) Toto nariadenie by malo zohľadniť záväzok stanovený v spoločnom vyhlásení Európskeho parlamentu, Rady a Komisie z 26. januára 2022 s názvom Európske vyhlásenie o digitálnych právach a zásadách v digitálnom desaťročí na ochranu záujmov našich demokracií, ľudí, podnikov a verejných inštitúcií Únie pred kybernetickobezpečnostnými rizikami a počítačovou kriminalitou vrátane porušenia ochrany údajov a krádeže identity alebo manipulácie s ňou.

(57) S cieľom doplniť určité nepodstatné prvky tohto nariadenia by sa mala na Komisiu delegovať právomoc prijímať akty v súlade s článkom 290 ZFEÚ s cieľom spresniť druhy a počet služieb reakcie potrebných pre rezervu EÚ na účely kybernetickej bezpečnosti. Je osobitne dôležité, aby Komisia počas prípravných prác uskutočnila príslušné konzultácie, a to aj na úrovni expertov, a aby tieto konzultácie vykonávala v súlade so zásadami stanovenými v Medziinštitucionálnej dohode z 13. apríla 2016 o lepšej tvorbe práva[20]. Predovšetkým v záujme rovnakého zastúpenia pri príprave delegovaných aktov sa všetky dokumenty doručujú Európskemu parlamentu a Rade v rovnakom čase ako expertom z členských štátov, a experti Európskeho parlamentu a Rady majú systematicky prístup na zasadnutia skupín expertov Komisie, ktoré sa zaoberajú prípravou delegovaných aktov.

[20] Ú. v. EÚ L 123, 12.5.2016, s. 1, ELI: http://data.europa.eu/eli/agree_interinstit/2016/512/oj.

(58) V záujme zabezpečenia jednotných podmienok vykonávania tohto nariadenia by sa mali na Komisiu preniesť vykonávacie právomoci s cieľom ďalej spresniť podrobné procedurálne dojednania prideľovania podporných služieb rezervy EÚ na účely kybernetickej bezpečnosti. Uvedené právomoci by sa mali vykonávať v súlade s nariadením Európskeho parlamentu a Rady (EÚ) č. 182/2011[21].

(59) Bez toho, aby boli dotknuté pravidlá týkajúce sa ročného rozpočtu Únie podľa zmlúv, by Komisia mala pri posudzovaní rozpočtových a personálnych potrieb agentúry ENISA zohľadniť povinnosti vyplývajúce z tohto nariadenia.

(60) Komisia by mala pravidelne vykonávať hodnotenie opatrení stanovených v tomto nariadení. Prvé takéto hodnotenie by sa malo uskutočniť v prvých dvoch rokoch po dni nadobudnutia účinnosti tohto nariadenia a potom aspoň každé štyri roky, pričom sa zohľadní načasovanie revízie viacročného finančného rámca stanoveného podľa článku 312 ZFEÚ. Komisia by mala predložiť správu o dosiahnutom pokroku Európskemu parlamentu a Rade. S cieľom posúdiť rôzne požadované prvky vrátane rozsahu informácií zdieľaných v rámci európskeho systému varovania o kybernetickej bezpečnosti by sa Komisia mala opierať výlučne o informácie, ktoré sú ľahko dostupné alebo poskytnuté dobrovoľne. Vzhľadom na geopolitický vývoj a s cieľom zabezpečiť kontinuitu a ďalší rozvoj opatrení stanovených v tomto nariadení po roku 2027 je dôležité, aby Komisia vyhodnotila potrebu prideliť primeraný rozpočet vo viacročnom finančnom rámci na roky 2028 až 2034.

---

[21] Nariadenie Európskeho parlamentu a Rady (EÚ) č. 182/2011 zo 16. februára 2011, ktorým sa ustanovujú pravidlá a všeobecné zásady mechanizmu, na základe ktorého členské štáty kontrolujú vykonávanie vykonávacích právomocí Komisie (Ú. v. EÚ L 55, 28.2.2011, s. 13, ELI: https://eur-lex.europa.eu/eli/reg/2011/182/oj).

(61) Keďže ciele tohto nariadenia, a to posilnenie konkurenčného postavenia priemyslu a služieb v Únii v celom digitálnom hospodárstve a prispievanie k technologickej suverenite a otvorenej strategickej autonómii Únie v oblasti kybernetickej bezpečnosti, nie je možné uspokojivo dosiahnuť na úrovni členských štátov, ale z dôvodov rozsahu alebo dôsledkov činnosti ich možno lepšie dosiahnuť na úrovni Únie, môže Únia prijať opatrenia v súlade so zásadou subsidiarity stanovenou v článku 5 Zmluvy o EÚ. V súlade so zásadou proporcionality podľa uvedeného článku toto nariadenie neprekračuje rámec nevyhnutný na dosiahnutie uvedených cieľov,

PRIJALI TOTO NARIADENIE:

Kapitola I
Všeobecné ustanovenia

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 zriadením:

   a) celoeurópskej siete kybernetických centier (ďalej len „európsky systém varovania pred kybernetickobezpečnostnými hrozbami“) s cieľom vybudovať a posilniť spôsobilosti koordinovaného odhaľovania a spoločnej situačnej informovanosti;

   b) mechanizmu na riešenie kybernetickobezpečnostných núdzových situácií s cieľom podporiť členské štáty pri príprave na významné kybernetické bezpečnostné incidenty a rozsiahle kybernetické bezpečnostné incidenty a podporiť iných používateľov pri reakcii na významné kybernetické bezpečnostné incidenty a rozsiahle rovnocenné kybernetické bezpečnostné incidenty, pri ich zmierňovaní a začatí zotavenia sa z nich;

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

2. Týmto nariadením sa sledujú všeobecné ciele posilniť konkurenčné postavenie priemyslu a služieb v Únii v celom digitálnom hospodárstve vrátane mikropodnikov a malých a stredných podnikov, ako aj startupov, a prispieť k technologickej suverenite a otvorenej strategickej autonómii Únie v oblasti kybernetickej bezpečnosti, a to aj podporou inovácií na digitálnom jednotnom trhu. Tieto ciele sleduje posilňovaním solidarity na úrovni Únie, posilňovaním ekosystému kybernetickej bezpečnosti, zvyšovaním kybernetickej odolnosti členských štátov a rozvíjaním zručností, know-how, schopností a kompetencií pracovnej sily v súvislosti s kybernetickou bezpečnosťou.

3. Všeobecné ciele uvedené v odseku 2 sa dosahujú prostredníctvom týchto špecifických cieľov:

a) posilniť spoločné koordinované spôsobilosti Únie a spoločnú situačnú informovanosť v oblasti odhaľovania kybernetických hrozieb a incidentov;

b) posilniť pripravenosť subjektov pôsobiacich v odvetviach s vysokou úrovňou kritickosti alebo subjektov pôsobiacich v iných kritických odvetviach v celej Únii a posilniť solidaritu rozvojom koordinovaného testovania pripravenosti a posilnených kapacít reakcie a zotavenia na riešenie významných kybernetických bezpečnostných incidentov, rozsiahlych kybernetických bezpečnostných incidentov alebo rozsiahlych rovnocenných kybernetických bezpečnostných incidentov vrátane možnosti sprístupniť podporu Únie týkajúcu sa reakcie na kybernetické bezpečnostné incidenty tretím krajinám pridruženým k programu Digitálna Európa;

c) zvýšiť odolnosť Únie a prispieť k účinnej reakcii prostredníctvom skúmania a posudzovania významných kybernetických bezpečnostných incidentov alebo rozsiahlych kybernetických bezpečnostných incidentov vrátane získavania poznatkov a vo vhodných prípadoch odporúčaní.

4. Opatrenia v rámci tohto nariadenia sa vykonávajú s náležitým ohľadom na právomoci členských štátov a dopĺňajú činnosti siete jednotiek CSIRT, siete EU-CyCLONe a skupiny pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti.

5. Týmto nariadením nie sú dotknuté základné funkcie štátu členských štátov vrátane zabezpečovania územnej celistvosti štátu, udržiavania verejného poriadku a zabezpečovania národnej bezpečnosti. Predovšetkým národná bezpečnosť ostáva vo výlučnej zodpovednosti každého členského štátu.

6. Zdieľanie alebo výmena informácií podľa tohto nariadenia, ktoré sú dôverné podľa predpisov Únie alebo vnútroštátnych predpisov, by sa mala zúžiť na informácie, ktoré sú relevantné a primerané účelu tohto zdieľania alebo výmeny. Takýmto zdieľaním alebo výmenou informácií sa zachováva dôvernosť informácií a chránia sa bezpečnostné a obchodné záujmy dotknutých subjektov. Nezahŕňa to poskytovanie informácií, ktorých zverejnenie by bolo v rozpore so základnými záujmami členských štátov v oblasti národnej bezpečnosti, verejnej bezpečnosti alebo obrany.

Článok 2

Vymedzenie pojmov

Na účely tohto nariadenia sa uplatňuje toto vymedzenie pojmov:

1. „cezhraničné kybernetické centrum“ je platforma s účasťou viacerých krajín zriadená písomnou dohodou o konzorciu, ktorou sa v koordinovanej sieťovej štruktúre spájajú národné kybernetické centrá aspoň z troch členských štátov, a ktorá je určená na zlepšenie monitorovania, odhaľovania a analýzy kybernetických hrozieb na predchádzanie incidentom a na podporu tvorby spravodajských informácií o kybernetických hrozbách, najmä prostredníctvom výmeny relevantných údajov a informácií, vo vhodných prípadoch anonymizovaných, ako aj prostredníctvom zdieľania najmodernejších nástrojov a spoločného rozvoja spôsobilostí v oblasti odhaľovania kybernetických hrozieb, ich analýzy, prevencie a ochrany pred nimi v dôveryhodnom prostredí;

2. „hostiteľské konzorcium“ je konzorcium zložené zo zúčastnených členských štátov , ktoré súhlasili so zriadením cezhraničného kybernetického centra a s prispievaním na účely nadobudnutia nástrojov, infraštruktúry alebo služieb pre cezhraničné kybernetické centrum a na jeho prevádzku;

3. „jednotka CSIRT“ je jednotka CSIRT určená alebo zriadená podľa článku 10 smernice (EÚ) 2022/2555;

4. „subjekt“ je subjekt v zmysle vymedzenia v článku 6 bode 38 smernice (EÚ) 2022/2555;

5. „subjekty pôsobiace v odvetviach s vysokou úrovňou kritickosti“ sú druhy subjektov uvedené v prílohe I k smernici (EÚ) 2022/2555;

6. „subjekty pôsobiace v iných kritických odvetviach“ sú druhy subjektov uvedené v prílohe II k smernici (EÚ) 2022/2555;

7. „riziko“ je riziko v zmysle vymedzenia v článku 6 bode 9 smernice (EÚ) 2022/2555;

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

9. „incident“ je incident v zmysle vymedzenia v článku 6 bode 6 smernice (EÚ) 2022/2555;

10. „významný kybernetický bezpečnostný incident“ je incident, ktorý spĺňa kritériá stanovené v článku 23 ods. 3 smernice (EÚ) 2022/2555;

11. „závažný incident“ je závažný incident v zmysle vymedzenia v článku 3 bode 8 nariadenia Európskeho parlamentu a Rady (EÚ, Euratom) 2023/2841[22];

12. „rozsiahly kybernetický bezpečnostný incident“ je rozsiahly kybernetický incident v zmysle vymedzenia v článku 6 bode 7 smernice (EÚ) 2022/2555;

[22] Nariadenie Európskeho parlamentu a Rady (EÚ, Euratom) 2023/2841 z 13. decembra 2023, ktorým sa stanovujú opatrenia na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v inštitúciách, orgánoch, úradoch a agentúrach Únie (Ú. v. EÚ L, 2023/2841, 18.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2841/oj).

13. „rozsiahly rovnocenný kybernetický bezpečnostný incident“ je v prípade inštitúcií, orgánov, úradov a agentúr Únie závažný incident a v prípade tretích krajín pridružených k programu Digitálna Európa incident, ktorý spôsobí narušenie na úrovni presahujúcej schopnosť dotknutej tretej krajiny pridruženej k programu Digitálna Európa reagovať na tento incident;

14. „tretia krajina pridružená k programu Digitálna Európa“ je tretia krajina, ktorá je zmluvnou stranou dohody s Úniou, ktorá jej umožňuje účasť na programe Digitálna Európa podľa článku 10 nariadenia (EÚ) 2021/694;

15. „verejný obstarávateľ“ je Komisia alebo v rozsahu, v akom bola prevádzka a správa rezervy EÚ na účely kybernetickej bezpečnosti zverená agentúre ENISA podľa článku 14 ods. 5, agentúra ENISA;

16. „poskytovateľ riadených bezpečnostných služieb“ je poskytovateľ riadených bezpečnostných služieb v zmysle vymedzenia v článku 6 bode 40 smernice (EÚ) 2022/2555;

17. „dôveryhodní poskytovatelia riadených bezpečnostných služieb“ sú poskytovatelia riadených bezpečnostných služieb, ktorí sú vybratí a zaradení do rezervy EÚ na účely kybernetickej bezpečnosti v súlade s článkom 17.

Kapitola II
Európsky systém varovania pred kybernetickobezpečnostnými hrozbami

Článok 3

Zriadenie európskeho systému varovania pred kybernetickobezpečnostnými hrozbami

1. Zriaďuje sa európsky systém varovania pred kybernetickobezpečnostnými hrozbami na podporu rozvoja pokročilých spôsobilostí Únie v oblasti odhaľovania, analýzy a spracúvania údajov v súvislosti s kybernetickými hrozbami a na predchádzanie incidentom v Únii, ktorý je celoeurópskou sieťou infraštruktúry, ktorú tvoria národné kybernetické centrá a cezhraničné kybernetické centrá, ktoré sa pripájajú dobrovoľne.

2. Európsky systém varovania pred kybernetickobezpečnostnými hrozbami:

   a) prispieva k lepšej ochrane pred kybernetickobezpečnostnými hrozbami a k reakciám na ne podporou a spoluprácou s príslušnými subjektmi, najmä s jednotkami CSIRT, sieťou jednotiek CSIRT, sieťou EU-CyCLONe a príslušnými orgánmi určenými alebo zriadenými podľa článku 8 ods. 1 smernice (EÚ) 2022/2555, a posilňuje ich spôsobilosti;

   b) zhromažďuje relevantné údaje a informácie o kybernetických hrozbách a incidentoch z rôznych zdrojov v rámci cezhraničných kybernetických centier a zdieľa analyzované alebo súhrnné informácie prostredníctvom cezhraničných kybernetických centier, v relevantných prípadoch so sieťou jednotiek CSIRT;

c) zhromažďuje a podporuje tvorbu vysokokvalitných využiteľných informácií a spravodajských informácií o kybernetických hrozbách, pričom používa najmodernejšie nástroje a pokročilé technológie a zdieľa tieto informácie a spravodajské informácie o kybernetických hrozbách;

d) prispieva k posilneniu koordinovaného odhaľovania kybernetických hrozieb a spoločnej situačnej informovanosti v celej Únii a k vydávaniu varovaní, a to v relevantných prípadoch aj poskytovaním konkrétnych odporúčaní subjektom;

e) poskytuje služby a činnosti pre komunitu v oblasti kybernetickej bezpečnosti v Únii vrátane prispievania k rozvoju pokročilých nástrojov a technológií, ako sú umelá inteligencia a nástroje analýzy údajov.

3. Opatrenia, ktorými sa vykonáva európsky systém varovania pred kybernetickobezpečnostnými hrozbami, sa podporujú financovaním z programu Digitálna Európa a vykonávajú sa v súlade s nariadením (EÚ) 2021/694, najmä s jeho špecifickým cieľom 3.

Článok 4

Národné kybernetické centrá

1. Ak sa členský štát rozhodne zúčastniť sa na európskom systéme varovania pred kybernetickobezpečnostnými hrozbami, určí alebo v príslušných prípadoch zriadi národné kybernetické centrum na účely tohto nariadenia.

2. Národné kybernetické centrum je jediným subjektom, ktorý podlieha právomoci členského štátu. Môže to byť jednotka CSIRT alebo v príslušných prípadoch vnútroštátny orgán pre riadenie kybernetických kríz alebo iný príslušný orgán určený alebo zriadený podľa článku 8 ods. 1 smernice (EÚ) 2022/2555, alebo iný subjekt. Národné kybernetické centrum musí:

   a) mať 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 prispievať k cezhraničnému kybernetickému centru, ako sa uvádza v článku 5; a

   b) byť schopné odhaľovať, zhromažďovať a analyzovať údaje a informácie relevantné pre kybernetické hrozby a incidenty, ako sú napríklad spravodajské informácie o kybernetických hrozbách, a to najmä využívaním najmodernejších technológií, s cieľom predchádzať incidentom.

3. V rámci funkcií uvedených v odseku 2 tohto článku môžu národné kybernetické centrá spolupracovať so subjektmi súkromného sektora na výmene relevantných údajov a informácií na účely odhaľovania a prevencie kybernetických hrozieb a incidentov, a to aj s odvetvovými a medziodvetvovými komunitami kľúčových a dôležitých subjektov, ako sa uvádza v článku 3 smernice (EÚ) 2022/2555. Vo vhodných prípadoch a v súlade s právom Únie a vnútroštátnym právom, informácie požadované alebo prijaté národnými kybernetickými centrami môžu zahŕňať údaje z telemetrie, senzorov a logovania.

4. Členský štát vybraný podľa článku 9 ods. 1 sa zaviaže požiadať svoje národné kybernetické centrum o účasť na cezhraničnom kybernetickom centre.

Článok 5

Cezhraničné kybernetické centrá

1. Ak sú aspoň tri členské štáty odhodlané zabezpečiť, aby ich národné kybernetické centrá spolupracovali na koordinácii svojich činností v oblasti odhaľovania a monitorovania kybernetických hrozieb, tieto členské štáty môžu na účely tohto nariadenia zriadiť hostiteľské konzorcium.

2. Hostiteľské konzorcium je zložené z najmenej troch zúčastnených členských štátov, ktoré súhlasili so zriadením cezhraničného kybernetického centra a s prispievaním na účely nadobudnutia nástrojov, infraštruktúry alebo služieb pre cezhraničné kybernetické centrum a na jeho prevádzku, v súlade s odsekom 4.

3. Ak sa hostiteľské konzorcium vyberie v súlade s článkom 9 ods. 3, jeho členovia uzavrú písomnú dohodu o konzorciu, ktorá:

   a) stanovuje vnútorné mechanizmy na vykonávanie dohody o hosťovaní a používaní uvedenej v článku 9 ods. 3;

   b) zriaďuje cezhraničné kybernetické centrum hostiteľského konzorcia; a

   c) zahŕňa osobitné doložky požadované podľa článku 6 ods. 1 a 2.

4. Cezhraničné kybernetické centrum je platforma viacerých krajín zriadená písomnou dohodou o konzorciu, ako sa uvádza v odseku 3. Do koordinovanej štruktúry siete spája národné kybernetické centrá členských štátov hostiteľského konzorcia. Je navrhnuté na zlepšenie monitorovania, odhaľovania a analýzy kybernetických hrozieb, predchádzanie incidentom a podporu získavania spravodajských informácií o kybernetických hrozbách, najmä prostredníctvom výmeny relevantných údajov a informácií, vo vhodných prípadoch anonymizovaných, ako aj prostredníctvom spoločného využívania najmodernejších nástrojov a spoločného rozvoja spôsobilostí v oblasti odhaľovania kybernetických hrozieb, ich analýzy, prevencie a ochrany pred nimi v dôveryhodnom prostredí.

5. Cezhraničné kybernetické centrum je na právne účely zastupované členom zodpovedajúceho hostiteľského konzorcia, ktorý koná ako koordinátor, alebo hostiteľským konzorciom, ak má právnu subjektivitu. Zodpovednosť za dodržiavanie tohto nariadenia a dohody o hosťovaní a používaní zo strany cezhraničného kybernetického centra sa určí v písomnej dohode o konzorciu uvedenej v odseku 3.

6. Členský štát sa môže pripojiť k existujúcemu hostiteľskému konzorciu so súhlasom členov hostiteľského konzorcia. Písomná dohoda o konzorciu uvedená v odseku 3 a dohoda o hosťovaní a používaní sa zodpovedajúcim spôsobom upravia. Toto nemá vplyv na vlastnícke práva Európskeho centra priemyselných, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti (ďalej len „ECCC“) na nástroje, infraštruktúru alebo služby, ktoré boli už spoločne obstarané s týmto hostiteľským konzorciom.

Článok 6

Spolupráca a zdieľanie informácií v rámci cezhraničných kybernetických centier a medzi nimi

1. Členovia hostiteľského konzorcia zabezpečia, aby ich národné kybernetické centrá v súlade s písomnou dohodou o konzorciu uvedenou v článku 5 ods. 3 zdieľali relevantné informácie, vo vhodných prípadoch anonymizované, ako napríklad informácie týkajúce sa kybernetických hrozieb, udalostí odvrátených v poslednej chvíli, zraniteľností, techník a postupov, indikátorov kompromitácie, nepriateľských taktík, informácií špecifických pre jednotlivé hrozby a aktérov, výstrah a odporúčaní týkajúcich sa konfigurácie kybernetických bezpečnostných nástrojov na odhaľovanie kybernetických útokov, medzi sebou v rámci cezhraničného kybernetického centra, ak takéto zdieľanie informácií:

   a) podporuje a zlepšuje odhaľovanie kybernetických hrozieb a posilňuje spôsobilosti siete jednotiek CSIRT predchádzať incidentom a reagovať na ne alebo zmierňovať ich vplyv;

   b) zvyšuje úroveň kybernetickej bezpečnosti, napríklad 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, fázami reakcie a zotavenia sa alebo podporou spoločného výskumu hrozieb verejnými a súkromnými subjektmi.

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

a) záväzok zabezpečiť medzi členmi hostiteľského konzorcia zdieľanie informácií uvedených v odseku 1 a podmienky, na základe ktorých sa tieto informácie majú zdieľať;

b) rámec riadenia, ktorým sa objasňuje a stimuluje zdieľanie relevantných informácií všetkými účastníkmi, vo vhodných prípadoch anonymizovaných, ako sa uvádza v odseku;

c) ciele v súvislosti s prispievaním k vývoju pokročilých nástrojov a technológií, ako napríklad umelej inteligencie a nástrojov analýzy údajov.

V písomnej dohode o konzorciu sa môže stanoviť, že informácie uvedené v odseku 1 sa majú zdieľať v súlade s právom Únie a vnútroštátnym právom.

3. Cezhraničné kybernetické centrá uzatvárajú medzi sebou dohody o spolupráci, v ktorých sa určia zásady interoperability a zdieľania informácií medzi cezhraničnými kybernetickými centrami. Cezhraničné kybernetické centrá informujú Komisiu o uzavretých dohodách o spolupráci.

4. Zdieľanie informácií, ako sa uvádza v odseku 1, medzi cezhraničnými kybernetickými centrami sa zabezpečuje vysokou úrovňou interoperability. Na podporu takejto interoperability agentúra ENISA v úzkej spolupráci s Komisiou bez zbytočného odkladu a v každom prípade do ... [12 mesiacov odo dňa nadobudnutia účinnosti tohto nariadenia] vydá usmernenia pre interoperabilitu, v ktorých sa spresnia najmä formáty a protokoly na zdieľanie informácií, pričom zohľadní medzinárodné normy a najlepšie postupy, ako aj fungovanie akýchkoľvek zriadených cezhraničných kybernetických centier. Požiadavky na interoperabilitu stanovené v dohodách o spolupráci cezhraničných kybernetických centier vychádzajú z usmernení vydaných agentúrou ENISA.

Článok 7

Spolupráca a zdieľanie informácií so sieťami na úrovni Únie

1. Cezhraničné kybernetické centrá a sieť jednotiek CSIRT úzko spolupracujú najmä na účely zdieľania informácií. Na tento účel sa dohodnú na procedurálnych dojednaniach týkajúcich sa spolupráce a zdieľania relevantných informácií a bez toho, aby bol dotknutý odsek 2, na druhoch informácií, ktoré sa majú zdieľať.

2. Ak cezhraničné kybernetické centrá získajú informácie týkajúce sa potenciálneho alebo prebiehajúceho rozsiahleho kybernetického bezpečnostného incidentu, na účely spoločnej situačnej informovanosti zabezpečia, aby sa relevantné informácie, ako aj včasné varovania bez zbytočného odkladu poskytli orgánom členských štátov a Komisii prostredníctvom siete EU-CyCLONe a siete jednotiek CSIRT.

Článok 8

Bezpečnosť

1. Členské štáty, ktoré sa zúčastňujú na európskom systéme varovania pred kybernetickobezpečnostnými hrozbami, zaistia vysokú úroveň kybernetickej bezpečnosti vrátane dôvernosti a bezpečnosti údajov, ako aj fyzickej bezpečnosti infraštruktúry európskeho systému varovania pred kybernetickobezpečnostnými hrozbami a zaistia primerané spravovanie a kontrolu siete takým spôsobom, aby bola chránená pred hrozbami a aby bola zaistená jej bezpečnosť a bezpečnosť systémov vrátane bezpečnosti údajov a informácií, ktoré sa zdieľajú prostredníctvom siete.

2. Členské štáty, ktoré sa zúčastňujú na európskom systéme varovania pred kybernetickobezpečnostnými hrozbami, zabezpečia, aby zdieľanie informácií uvedených v článku 6 ods. v rámci európskeho systému varovania pred kybernetickobezpečnostnými hrozbami so žiadnym iným subjektom ako orgánom verejnej moci alebo subjektom členského štátu nemalo negatívny vplyv na bezpečnostné záujmy Únie alebo členských štátov.

Článok 9

Financovanie európskeho systému varovania pred kybernetickobezpečnostnými hrozbami

1. Na základe výzvy na vyjadrenie záujmu pre členské štáty, ktoré majú v úmysle zúčastniť sa na európskom systéme varovania pred kybernetickobezpečnostnými hrozbami centrum ECCC vyberie členské štáty, ktoré sa spolu s centrom ECCC zúčastnia spoločného obstarávania nástrojov, infraštruktúry alebo služieb s cieľom zriadiť alebo posilniť spôsobilosti národných kybernetických centier určených alebo zriadených podľa článku 4 ods. 1. Centrum ECCC môže udeľovať vybraným členským štátom granty na financovanie prevádzky takýchto nástrojov, infraštruktúry alebo služieb. Finančný príspevok Únie pokrýva najviac 50 % obstarávacích nákladov na nástroje, infraštruktúru alebo služby a najviac 50 % prevádzkových nákladov. Vybrané členské štáty pokryjú zvyšné náklady. Pred spustením postupu nadobudnutia nástrojov, infraštruktúry alebo služieb centrum ECCC a vybrané členské štáty uzavrú dohodu o hosťovaní a používaní, ktorou sa upravuje používanie nástrojov, infraštruktúry alebo služieb.

2. Ak národné kybernetické centrum členského štátu nie je účastníkom cezhraničného kybernetického centra do dvoch rokov odo dňa nadobudnutia nástrojov, infraštruktúry alebo služieb alebo od dátumu, keď dostalo grantové financovanie, podľa toho, čo nastane skôr, tento členský štát nie je oprávnený na ďalšiu podporu Únie podľa tejto kapitoly, pokiaľ sa nepripojí k cezhraničnému kybernetickému centru.

3. V nadväznosti na výzvu na vyjadrenie záujmu centrum ECCC vyberie hostiteľské konzorcium na účely účasti na spoločnom obstarávaní nástrojov, infraštruktúry alebo služieb s centrom ECCC. Na financovanie prevádzky týchto nástrojov, infraštruktúry alebo služieb môže centrum ECCC udeliť hostiteľskému konzorciu grant. Finančný príspevok Únie pokrýva najviac 75 % obstarávacích nákladov na nástroje, infraštruktúr alebo služby a najviac 50 % prevádzkových nákladov. Hostiteľské konzorcium pokrýva zvyšné náklady. Pred spustením postupu nadobudnutia nástrojov, infraštruktúry alebo služieb centrum ECCC a hostiteľské konzorcium uzavrú dohodu o hosťovaní a používaní, ktorou sa upravuje používanie nástrojov, infraštruktúry alebo služieb.

4. Centrum ECCC pripraví aspoň každé dva roky mapovanie potrebných nástrojov, infraštruktúry alebo služieb a primeranej kvality na zriadenie alebo posilnenie spôsobilostí národných kybernetických centier a cezhraničných kybernetických centier a ich dostupnosti, a to aj od právnych subjektov usadených alebo považovaných za usadené v členských štátoch a kontrolovaných členskými štátmi alebo štátnymi príslušníkmi členských štátov. Pri príprave mapovania centrum ECCC konzultuje so sieťou jednotiek CSIRT, všetkými existujúcimi cezhraničnými kybernetickými centrami, agentúrou ENISA a Komisiou.

Kapitola III
Mechanizmus na riešenie kybernetickobezpečnostných núdzových situácií

Článok 10

Zriadenie mechanizmu na riešenie kybernetickobezpečnostných núdzových situácií

1. Zriaďuje sa mechanizmus na riešenie kybernetickobezpečnostných núdzových situácií (ďalej len „mechanizmus“) s cieľom podporovať zlepšovanie odolnosti Únie voči kybernetickým hrozbám a prípravu, v duchu solidarity, na krátkodobý vplyv významných kybernetických bezpečnostných incidentov, rozsiahlych kybernetických bezpečnostných incidentov a rozsiahlym rovnocenných kybernetických bezpečnostných incidentov a jeho zmierňovanie.

2. V prípade členských štátov sa opatrenia v rámci mechanizmu na riešenie kybernetickobezpečnostných núdzových situácií poskytujú na požiadanie a dopĺňajú úsilie a opatrenia členských štátov s cieľom pripraviť sa na incidenty, reagovať na ne a zotaviť sa z nich.

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

4. Opatrenia v rámci mechanizmu na riešenie kybernetickobezpečnostných núdzových situácií sa vykonávajú predovšetkým prostredníctvom centra ECCC v súlade s nariadením (EÚ) 2021/887. Opatrenia, ktorými sa vykonáva rezerva EÚ na účely kybernetickej bezpečnosti uvedená v článku 11 písm. b) tohto nariadenia, však vykonáva Komisia a agentúra ENISA.

Článok 11

Druhy opatrení

Mechanizmom na riešenie kybernetickobezpečnostných núdzových situácií sa podporujú tieto druhy opatrení:

a) opatrenia v oblasti pripravenosti, a to:

   i) koordinované testovanie pripravenosti subjektov pôsobiacich v odvetviach s vysokou úrovňou kritickosti v celej Únii, ako sa uvádzajú v článku 12;

   ii) iné opatrenia v oblasti pripravenosti pre subjekty pôsobiace v odvetviach s vysokou úrovňou kritickosti alebo subjekty pôsobiace v iných kritických odvetviach, ako sa uvádza v článku 13;

b) opatrenia , ktorými sa podporuje reakcia na významné kybernetické bezpečnostné incidenty, rozsiahle kybernetické bezpečnostné incidenty alebo rozsiahle rovnocenné kybernetické bezpečnostné incidenty a začína zotavenie sa z nich a ktoré majú poskytovať dôveryhodní poskytovatelia riadených bezpečnostných služieb, ktorí sa zúčastňujú na rezerve EÚ na účely kybernetickej bezpečnosti zriadenej podľa článku 14;

c) opatrenia podporujúce vzájomnú pomoc, ako sa uvádza v článku 18.

Článok 12

Koordinované testovanie pripravenosti subjektov

1. Mechanizmus na riešenie kybernetickobezpečnostných núdzových situácií podporuje dobrovoľné koordinované testovanie pripravenosti subjektov pôsobiacich v odvetviach s vysokou úrovňou kritickosti.

2. Koordinované testovanie pripravenosti môže pozostávať z činností pripravenosti, ako sú napríklad penetračné testovanie, a posudzovania hrozieb.

3. Podpora opatrení v oblasti pripravenosti podľa tohto článku sa poskytuje členským štátom predovšetkým vo forme grantov a za podmienok stanovených v príslušných pracovných programoch uvedených v článku 24 nariadenia (EÚ) 2021/694.

4. Komisia na účely podpory koordinovaného testovania pripravenosti subjektov uvedeného v článku 11 písm. a) bodu i) tohto nariadenia v celej Únii po konzultácii so skupinou pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti, so sieťou EU-CyCLONe a s agentúrou ENISA identifikuje spomedzi odvetví s vysokou úrovňou kritickosti uvedených v prílohe I k smernici (EÚ) 2022/2555 dotknuté odvetvia alebo pododvetvia, pre ktoré sa môže vydať výzva na udelenie grantov. Účasť členských štátov na týchto výzvach na predkladanie návrhov je dobrovoľná.

5. Pri určovaní odvetví alebo pododvetví uvedených v odseku 4 Komisia zohľadní koordinované posúdenia rizík a testovanie odolnosti na úrovni Únie a ich výsledky.

6. Skupina pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti v spolupráci s Komisiou, vysokým predstaviteľom Únie pre zahraničné veci a bezpečnostnú politiku (ďalej len „vysoký predstaviteľ“) a agentúrou ENISA a v rámci jej mandátu so sieťou EU-CyCLONe vypracuje spoločné scenáre rizík a metodiky pre koordinované testovanie pripravenosti uvedené v článku 11 písm. a) bode i) a vo vhodných prípadoch pre iné opatrenia v oblasti pripravenosti uvedené v písmene a) bode ii) uvedeného článku.

7. Ak sa subjekt pôsobiaci v odvetví s vysokou úrovňou kritickosti dobrovoľne zúčastňuje na koordinovanom testovaní pripravenosti a výsledkom tohto testovania sú odporúčania konkrétnych opatrení, ktoré by zúčastnený subjekt mohol začleniť do plánu nápravy, orgán členského štátu zodpovedný za koordinované testovanie pripravenosti vo vhodných prípadoch preskúma opatrenia prijaté zúčastnenými subjektmi v nadväznosti na uvedené opatrenia s cieľom posilniť pripravenosť.

Článok 13

Iné opatrenia v oblasti pripravenosti

1. Mechanizmus na riešenie kybernetickobezpečnostných núdzových situácií podporuje opatrenia v oblasti pripravenosti, na ktoré sa nevzťahuje článok 12. Takéto opatrenia zahŕňajú opatrenia v oblasti pripravenosti pre subjekty v odvetviach, ktoré neboli určené na koordinované testovanie pripravenosti podľa článku 12. Takéto opatrenia môžu podporovať monitorovanie zraniteľnosti, monitorovanie rizík, cvičenia a odbornú prípravu.

2. Podpora opatrení v oblasti pripravenosti podľa tohto článku sa poskytuje členským štátom na požiadanie a predovšetkým vo forme grantov a za podmienok stanovených v príslušných pracovných programoch uvedených v článku 24 nariadenia (EÚ) 2021/694.

Článok 14

Vytvorenie rezervy EÚ na účely kybernetickej bezpečnosti

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

2. Rezerva EÚ na účely kybernetickej bezpečnosti sa pozostáva zo služieb reakcie poskytovaných dôveryhodnými poskytovateľmi riadených bezpečnostných služieb vybratými v súlade s kritériami stanovenými v článku 17 ods. 2. Súčasťou rezervy EÚ na účely kybernetickej bezpečnosti môžu byť vopred vyčlenené služby. Vopred vyčlenené služby dôveryhodného poskytovateľa riadených bezpečnostných služieb musia byť konvertibilné na služby pripravenosti súvisiace s predchádzaním incidentom a reakciou na ne, keď sa tieto vopred poskytnuté služby nevyužijú na reakciu na incidenty v čase, na ktorý sú tieto služby vopred vyčlenené. Rezerva EÚ na účely kybernetickej bezpečnosti sa môže na požiadanie nasadiť vo všetkých členských štátoch, v inštitúciách, orgánoch, úradoch a agentúrach Únie a v tretích krajinách pridružených k programu Digitálna Európa, ako sa uvádza v článku 19 ods. 1.

3. Používatelia služieb poskytovaných rezervou EÚ na účely kybernetickej bezpečnosti pozostávajú z:

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

b) tímu CERT-EU, v súlade s článkom 13 nariadenia (EÚ, Euratom) 2023/2841;

c) príslušných orgánov, ako sú jednotky pre riešenie počítačových bezpečnostných incidentov a orgány tretích krajín pridružených k programu Digitálna Európa pre riadenie kybernetických kríz v súlade s článkom 19 ods. 8.

4. Celkovú zodpovednosť za vykonávanie rezervy EÚ na účely kybernetickej bezpečnosti nesie Komisia. Komisia určuje priority a vývoj rezervy EÚ na účely kybernetickej bezpečnosti v koordinácii so skupinou pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti a v súlade požiadavkami používateľov uvedených v odseku 3, dohliada na jej vykonávanie a zaisťuje komplementárnosť, súdržnosť, synergie a prepojenia s ďalšími podpornými opatreniami podľa tohto nariadenia, ako aj s ďalšími opatreniami a programami Únie. Tieto priority sa každé dva roky preskúmajú a vo vhodných prípadoch zrevidujú. Komisia informuje Európsky parlament a Radu o týchto prioritách a všetkých ich revíziách.

5. Bez toho, aby bola dotknutá celková zodpovednosť Komisie za vykonávanie rezervy EÚ na účely kybernetickej bezpečnosti uvedenej v odseku 4 tohto článku, a s výhradou dohody o príspevku v zmysle vymedzenia v článku 2 bode 19 nariadenia (EÚ, Euratom) 2024/2509, Komisia zverí prevádzku a správu rezervy EÚ na účely kybernetickej bezpečnosti, a to úplne alebo čiastočne, agentúre ENISA. Aspekty, ktoré nie sú zverené agentúre ENISA, naďalej podliehajú priamemu riadeniu zo strany Komisie.

6. Agentúra ENISA vypracuje aspoň každé dva roky mapovanie služieb, ktoré potrebujú používatelia uvedení v odseku 3 písm. a) a b) tohto článku. Mapovanie zahŕňa aj dostupnosť takýchto služieb, a to aj od právnych subjektov, ktoré sú usadené alebo sa považujú za usadené v členských štátoch a sú pod kontrolou členských štátov alebo štátnych príslušníkov členských štátov. Agentúra ENISA pri mapovaní tejto dostupnosti posúdi zručnosti a kapacity pracovnej sily Únie v oblasti kybernetickej bezpečnosti relevantné z hľadiska cieľov rezervy EÚ na účely kybernetickej bezpečnosti. Pri príprave mapovania agentúra ENISA konzultuje so skupinou pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti, sieťou EU-CyCLONe, Komisiou a v príslušných prípadoch medziinštitucionálnou radou pre kybernetickú bezpečnosť zriadenou podľa článku 10 nariadenia (EÚ, Euratom) 2023/2841 (IICB). Pri mapovaní dostupnosti služieb agentúra ENISA konzultuje aj s príslušnými zainteresovanými stranami z odvetvia kybernetickej bezpečnosti vrátane poskytovateľov riadených bezpečnostných služieb. Agentúra ENISA po informovaní Rady a po konzultácii so sieťou EU-CyCLONe, Komisiou a v relevantných prípadoch s vysokým predstaviteľom vypracuje podobné mapovanie s cieľom identifikovať potreby používateľov uvedených v odseku 3 písm. c) tohto článku.

7. Komisia je splnomocnená prijímať delegované akty v súlade s článkom 23 s cieľom doplniť toto nariadenie stanovením druhu a počtu služieb reakcie potrebných pre rezervu EÚ na účely kybernetickej bezpečnosti. Pri príprave týchto delegovaných aktov Komisia zohľadní mapovanie uvedené v odseku 6 tohto článku a môže si vymieňať poradenstvo a spolupracovať so skupinou pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti a agentúrou ENISA.

Článok 15

Žiadosti o podporu z rezervy EÚ na účely kybernetickej bezpečnosti

1. Používatelia uvedení v článku 14 ods. 3 môžu požiadať o služby z rezervy EÚ na účely kybernetickej bezpečnosti na podporu reakcie na významné kybernetické bezpečnostné incidenty, rozsiahle kybernetické bezpečnostné incidenty alebo rozsiahle rovnocenné kybernetické bezpečnostné incidenty a na začatie zotavenia sa z nich.

2. Aby mohli používatelia uvedení v článku 14 ods. 3 prijímať podporu z rezervy EÚ na účely kybernetickej bezpečnosti, prijmú všetky primerané opatrenia na zmiernenie účinkov incidentu, v prípade ktorého sa požaduje podpora, v relevantných prípadoch vrátane poskytnutia priamej technickej pomoci a ďalších zdrojov s cieľom pomôcť pri reakcii na incident a pri úsilí o zotavenie sa.

3. Žiadosti o podporu sa postupujú verejnému obstarávateľovi takto:

   a) v prípade používateľov uvedených v článku 14 ods. 3 písm. a) tohto nariadenia prostredníctvom jednotného kontaktného miesta určeného alebo zriadeného podľa článku 8 ods. 3 smernice (EÚ) 2022/2555;

b) v prípade používateľa uvedeného v článku 14 ods. 3 písm. b) týmto používateľom;

c) v prípade používateľov uvedených v článku 14 ods. 3 písm. c) prostredníctvom jednotného kontaktného miesta uvedeného v článku 19 ods. 9.

4. V prípade žiadostí používateľov uvedených v článku 14 ods. 3 písm. a) informujú členské štáty sieť jednotiek CSIRT a vo vhodných prípadoch sieť EU-CyCLONe o žiadostiach ich používateľov o podporu pri reakcii na incidenty a pri počiatočnom zotavení sa z nich.

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

a) primerané informácie týkajúce sa postihnutého subjektu a potenciálneho vplyvu incidentu na:

i) v prípade používateľov uvedených v článku 14 ods. 3 písm. a) postihnuté členské štáty a používateľov vrátane rizika rozšírenia do iného členského štátu;

ii) v prípade používateľa uvedeného v článku 14 ods. 3 písm. b) postihnuté inštitúcie, orgány, úrady alebo agentúry Únie;

iii) v prípade používateľov uvedených v článku 14 ods. 3 písm. c) postihnuté krajiny pridružené k programu Digitálna Európa;

b) informácie týkajúce sa vyžiadanej služby spolu s plánovaným použitím vyžiadanej podpory vrátane uvedenia odhadovaných potrieb;

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

d) v relevantných prípadoch dostupné informácie o ďalších formách podpory dostupnej pre postihnutý subjekt.

6. Na uľahčenie predkladania žiadostí o podporu z rezervy EÚ na účely kybernetickej bezpečnosti vypracuje agentúra ENISA v spolupráci s Komisiou a sieťou EU-CyCLONe vzor.

7. Komisia môže prostredníctvom vykonávacích aktov bližšie určiť podrobné procedurálne dojednania týkajúce sa spôsobu, akým sa služby podpory rezervy EÚ na účely kybernetickej bezpečnosti vyžiadajú a spôsobu, akým sa má na tieto žiadosti odpovedať podľa tohto článku, článku 16 ods. 1 a článku 19 ods. 10, vrátane dojednaní na predkladanie takýchto žiadostí a poskytovanie odpovedí a vzorov správ uvedených v článku 16 ods. 9. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 24 ods. 2.

Článok 16

Vykonávanie podpory z rezervy EÚ na účely kybernetickej bezpečnosti

1. V prípade žiadostí používateľov uvedených v článku 14 ods. 3 písm. a) a b) žiadosti o podporu z rezervy EÚ na účely kybernetickej bezpečnosti posudzuje verejný obstarávateľ. Odpoveď sa zašle používateľom uvedeným v článku 14 ods. 3 písm. a) a b) bezodkladne a v každom prípade najneskôr do 48 hodín od predloženia žiadosti, aby sa zabezpečila účinnosť podpory. Verejný obstarávateľ informuje Radu a Komisiu o výsledkoch procesu.

2. Pokiaľ ide o informácie zdieľané počas vyžiadania a poskytovania služieb rezervy EÚ na účely kybernetickej bezpečnosti, všetky strany zapojené do uplatňovania tohto nariadenia:

   a) obmedzia používanie a zdieľanie týchto informácií na to, čo je potrebné na plnenie ich povinností alebo funkcií podľa tohto nariadenia;

   b) používajú a zdieľajú všetky informácie, ktoré sú dôverné alebo utajované podľa práva Únie a vnútroštátneho práva, len v súlade s uvedeným právom; a

   c) zabezpečia účinnú, efektívnu a bezpečnú výmenu informácií, vo vhodných prípadoch využívajúc a dodržiavajúc príslušné protokoly na zdieľanie informácií vrátane semaforového protokolu.

3. Pri posudzovaní jednotlivých žiadostí podľa článku 16 ods. 1 a článku 19 ods. 10 verejný obstarávateľ alebo Komisia, podľa príslušného prípadu, najprv posúdi, či sú splnené kritériá uvedené v článku 15 ods. 1 a 2. Ak je to tak, posúdi trvanie a povahu podpory, ktorá je primeraná, so zreteľom na cieľ uvedený v článku 1 ods. 3 písm. b) a v relevantných prípadoch na tieto kritériá:

a) rozsah a závažnosť incidentu;

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

c) potenciálny vplyv incidentu na postihnuté členské štáty, na inštitúcie, orgány, úrady alebo agentúry Únie alebo na tretie krajiny pridružené k programu Digitálna Európa;

d) potenciálny cezhraničný charakter incidentu a riziko presahovania na ďalšie členské štáty, na inštitúcie, orgány, úrady alebo agentúry Únie alebo na tretie krajiny pridružené k programu Digitálna Európa;

e) opatrenia prijaté používateľom s cieľom pomôcť pri reakcii na incident a pri úsilí o počiatočné zotavenie sa, ako sa uvádza v článku 15 ods. 2.

4. S cieľom priorizovať žiadosti v prípade súbežných žiadostí používateľov uvedených v článku 14 ods. 3 sa v relevantných prípadoch zohľadnia kritériá uvedené v odseku 3 tohto článku bez toho, aby bola dotknutá zásada lojálnej spolupráce medzi členskými štátmi a inštitúciami, orgánmi, úradmi a agentúrami Únie. Ak sa dve alebo viaceré žiadosti posudzujú ako rovnocenné podľa uvedených kritérií, žiadostiam používateľov z členských štátov sa prisúdi vyššia priorita. Ak bola prevádzka a správa rezervy EÚ na účely kybernetickej bezpečnosti úplne alebo čiastočne zverená agentúre ENISA podľa článku 14 ods. 5, agentúra ENISA a Komisia úzko spolupracujú s cieľom uprednostniť žiadosti v súlade s týmto odsekom.

5. Služby rezervy EÚ na účely kybernetickej bezpečnosti sa poskytujú v súlade s osobitnými dohodami medzi dôveryhodným poskytovateľom riadených bezpečnostných služieb a používateľom, ktorému sa poskytuje podpora v rámci rezervy EÚ na účely kybernetickej bezpečnosti. Tieto služby sa môžu poskytovať v súlade s osobitnými dohodami medzi dôveryhodným poskytovateľom riadených bezpečnostných služieb, používateľom a postihnutým subjektom. Všetky dohody uvedené v tomto odseku zahŕňajú okrem iného podmienky zodpovednosti.

6. Dohody uvedené v odseku 5 vychádzajú zo vzorov vypracovaných agentúrou ENISA po konzultácii s členskými štátmi a vo vhodných prípadoch s inými používateľmi rezervy EÚ na účely kybernetickej bezpečnosti.

7. Komisia, agentúra ENISA a používatelia rezervy EÚ na účely kybernetickej bezpečnosti nenesú zmluvnú zodpovednosť za škodu spôsobenú tretím stranám v dôsledku služieb poskytnutých v rámci vykonávania rezervy EÚ na účely kybernetickej bezpečnosti.

8. Používatelia môžu využívať služby rezervy EÚ na účely kybernetickej bezpečnosti poskytované v reakcii na žiadosť podľa článku 15 ods. 1 len s cieľom podporiť reakciu na významné kybernetické bezpečnostné incidenty, rozsiahle kybernetické bezpečnostné incidenty alebo rozsiahle rovnocenné kybernetické bezpečnostné incidenty a začať zotavenie sa z nich. Tieto služby môžu využívať len v súvislosti:

   a) so subjektmi pôsobiacimi v odvetviach s vysokou úrovňou kritickosti alebo subjektmi pôsobiacimi v iných kritických odvetviach v prípade používateľov uvedených v článku 14 ods. 3 písm. a) a rovnocennými subjektmi v prípade používateľov uvedených v článku 14 ods. 3 písm. c); a

   b) s inštitúciami, orgánmi, úradmi a agentúrami Únie v prípade používateľa uvedeného v článku 14 ods. 3 písm. b).

9. Do dvoch mesiacov od skončenia podpory používateľa, ktorým bola poskytnutá podpora, poskytnú súhrnnú správu o poskytnutých službách, dosiahnutých výsledkoch a získaných poznatkoch:

   a) Komisii, agentúre ENISA, sieti jednotiek CSIRT a sieti EU-CyCLONe v prípade používateľov uvedených v článku 14 ods. 3 písm. a);

   b) Komisii, agentúre ENISA a rade IICB prípade používateľa uvedeného v článku 14 ods. 3 písm. b);

c) Komisii v prípade používateľov uvedených v článku 14 ods. 3 písm. c).

Komisia postúpi všetky súhrnné správy prijaté od používateľov uvedených v článku 14 ods. 3 podľa prvého pododseku písm. c) tohto odseku Rade a vysokému predstaviteľovi.

10. Ak bola prevádzka a správa rezervy EÚ na účely kybernetickej bezpečnosti úplne alebo čiastočne zverená agentúre ENISA podľa článku 14 ods. 5 tohto nariadenia, agentúra ENISA v tomto ohľade pravidelne podáva správy Komisii a konzultuje s ňou. V tejto súvislosti agentúra ENISA bezodkladne zašle Komisii všetky žiadosti, ktoré dostane od používateľov uvedených v článku 14 ods. 3 písm. c) tohto nariadenia, a ak je to potrebné na účely priorizácie podľa tohto článku, všetky žiadosti, ktoré dostala od používateľov uvedených v článku 14 ods. 3 písm. a) alebo b) tohto nariadenia. Povinnosťami uvedenými v tomto odseku nie je dotknutý článok 14 nariadenia (EÚ) 2019/881.

11. V prípade používateľov uvedených v článku 14 ods. 3 písm. a) a b) verejný obstarávateľ pravidelne a aspoň dvakrát ročne podáva skupine pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti správu o využívaní a výsledkoch podpory.

12. V prípade používateľov uvedených v článku 14 ods. 3 písm. c) Komisia podáva Rade správu a informuje vysokého predstaviteľa pravidelne a aspoň dvakrát ročne o využívaní a výsledkoch podpory.

Článok 17

Dôveryhodní poskytovatelia riadených bezpečnostných služieb

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) 2024/2509 a v súlade s týmito zásadami:

   a) zaistiť, aby súčasťou služieb zahrnutých v rezerve EÚ na účely kybernetickej bezpečnosti boli ako celok služby, ktoré môžu byť nasadené vo všetkých členských štátoch, pričom sa zohľadňujú najmä vnútroštátne požiadavky na poskytovanie takýchto služieb vrátane jazykov, 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 Únie tým, že bude prispievať k cieľom stanoveným v článku 3 nariadenia (EÚ) 2021/694 vrátane podpory rozvíjania zručností v oblasti kybernetickej bezpečnosti v Únii.

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

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

b) poskytovateľ a všetky príslušné dcérske spoločnosti a subdodávatelia dodržiavajú príslušné pravidlá ochrany utajovaných skutočností a majú zavedené vhodné opatrenia v relevantných prípadoch vrátane vzájomných dohôd na ochranu dôverných informácií týkajúcich sa služby, a najmä dôkazov, zistení a správ;

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 do služby, ak to požaduje členský štát;

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

f) poskytovateľ disponuje hardvérovým a softvérovým vybavením potrebným na podporu požadovanej služby, ktoré nesmie obsahovať známe využiteľné zraniteľnosti, musí zahŕňať najnovšie bezpečnostné aktualizácie a v každom prípade musí spĺňať všetky príslušné ustanovenia nariadenia Európskeho parlamentu a Rady (EÚ) 2024/...[23+];

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

h) poskytovateľ je schopný poskytnúť službu v krátkom čase v členských štátoch, v ktorých môže službu poskytovať;

i) poskytovateľ je schopný poskytnúť službu v jednom alebo vo viacerých úradných jazykoch inštitúcií Únie alebo členského štátu, ako to vyžadujú členské štáty alebo používatelia uvedení v článku 14 ods. 3 písm. b) a c), v ktorých poskytovateľ môže poskytnúť službu;

j) po zavedení európskej schémy certifikácie kybernetickej bezpečnosti pre riadené bezpečnostné služby podľa nariadenia (EÚ) 2019/881 musí byť poskytovateľ certifikovaný v súlade s uvedenou schémou do dvoch rokov od začiatku uplatňovania uvedenej schémy;

---

[23] Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/... z ... o horizontálnych požiadavkách kybernetickej bezpečnosti pre produkty s digitálnymi prvkami a o zmene nariadení (EÚ) č. 168/2013 a (EÚ) 2019/1020 a smernice (EÚ) 2020/1828 (akt o kybernetickej odolnosti) (Ú. v EÚ L ..., …, ELI: …).

[+] Ú. v.: vložte, prosím, do textu číslo nariadenia nachádzajúceho sa v dokumente PE-CONS 100/23 (2022/0272(COD)) a do poznámky pod čiarou vložte číslo, dátum, odkaz na uverejnenie v úradnom vestníku a odkaz na ELI uvedeného nariadenia.

k) poskytovateľ zahrnie do ponuky podmienky prevodu pre všetky nevyužité služby reakcie na incidenty, ktoré by sa mohli previesť na služby pripravenosti úzko súvisiace s reakciou na incidenty, ako sú napríklad cvičenia alebo školenia.

3. Na účely obstarávania služieb pre rezervu EÚ na účely kybernetickej bezpečnosti môže verejný obstarávateľ vo vhodných prípadoch vypracovať dodatočné kritériá a požiadavky ku kritériám a požiadavkám uvedeným v odseku 2, a to v úzkej spolupráci s členskými štátmi.

Článok 18

Opatrenia podporujúce vzájomnú pomoc

1. Mechanizmus na riešenie núdzových situácií v oblasti kybernetickej bezpečnosti poskytuje podporu technickej pomoci od jedného členského štátu inému členskému štátu, ktorý čelí významnému kybernetickému bezpečnostnému incidentu alebo rozsiahlemu kybernetickému bezpečnostnému incidentu, a to vrátanie prípadov uvedených v článku 11 ods. 3 písm. f) smernice (EÚ) 2022/2555.

2. Podpora na technickú vzájomnú pomoc uvedenú v odseku 1 tohto článku sa poskytuje vo forme grantov a za podmienok stanovených v príslušných pracovných programoch uvedených v článku 24 nariadenia (EÚ) 2021/694.

Článok 19

Podpora tretím krajinám pridruženým k programu Digitálna Európa

1. Tretia krajina pridružená k programu Digitálna Európa môže požiadať o podporu z rezervy EÚ na účely kybernetickej bezpečnosti, ak sa v dohode, prostredníctvom ktorej je pridružená k programu Digitálna Európa, stanovuje účasť na rezerve na účely kybernetickej bezpečnosti. Uvedená dohoda obsahuje ustanovenia, ktorými sa od dotknutej tretej krajiny pridruženej k programu Digitálna Európa vyžaduje, aby dodržiavala povinnosti stanovené v odsekoch 2 a 9 tohto článku. Na účely účasti tretej krajiny na rezerve EÚ na účely kybernetickej bezpečnosti môže čiastočné pridruženie tretej krajiny k programu Digitálna Európa zahŕňať pridruženie obmedzené na operačný cieľ uvedený v článku 6 ods. 1 písm. g) nariadenia (EÚ) 2021/694.

2. Do troch mesiacov od uzavretia dohody uvedenej v odseku 1 a v každom prípade pred prijatím akejkoľvek podpory z rezervy EÚ na účely kybernetickej bezpečnosti tretie krajiny pridružené k programu Digitálna Európa poskytnú Komisii 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 kybernetické bezpečnostné incidenty alebo rozsiahle rovnocenné kybernetické bezpečnostné incidenty, ako aj informácií o zodpovedných vnútroštátnych subjektoch vrátane jednotiek pre riešenie počítačových bezpečnostných incidentov alebo rovnocenných subjektov, o ich spôsobilostiach a zdrojoch, ktoré sú im pridelené. Tretia krajina pridružená k programu Digitálna Európa pravidelne, najmenej však raz ročne, poskytuje aktualizácie týchto informácií. Komisia poskytne tieto informácie vysokému predstaviteľovi a agentúre ENISA na účely uľahčenia uplatňovania odseku 11.

3. Komisia v súvislosti s každou treťou krajinou pridruženou k programu Digitálna Európa uvedenou v odseku 1 pravidelne a aspoň raz ročne posudzuje tieto kritériá:

a) či daná krajina dodržiava podmienky dohody uvedenej v odseku 1, pokiaľ sa tieto podmienky týkajú účasti na rezerve EÚ na účely kybernetickej bezpečnosti;

b) či daná krajina na základe informácií uvedených v odseku 2 prijala primerané kroky s cieľom pripraviť sa na významné kybernetické bezpečnostné incidenty alebo rozsiahle rovnocenné kybernetické bezpečnostné incidenty; a

c) či je poskytovanie podpory v súlade s politikou Únie voči tejto krajine a celkovými vzťahmi s ňou, ako aj v súlade s inými politikami Únie v oblasti bezpečnosti.

Komisia sa pri vykonávaní posúdenia uvedeného v prvom pododseku poradí s vysokým predstaviteľom, pokiaľ ide o kritérium uvedené v písmene c) uvedeného pododseku.

Ak Komisia dospeje k záveru, že tretia krajina pridružená k programu Digitálna Európa spĺňa všetky podmienky uvedené v prvom pododseku, predloží Rade návrh na prijatie vykonávacieho aktu v súlade s odsekom 4, ktorým sa povolí poskytovanie podpory z rezervy EÚ na účely kybernetickej bezpečnosti tejto krajine.

4. Rada môže prijať vykonávacie akty uvedené v odseku 3. Tieto vykonávacie akty sa uplatňujú najviac jeden rok. Môžu sa obnoviť. Môžu zahŕňať limit, nie kratší ako 75 dní, na počet dní, počas ktorých sa môže poskytnúť podpora na základe jedinej žiadosti.

Na účely tohto článku Rada koná urýchlene a spravidla prijme vykonávacie akty uvedené v tomto odseku do ôsmich týždňov od prijatia relevantného návrhu Komisie podľa odseku 3 tretieho pododseku.

5. Rada môže na návrh Komisie kedykoľvek zmeniť alebo zrušiť vykonávací akt prijatý podľa odseku 4.

Ak sa Rada domnieva, že došlo k významnej zmene týkajúcej sa kritéria uvedeného v odseku 3 prvom pododseku písm. c), môže na základe riadne odôvodnenej iniciatívy jedného alebo viacerých členských štátov zmeniť alebo zrušiť vykonávací akt prijatý podľa odseku 4.

6. Rada pri výkone svojich vykonávacích právomocí podľa tohto článku uplatňuje kritériá uvedené v odsek 3 prvom pododseku a vysvetlí svoje posúdenie týchto kritérií. Rada vysvetlí významnú zmenu uvedenú v uvedenom pododseku najmä v prípade, ak koná z vlastnej iniciatívy podľa odseku 5 druhého pododseku.

7. Podpora z rezervy EÚ na účely kybernetickej bezpečnosti poskytovaná tretej krajine pridruženej k programu Digitálna Európa musí byť v súlade so všetkými osobitnými podmienkami stanovenými v dohode uvedenej v odseku 1.

8. Medzi používateľov z tretích krajín pridružených k programu Digitálna Európa oprávnených prijímať služby z rezervy EÚ na účely kybernetickej bezpečnosti patria príslušné orgány, ako napríklad jednotky pre riešenie počítačových bezpečnostných incidentov alebo rovnocenné subjekty a orgány pre riadenie kybernetických kríz.

9. Každá tretia krajina pridružená k programu Digitálna Európa, 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.

10. Žiadosti o podporu z rezervy EÚ na účely kybernetickej bezpečnosti podľa tohto článku posudzuje Komisia. Verejný obstarávateľ môže poskytnúť podporu tretej krajine len vtedy a dovtedy, kým je v platnosti vykonávací akt Rady, ktorým sa povoľuje takáto podpora vo vzťahu k tejto krajine, prijatý podľa odseku 4 tohto článku. Odpoveď sa bez zbytočného odkladu zašle používateľom uvedeným v článku 14 ods. 3 písm. c).

11. Po prijatí žiadosti o podporu podľa tohto článku Komisia bezodkladne informuje Radu. Komisia informuje Radu o posúdení žiadosti. Komisia spolupracuje aj s vysokým predstaviteľom, pokiaľ ide o prijaté žiadosti a vykonávanie priznanej podpory tretím krajinám pridruženým k programu Digitálna Európa z rezervy EÚ na účely kybernetickej bezpečnosti. Komisia popri tom zohľadní aj akékoľvek názory, ktoré poskytla agentúra ENISA v súvislosti s týmito žiadosťami.

Článok 20

Koordinácia s mechanizmami krízového riadenia Únie

1. V prípadoch, keď sú významné kybernetické bezpečnostné incidenty, rozsiahle kybernetické bezpečnostné incidenty alebo rozsiahle rovnocenné kybernetické bezpečnostné incidenty spôsobené katastrofami v zmysle vymedzenia v článku 4 ods. 1 rozhodnutia 1313/2013/EÚ alebo majú za následok takéto katastrofy, podporou poskytovanou podľa tohto nariadenia pri reakcii na takéto incidenty sa dopĺňajú opatrenia podľa uvedeného rozhodnutia, pričom toto rozhodnutie ňou nie je dotknuté.

2. V prípade rozsiahleho kybernetického bezpečnostného incidentu alebo rozsiahleho rovnocenného kybernetického bezpečnostného incidentu, keď sa aktivujú dojednania EÚ o integrovanej politickej reakcii na krízu podľa vykonávacieho rozhodnutia Rady (EÚ) 2018/1993 (ďalej len „dojednania IPRK“), sa podpora podľa tohto nariadenia pri reakcii na takýto incident vykonáva v súlade s príslušnými postupmi v rámci dojednaní IPRK.

Kapitola IV
Európsky mechanizmus preskúmania kybernetických bezpečnostných incidentov

Článok 21

Európsky mechanizmus preskúmania kybernetických bezpečnostných incidentov

1. Na žiadosť Komisie alebo siete EU-CyCLONe, agentúra ENISA s podporou siete jednotiek CSIRT a so súhlasom dotknutého členského štátu preskúma a posúdi kybernetické hrozby, známe využiteľné zraniteľnosti a zmierňujúce opatrenia, pokiaľ ide o konkrétny významný kybernetický bezpečnostný incident alebo rozsiahly kybernetický bezpečnostný incident. Po dokončení preskúmania a posúdenia incidentu a s cieľom zabrániť alebo zmierniť budúce incidenty na základe získaných poznatkov predloží agentúra ENISA správu o preskúmaní incidentu sieti EU-CyCLONe, sieti jednotiek CSIRT, dotknutým členským štátom a Komisii s cieľom podporiť ich pri plnení ich úloh, najmä úlohy stanovené v článkoch 15 a 16 smernice (EÚ) 2022/2555. Ak má incident vplyv na tretiu krajinu pridruženú k programu Digitálna Európa, agentúra ENISA poskytne správu Rade. V takýchto prípadoch Komisia správu poskytne vysokému predstaviteľovi.

2. S cieľom vypracovať správu o preskúmaní incidentu uvedenú v odseku 1 tohto článku agentúra ENISA spolupracuje so všetkými príslušnými zainteresovanými stranami a získava od nich spätnú väzbu vrátane zástupcov členských štátov, Komisie a iných relevantných inštitúcií, orgánov, úradov a agentúr Únie, odvetvia vrátane poskytovateľov riadených bezpečnostných služieb a používateľov služieb v oblasti kybernetickej bezpečnosti. Vo vhodných prípadoch agentúra ENISA v spolupráci s jednotkami CSIRT a v relevantných prípadoch s príslušnými orgánmi určenými alebo zriadenými podľa článku 8 ods. 1 podľa smernice (EÚ) 2022/2555 spolupracuje aj so subjektmi postihnutými významnými kybernetickými bezpečnostnými incidentmi alebo rozsiahlymi kybernetickými bezpečnostnými incidentmi. Zástupcovia, s ktorými sa uskutočňujú konzultácie, oznámia každý potenciálny konflikt záujmov.

3. Súčasťou správy o preskúmaní incidentu uvedenej v odseku 1 tohto článku je preskúmanie a analýza konkrétneho významného kybernetického bezpečnostného incidentu alebo rozsiahleho kybernetického bezpečnostného incidentu vrátane hlavných príčin, známych využiteľných zraniteľností a získaných poznatkov. Agentúra ENISA zabezpečí, aby bola správa v súlade s právom Únie alebo vnútroštátnym právom v oblasti ochrany citlivých alebo utajovaných skutočností. Ak o to príslušné členské štáty alebo iní používatelia uvedení v článku 14 ods. 3, ktorých sa incident týka, požiadajú, údaje a informácie uvedené v správe sa anonymizujú. Neobsahuje žiadne podrobnosti o aktívne zneužívaných zraniteľných miestach, ktoré zostávajú neopravené.

4. Vo vhodných prípadoch sa v správe o preskúmaní incidentu uvádzajú odporúčania na zlepšenie prístupu Únie ku kybernetickej bezpečnosti a táto správa môže obsahovať najlepšie postupy a poznatky získané od príslušných zainteresovaných strán.

5. Agentúra ENISA môže vydať verejne dostupnú verziu správy o preskúmaní incidentu. Uvedená verzia správy obsahuje len spoľahlivé verejné informácie alebo iné spoľahlivé informácie so súhlasom dotknutých členských štátov a, pokiaľ ide o informácie týkajúce sa používateľa, ako sa uvádza v článku 14 ods. 3 písm. b) alebo c), so súhlasom daného používateľa.

Kapitola V
Záverečné ustanovenia

Článok 22

Zmeny nariadenia (EÚ) 2021/694

Nariadenie (EÚ) 2021/694 sa mení takto:

1. Článok 6 sa mení takto:

a) odsek 1 sa mení takto:

i) vkladá sa toto písmeno:

„aa) podpora rozvoja európskeho systému varovania pred kybernetickobezpečnostnými hrozbami zriadeného podľa článku 3 nariadenia Európskeho parlamentu a Rady (EÚ) …/…[*+] (ďalej len „európsky systém varovania pred kybernetickobezpečnostnými hrozbami“) vrátane rozvoja, nasadenia a prevádzky národných kybernetických a cezhraničných kybernetických centier, ktoré prispievajú k situačnej informovanosti v Únii a k zlepšovaniu spôsobilostí Únie v oblasti spravodajských informácií o kybernetických hrozbách;

---

[*] Nariadenie Európskeho parlamentu a Rady (EÚ) .../... z ..., ktorým sa stanovujú opatrenia na posilnenie solidarity a kapacít v Únii na odhaľovanie kybernetických hrozieb a incidentov, prípravu a reakciu na ne a ktorým sa mení nariadenie (EÚ) 2021/694 (akt o kybernetickej solidarite) (Ú. v. EÚ L, …, ELI: …).“;

[+] Ú. v.: vložte, prosím, do textu číslo nariadenia nachádzajúceho sa v PE-CONS 94/24 (2023/0109(COD)) a vložte číslo, dátum, odkaz na uverejnenie a odkaz ELI uvedeného nariadenia do poznámky pod čiarou.

ii) dopĺňa sa toto písmeno:

„g) zriadenie a prevádzkovanie mechanizmu na riešenie kybernetickobezpečnostných núdzových situácií zriadeného podľa článku 10 nariadenia (EÚ) .../...[+] vrátane rezervy EÚ na účely kybernetickej bezpečnosti vytvorenej podľa článku 14 uvedeného nariadenia (ďalej len „rezerva EÚ na účely kybernetickej bezpečnosti“) s cieľom podporovať členské štáty pri príprave na významné kybernetické bezpečnostné incidenty a rozsiahle kybernetické bezpečnostné incidenty a pri reakcii na ne, a to doplnkovo k vnútroštátnym zdrojom a spôsobilostiam a iným formám podpory dostupným na úrovni Únie, a podporovať ostatných používateľov pri reakcii na významné kybernetické bezpečnostné incidenty a rozsiahle rovnocenné kybernetické bezpečnostné incidenty;“;

b) odsek 2 sa nahrádza takto:

„2. Akcie v rámci špecifického cieľa 3 sa vykonávajú predovšetkým 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[*]. Rezervu EÚ na účely kybernetickej bezpečnosti však vykonáva Komisia a, v súlade s článkom 14 ods. 6 nariadenia (EÚ) .../...[+] agentúra ENISA.

---

[*] 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).“

[+] Ú. v.: vložte, prosím, do textu číslo nariadenia nachádzajúceho sa v dokumente PE-CONS 94/24 (2023/0109(COD)).

2. Článok 9 sa mení takto:

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

„b) 1 760 806 000 EUR na špecifický cieľ 2 – Umelá inteligencia;

c) 1 372 020 000 EUR na špecifický cieľ 3 – Kybernetická bezpečnosť a dôvera;

d) 482 640 000 EUR na špecifický cieľ 4 – Pokročilé digitálne zručnosti;“;

b) dopĺňa sa tento odsek:

„8. Odchylne od článku 12 ods. 1 nariadenia o rozpočtových pravidlách sa nepoužité viazané a platobné rozpočtové prostriedky na akcie v súvislosti s vykonávaním rezervy EÚ na účely kybernetickej bezpečnosti a akcií podporujúcich vzájomnú pomoc podľa nariadenia (EÚ) …/…[+], 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. Európsky Parlament a Rada sú informovaní o rozpočtových prostriedkoch prenesených podľa článku 12 ods. 6 nariadenia o rozpočtových pravidlách.“

[+] Ú. v.: vložte, prosím, do textu číslo nariadenia nachádzajúceho sa v dokumente PE-CONS 94/24 (2023/0109(COD)).

3. Článok 12 sa mení takto:

a) vkladajú sa nasledovné odseky:

„5a. Odsek 5 sa neuplatňuje, pokiaľ ide o právne subjekty usadené v Únii, ale sú kontrolované z tretích krajín, na žiadne akcie, ktorým sa vykonáva európsky systém varovania pred kybernetickobezpečnostnými hrozbami, ak sú v súvislosti s dotknutou akciou splnené obe tieto podmienky:

a) existuje skutočné riziko vzhľadom na výsledky mapovania vykonaného podľa článku 9 ods. 4 nariadenia (EÚ) .../...[+], že potrebné a dostatočné nástroje, infraštruktúra a služby na to, aby táto akcia primerane prispela k cieľu európskeho systému varovania o kybernetickej bezpečnosti, nebudú k dispozícii od právnych subjektov usadených alebo považovaných za usadených v členských štátoch a kontrolovaných členskými štátmi alebo štátnymi príslušníkmi členských štátov;

b) bezpečnostné riziko obstarávania od takýchto právnych subjektov v rámci európskeho systému varovania o kybernetickej bezpečnosti je primerané prínosom a neoslabuje základné bezpečnostné záujmy Únie a jej členských štátov.

[+] Ú. v.: vložte, prosím, do textu číslo nariadenia nachádzajúceho sa v dokumente PE-CONS 94/24 (2023/0109(COD)).

5b. Odsek 5 sa neuplatňuje, pokiaľ ide o právne subjekty, ktoré sú usadené v Únii, ale sú kontrolované z tretích krajín, na žiadnu akciu, ktorou sa vykonáva rezerva EÚ na účely kybernetickej bezpečnosti, ak sú v súvislosti s dotknutou akciou splnené obe tieto podmienky:

a) existuje skutočné riziko vzhľadom na výsledky mapovania vykonaného podľa článku 14 ods. 6 nariadenia (EÚ) .../...[+], že potrebné technológie, odborné znalosti alebo kapacity z rezervy EÚ na účely kybernetickej bezpečnosti na to, aby primerane vykonávala svoje funkcie, nebudú k dispozícii od právnych subjektov usadených alebo považovaných za usadených v členských štátoch a kontrolovaných členskými štátmi alebo štátnymi príslušníkmi členských štátov;

b) bezpečnostné riziko vrátane takýchto právnych subjektov v rámci rezervy EÚ na účely kybernetickej bezpečnosti je primerané prínosom a neoslabuje základné bezpečnostné záujmy Únie a jej členských štátov.“;

[+] Ú. v.: vložte, prosím, do textu číslo nariadenia nachádzajúceho sa v dokumente PE-CONS 94/24 (2023/0109(COD)).

b) odsek 6 sa nahrádza takto:

„6. Ak je to riadne odôvodnené z bezpečnostných dôvodov, v pracovnom programe sa takisto môže stanoviť, že právne subjekty usadené v pridružených krajinách a právne subjekty, ktoré sú usadené v Únii, ale kontrolované z tretích krajín, môžu byť oprávnené na účasť na všetkých alebo niektorých akciách v rámci špecifických cieľov 1 a 2 len vtedy, ak spĺňajú požiadavky, ktoré majú tieto právne subjekty spĺňať, aby sa zaručila ochrana základných bezpečnostných záujmov Únie a členských štátov a aby sa zabezpečila ochrana informácií obsiahnutých v utajovaných dokumentoch. Uvedené požiadavky sú stanovené v pracovnom programe.

Prvý pododsek sa tiež uplatňuje, pokiaľ ide o právne subjekty usadené v Únii, ale sú kontrolované z tretích krajín, na akcie v rámci špecifického cieľa 3:

a) vykonávať európsky systém varovania pred kybernetickobezpečnostnými hrozbami, keď sa uplatňuje odsek 5a; a

b) vykonávať rezervu EÚ na účely kybernetickej bezpečnosti, keď sa uplatňuje odsek 5b.“

4. V článku 14 sa odsek 2 nahrádza takto:

„2. Z programu sa môže poskytovať financovanie v akejkoľvek forme stanovenej v nariadení o rozpočtových pravidlách, a to aj najmä prostredníctvom verejného obstarávania ako primárnej formy 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 v zmysle vymedzení v smerniciach Európskeho parlamentu a Rady 2014/24/EÚ* a 2014/25/EÚ**.

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 verejného obstarávania pre rezervu EÚ na účely kybernetickej bezpečnosti, 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 tohto nariadenia. 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 168 ods. 3 nariadenia Európskeho parlamentu a Rady (EÚ, Euratom) 2024/2509[***], postačuje na udelenie mandátu konať Komisii alebo agentúre ENISA žiadosť jednej tretej krajiny.

Pri vykonávaní postupov verejného obstarávania pre rezervu EÚ na účely kybernetickej bezpečnosti, môžu Komisia a agentúra ENISA konať ako centrálna obstarávacia organizácia s cieľom vykonávať obstarávanie na účet alebo v mene inštitúcií, orgánov, úradov alebo 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, úradom alebo agentúram Únie. Odchylne od článku 168 ods. 3 nariadenia (EÚ, Euratom) 2024/2509 postačuje na udelenie mandátu konať Komisii alebo agentúre ENISA žiadosť jednej inštitúcie, orgánu, úradu alebo agentúry Únie.

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

---

* 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).

** Smernica Európskeho parlamentu a Rady 2014/25/EÚ z 26. februára 2014 o obstarávaní vykonávanom subjektmi pôsobiacimi v odvetviach vodného hospodárstva, energetiky, dopravy a poštových služieb a o zrušení smernice 2004/17/ES (Ú. v. EÚ L 94, 28.3.2014, s. 243).

*** Nariadenie Európskeho parlamentu a Rady (EÚ, Euratom) 2024/2509 z 23. septembra 2024 o rozpočtových pravidlách, ktoré sa vzťahujú na všeobecný rozpočet Únie (Ú. v. EÚ L, 2024/2509, ELI: http://data.europa.eu/eli/reg/2024/2509/oj).“

5. Dopĺňa sa tento článok:

„*Článok 16a*

Kolízia pravidiel

V prípade opatrení, ktorými sa vykonáva európsky systém varovania pred kybernetickobezpečnostnými hrozbami, sú príslušnými pravidlami pravidlá stanovené v článkoch 4, 5 a 9 nariadenia (EÚ) …/…[+]. V prípade kolízie medzi ustanoveniami tohto nariadenia a článkami 4, 5 a 9 nariadenia (EÚ) .../...[+], uvedené články majú prednosť a uplatňujú sa na tieto osobitné opatrenia.

[+] Ú. v.: vložte, prosím, do textu číslo nariadenia nachádzajúceho sa v dokumente PE-CONS 94/24 (2023/0109(COD)).

V prípade opatrení, ktorými sa vykonáva rezerva EÚ na účely kybernetickej bezpečnosti , sú osobitné pravidlá účasti tretích krajín pridružených k programu stanovené v článku 19 nariadenia (EÚ) .../...[+]. V prípade kolízie medzi ustanoveniami tohto nariadenia a článkom 19 nariadenia (EÚ) .../...[+], uvedený článok 19 má prednosť a uplatňuje sa na tieto osobitné opatrenia.“

6. Článok 19 sa nahrádza takto:

„*Článok 19*
Granty

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 centrum ECCC udeliť členským štátom vybraným podľa článku 9 nariadenia (EÚ) .../...[+] priamo bez výzvy na predkladanie návrhov a hostiteľskému konzorciu uvedenému v článku 5 nariadenia (EÚ) .../...[+] v súlade s článkom 195 ods. 1 písm. d) nariadenia o rozpočtových pravidlách.

Podporu vo forme grantov pre mechanizmus na riešenie núdzových situácií v oblasti kybernetickej bezpečnosti, môže centrum ECCC v súlade s článkom 195 ods. 1 písm. d) nariadenia o rozpočtových pravidlách udeliť členským štátom priamo bez výzvy na predkladanie návrhov.

[+] Ú. v.: vložte, prosím, do textu číslo nariadenia nachádzajúceho sa v dokumente PE-CONS 94/24 (2023/0109(COD)).

V prípade akcií podporujúcich vzájomnú pomoc stanovenú v článku 18 nariadenia (EÚ) .../...[+] informuje centrum ECCC Komisiu a agentúru ENISA o žiadostiach členských štátov o priame granty bez výzvy na predkladanie návrhov.

V prípade akcií podporujúcich vzájomnú pomoc stanovenú v článku 18 nariadenia (EÚ) .../...[+] 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.“

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

Článok 23

Vykonávanie delegovania právomoci

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

2. Právomoc prijímať delegované akty uvedené v článku 14 ods. 7 sa Komisii udeľuje na dobu piatich rokov od ... [deň nadobudnutia účinnosti tohto nariadenia]. Komisia vypracuje správu týkajúcu sa delegovania právomoci najneskôr deväť mesiacov pred uplynutím tohto päťročného obdobia. Delegovanie právomoci sa automaticky predlžuje o rovnako dlhé obdobia, pokiaľ Európsky parlament alebo Rada nevznesú voči takémuto predĺženiu námietku najneskôr tri mesiace pred koncom každého obdobia.

[+] Ú. v.: vložte, prosím, do textu číslo nariadenia nachádzajúceho sa v dokumente PE-CONS 94/24 (2023/0109(COD)).

3. Delegovanie právomoci uvedené v článku 14 ods. 7 môže Európsky parlament alebo Rada kedykoľvek odvolať. Rozhodnutím o odvolaní sa ukončuje delegovanie právomoci, ktoré sa v ňom uvádza. Rozhodnutie nadobúda účinnosť dňom nasledujúcim po jeho uverejnení v *Úradnom vestníku Európskej únie* alebo k neskoršiemu dátumu, ktorý je v ňom určený. Nie je ním dotknutá platnosť delegovaných aktov, ktoré už nadobudli účinnosť.

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

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

6. Delegovaný akt prijatý podľa článku 14 ods. 7 nadobudne účinnosť, len ak Európsky parlament alebo Rada voči nemu nevzniesli námietku v lehote dvoch mesiacov odo dňa oznámenia uvedeného aktu Európskemu parlamentu a Rade alebo ak pred uplynutím uvedenej lehoty Európsky parlament a Rada informovali Komisiu o svojom rozhodnutí nevzniesť námietku. Na podnet Európskeho parlamentu alebo Rady sa táto lehota predĺži o dva mesiace.

Článok 24

Postup výboru

1. Komisii pomáha koordinačný výbor programu Digitálna Európa uvedený v článku 31 ods. 1 nariadenia (EÚ) 2021/694. Uvedený výbor je výborom v zmysle nariadenia (EÚ) č. 182/2011.

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

Článok 25

Hodnotenie a preskúmanie

1. Komisia do ... [dvoch rokov odo dňa nadobudnutia účinnosti tohto nariadenia] a potom najmenej každé štyri roky zhodnotí fungovanie opatrení stanovených v tomto nariadení a predloží správu Európskemu parlamentu a Rade.

2. V hodnotení uvedenom v odseku 1 sa posúdi najmä:

a) počet zriadených národných kybernetických a cezhraničných kybernetických centier, rozsah zdieľaných informácií vrátane, ak je to možné, vplyvu na prácu siete jednotiek CSIRT a rozsah, v akom prispeli k posilneniu spoločného odhaľovania kybernetických hrozieb a incidentov v Únii a k situačnej informovanosti o kybernetických hrozbách a incidentoch a k vývoju najmodernejších technológií; využívanie financovania z programu Digitálna Európa na infraštruktúru nástrojov kybernetickej bezpečnosti alebo spoločne obstarané služby; a ak sú informácie k dispozícii, úroveň spolupráce medzi národnými kybernetickými centrami a odvetvovými a medziodvetvovými komunitami kľúčových a dôležitých subjektov, ako sa uvádza v článku 3 smernice (EÚ) 2022/2555;

b) využívanie a účinnosť opatrení v rámci mechanizmu na riešenie kybernetickobezpečnostných núdzových situácií na podporu pripravenosti vrátane odbornej prípravy, reakcie na významné kybernetické bezpečnostné incidenty, rozsiahle kybernetické bezpečnostné incidenty a rozsiahle rovnocenné kybernetické bezpečnostné incidenty a počiatočného zotavenia sa z nich, vrátane využívania finančných prostriedkov programu Digitálna Európa a získaných poznatkov a odporúčaní z vykonávania mechanizmu na riešenie kybernetickobezpečnostných núdzových situácií;

c) využívanie a účinnosť rezervy EÚ na účely kybernetickej bezpečnosti vo vzťahu k typu používateľov vrátane využívania financovania programu Digitálna Európa, využívanie služieb vrátane ich typu, priemerný čas na odpoveď na žiadosti a na použitie rezervy EÚ na účely kybernetickej bezpečnosti, percentuálny podiel služieb prevedených na služby pripravenosti súvisiace s predchádzaním incidentom a reakciou na ne a získané poznatky a odporúčania z vykonávania rezervy EÚ na účely kybernetickej bezpečnosti;

d) prispievanie tohto nariadenia k posilneniu konkurenčného postavenia priemyslu a služieb v Únii v celom digitálnom hospodárstve vrátane mikropodnikov a malých a stredných podnikov, ako aj startupov, a prispievanie k celkovému cieľu posilnenia zručností v oblasti kybernetickej bezpečnosti a kapacít pracovnej sily.

3. Na základe správ uvedených v odseku 1 Komisia vo vhodných prípadoch predloží Európskemu parlamentu a Rade legislatívny návrh na zmenu tohto nariadenia.

Článok 26

Nadobudnutie účinnosti

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

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

V Bruseli

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

PRÍLOHA

Nariadenie (EÚ) 2021/694 sa mení takto:

1. V prílohe II sa oddiel „Špecifický cieľ 3 – Kybernetická bezpečnosť a dôvera“ nahrádza takto:

„Špecifický cieľ 3 – Kybernetická bezpečnosť a dôvera

Programom sa stimuluje posilnenie, budovanie a nadobúdanie kapacít nevyhnutných na zabezpečenie digitálneho hospodárstva, spoločnosti a demokracie v Únii posilnením priemyselného potenciálu a konkurencieschopnosti Únie v oblasti kybernetickej bezpečnosti, ako aj zlepšením možností verejného a súkromného sektora chrániť občanov a podniky pred kybernetickými hrozbami, a to aj podporou vykonávania smernice (EÚ) 2016/1148.

Počiatočné a vo vhodných prípadoch následné akcie v rámci tohto cieľa zahŕňajú:

1. Spoločné investovanie s členskými štátmi do vyspelého vybavenia, infraštruktúry a know-how v oblasti kybernetickej bezpečnosti, ktoré sú nevyhnutné na ochranu kritických infraštruktúr a Jednotného digitálneho trhu ako celku. Takéto spoločné investovanie by mohlo zahŕňať investície do kvantových zariadení a dátových zdrojov kybernetickej bezpečnosti, situačnej informovanosti v kybernetickom priestore vrátane národných kybernetických centier a cezhraničných kybernetických centier, ktoré tvoria európsky systém varovania pred kybernetickobezpečnostnými hrozbami, ako aj do ďalších nástrojov, ktoré sa sprístupnia verejnému a súkromnému sektoru v celej Európe.

2. Rozšírenie existujúcich technologických kapacít a prepojenie kompetenčných centier v členských štátoch a zabezpečenie toho, aby tieto kapacity zodpovedali potrebám verejného sektora a priemyslu, a to aj prostredníctvom produktov a služieb, ktorými sa zvyšuje kybernetická bezpečnosť a dôvera na Jednotnom digitálnom trhu.

3. Zabezpečenie rozsiahleho zavádzania účinných najmodernejších riešení v oblasti kybernetickej bezpečnosti a dôvery v členských štátoch. Takéto zavádzanie zahŕňa posilnenie ochrany a bezpečnosti produktov od ich návrhu až po ich komerčné využitie.

4. Podpora odstraňovania nedostatku zručností v oblasti kybernetickej bezpečnosti, s ohľadom na rodovú rovnováhu, napríklad zosúladením programov v oblasti kybernetickej bezpečnosti, ich prispôsobením konkrétnym potrebám daného odvetvia a uľahčením prístupu k cielenej špecializovanej odbornej príprave.

5. Podpora solidarity medzi členskými štátmi pri príprave na významné kybernetické bezpečnostné incidenty a rozsiahle kybernetické bezpečnostné incidenty a reakcii na ne prostredníctvom cezhraničného nasadenia služieb kybernetickej bezpečnosti vrátane podpory vzájomnej pomoci medzi orgánmi verejnej správy a vytvorenia rezervy dôveryhodných poskytovateľov riadených bezpečnostných služieb v oblasti kybernetickej bezpečnosti na úrovni Únie.“

2. V prílohe II sa oddiel „Špecifický cieľ 3 – Kybernetická bezpečnosť a dôvera“ nahrádza takto:

„Špecifický cieľ 3 – Kybernetická bezpečnosť a dôvera

3.1. Počet infraštruktúr alebo nástrojov kybernetickej bezpečnosti alebo oboje, získaných prostredníctvom spoločného verejného obstarávania, a to aj v kontexte európskeho systému varovania pred kybernetickobezpečnostnými hrozbami.

3.2. Počet používateľov a používateľských komunít s prístupom k európskym zariadeniam kybernetickej bezpečnosti.

3.3 Počet akcií, ktorými sa podporuje pripravenosť na kybernetické incidenty a reakcia na ne v rámci mechanizmu na riešenie kybernetickobezpečnostných núdzových situácií.“

V súvislosti s týmto aktom bolo urobené vyhlásenie, ktoré možno nájsť v [Úrad pre publikácie: Ú. v. EÚ C XXX, XX.XX.2024, s. XX] a na tomto odkaze: [Úrad pre publikácie: vložte odkaz na vyhlásenie].