EVROPSKÁ UNIE

EVROPSKÝ PARLAMENT **RADA**

Brusel 20. listopadu 2024
(OR. en)

2023/0109(COD) **PE-CONS 94/24**

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

PRÁVNÍ PŘEDPISY A JINÉ AKTY

Předmět:	NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY, kterým se stanovují opatření k posílení solidarity a kapacit v Unii pro odhalování kybernetických hrozeb a incidentů a pro připravenost a reakci na ně a mění nařízení (EU) 2021/694 (nařízení o kybernetické solidaritě)

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY

(EU) 2024/…

ze dne ...,

kterým se stanovují opatření k posílení solidarity a kapacit v Unii pro odhalování kybernetických hrozeb a incidentů a pro připravenost a reakci na ně a mění nařízení (EU) 2021/694 (nařízení o kybernetické solidaritě)

EVROPSKÝ PARLAMENT A RADA EVROPSKÉ UNIE,

s ohledem na Smlouvu o fungování Evropské unie, a zejména na čl. 173 odst. 3 a čl. 322 odst. 1 písm. a) této smlouvy,

s ohledem na návrh Evropské komise,

po postoupení návrhu legislativního aktu vnitrostátním parlamentům,

s ohledem na stanovisko Účetního dvora[1],

s ohledem na stanovisko Evropského hospodářského a sociálního výboru[2],

s ohledem na stanovisko Výboru regionů[3],

v souladu s řádným legislativním postupem[4],

---

1 Stanovisko ze dne 18. dubna 2023 (dosud nezveřejněné v Úředním věstníku.

2 Úř. věst. C 349, 29.9.2023, s. 167.

3 Úř. věst. C, C/2024/1049, 9.2.2024, ELI: http://data.europa.eu/eli/C/2024/1049/oj.

4 Postoj Evropského parlamentu ze dne 24. dubna 2024 (dosud nezveřejněný v Úředním věstníku) a rozhodnutí Rady ze dne …

vzhledem k těmto důvodům:

(1) S ohledem na stále větší propojenost a vzájemnou závislost veřejné správy, podniků a občanů členských států napříč odvětvími a hranicemi se používání informačních a komunikačních technologií a závislost na nich staly základním aspektem ve všech odvětvích hospodářské činnosti a ve společnosti, což zároveň přináší možné zranitelnosti.

(2) Rozsah, četnost a dopad kybernetických bezpečnostních incidentů, včetně útoků na dodavatelský řetězec, jejichž cílem je kybernetická špionáž, ransomware nebo narušení, se zvyšuje v celé Unii i na světové úrovni. Tyto incidenty představují zásadní hrozbu pro fungování síťových a informačních systémů. Vzhledem k rychle se vyvíjejícímu prostředí hrozeb vyžaduje hrozba možných rozsáhlých kybernetických bezpečnostních incidentů, které mohou vést k významnému narušení či poškození kritické infrastruktury, větší připravenost unijního rámce kybernetické bezpečnosti. Tato hrozba přesahuje rámec útočné války Ruska proti Ukrajině a vzhledem k množství subjektů, které se podílejí na stávajícím geopolitickém napětí, bude pravděpodobně trvat i nadále. Tyto incidenty mohou narušit poskytování veřejných služeb, jelikož se kybernetické útoky často zaměřují na místní, regionální nebo celostátní veřejné služby a infrastrukturu, přičemž obzvláště zranitelné jsou místní orgány, mimo jiné z důvodu jejich omezených zdrojů. Mohou narušit i výkon hospodářských činností, a to i ve vysoce kritických odvětvích nebo dalších kritických odvětvích, způsobit značné finanční ztráty, podkopat důvěru uživatelů, způsobit velké škody hospodářství a demokratickým systémům Unie a mohou mít i následky ohrožující zdraví nebo život. Kybernetické bezpečnostní incidenty jsou navíc nepředvídatelné, protože se často objevují a vyvíjejí rychle, nejsou omezeny na žádnou konkrétní zeměpisnou oblast a současně se vyskytují nebo se okamžitě šíří v mnoha zemích. Proto je důležité zajistit úzkou spolupráci mezi veřejným sektorem, soukromým sektorem, akademickou obcí, občanskou společností a sdělovacími prostředky.

(3) Je nezbytné posílit konkurenceschopnost průmyslu a služeb v Unii v rámci celé digitalizované ekonomiky a podpořit jejich digitální transformaci zvýšením úrovně kybernetické bezpečnosti na jednotném digitálním trhu, jak se doporučuje ve třech různých návrzích konference o budoucnosti Evropy. Je nutné zvýšit odolnost občanů, podniků, včetně mikropodniků, malých a středních podniků a začínajících podniků, a subjektů provozujících kritickou infrastrukturu vůči rostoucím kybernetickým hrozbám, které mohou mít ničivý společenský a hospodářský dopad. Proto je třeba investovat do infrastruktury a služeb a do vytváření schopností pro rozvoj dovedností v oblasti kybernetické bezpečnosti, které by podpořily rychlejší odhalování kybernetických hrozeb a incidentů a rychlejší reakci na ně. Kromě toho potřebují členské státy pomoc, aby se mohly lépe připravit na významné kybernetické bezpečnostní incidenty a rozsáhlé kybernetické bezpečnostní incidenty, reagovat na ně a zajistit počáteční zotavení se z nich. Unie by měla na základě stávajících struktur a v úzké spolupráci s nimi rovněž zvýšit své kapacity v těchto oblastech, zejména pokud jde o shromažďování a analýzu dat o kybernetických hrozbách a incidentech.

(4) Unie již přijala řadu opatření ke snížení zranitelnosti a zvýšení odolnosti kritické infrastruktury a subjektů vůči rizikům, zejména nařízení Evropského parlamentu a Rady (EU) 2019/881[5], směrnice Evropského parlamentu a Rady 2013/40/EU[6] a (EU) 2022/2555[7] a doporučení Komise (EU) 2017/1584[8]. V doporučení Rady ze dne 8. prosince 2022 týkajícím se celounijního koordinovaného přístupu za účelem posílení odolnosti kritické infrastruktury se navíc členské státy vyzývají, aby přijaly opatření a aby spolupracovaly mezi sebou navzájem, s Komisí a dalšími příslušnými orgány veřejné moci, jakož i s dotčenými subjekty s cílem zvýšit odolnost kritické infrastruktury používané k poskytování základních služeb na vnitřním trhu.

---

5 Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti“) (Úř. věst. L 151, 7.6.2019, s. 15).

6 Směrnice Evropského parlamentu a Rady 2013/40/EU ze dne 12. srpna 2013 o útocích na informační systémy a nahrazení rámcového rozhodnutí Rady 2005/222/SVV (Úř. věst. L 218, 14.8.2013, s. 8).

7 Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2) (Úř. věst. L 333, 27.12.2022, s. 80).

8 Doporučení Komise (EU) 2017/1584 ze dne 13. září 2017 o koordinované reakci na rozsáhlé kybernetické bezpečnostní incidenty a krize (Úř. věst. L 239, 19.9.2017, s. 36).

(5) Vzhledem k rostoucím rizikům v oblasti kybernetické bezpečnosti a k celkově složitému prostředí hrozeb s jasným rizikem rychlého rozšíření incidentů z jednoho členského státu do ostatních a ze třetí země do Unie je nutné posílit solidaritu na úrovni Unie, aby bylo možné lépe odhalovat kybernetické hrozby a incidenty, připravovat se na ně, reagovat na ně i se zotavit z jejich následků, zejména rozšířením schopností stávajících struktur. Kromě toho závěry Rady ze dne 23. května 2022 o kybernetické pozici EU vyzvaly Komisi, aby předložila návrh nového fondu pro reakci na mimořádné události v oblasti kybernetické bezpečnosti.

(6) Ve společném sdělení Komise a vysokého představitele Unie pro zahraniční věci a bezpečnostní politiku Evropskému parlamentu a Radě ze dne 10. listopadu 2022 o politice kybernetické obrany EU byla oznámena iniciativa EU pro kybernetickou solidaritu s cíli posílit společné schopnosti EU v oblasti odhalování, situačního povědomí a reakce podporou zavádění infrastruktury EU v podobě bezpečnostních operačních středisek, podporovat postupné vytváření kybernetické rezervy na úrovni EU se službami důvěryhodných soukromých poskytovatelů a testování kritických subjektů na potenciální zranitelnosti na základě posouzení rizik v EU.

(7) Je nezbytné zvýšit odhalování kybernetických hrozeb a incidentů a rozšířit situační povědomí o nich v celé Unii a posílit solidaritu tím, že se zvýší připravenost a schopnost členských států a Unie předcházet významným kybernetickým bezpečnostním incidentům a rozsáhlým kybernetickým bezpečnostním incidentům a reagovat na ně. Proto by měla být zřízena celoevropská síť kybernetických center (dále jen „Evropský systém varování v oblasti kybernetické bezpečnosti“) s cílem vybudovat koordinovanou schopnost v oblasti odhalování hrozeb a získávání situačního povědomí, která rozšíří schopnost Unie odhalovat hrozby a sdílet informace; měl by být zřízen mechanismus pro mimořádné události v oblasti kybernetické bezpečnosti, který by podporoval členské státy na jejich žádost při přípravě na významné kybernetické bezpečnostní incidenty a rozsáhlé kybernetické bezpečnostní incidenty, při reakci na ně, zmírňování jejich dopadu a počáteční obnově po nich, a který by podporoval další uživatele při reakci na významné kybernetické bezpečnostní incidenty a incidenty obdobné rozsáhlým kybernetickým bezpečnostním incidentům; měl by být zřízen evropský mechanismus přezkumu kybernetických bezpečnostních incidentů, který by přezkoumával a posuzoval konkrétní významné kybernetické bezpečnostní incidenty nebo rozsáhlé kybernetické bezpečnostní incidenty. Akce prováděné podle tohoto nařízení by se měla provádět s náležitým ohledem na pravomoci členských států a měla by doplňovat činnost sítě CSIRT, Sítě styčných organizací pro řešení kybernetických krizí (EU-CyCLONe) nebo skupiny pro spolupráci (dále jen „skupina pro spolupráci NIS“,) zřízených podle směrnice (EU) 2022/2555, aniž by docházelo ke zdvojování činnosti. Těmito akcemi nejsou dotčeny články 107 a 108 Smlouvy o fungování Evropské unie (dále jen „Smlouva o fungování EU“).

(8) K dosažení těchto cílů je rovněž nezbytné v některých oblastech změnit nařízení Evropského parlamentu a Rady (EU) 2021/694[9]. Tímto nařízením by mělo být změněno nařízení (EU) 2021/694, zejména pokud jde o doplnění nových operačních cílů týkajících se Evropského systému varování v oblasti kybernetické bezpečnosti a mechanismu pro mimořádné události v oblasti kybernetické bezpečnosti v rámci specifického cíle č. 3 programu Digitální Evropa, který má zajistit odolnost, integritu a důvěryhodnost jednotného digitálního trhu, posílit kapacity pro monitorování kybernetických útoků a kybernetických hrozeb a pro reakci na ně a prohloubit přeshraniční spolupráci a upevnit koordinaci v oblasti kybernetické bezpečnosti. Evropský systém varování v oblasti kybernetické bezpečnosti by mohl hrát důležitou úlohu v podpoře členských států při předvídání kybernetických hrozeb a ochraně před nimi, zatímco rezerva EU pro kybernetickou bezpečnost by mohla hrát významnou roli v podpoře členských států, orgánů, institucí a jiných subjektů Unie a třetích zemí přidružených k programu Digitální Evropa při reakci na významné kybernetické bezpečnostní incidenty, rozsáhlé kybernetické bezpečnostní incidenty a incidenty obdobné rozsáhlým kybernetickým bezpečnostním incidentům a při zmírňování jejich dopadu. Tento dopad by mohl zahrnovat značnou hmotnou či nehmotnou újmu a závažná rizika v oblasti veřejné bezpečnosti a ochrany. S ohledem na konkrétní úlohu, kterou by mohly hrát Evropský systém varování v oblasti kybernetické bezpečnosti a rezerva EU pro kybernetickou bezpečnost, by tímto nařízením mělo být změněno nařízení (EU) 2021/694, pokud jde o účast právních subjektů, které jsou usazeny v Unii, ale jsou řízeny ze třetích zemí, pokud existuje reálné riziko, že v Unii nejsou k dispozici nezbytné a dostatečné nástroje, infrastruktura a služby nebo technologie, odborné znalosti a kapacita, přičemž přínos zapojení těchto subjektů převažuje nad bezpečnostním rizikem. Měly by být stanoveny konkrétní podmínky, za nichž může být na akce zavádějící Evropský systém varování v oblasti kybernetické bezpečnosti a rezervu EU pro kybernetickou bezpečnost poskytnuta finanční podpora, a měly by být vymezeny mechanismy řízení a koordinace nezbytné k dosažení zamýšlených cílů. Další změny nařízení (EU) 2021/694 by měly zahrnovat popis navrhovaných akcí v rámci nových operačních cílů a měřitelné ukazatele, kterými se bude sledovat plnění těchto nových operačních cílů.

---

[9] Nařízení Evropského parlamentu a Rady (EU) 2021/694 ze dne 29. dubna 2021, kterým se zavádí program Digitální Evropa a zrušuje rozhodnutí (EU) 2015/2240 (Úř. věst. L 166, 11.5.2021, s. 1).

(9) Pro posílení reakce Unie na kybernetické hrozby a incidenty je zásadní spolupráce s mezinárodními institucemi, jakož i s důvěryhodnými a podobně smýšlejícími mezinárodními partnery. V této souvislosti by se důvěryhodnými a podobně smýšlejícími mezinárodními partnery měly rozumět země, které sdílejí zásady, jež byly inspirací pro vznik Unie, totiž demokracie, právní stát, všeobecné platnosti a nedělitelnost lidských práv a základních svobod, úcta k lidské důstojnosti, zásada rovnosti a solidarity a dodržování zásad Charty Organizace spojených národů a mezinárodního práva a které neohrožují základní bezpečnostní zájmy Unie nebo jejích členských států. Tato spolupráce by mohla být přínosná i s ohledem na akce uvedené v tomto nařízení, zejména pokud jde o Evropský systém varování v oblasti kybernetické bezpečnosti a rezervu EU pro kybernetickou bezpečnost. Nařízení (EU) 2021/694by mělo stanovit, že zadávací řízení pro Evropský systém varování v oblasti kybernetické bezpečnosti a rezervu EU pro kybernetickou bezpečnost by měla být za určitých podmínek týkajících se dostupnosti a bezpečnosti otevřena právnickým osobám řízeným ze třetích zemí, s výhradou bezpečnostních požadavků. Při posuzování bezpečnostního rizika spojeného s takovýmto zajištěním přístupu k zadávání veřejných zakázek je důležité zohlednit zásady a hodnoty, které Unie sdílí s podobně smýšlejícími mezinárodními partnery, pokud tyto zásady a hodnoty souvisejí se základními bezpečnostními zájmy Unie. Kromě toho by při zvažování těchto bezpečnostních požadavků podle nařízení (EU) 2021/694 mohlo být zohledněno několik prvků, jako je podniková struktura a rozhodovací proces daného subjektu, bezpečnost dat a utajovaných nebo citlivých informací a zajištění toho, aby výsledky opatření nepodléhaly kontrole nebo omezením ze strany nezpůsobilých třetích zemí.

(10) Financování akcí podle tohoto nařízení by mělo být stanoveno v nařízení (EU) 2021/694, které by mělo zůstat příslušným základním aktem pro akce zakotvené ve specifickém cíli č. 3 programu Digitální Evropa. Konkrétní podmínky účasti týkající se jednotlivých akcí budou stanoveny v příslušných pracovních programech v souladu s příslušným ustanovením nařízení (EU) 2021/694.

(11) Na toto nařízení se použijí horizontální finanční pravidla přijatá Evropským parlamentem a Radou na základě článku 322 Smlouvy o fungování EU. Tato pravidla jsou stanovena v nařízení Evropského parlamentu a Rady (EU, Euratom) 2024/2509[10] a upravují zejména postupy týkající se sestavování a plnění rozpočtu Unie a kontroly odpovědnosti účastníků finančních operací. Pravidla přijatá na základě článku 322 Smlouvy o fungování EU rovněž zahrnují obecný režim podmíněnosti na ochranu rozpočtu Unie, jak je stanoveno v nařízení Evropského parlamentu a Rady (EU, Euratom) 2020/2092[11].

---

[10] Nařízení Evropského parlamentu a Rady 2024/2509 (EU, Euratom) 2024/2509 ze dne 23. září 2024, kterým se stanoví finanční pravidla pro souhrnný rozpočet Unie (přepracované znění) (Úř. věst. L, 2024/2509, 26.9.2024, ELI: http://data.europa.eu/eli/reg/2024/2509/oj).

[11] Nařízení Evropského parlamentu a Rady (EU, Euratom) 2020/2092 ze dne 16. prosince 2020 o obecném režimu podmíněnosti na ochranu rozpočtu Unie (Úř. věst. L 433 I, 22.12.2020, s. 1, ELI: http://data.europa.eu/eli/reg/2020/2092/oj).

(12) Ačkoli opatření v oblasti prevence a připravenosti mají zásadní význam z hlediska posílení odolnosti Unie vůči významným kybernetickým bezpečnostním incidentům, rozsáhlým kybernetickým bezpečnostním incidentům a incidentům obdobným rozsáhlým kybernetickým bezpečnostním incidentům, výskyt, načasování a rozsah těchto incidentů jsou ze své podstaty nepředvídatelné. Finanční zdroje potřebné k zajištění odpovídající reakce se mohou rok od roku značně lišit a měly by být okamžitě k dispozici. Sladění rozpočtové zásady předvídatelnosti s nutností rychle reagovat na nové potřeby tedy vyžaduje úpravu finančního zajištění pracovních programů. Je proto vhodné povolit kromě převádění prostředků schválených podle čl. 12 odst. 4 nařízení (EU, Euratom) 2024/2509 do dalšího roku i převádění nevyužitých prostředků, ale pouze na následující rok a pouze na rezervu EU pro kybernetickou bezpečnost a akce na podporu vzájemné pomoci.

(13) Aby bylo možné účinněji předcházet kybernetickým hrozbám a incidentům, vyhodnocovat je, reagovat na ně a zotavit se z nich, je nutné získat komplexnější znalosti o hrozbách pro kritická aktiva a infrastrukturu na území Unie, včetně jejich zeměpisného rozložení, vzájemného propojení a možných dopadů v případě kybernetických útoků na tuto infrastrukturu. Proaktivní přístup k identifikaci kybernetických hrozeb, k jejich zmírňování a předcházení těmto hrozbám zahrnuje rozšíření kapacity v oblasti schopností pokročilého odhalování. Evropský systém varování v oblasti kybernetické bezpečnosti by se měl skládat z několika interoperabilních přeshraničních kybernetických center, z nichž každé sdružuje alespoň tři národní kybernetická centra. Tato infrastruktura by měla sloužit zájmům a potřebám členských států a Unie v oblasti kybernetické bezpečnosti a využívat nejmodernější technologie pro pokročilé shromažďování relevantních a případně anonymizovaných dat a informací a analytické nástroje, zlepšovat koordinované schopnosti odhalování a řízení v oblasti kybernetické bezpečnosti a poskytovat situační povědomí v reálném čase. Tato infrastruktura by měla sloužit ke zlepšení pozice v oblasti kybernetické bezpečnosti zvýšením odhalování, agregace a analýzy dat a informací s cílem předcházet kybernetickým hrozbám a incidentům, a tím doplňovat a podporovat subjekty a sítě Unie odpovědné za řešení kybernetických krizí v Unii, zejména síť „EU-CyCLONe“.

(14) Účast v Evropském systému varování v oblasti kybernetické bezpečnosti je pro členské státy dobrovolná. Každý členský stát by měl na vnitrostátní úrovni určit jeden subjekt, který bude pověřen koordinací činnosti v oblasti odhalování kybernetických hrozeb v daném členském státě. Tato národní kybernetická centra by měla na vnitrostátní úrovni fungovat jako referenční bod a brána pro účast v Evropském systému varování v oblasti kybernetické bezpečnosti a měla by zajistit, aby informace o kybernetických hrozbách od veřejných a soukromých subjektů byly na vnitrostátní úrovni sdíleny a shromažďovány účinně a efektivně. Národní kybernetická centra by mohla prohloubit spolupráci a rozšířit sdílení informací mezi veřejnými a soukromými subjekty a mohla by rovněž podporovat výměnu relevantních dat a informací s příslušnými odvětvovými a meziodvětvovými komunitami, včetně příslušných odvětvových center pro sdílení a analýzu informací (dále jen „centra ISAC“). Z hlediska posílení kybernetické odolnosti Unie má zásadní význam úzká a koordinovaná spolupráce mezi veřejnými a soukromými subjekty. Tato spolupráce je obzvláště cenná v souvislosti se sdílením poznatků o kybernetických hrozbách (tzv. „cyber threat intelligence“) za účelem zlepšení aktivní kybernetické ochrany. V rámci této spolupráce a sdílení informací by si národní kybernetická centra mohla vyžádat a obdržet konkrétní informace. Tímto nařízením není těmto národním centrům uložena povinnost takové žádosti prosazovat ani jim k tomu nejsou zmocněny. Ve vhodných případech a v souladu s právem Unie a členských států by požadované nebo obdržené informace mohly zahrnovat telemetrii, údaje z čidel a údaje o přihlášeních od subjektů, jako jsou poskytovatelé řízených bezpečnostních služeb, které působí ve vysoce kritických odvětvích nebo v dalších kritických odvětvích v daném členském státě, s cílem zlepšit rychlé odhalování potenciálních kybernetických hrozeb a incidentů v dřívější fázi, a zlepšit tak situační povědomí. Pokud národní kybernetické centrum není příslušným orgánem určeným nebo zřízeným příslušným členským státem podle čl. 8 odst. 1 směrnice (EU) 2022/2555, je nezbytné, aby v souvislosti s žádostmi o tyto údaje a s jejich přijímáním koordinovalo svou činnost s tímto příslušným orgánem.

(15) V rámci Evropského systému varování v oblasti kybernetické bezpečnosti by měla být zřízena řada přeshraničních kybernetických center. Tato přeshraniční kybernetická centra by měla sdružovat národní kybernetická centra alespoň ze tří členských států, aby bylo možné plně využít výhod přeshraničního odhalování hrozeb a sdílení a správy informací. Obecným cílem přeshraničních kybernetických center by mělo být posílení kapacit pro analýzu, prevenci a odhalování kybernetických hrozeb a podpora získávání vysoce kvalitních poznatků o kybernetických hrozbách, zejména prostřednictvím sdílení relevantních a v příslušných případech anonymizovaných informací z různých zdrojů, ať už veřejných nebo soukromých, v rámci důvěryhodného a zabezpečeného prostředí, jakož i prostřednictvím sdílení a společného využívání nejmodernějších nástrojů a společným rozvojem schopností odhalování, analýzy a prevence v důvěryhodném a zabezpečeném prostředí. Přeshraniční kybernetická centra by měla poskytnout nové dodatečné kapacity, které by vycházely ze stávajících bezpečnostních operačních středisek, týmů CSIRT a dalších příslušných subjektů, včetně sítě týmů CSIRT, a doplňovaly je.

(16) Členský stát vybraný Evropským průmyslovým, technologickým a výzkumným centrem kompetencí pro kybernetickou bezpečnost (dále jen „centrum ECCC“) zřízeným nařízením Evropského parlamentu a Rady (EU) 2021/887[12] na základě výzvy k vyjádření zájmu o zřízení národního kybernetického centra nebo rozšíření jeho schopností by měl společně s centrem ECCC zakoupit příslušné nástroje, infrastrukturu a služby. Tento členský stát by měl být způsobilý k získání grantu na provoz těchto nástrojů, infrastruktury nebo služeb. Hostitelské konsorcium složené nejméně ze tří členských států, které centrum ECCC vybralo na základě výzvy k vyjádření zájmu o zřízení přeshraničního kybernetického centra nebo rozšíření jeho schopností by mělo zakoupit příslušné nástroje, infrastrukturu nebo služby společně s centrem ECCC. Toto hostitelské konsorcium by mělo být způsobilé k získání grantu na provoz těchto nástrojů, infrastruktury nebo služeb. Zadávací řízení na nákup příslušných nástrojů, infrastruktury nebo služeb by mělo provádět centrum ECCC společně s příslušnými vybranými veřejnými zadavateli z členských států, následně po takových výzvách k vyjádření zájmu. Takové zadávání veřejných zakázek by mělo být v souladu s čl. 168 odst. 2 nařízení (EU, Euratom) 2024/2509 a finančními pravidly centra ECCC. Soukromé subjekty by proto neměly být způsobilé k účasti na výzvách k vyjádření zájmu o nákup nástrojů, infrastruktury nebo služeb společně s centrem ECCC nebo k získání grantů na provoz těchto nástrojů, infrastruktury nebo služeb. Členské státy by však měly mít v souladu s unijním a vnitrostátním právem možnost zapojit soukromé subjekty do zřízení, rozšíření a provozu svého národního kybernetického centra a přeshraničního kybernetického centra jinými způsoby, které považují za vhodné. Soukromé subjekty by rovněž mohly být způsobilé k získání finančních prostředků Unie v souladu s nařízením (EU) 2021/887 za účelem poskytování podpory národním kybernetickým centrům.

---

[12] Nařízení Evropského parlamentu a Rady (EU) 2021/887 ze dne 20. května 2021, kterým se zřizuje Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost a síť národních koordinačních center (Úř. věst. L 202, 8.6.2021, s. 1, ELI: http://data.europa.eu/eli/reg/2021/887/oj).

(17) Ke zlepšení odhalování kybernetických hrozeb a k lepšímu situačnímu povědomí v Unii, by se měl členský stát, který je na základě výzvy k vyjádření zájmu vybrán ke zřízení národního kybernetického centra nebo k rozšíření jeho schopností, zavázat, že požádá o účast na činnosti přeshraničního kybernetického centra. Pokud se členský stát nezačne účastnit činnosti přeshraničního kybernetického centra do dvou let ode dne, kdy byly nástroje, infrastruktura nebo služby pořízeny nebo kdy obdrželo grantové financování, podle toho, co nastane dříve, neměl by mít právo se účastnit v rámci Evropského systému varování v oblasti kybernetické bezpečnosti dalších podpůrných unijních akcí zaměřených na rozšíření schopností jeho národního kybernetického centra. V takových případech by se subjekty z členských států mohly stále účastnit výzev k podávání návrhů týkajících se jiných témat v rámci programu Digitální Evropa nebo jiných unijních programů financování, včetně výzev týkajících se kapacity zajišťující odhalování v oblasti kybernetické bezpečnosti a sdílení informací, za předpokladu, že splňují kritéria způsobilosti stanovená v těchto programech.

(18) Týmy CSIRT si vyměňují informace v rámci sítě CSIRT v souladu se směrnicí (EU) 2022/2555. Evropský systém varování v oblasti kybernetické bezpečnosti by měl představovat novou schopnost, která by doplňovala síť týmů CSIRT tím, že by přispívala k zajištění situačního povědomí v Unii, což by umožnilo posílit schopnosti týmů CSIRT. Přeshraniční kybernetická centra by měla koordinovat svou činnost se sítí CSIRT a úzce s ní spolupracovat. Měla by jednat na základě shromažďování dat a sdílení relevantních a případně anonymizovaných informací o kybernetických hrozbách od veřejných a soukromých subjektů, zvyšovat hodnotu těchto dat a informací prostřednictvím odborné analýzy a společně pořízené infrastruktury a nejmodernějších nástrojů a přispívat k technologické suverenitě Unie, její otevřené strategické autonomii, konkurenceschopnosti a odolnosti a k rozvoji schopností Unie.

(19) Přeshraniční kybernetická centra by měla fungovat jako ústřední body umožňující široké shromažďování příslušných dat a poznatků o kybernetických hrozbách a umožňovat šíření informací o hrozbách mezi velkým a různorodým souborem zúčastněných stran, jako jsou týmy pro reakci na počítačové hrozby (dále jen „týmy CERT“), týmy CSIRT, centra ISAC a provozovatelé kritické infrastruktury. Členové hostitelského konsorcia by měli v dohodě o konsorciu upřesnit příslušné informace, které mají být sdíleny mezi účastníky dotčeného přeshraničního kybernetického centra. Informace vyměňované mezi účastníky přeshraničního kybernetického centra by mohly zahrnovat například data ze sítí a čidel, informace o hrozbách, indikátory narušení a kontextualizované informace o incidentech, kybernetických hrozbách, významných událostech, zranitelnostech, technikách a postupech, nepřátelských taktikách, konkrétních informacích o aktérech hrozeb, varováních v oblasti kybernetické bezpečnosti a o doporučení týkajících se konfigurace nástrojů kybernetické bezpečnosti pro odhalování kybernetických útoků. Přeshraniční kybernetická centra by kromě toho měla mezi sebou uzavírat také dohody o spolupráci. V těchto dohodách o spolupráci by měly být stanoveny zejména zásady sdílení informací a aspekty týkající se interoperability. Jejich ustanovení týkající se interoperability, zejména formátů a protokolů pro sdílení informací, by se měla řídit po pokyny pro interoperabilitu vydanými Agenturou Evropské unie pro kybernetickou bezpečnost zřízenou nařízením (EU) 2019/881 (ENISA), a proto by měla z těchto pokynů vycházet. Tyto pokyny by měly být vydány rychle, aby se zajistilo, že je přeshraniční kybernetická centra budou moci zohlednit již v rané fázi. Měly by zohledňovat mezinárodní normy a osvědčené postupy a fungování všech zřízených přeshraničních kybernetických center.

(20) Přeshraniční kybernetická centra by měla úzce spolupracovat se sítí CSIRT, aby byla zajištěna jejich součinnost a aby se jejich činnost doplňovala. Za tímto účelem by se měly dohodnout na procesních ujednáních o spolupráci a o výměně příslušných informací. To by mohlo zahrnovat sdílení relevantních informací o kybernetických hrozbách a významných kybernetických bezpečnostních incidentech a zajišťovat, aby se přeshraniční kybernetická centra dělila se sítí CSIRT o své zkušenosti s nejmodernějšími nástroji, zejména s technologií umělé inteligence a analýzy dat, které se v rámci těchto center používají.

(21) Společné situační povědomí mezi příslušnými orgány je nezbytným předpokladem připravenosti a koordinace v celé Unii, pokud jde o významné kybernetické bezpečnostní incidenty a rozsáhlé kybernetické bezpečnostní incidenty. Směrnice (EU) 2022/2555 zřizuje síť EU–CyCLONe za účelem podpory koordinovaného řešení rozsáhlých kybernetických bezpečnostních incidentů a krizí na operativní úrovni a pro zajištění pravidelné výměny relevantních informací mezi členskými státy a orgány, institucemi nebo jinými subjekty Unie. Směrnice (EU) 2022/2555 zřídila také sít CSIRT s cílem podporovat rychlou a účinnou operativní spolupráci mezi členskými státy. Za účelem získání situačního povědomí a zajištění větší solidarity by v situaci, kdy přeshraniční kybernetické centrum získá informace týkající se potenciálního nebo probíhajícího rozsáhlého kybernetického bezpečnostního incidentu, mělo poskytnout příslušné informace síti CSIRT a v rámci včasného varování informovat síť EU-CyCLONe. V závislosti na situaci mohou informace, které mají být poskytovány, zahrnovat zejména technické informace, informace o povaze a motivech útočníka nebo potenciálního útočníka a jiné než technické údaje vyšší úrovně o potenciálním nebo probíhajícím rozsáhlém kybernetickém bezpečnostním incidentu. V této souvislosti je třeba věnovat náležitou pozornost zásadě „vědět jen to nejnutnější“ a potenciálně citlivé povaze sdělovaných informací. Směrnice (EU) 2022/2555 rovněž znovu vyjmenovává povinnosti Komise v rámci mechanismu civilní ochrany Unie zřízeného rozhodnutím Evropského parlamentu a Rady č. 1313/2013/EU[13] a její odpovědnost za poskytování analytických zpráv v rámci opatření EU pro integrovanou politickou reakci na krize (dále jen „opatření IPCR“) podle prováděcího rozhodnutí (EU) 2018/1993[14].

---

13 Rozhodnutí Evropského parlamentu a Rady č. 1313/2013/EU ze dne 17. prosince 2013 o mechanismu civilní ochrany Unie (Úř. věst. L 347, 20.12.2013, s. 924, ELI: http://data.europa.eu/eli/dec/2013/1313/oj).

14 Prováděcí rozhodnutí Rady (EU) 2018/1993 ze dne 11. prosince 2018 o opatřeních pro integrovanou politickou reakci EU na krize (Úř. věst. L 320, 17.12.2018, s. 284, ELI: http://data.europa.eu/eli/dec_impl/2018/1993/oj).

Pokud přeshraniční kybernetická centra sdílejí se sítí EU-CyCLONe a sítí CSIRT relevantní informace a včasná varování týkající se potenciálního nebo probíhajícího rozsáhlého kybernetického bezpečnostního incidentu, je naprosto nezbytné, aby byly tyto informace prostřednictvím těchto sítí sdělovány orgánům členských států i Komise. V této souvislosti směrnice (EU) 2022/2555 stanoví, že účelem sítě EU-CyCLONe je podpořit koordinované řešení rozsáhlých kybernetických bezpečnostních incidentů a krizí na operativní úrovni a zajistit pravidelnou výměnu relevantních informací mezi členskými státy a orgány, institucemi a jinými subjekty Unie. K úkolům této sítě patří získávání společného situačního povědomí o těchto incidentech a krizích. Je nanejvýš důležité, aby síť EU-CyCLONe v souladu s tímto účelem a se svými úkoly zajistila, aby tyto informace byly okamžitě sdělovány příslušným zástupcům členských států a Komisi. Za tímto účelem je naprosto nezbytné, aby jednací řád sítě EU-CyCLONe obsahoval vhodná ustanovení.

(22) Subjekty, které se účastní Evropského systému varování v oblasti kybernetické bezpečnosti, by měly zajistit vysokou úroveň vzájemné interoperability, případně včetně interoperability formátů dat, taxonomie, nástrojů pro zpracování a analýzu dat. Měly by rovněž zajistit bezpečné komunikační kanály, minimální úroveň zabezpečení aplikační vrstvy a přehled situačního povědomí a ukazatele. Při přijetí společné taxonomie a vypracování vzoru situačních zpráv pro popis příčin zjištěných kybernetických hrozeb a rizik by se měla zohlednit již vykonaná práce v souvislosti s uplatňováním směrnice (EU) 2022/2555.

(23) Aby se umožnila rozsáhlá výměna relevantních dat a informací o kybernetických hrozbách z různých zdrojů v důvěryhodném a zabezpečeném prostředí, měly by být subjekty zapojené do Evropského systému varování v oblasti kybernetické bezpečnosti vybaveny nejmodernějšími a vysoce bezpečnými nástroji, vybavením a infrastrukturou, jakož i kvalifikovaným personálem. Díky tomu by mělo být možné zlepšit kapacity kolektivního odhalování a včasná varování orgánů a příslušných subjektů, zejména s využitím nejnovějších technologií umělé inteligence a analýzy dat.

(24) Při shromažďování, analýze, sdílení a výměně relevantních dat a informací by Evropský systém varování v oblasti kybernetické bezpečnosti měl posílit technologickou suverenitu Unie a otevřenou strategickou autonomii v oblasti kybernetické bezpečnosti, konkurenceschopnost a odolnost. Shromažďování kvalitních vybraných dat by mohlo rovněž přispět k rozvoji pokročilých technologií umělé inteligence a analýzy dat. Pro účinné shromažďování vysoce kvalitních dat jsou i nadále nezbytné lidský dohled a za tímto účelem i kvalifikovaní pracovníci.

(25) Ačkoliv je Evropský systém varování v oblasti kybernetické bezpečnosti civilní projekt, větší civilní schopnosti v oblasti odhalování a situačního povědomí vyvinuté k ochraně kritické infrastruktury by mohly být přínosem pro komunitu kybernetické obrany.

(26) Sdílení informací mezi účastníky Evropského systému varování v oblasti kybernetické bezpečnosti by mělo být v souladu se stávajícími právními požadavky, zejména s unijním a vnitrostátním právem v oblasti ochrany údajů, jakož i s pravidly Unie pro hospodářskou soutěž, kterými se řídí výměna informací. Příjemce informací by měl v rozsahu, v jakém je zpracování osobních údajů nezbytné, zavést technická a organizační opatření, která zajistí práva a svobody subjektů údajů, a zničit údaje, jakmile již nebudou pro stanovený účel potřebné, a informovat subjekt, který údaje zpřístupnil, že údaje byly zničeny.

(27) Zachování důvěrnosti a bezpečnosti informací má zásadní význam pro všechny tři pilíře tohoto nařízení, ať už jde o podporu sdílení nebo výměny informací v rámci Evropského systému varování v oblasti kybernetické bezpečnosti, o ochranu zájmů subjektů žádajících o podporu v rámci mechanismu pro mimořádné situace v oblasti kybernetické bezpečnosti nebo o zajištění toho, aby zprávy v rámci evropského mechanismu přezkumu kybernetických bezpečnostních incidentů mohly přinést užitečná poučení, aniž by to mělo negativní dopad na subjekty zasažené incidenty. Účast členských států a subjektů na těchto mechanismech závisí na vztazích mezi jejich složkami založenými na důvěře. Pokud jsou informace podle unijních nebo vnitrostátních pravidel důvěrné, mělo by být jejich sdílení nebo výměna podle tohoto nařízení omezeno na to, co je relevantní a přiměřené z hlediska účelu sdílení nebo výměny. Při sdílení nebo výměnách těchto informací by se měla zachovávat důvěrnost předmětných informací a chránit bezpečnost a obchodní zájmy příslušných subjektů. Ke sdílení nebo výměně informací podle tohoto nařízení by mohlo docházet prostřednictvím dohod o zachování mlčenlivosti nebo pokynů pro šíření informací, jako je protokol TLP (Traffic Light Protocol). Tento protokol je třeba chápat jako prostředek k poskytování informací o veškerých omezeních, pokud jde o další šíření informací. Používá se téměř ve všech týmech CSIRT a v některých centrech ISAC. Pokud jde o Evropský systém varování v oblasti kybernetické bezpečnosti, měla by být v dohodách o hostitelských konsorciích stanovena kromě těchto obecných požadavků i zvláštní pravidla týkající se podmínek pro sdílení informací v rámci dotčeného přeshraničního kybernetického centra. Tyto dohody by mohly obsahovat zejména požadavek, aby ke sdílení informací docházelo pouze v souladu s unijním a vnitrostátním právem.

(28) Pokud jde o vytvoření rezervy EU pro kybernetickou bezpečnost, jsou nezbytná zvláštní pravidla týkající se důvěrnosti dat. Podpora bude požadována, posuzována a poskytována v kontextu krize a ve vztahu k subjektům působícím v citlivých odvětvích. Aby bylo zajištěno účinné fungování rezervy EU pro kybernetickou bezpečnost, je klíčové, aby uživatelé a subjekty mohli sdílet veškeré informace, které jsou nezbytné k tomu, aby každý subjekt mohl plnit svou úlohu při posuzování žádostí a zavádění podpory, a neprodleně k nim poskytnout přístup. V tomto nařízení by proto mělo být stanoveno, že všechny tyto informace mají být používány a sdíleny pouze tehdy, je-li to nezbytné pro provoz rezervy EU pro kybernetickou bezpečnost, a že informace, které jsou podle unijního a vnitrostátního práva důvěrné nebo utajované, mají být používány a sdíleny pouze v souladu s tímto právem. Kromě toho by uživatelé měli mít k dalšímu upřesnění omezení možnost používat ve vhodných případech protokoly pro sdílení informací, jako jsou protokoly TLP. I když mají uživatelé v tomto ohledu prostor pro uvážení, je důležité, aby při uplatňování těchto omezení zohlednili možné důsledky, zejména pokud jde o opožděné posouzení nebo poskytnutí požadovaných služeb. Z hlediska účinnosti rezervy EU pro kybernetickou bezpečnost je důležité, aby veřejný zadavatel uživateli objasnil tyto důsledky předtím, než uživatel žádost podá. Tyto záruky jsou omezeny na žádost o služby poskytované v rámci rezervy EU pro kybernetickou bezpečnost a na jejich poskytování a nemají vliv na výměnu informací v jiných souvislostech, například při zadávání veřejných zakázek na služby poskytované v rámci této rezervy.

(29) Vzhledem k rostoucím rizikům a počtu incidentů, které postihují členské státy, je nezbytné zřídit nástroj krizové podpory, totiž mechanismus pro mimořádné situace v oblasti kybernetické bezpečnosti, který by zvýšil odolnost Unie vůči významným kybernetickým bezpečnostním incidentům, rozsáhlým kybernetickým bezpečnostním incidentům a incidentům obdobným rozsáhlým kybernetickým bezpečnostním incidentům a doplnil akce členských států prostřednictvím mimořádné finanční podpory pro připravenost, reakci na incidenty a počáteční obnovení základních služeb. Vzhledem k tomu, že úplné zotavení z incidentu je komplexním procesem obnovy fungování subjektu zasaženého incidentem do stavu z doby před incidentem a mohlo by být dlouhým procesem, který s sebou nese značné náklady, měla by být podpora z rezervy EU pro kybernetickou bezpečnost omezena na počáteční fázi procesu zotavení, což povede k obnovení základních funkcí systémů. Mechanismus pro mimořádné situace v oblasti kybernetické bezpečnosti by měl umožnit rychlé a účinné nasazení pomoci za vymezených okolností a jasných podmínek a umožnit pečlivé sledování a hodnocení toho, jak byly zdroje využity. Ačkoli primární odpovědnost za předcházení incidentům a krizím i za připravenost a reakci na ně nesou i nadále členské státy, mechanismus pro mimořádné události v oblasti kybernetické bezpečnosti podporuje solidaritu mezi členskými státy v souladu s čl. 3 odst. 3 Smlouvy o Evropské unii („dále jen „Smlouva o EU“).

(30) Mechanismus pro mimořádné události v oblasti kybernetické bezpečnosti by měl členským státům poskytovat podporu doplňující jejich vlastní opatření a zdroje a další stávající možnosti podpory v případě reakce na významné kybernetické bezpečnostní incidenty a rozsáhlé kybernetické bezpečnostní incidenty a počáteční obnovy po nich, jako jsou služby poskytované agenturou ENISA v souladu s jejím mandátem, koordinovaná reakce a pomoc ze strany sítě CSIRT, podpora při zmírňování následků ze strany sítě EU-CyCLONe, jakož i vzájemná pomoc mezi členskými státy, a to i v kontextu čl. 42 odst. 7 Smlouvy o EU, týmy rychlé reakce v kybernetickém prostoru v rámci stálé strukturované spolupráce zřízené podle rozhodnutí Rady (SZBP) 2017/2315[15]. Měl by zajistit, aby byly k dispozici specializované prostředky na podporu připravenosti a reakce na kybernetické bezpečnostní incidenty v celé Unii a ve třetích zemích přidružených k programu Digitální Evropa a na zotavení z těchto incidentů.

[15] Rozhodnutí Rady (SZBP) 2017/2315 ze dne 11. prosince 2017, kterým se zřizuje stálá strukturovaná spolupráce a stanoví seznam zúčastněných členských států (Úř. věst. 331. 14.12.2017, s. 57, ELI: http://data.europa.eu/eli/dec/2017/2315/oj).

(31) Tímto nařízením nejsou dotčeny postupy a rámce pro koordinaci reakcí na krize na úrovni Unie, zejména směrnice (EU) 2022/2555, mechanismus civilní ochrany Unie zřízený rozhodnutím Evropského parlamentu a Rady č. 1313/2013/EU[16], opatření IPCR a doporučení Komise (EU) 2017/1584[17]. Podpora poskytovaná v rámci mechanismu pro mimořádné události v oblasti kybernetické bezpečnosti může doplňovat pomoc poskytovanou v rámci společné zahraniční a bezpečnostní politiky a společné bezpečnostní a obranné politiky, a to i prostřednictvím týmů rychlé kybernetické reakce, přičemž je nutné přihlížet k civilní povaze mechanismu pro mimořádné události v kybernetické oblasti. Podpora poskytovaná v rámci mechanismu pro mimořádné události v oblasti kybernetické bezpečnosti může doplňovat akce prováděné v souvislosti s čl. 42 odst. 7 Smlouvy o EU, včetně pomoci poskytované jedním členským státem jinému členskému státu, nebo může být součástí společné reakce Unie a členských států či být poskytována v situacích uvedených v článku 222 Smlouvy o fungování EU. Uplatňování tohoto nařízení by mělo být v případě potřeby koordinováno s prováděním opatření v rámci souboru nástrojů kybernetické diplomacie.

---

[16] Rozhodnutí Evropského parlamentu a Rady č. 1313/2013/EU ze dne 17. prosince 2013 o mechanismu civilní ochrany Unie (Úř. věst. L 347, 20.12.2013, s. 924).

[17] Doporučení Komise (EU) 2017/1584 ze dne 13. září 2017 o koordinované reakci na rozsáhlé kybernetické bezpečnostní incidenty a krize (Úř. věst. L 239, 19.9.2017, s. 36).

(32) Pomoc poskytovaná podle tohoto nařízení by měla podporovat a doplňovat akce prováděné členskými státy na vnitrostátní úrovni. Za tímto účelem by měla být zajištěna úzká spolupráce a konzultace mezi Komisí, agenturou ENISA, členskými státy a případně centrem ECCC. Při žádosti o podporu v rámci mechanismu pro mimořádné události v oblasti kybernetické bezpečnosti by měl členský stát poskytnout relevantní informace, které odůvodňují potřebu podpory.

(33) Směrnice (EU) 2022/2555 vyžaduje, aby členské státy určily nebo zřídily jeden nebo více orgánů pro řešení kybernetických krizí a zajistily, aby tyto orgány měly k dispozici odpovídající zdroje pro účinné a účelné plnění svěřených úkolů. Požaduje také, aby členské státy určily schopnosti, prostředky a postupy, které mohou být nasazeny v případě krize, a aby přijaly národní plán reakce na rozsáhlé kybernetické bezpečnostní incidenty a krize, v němž budou stanoveny cíle a způsoby řešení rozsáhlých kybernetických bezpečnostních incidentů a krizí. Členské státy jsou rovněž povinny zřídit jeden nebo více týmů CSIRT, které budou odpovídat za řešení incidentů podle řádně vymezeného postupu a budou pokrývat alespoň odvětví, pododvětví a druhy subjektů spadající do oblasti působnosti uvedené směrnice, a zajistit, aby tyto týmy měly pro účinné plnění svých úkolů odpovídající zdroje. Tímto nařízením není dotčena úloha Komise při zajišťování toho, aby členské státy plnily povinnosti vyplývající ze směrnice (EU) 2022/2555. Mechanismus pro mimořádné události v oblasti kybernetické bezpečnosti by měl poskytovat pomoc pro akce zaměřené na zvýšení připravenosti, jakož i pro akce prováděné v reakci na incidenty s cílem zmírnit dopady významných kybernetických bezpečnostních incidentů a rozsáhlých kybernetických bezpečnostních incidentů, podpořit počáteční obnovu nebo obnovit fungování služeb, které poskytují subjekty působící ve vysoce kritických odvětvích nebo subjekty působící v dalších kritických odvětvích.

(34) V rámci akcí v oblasti připravenosti by měla být za účelem prosazování jednotného přístupu a posílení bezpečnosti v celé Unii a na jejím vnitřním trhu poskytována podpora pro koordinované testování a posuzování kybernetické bezpečnosti subjektů působících ve vysoce kritických odvětvích určených podle směrnice (EU) 2022/2555, mimo jiné prostřednictvím cvičení a školení. Za tímto účelem by měla Komise po konzultacích s agenturou ENISA, se skupinou pro spolupráci NIS a se sítí EU-CyCLONe pravidelně určovat příslušná odvětví nebo pododvětví, která by měla být způsobilá pro získání finanční podpory na koordinované testování připravenosti na úrovni Unie. Odvětví nebo pododvětví by měla být vybrána z vysoce kritických odvětví uvedených v příloze I směrnice (EU) 2022/2555. Koordinované testování připravenosti by mělo být založeno na společných rizikových scénářích a metodikách.

Při výběru odvětví a vypracování rizikových scénářů by se měla zohlednit příslušná hodnocení rizik a rizikové scénáře pro celou Unii, včetně potřeby vyhnout se zdvojování, jako jsou hodnocení rizik a rizikové scénáře, které požaduje Rada v závěrech o rozvoji pozice Evropské unie v oblasti kybernetické bezpečnosti, které provádějí Komise, vysoký představitel Unie pro zahraniční věci a bezpečnostní politiku (dále jen „vysoký představitel“) a skupina pro spolupráci NIS v koordinaci s příslušnými civilními i vojenskými orgány a agenturami a se zavedenými sítěmi včetně sítě EU CyCLONe, jakož i posouzení rizik komunikačních sítí a infrastruktur, které požaduje společná výzva ministrů z Nevers a které provádí skupina pro spolupráci NIS za podpory Komise a agentury ENISA a ve spolupráci se Sdružením evropských regulačních orgánů v oblasti elektronických komunikací zřízeném nařízením Evropského parlamentu a Rady (EU) 2018/1971[18], koordinované posouzení bezpečnostních rizik kritických dodavatelských řetězců na úrovni Unie, které má být prováděno podle článku 22 směrnice (EU) 2022/2555, a testování digitální provozní odolnosti podle nařízení Evropského parlamentu a Rady (EU) 2022/2554[19]. Při výběru odvětví by se mělo zohlednit rovněž doporučení Rady o celounijním koordinovaném přístupu za účelem posílení odolnosti kritické infrastruktury.

---

[18] Nařízení Evropského parlamentu a Rady (EU) 2018/1971 ze dne 11. prosince 2018 o zřízení Sdružení evropských regulačních orgánů v oblasti elektronických komunikací (BEREC) a Agentury na podporu BEREC (Úřad BEREC), o změně nařízení (EU) 2015/2120 a o zrušení nařízení (ES) č. 1211/2009 (Už. věst. L 321, 17.12.2018, s. 1).

[19] Nařízení Evropského parlamentu a Rady (EU) 2022/2554 ze dne 14. prosince 2022 o digitální provozní odolnosti finančního sektoru a o změně nařízení (ES) č. 1060/2009, (EU) č. 648/2012, (EU) č. 600/2014, (EU) č. 909/2014 a (EU) 2016/1011 (Úř. věst. L 333, 27.12.2022, s. 1).

(35) Mechanismus pro mimořádné události v oblasti kybernetické bezpečnosti by měl navíc poskytovat podporu pro další akce v oblasti připravenosti a podporovat připravenost v jiných odvětvích, na něž se nevztahuje koordinované testování připravenosti subjektů působících ve vysoce kritických odvětvích nebo subjektů působících v dalších kritických odvětvích. Tato opatření by mohla zahrnovat různé druhy činnosti v oblasti vnitrostátní připravenosti.

(36) Pokud členské státy obdrží granty na podporu akcí v oblasti připravenosti, mohou se těchto akcí dobrovolně účastnit subjekty ve vysoce kritických odvětvích. Osvědčeným postupem je, že v návaznosti na tyto akce vypracují zúčastněné subjekty plán nápravy za účelem provedení veškerých výsledných doporučení týkajících se konkrétních opatření, aby měly z akcí v oblasti připravenosti co největší prospěch. I když je důležité, aby členské státy v rámci opatření požadovaly, aby zúčastněné subjekty vypracovaly a uplatňovaly tyto plány nápravy, členským státům není tímto nařízením uložena povinnost takové žádosti prosazovat ani jim k tomu nejsou zmocněny. Těmito žádostmi nejsou dotčeny požadavky na subjekty ani pravomoci příslušných orgánů v oblasti dohledu v souladu se směrnicí (EU) 2022/2555.

(37) Mechanismus pro mimořádné události v oblasti kybernetické bezpečnosti by měl rovněž poskytovat podporu pro akce prováděné v reakci na incidenty s cílem zmírnit dopady významných kybernetických bezpečnostních incidentů, rozsáhlých kybernetických bezpečnostních incidentů a incidentů obdobným rozsáhlým kybernetickým bezpečnostním incidentům, podpořit počáteční obnovu nebo obnovit fungování základních služeb. V případě potřeby by měl doplňovat mechanismus civilní ochrany Unie, aby byl zajištěn komplexní přístup k reakci na dopady incidentů na občany.

(38) Mechanismus pro mimořádné události v oblasti kybernetické bezpečnosti by měl podporovat technickou pomoc poskytovanou jedním členským státem jinému členskému státu, který je zasažen významným kybernetickým bezpečnostním incidentem nebo rozsáhlým kybernetickým bezpečnostním incidentem, a to i prostřednictvím sítě CSIRT podle čl. 11 odst. 3 písm. f) směrnice (EU) 2022/2555. Členské státy poskytující tuto pomoc by měly mít možnost předkládat žádosti o úhradu nákladů spojených s vysláním týmů odborníků v rámci vzájemné pomoci. Způsobilé náklady mohou zahrnovat cestovní výdaje, výdaje na ubytování a denní příspěvky pro odborníky na kybernetickou bezpečnost.

(39) Vzhledem k zásadní úloze, kterou hrají soukromé podniky při odhalování rozsáhlých kybernetických bezpečnostních incidentů a incidentů obdobných rozsáhlým kybernetickým bezpečnostním incidentům a při připravenosti a reakci na ně, je důležité uznat hodnotu dobrovolné spolupráce s těmito podniky, v jejímž rámci nabízejí v případech rozsáhlých kybernetických bezpečnostních incidentů a krizí a incidentů obdobných rozsáhlým kybernetickým bezpečnostním incidentům a krizí své služby bezúplatně. Agentura ENISA by ve spolupráci se sítí EU-CyCLONe mohla sledovat vývoj těchto iniciativ bez nároku na odměnu a podporovat jejich soulad s kritérii platnými pro důvěryhodné poskytovatele řízených bezpečnostních služeb podle tohoto nařízení, a to i pokud jde o důvěryhodnost soukromých podniků, jejich zkušenosti a schopnost bezpečně nakládat s citlivými informacemi.

(40) V rámci mechanismu pro mimořádné situace v oblasti kybernetické bezpečnosti by měla být postupně zřízena rezerva EU pro kybernetickou bezpečnost, která by se skládala ze služeb důvěryhodných poskytovatelů řízených bezpečnostních služeb na podporu akcí prováděných v reakci na incidenty a počáteční obnovy v případě významných kybernetických bezpečnostních incidentů, rozsáhlých kybernetických bezpečnostních incidentů nebo incidentů obdobných rozsáhlým kybernetickým bezpečnostním incidentům, které mají dopad na členské státy, orgány, instituce nebo jiné subjekty Unie nebo na třetí země přidružené k programu Digitální Evropa. Rezerva EU pro kybernetickou bezpečnost by měla zajistit dostupnost a připravenost služeb. Měla by proto zahrnovat služby, které jsou předem přislíbeny, včetně například kapacit, které jsou v pohotovostním režimu a mohou být nasazeny v krátké lhůtě. Služby v rámci rezervy EU pro kybernetickou bezpečnost by měly sloužit jako podpora vnitrostátním orgánům při poskytování pomoci zasaženým subjektům působícím ve vysoce kritických odvětvích nebo působícím v dalších kritických odvětvích jako doplněk jejich vlastních akcí na vnitrostátní úrovni. Služby v rámci rezervy EU pro kybernetickou bezpečnost by měly být schopny za podobných podmínek rovněž sloužit také na podporu orgánů, institucí nebo jiných subjektů Unie. Rezerva EU pro kybernetickou bezpečnost může přispět také k posílení konkurenčního postavení průmyslu a služeb v Unii v celé digitální ekonomice, včetně mikropodniků, malých a středních podniků a začínajících podniků, mimo jiné na základě pobídek k investování do výzkumu a inovací. Při zadávání zakázek na služby pro tuto rezervu je důležité zohlednit evropský rámec dovedností v oblasti kybernetické bezpečnosti (ECSF). Při žádání o podporu z rezervy EU pro kybernetickou bezpečnost by uživatelé měli do své žádosti zahrnout vhodné informace o zasaženém subjektu a potenciálním dopadu, informace o požadované službě z rezervy EU pro kybernetickou bezpečnost a o podpoře poskytnuté postiženému subjektu na vnitrostátní úrovni, které by měly být zohledněny při posuzování žádosti žadatele. Aby byla zajištěna doplňkovost s jinými formami podpory, které má zasažený subjekt k dispozici, měla by žádost obsahovat, pokud jsou k dispozici, informace o existujících smluvních ujednáních týkajících se služeb v oblasti reakce na incident a počáteční obnovy i o pojistných smlouvách, které by se mohly vztahovat na daný druh incidentu.

(41) Aby bylo zajištěno účinné využívání finančních prostředků Unie, měly by být tyto prostředky v případě, že předem přislíbené služby v rámci rezervy EU pro kybernetickou bezpečnost nejsou využívány k reakci na incidenty po dobu, na kterou byly přislíbeny, v souladu s příslušnou smlouvou přeměněny na služby připravenosti související s prevencí incidentů a reakcí na ně. Tyto služby by měly být doplňkové a neměly by zdvojovat akce v oblasti připravenosti, která má řídit centrum ECCC.

(42) Žádosti o podporu z rezervy EU pro kybernetickou bezpečnost ze strany orgánů členských států pro řešení kybernetických krizí a týmů CSIRT nebo služby CERT-EU podané jménem orgánů, institucí a jiných subjektů Unie by měl posuzovat veřejný zadavatel. Pokud byla agentura ENISA pověřena správou a provozem rezervy EU pro kybernetickou bezpečnost, je tímto veřejným zadavatelem agentura ENISA. Žádosti o podporu ze strany třetích zemí přidružených k programu Digitální Evropa by měla posuzovat Komise. S cílem usnadnit podávání a posuzování žádostí o podporu by agentura ENISA mohla zřídit bezpečnou platformu.

(43) Pokud je přijato více souběžných žádostí, měly by se jednotlivé žádosti upřednostňovat v souladu s kritérii stanovenými v tomto nařízení. S ohledem na obecné cíle tohoto nařízení by tato kritéria měla zahrnovat rozsah a závažnost incidentu, druh zasaženého subjektu, potenciální dopad incidentu na zasažené členské státy a uživatele, potenciální přeshraniční povahu incidentu a riziko rozšíření a opatření, která uživatel již přijal na pomoc při reakci a počáteční obnově. S ohledem na tyto cíle a vzhledem k tomu, že žádosti uživatelů z členských států jsou určeny výhradně na podporu subjektů působících ve vysoce kritických odvětvích nebo subjektů působících v dalších kritických odvětvích v celé Unii, je vhodné dát v případech, kdy vedou tato kritéria k posouzení dvou nebo více žádostí jako rovnocenných, vyšší prioritu žádostem uživatelů z členských států. Tím nejsou dotčeny povinnosti členských států přijmout opatření na ochranu orgánů, institucí a jiných subjektů Unie a na pomoc těmto orgánům, institucím a jiným subjektům, které mají podle příslušných dohod o hostování.

(44) Celkovou odpovědnost za provádění rezervy EU pro kybernetickou bezpečnost by měla nést Komise. Vzhledem k rozsáhlým zkušenostem, které agentura ENISA získala s opatřeními na podporu kybernetické bezpečnosti, je ENISA nejvhodnější agenturou pro provedení rezervy EU pro kybernetickou bezpečnost. Proto by Komise měla agenturu ENISA částečně, nebo pokud to považuje za vhodné, zcela pověřit provozem a správou rezervy EU pro kybernetickou bezpečnost. Toto pověření by mělo být prováděno v souladu s příslušnými pravidly podle nařízení (EU, Euratom) 2024/2509, a zejména by mělo podléhat splnění příslušných podmínek pro podpis dohody o příspěvcích. Veškeré aspekty provozu a správy rezervy EU pro kybernetickou bezpečnost, které nejsou svěřeny agentuře ENISA, by měly podléhat přímému řízení ze strany Komise, a to i před podpisem dohody o příspěvcích.

(45) Členské státy by měly hrát klíčovou úlohu při vytváření a vyslání rezervy EU pro kybernetickou bezpečnost, stejně jako v období po jejím zavedení. Vzhledem k tomu, že nařízení (EU) 2021/694 je příslušným základním aktem pro akce zaměřená na provádění rezervy EU pro kybernetickou bezpečnost, měla by být opatření v rámci této rezervy stanovena v pracovních programech uvedených v článku 24 nařízení (EU) 2021/694. Podle odstavce 6 uvedeného článku má tyto pracovní programy přijmout Komise prostřednictvím prováděcích aktů přijatých přezkumným postupem. Kromě toho by Komise měla v koordinaci se skupinou pro spolupráci NIS určit priority a vývoj rezervy EU pro kybernetickou bezpečnost.

(46) Smlouvy uzavřené v rámci rezervy EU pro kybernetickou bezpečnost by neměly mít vliv na vztahy mezi podniky ani na existující povinnosti mezi zasaženým subjektem nebo uživateli a poskytovatelem služeb.

(47) Pro účely výběru soukromých poskytovatelů služeb, kteří budou poskytovat služby v rámci rezervy EU pro kybernetickou bezpečnost, je nezbytné stanovit soubor minimálních kritérií a požadavků, která by měla být zahrnuta do výzvy k podávání nabídek za účelem výběru těchto poskytovatelů, aby bylo zajištěno naplnění potřeb orgánů členských států, subjektů působících ve vysoce kritických odvětvích nebo subjektů působících v dalších kritických odvětvích. Aby bylo možné řešit konkrétní potřeby členských států, měl by veřejný zadavatel při zadávání zakázek na služby pro rezervu EU pro kybernetickou bezpečnost případně vypracovat dodatečná výběrová kritéria a požadavky nad rámec kritérií stanovených v tomto nařízení. Je důležité podporovat účast menších poskytovatelů služeb působících na regionální a místní úrovni.

(48) Při výběru poskytovatelů služeb, kteří mají být zařazeni do rezervy EU pro kybernetickou bezpečnost, by měl veřejný zadavatel usilovat o zajištění toho, aby tato rezerva jako celek obsahovala ty poskytovatele, kteří jsou schopni vyhovět jazykovým požadavkům uživatelů. Za tímto účelem by měl veřejný zadavatel před vypracováním zadávací dokumentace zjistit, zda potenciální uživatelé rezervy EU pro kybernetickou bezpečnost nemají nějaké zvláštní jazykové požadavky, aby mohly být podpůrné služby v rámci této rezervy poskytovány v tom z úředních jazyků orgánů Unie nebo členského státu, kterému uživatel nebo zasažený subjekt pravděpodobně rozumí. V případě, že uživatel potřebuje pro poskytování podpůrných služeb v rámci rezervy více než jeden jazyk a tyto služby byly pro tohoto uživatele pořizovány v těchto jazycích, měl by mít uživatel možnost v žádosti o podporu z rezervy EU pro kybernetickou bezpečnost uvést, ve kterém z těchto jazyků by měly být poskytnuty služby v souvislosti s konkrétním incidentem, který vedl k podání žádosti.

(49) Na podporu zřízení rezervy EU pro kybernetickou bezpečnost je důležité, aby Komise požádala agenturu ENISA, aby připravila návrh schématu certifikace v oblasti kybernetické bezpečnosti pro řízené bezpečnostní služby podle nařízení (EU) 2019/881 v oblastech, na které se vztahuje mechanismus pro mimořádné události v oblasti kybernetické bezpečnosti.

(50) Na podporu cílů tohoto nařízení, kterými jsou podpora společného situačního povědomí, zvýšení odolnosti Unie a umožnění účinné reakce na významné kybernetické bezpečnostní incidenty a rozsáhlé kybernetické bezpečnostní incidenty, by měla mít Komise nebo síť EU-CyCLONe možnost požádat s pomocí sítě CSIRT a se souhlasem dotčených členských států agenturu ENISA o přezkum a posouzení kybernetických hrozeb, známých zneužitelných zranitelností a akcí ke zmírnění dopadů v souvislosti s konkrétním významným kybernetickým bezpečnostním incidentem nebo rozsáhlým kybernetickým bezpečnostním incidentem. Po dokončení přezkumu a posouzení incidentu by agentura ENISA měla ve spolupráci s dotčeným členským státem, příslušnými zúčastněnými stranami, včetně zástupců soukromého sektoru, Komise a dalších příslušných orgánů, institucí a jiných subjektů Unie, vypracovat zprávu o přezkumu incidentu. Na základě spolupráce se zúčastněnými stranami, včetně soukromého sektoru, by se zpráva o přezkumu konkrétních incidentů měla zaměřit na posouzení příčin, dopadu a zmírnění následků incidentu poté, co k němu došlo. Zvláštní pozornost by měla být věnována příspěvkům a zkušenostem sdíleným poskytovateli řízených bezpečnostních služeb, kteří splňují podmínky nejvyšší profesní bezúhonnosti, nestrannosti a požadované technické odbornosti podle požadavků tohoto nařízení. Zpráva by měla být předložena síti EU-CyCLONe, síti CSIRT a Komisi a měla by být podkladem pro jejich práci i práci agentury ENISA. Pokud se incident týká třetí země přidružené k programu Digitální Evropa, měla by Komise poskytnout zprávu vysokému představiteli.

(51) S ohledem na nepředvídatelnou povahu kybernetických útoků a skutečnost, že se často neomezují na určitou zeměpisnou oblast a představují vysoké riziko rozšíření, přispívá posílení odolnosti sousedních zemí a jejich kapacity účinně reagovat na významné kybernetické bezpečnostní incidenty a na incidenty obdobné rozsáhlým kybernetickým bezpečnostním incident k ochraně Unie jako celku, a zejména jejího vnitřního trhu a průmyslu. Tato činnost by mohla dále přispět k diplomacii Unie v oblasti kybernetické bezpečnosti. Proto by měly třetí země přidružené k programu Digitální Evropa mít možnost požádat o podporu z rezervy EU pro kybernetickou bezpečnost na celém svém území nebo na jeho části, pokud je to stanoveno v dohodě, jejímž prostřednictvím je třetí země přidružena k programu Digitální Evropa. Financování třetích zemí přidružených k programu Digitální Evropa by mělo být Unií podporováno v rámci příslušných partnerství a nástrojů financování pro tyto země. Podpora by měla zahrnovat služby v oblasti reakce na významné kybernetické bezpečnostní incidenty nebo na incidenty obdobné rozsáhlým kybernetickým bezpečnostním incidentům a zahájení obnovy po těchto incidentech.

(52) Při poskytování podpory třetím zemím přidruženým k programu Digitální Evropa by měly platit podmínky stanovené v tomto nařízení pro rezervu EU pro kybernetickou bezpečnost a důvěryhodné poskytovatele řízených bezpečnostních služeb. Třetí země přidružené k programu Digitální Evropa by měly mít možnost požádat o pomoc v rámci rezervy EU pro kybernetickou bezpečnost, pokud jsou cílové subjekty, pro které žádají o podporu z rezervy EU pro kybernetickou bezpečnost, subjekty působícími ve vysoce kritických odvětvích nebo subjekty působícími v dalších kritických odvětvích a pokud zjištěné incidenty vedou v Unii k závažnému narušení provozu nebo se mohou rozšířit. Třetí země přidružené k programu Digitální Evropa by měly být způsobilé k získání podpory pouze v případě, že je v dohodě, jejímž prostřednictvím jsou přidruženy k programu Digitální Evropa, tato podpora výslovně stanovena. Kromě toho by tyto třetí země měly zůstat způsobilé pouze tehdy, jsou-li splněna tři kritéria. Za prvé, třetí země by měla plně dodržovat příslušné podmínky uvedené dohody. Za druhé, vzhledem k doplňkové povaze rezervy EU pro kybernetickou bezpečnost by třetí země měla přijmout odpovídající kroky k přípravě na významné kybernetické bezpečnostní incidenty nebo na incidenty obdobné rozsáhlým kybernetickým bezpečnostním incidentům. Za třetí, poskytování podpory z rezervy EU pro kybernetickou bezpečnost by mělo být v souladu s politikou Unie vůči této zemi a s celkovými vztahy Unie s touto zemí a s další politikou Unie v oblasti bezpečnosti. Při posuzování souladu s tímto třetím kritériem by Komise měla za účelem sladění poskytování této podpory se společnou zahraniční a bezpečnostní politikou konzultovat vysokého představitele.

(53) Poskytování podpory třetím zemím přidruženým k programu Digitální Evropa může ovlivnit vztahy se třetími zeměmi a bezpečnostní politiku Unie, a to i v rámci společné zahraniční a bezpečnostní politiky a společné obranné a bezpečnostní politiky. Je proto vhodné, aby byly Radě svěřeny prováděcí pravomoci, pokud jde o povolování a upřesňování doby, po niž může být tato podpora poskytována. Rada by měla jednat na základě návrhu Komise a náležitě přitom zohlednit posouzení uvedených tří kritérií ze strany Komise. Totéž by mělo platit pro prodlužování platnosti těchto aktů a návrhy na jejich změnu nebo zrušení. Pokud se Rada za výjimečných okolností domnívá, že došlo k významné změně okolností, pokud jde o třetí kritérium, měla by mít možnost jednat z vlastního podnětu a změnit či zrušit prováděcí akt, aniž by čekala na návrh Komise. Tyto významné změny budou pravděpodobně vyžadovat naléhavá opatření, budou mít obzvláště významné důsledky pro vztahy se třetími zeměmi a nebudou vyžadovat předběžné podrobné posouzení ze strany Komise. Kromě toho by Komise měla v souvislosti s žádostmi o podporu třetích zemích přidružených k programu Digitální Evropa a prováděním podpory poskytnuté takovýmto zemím spolupracovat s vysokým představitelem. Měla rovněž zohlednit případné stanovisko agentury ENISA ohledně těchto žádostí a podpory. Komise by navíc měla informovat Radu o výsledku posouzení žádostí, včetně relevantních úvah v tomto ohledu, a o využitých službách.

(54) Ve sdělení Komise ze dne 18. dubna 2023 o Akademii dovedností v oblasti kybernetické bezpečnosti se uznává nedostatek kvalifikovaných odborníků. Tyto dovednosti jsou potřebné pro splnění cílů tohoto nařízení. Unie naléhavě potřebuje odborníky se schopnostmi a kompetencemi, aby mohla předcházet kybernetickým útokům, odhalovat je, odrazovat od nich a bránit Unii, včetně její nejkritičtější infrastruktury, proti těmto útokům a zajistit její odolnost. Za tímto účelem je důležité podporovat spolupráci mezi zúčastněnými stranami, včetně soukromého sektoru, akademické obce a veřejného sektoru. Stejně důležité je také vytvořit na veškerém území Unie součinnost v oblasti investic do vzdělávání a školení s cílem podpořit zavádění ochranných prvků, které by zabránily odlivu mozků a zajistily, aby v některých regionech nedocházelo ve srovnání s jinými regiony k dalšímu prohlubování nedostatku dovedností. Je naléhavě nutné odstranit rozdíly v dovednostech v oblasti kybernetické bezpečnosti a zaměřit se přitom zejména na snižování genderových rozdílů v odvětví kybernetické bezpečnosti s cílem podpořit přítomnost žen a jejich účast na navrhování digitální správy.

(55) Pro podporu inovací na jednotném digitálním trhu je důležité posílit výzkum a inovace v oblasti kybernetické bezpečnosti s cílem přispět ke zvýšení odolnosti členských států a k dosažení otevřené strategické autonomie Unie, což obojí patří mezi cíle tohoto nařízení. Součinnost má zásadní význam pro prohloubení spolupráce a koordinace mezi různými zúčastněnými stranami, včetně soukromého sektoru, občanské společnosti a akademické obce.

(56) Toto nařízení by mělo zohledňovat závazek stanovený ve společném prohlášení Evropského parlamentu, Rady a Komise ze dne 26. ledna 2022 nazvaném „Evropské prohlášení o digitálních právech a zásadách pro digitální dekádu“ chránit zájmy demokracií, občanů, podniků a veřejných institucí Unie před riziky v oblasti kybernetické bezpečnosti a před kybernetickou kriminalitou, včetně úniku dat a krádeží identity nebo manipulace s ní.

(57) Za účelem doplnění některých méně podstatných prvků tohoto nařízení by měla být na Komisi přenesena pravomoc přijímat akty v souladu s článkem 290 Smlouvy o fungování EU, pokud jde o upřesnění druhů a počtu služeb reakce požadovaných pro rezervu EU pro kybernetickou bezpečnost. Je obzvláště důležité, aby Komise v rámci přípravné činnosti vedla odpovídající konzultace, a to i na odborné úrovni, a aby tyto konzultace probíhaly v souladu se zásadami stanovenými v interinstitucionální dohodě ze dne 13. dubna 2016 o zdokonalení tvorby právních předpisů[20]. Pro zajištění rovné účasti na vypracovávání aktů v přenesené pravomoci obdrží Evropský parlament a Rada veškeré dokumenty současně s odborníky z členských států a jejich odborníci mají automaticky přístup na zasedání skupin odborníků Komise, jež se věnují přípravě aktů v přenesené pravomoci.

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

(58) Za účelem zajištění jednotných podmínek k provedení tohoto nařízení by měly být Komisi svěřeny prováděcí pravomoci, pokud jde o další upřesnění podrobných procesních opatření pro přidělování podpůrných služeb z rezervy EU pro kybernetickou bezpečnost. Tyto pravomoci by měly být vykonávány v souladu s nařízením Evropského parlamentu a Rady (EU) č. 182/2011[21].

(59) Aniž jsou dotčena pravidla týkající se ročního rozpočtu Unie podle Smluv, měla by Komise při posuzování rozpočtových a personálních potřeb agentury ENISA zohlednit povinnosti vyplývající z tohoto nařízení.

(60) Komise by měla pravidelně vypracovávat hodnocení opatření stanovených v tomto nařízení. První takové hodnocení by mělo být vypracováno v prvních dvou letech ode dne vstupu tohoto nařízení v platnost a poté alespoň každé čtyři roky, přičemž se zohlední načasování revize víceletého finančního rámce stanoveného podle článku 312 Smlouvy o fungování EU. Zprávu o dosaženém pokroku předloží Komise Evropskému parlamentu a Radě. Aby bylo možné posoudit různé požadované prvky, včetně rozsahu informací sdílených v rámci Evropského systému varování v oblasti kybernetické bezpečnosti, měla by Komise vycházet výhradně z informací, které jsou snadno dostupné nebo dobrovolně poskytnuté. S ohledem na geopolitický vývoj a s cílem zajistit kontinuitu a další rozvoj opatření stanovených v tomto nařízení na období po roce 2027 je důležité, aby Komise vyhodnotila, zda není nezbytné vyčlenit ve víceletém finančním rámci na období 2028 až 2034 odpovídající rozpočtové prostředky.

---

[21] Nařízení Evropského parlamentu a Rady (EU) č. 182/2011 ze dne 16. února 2011, kterým se stanoví pravidla a obecné zásady způsobu, jakým členské státy kontrolují Komisi při výkonu prováděcích pravomocí (Úř. věst. L 55, 28.2.2011, s. 13, ELI: http://data.europa.eu/eli/reg/2011/182/oj).

(61) Jelikož cílů tohoto nařízení, totiž posílit konkurenceschopnost průmyslu a služeb v Unii v celé digitální ekonomice a přispět k technologické svrchovanosti a otevřené strategické autonomii Unie v oblasti kybernetické bezpečnosti, nemůže být dosaženo uspokojivě členskými státy, ale spíše jich, z důvodu rozsahu nebo účinků tohoto nařízení, může být lépe dosaženo na úrovni Unie, může Unie přijmout opatření v souladu se zásadou subsidiarity stanovenou v článku 5 Smlouvy o EU. V souladu se zásadou proporcionality stanovenou v uvedeném článku nepřekračuje toto nařízení rámec toho, co je nezbytné pro dosažení těchto cílů,

PŘIJALY TOTO NAŘÍZENÍ:

Kapitola I
Obecná ustanovení

Článek 1

Předmět a cíle

1. V tomto nařízení jsou stanovena opatření k posílení kapacit Unie pro odhalování kybernetických bezpečnostních hrozeb a incidentů, přípravu na ně a reakci na ně, zejména zřízením:

   a) celoevropské sítě kybernetických center (dále jen „Evropský systém varování v oblasti kybernetické bezpečnosti“) s cílem vybudovat a posílit koordinované schopnosti odhalování a společného situačního povědomí,

   b) mechanismu pro mimořádné události v oblasti kybernetické bezpečnosti, který bude podporovat členské státy při přípravě na významné kybernetické bezpečnostní incidenty a rozsáhlé kybernetické bezpečnostní incidenty, při reakci na ně, při omezování jejich dopadu a při zahajování obnovy po takových incidentech a podporovat další uživatele při reakci na významné kybernetické bezpečnostní incidenty nebo na incidenty obdobné rozsáhlým kybernetickým bezpečnostním incidentům,

   c) evropského mechanismu přezkumu kybernetických bezpečnostních incidentů, který bude přezkoumávat a posuzovat významné kybernetické bezpečnostní incidenty nebo rozsáhlé kybernetické bezpečnostní incidenty.

2. Toto nařízení sleduje obecné cíle, kterými je posílení konkurenceschopnosti průmyslu a služeb v Unii v celé digitální ekonomice, včetně mikropodniků a malých a středních podniků, jakož i začínajících podniků, a přispění k technologické suverenitě a otevřené strategické autonomii Unie v oblasti kybernetické bezpečnosti, mimo jiné podporou inovací na jednotném digitálním trhu. Nařízení sleduje tyto cíle upevňováním solidarity na úrovni Unie, posilováním ekosystému kybernetické bezpečnosti, zvyšováním kybernetické odolnosti členských států a rozvojem dovedností, know-how, schopností a kompetencí pracovní síly v oblasti kybernetické bezpečnosti.

3. Obecných cílů uvedených v odstavci 2 se dosahuje prostřednictvím těchto specifických cílů:

   a) posílit společné koordinované kapacity odhalování kybernetických hrozeb a incidentů v Unii a společné situační povědomí,

   b) posílit připravenost subjektů působících ve vysoce kritických odvětvích nebo v dalších kritických odvětvích v celé Unii a upevnit solidaritu vytvořením koordinovaného testování připravenosti a kapacit posílené reakce a obnovy pro reakci na významné kybernetické bezpečnostní incidenty, rozsáhlé kybernetické bezpečnostní incidenty nebo incidenty obdobné rozsáhlým kybernetickým bezpečnostním incidentům, včetně možnosti zpřístupnění podpory Unie pro reakci na kybernetické bezpečnostní incidenty třetím zemím přidruženým k programu Digitální Evropa,

c) zvýšit odolnost Unie a přispět k účinné reakci na incidenty přezkumem a posouzením významných kybernetických bezpečnostních incidentů nebo rozsáhlých kybernetických bezpečnostních incidentů, včetně vyvození poučení a případných doporučení.

4. Akce podle tohoto nařízení se provádějí s náležitým ohledem na pravomoci členských států a doplňují činnost prováděnou sítí CSIRT, sítí EU-CyCLONe a skupinou pro spolupráci NIS.

5. Tímto nařízením nejsou dotčeny základní funkce členských států, včetně zajištění územní celistvosti státu, udržování veřejného pořádku a ochrany národní bezpečnosti. Zejména národní bezpečnost zůstává i nadále ve výhradní pravomoci každého členského státu.

6. Sdílení nebo výměna informací podle tohoto nařízení, které mají podle unijních nebo vnitrostátních pravidel důvěrnou povahu, se omezuje na data, která jsou relevantní a přiměřená účelu tohoto sdílení nebo této výměny. Při tomto sdílení nebo výměně informací se zachovává důvěrnost dotčených informací a je chráněna bezpečnost a obchodní zájmy příslušných subjektů. To se netýká poskytování informací, jejichž zveřejnění by bylo v rozporu se základními zájmy členských států v oblasti národní bezpečnosti, veřejné bezpečnosti nebo obrany.

Článek 2

Definice

Pro účely tohoto nařízení se rozumí:

1) „přeshraničním kybernetickým centrem“ platforma, které se účastní více zemí, zřízená prostřednictvím písemné dohody o konsorciu, která v koordinované síťové struktuře sdružuje národní kybernetická centra alespoň ze tří členských států a která je určena ke zlepšení monitorování, odhalování a analýzy kybernetických hrozeb s cílem předcházet incidentům a podporovat získávání poznatků o kybernetických hrozbách, zejména prostřednictvím výměny relevantních a případně anonymizovaných dat a informací, jakož i sdílením nejmodernějších nástrojů a společným vývojem schopností odhalování, analýzy a prevence a ochrany v oblasti kybernetické bezpečnosti v důvěryhodném prostředí;

2) „hostitelským konsorciem“ konsorcium složené ze zúčastněných členských států, které souhlasily se zřízením nástrojů, infrastruktury nebo služeb pro přeshraniční kybernetické centrum a jeho provoz a s poskytnutím příspěvku na pořízení těchto nástrojů, infrastruktury nebo služeb;

3) „týmem CSIRT“ tým CSIRT, který byl určen nebo zřízen podle článku 10 směrnice (EU) 2022/2555;

4) „subjektem“ subjekt ve smyslu čl. 6 bodu 38 směrnice (EU) 2022/2555;

5) „subjekty působícími ve vysoce kritických odvětvích“ druhy subjektů uvedené v příloze *I* směrnice (EU) 2022/2555;

6) „subjekty působícími v dalších kritických odvětvích“ druhy subjektů uvedené v příloze II směrnice (EU) 2022/2555;

7) „rizikem“ riziko ve smyslu čl. 6 bodu 9 směrnice (EU) 2022/2555;

8) „kybernetickou hrozbou“ kybernetická hrozba ve smyslu čl. 2 bodu 8 nařízení (EU) 2019/881;

9) „incidentem“ incident ve smyslu čl. 6 bodu 6 směrnice (EU) 2022/2555;

10) „významným kybernetickým bezpečnostním incidentem“ kybernetický bezpečnostní incident, který splňuje kritéria stanovená v čl. 23 odst. 3 směrnice (EU) 2022/2555;

11) „závažným incidentem“ závažný incident ve smyslu čl. 3 bodě 8 nařízení Evropského parlamentu a Rady (EU, Euratom) č. 2023/2841[22];

12) „rozsáhlým kybernetickým bezpečnostním incidentem“ rozsáhlý kybernetický bezpečnostní incident ve smyslu čl. 6 bodu 7 směrnice (EU) 2022/2555;

---

[22] Nařízení Evropského parlamentu a Rady (EU, Euratom) 2023/2841 ze dne 13. prosince 2023, kterým se stanoví opatření k zajištění vysoké společné úrovně kybernetické bezpečnosti v orgánech, institucích a jiných subjektech Unie (Úř. věst. L, 2023/2841, 18.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2841/oj).

13) „incidentem obdobným rozsáhlému kybernetickému bezpečnostnímu incidentu“ v případě orgánů, institucí a jiných subjektů Unie závažný incident a v případě třetích zemí přidružených k programu Digitální Evropa incident, který způsobí takovou míru narušení, která přesahuje kapacitu dotčené třetí země přidružené k programu Digitální Evropa na něj reagovat;

14) „třetí zemí přidruženou k programu Digitální Evropa“ třetí země, která je smluvní stranou dohody s Unií umožňující její účast v programu Digitální Evropa podle článku 10 nařízení (EU) 2021/694;

15) „veřejným zadavatelem“ Komise nebo, v rozsahu, v němž byla provozem a správou rezervy EU pro kybernetickou bezpečnost pověřena agentura ENISA podle čl. 14 odst. 5 tohoto nařízení, agentura ENISA;

16) „poskytovatelem řízených bezpečnostních služeb“ poskytovatel řízených bezpečnostních služeb ve smyslu čl. 6 bodu 40 směrnice (EU) 2022/2555;

17) „důvěryhodnými poskytovateli řízených bezpečnostních služeb“ poskytovatelé řízených bezpečnostních služeb, kteří byli v souladu s článkem 17 vybráni k tomu, aby byli zapojeni do rezervy EU pro kybernetickou bezpečnost.

Kapitola II

Evropský systém varování v oblasti kybernetické bezpečnosti

Článek 3

Zřízení Evropského systému varování v oblasti kybernetické bezpečnosti

1. Zřizuje se Evropský systém varování v oblasti kybernetické bezpečnosti, což je celoevropská síť infrastruktury, která sestává z národních kybernetických center a přeshraničních kybernetických center, jež se k ní připojují dobrovolně, s cílem podpořit rozvoj pokročilých schopností Unie za účelem rozvíjení schopností Unie odhalovat, analyzovat a zpracovávat data v souvislosti s kybernetickými hrozbami v Unii a předcházet incidentům v Unii.

2. Evropský systém varování v oblasti kybernetické bezpečnosti:

   a) přispívá k lepší ochraně proti kybernetickým hrozbám a reakci na ně tím, že podporuje příslušné subjekty, zejména týmy CSIRT, síť CSIRT, síť EU-CyCLONe a příslušné orgány určené nebo zřízené podle článku 8 směrnice (EU) 2022/2555, spolupracuje s nimi a posiluje jejich schopnosti;

   b) shromažďuje relevantní data a informace o kybernetických hrozbách a incidentech z různých zdrojů v rámci přeshraničních kybernetických center a sdílí analyzované nebo agregované informace prostřednictvím přeshraničních kybernetických center a případně se sítí CSIRT;

c) shromažďuje a podporuje získávání kvalitních a použitelných informací a poznatků o kybernetických hrozbách s využitím nejmodernějších nástrojů a pokročilých technologií a sdílí tyto informace a poznatky o kybernetických hrozbách;

d) přispívá k posilování koordinovaného odhalování kybernetických hrozeb, k získání společného situačního povědomí v celé Unii a k vydávání varování, v relevantních případech včetně poskytováním konkrétních doporučení subjektům;

e) poskytuje služby a zajišťuje činnost pro komunitu kybernetické bezpečnosti v Unii, mimo jiné přispívá k vývoji pokročilých nástrojů a technologií, jako je umělá inteligence a nástroje analýzy dat.

3. Akce, kterými se provádí Evropský systém varování v oblasti kybernetické bezpečnosti, jsou podporovány z finančních prostředků programu Digitální Evropa a prováděny v souladu s nařízením (EU) 2021/694, zejména s jeho specifickým cílem č. 3.

Článek 4

Národní kybernetická centra

1. Pokud se členský stát rozhodne podílet se na Evropském systému varování v oblasti kybernetické bezpečnosti, určí nebo případně zřídí pro účely tohoto nařízení národní kybernetické centrum.

2. Národní kybernetické centrum je jedním subjektem a jedná z pověření členského státu. Může se jednat o tým CSIRT nebo případně o vnitrostátní orgán pro řešení kybernetických bezpečnostních krizí nebo jiný příslušný orgán určený nebo zřízený podle čl. 8 odst. 1 směrnice (EU) 2022/2555 či jiný subjekt. Národní kybernetické centrum musí být schopno:

   a) působit jako referenční bod a brána pro další veřejné a soukromé organizace na vnitrostátní úrovni pro účely shromažďování a analýzy informací o kybernetických bezpečnostních hrozbách a incidentech a přispívat k činnosti přeshraničního kybernetického centra podle článku 5; a

   b) odhalovat, agregovat a analyzovat data a informace týkající se kybernetických hrozeb a incidentů, jako jsou poznatky o kybernetických hrozbách, zejména s využitím nejmodernějších technologií, s cílem předcházet incidentům.

3. V rámci funkcí uvedených v odstavci 2 tohoto článku mohou národní kybernetická centra spolupracovat se subjekty soukromého sektoru a vyměňovat si relevantní údaje a informace za účelem odhalování kybernetických hrozeb a incidentů a předcházení těmto hrozbám a incidentům, a to i s odvětvovými a meziodvětvovými komunitami základních a důležitých subjektů podle článku 3 směrnice (EU) 2022/2555. Informace vyžádané nebo obdržené národními kybernetickými centry mohou ve vhodných případech zahrnovat v souladu s unijním a vnitrostátním právem telemetrické údaje, údaje z čidel a údaje o přihlášeních.

4. Členský stát vybraný podle čl. 9 odst. 1 se zaváže, že jeho národní kybernetické centrum požádá o účast v přeshraničním kybernetickém centru.

Článek 5

Přeshraniční kybernetická centra

1. Pokud hodlají alespoň tři členské státy zajistit, aby jejich národní kybernetická centra spolupracovala na koordinaci svých činností v oblasti odhalování a monitorování kybernetických hrozeb, mohou tyto členské státy pro účely tohoto nařízení zřídit hostitelské konsorcium.

2. Hostitelské konsorcium je složené nejméně ze tří zúčastněných členských států, které souhlasily se zřízením nástrojů, infrastruktury nebo služeb pro přeshraniční kybernetické centrum v souladu s odstavcem 4 a jeho provoz a s poskytnutím příspěvku na jejich pořízení.

3. Je-li hostitelské konsorcium vybráno podle čl. 9 odst. 3, jeho členové uzavřou písemnou dohodu o konsorciu:

   a) v níž je stanoveno vnitřní ujednání k provádění dohody o hostování a užívání podle čl. 9 odst. 3,

   b) kterou se zřizuje přeshraniční kybernetické centrum hostitelského konsorcia, a

   c) která zahrnuje zvláštní ustanovení požadovaná podle čl. 6 odst. 1 a 2.

4. Přeshraniční kybernetické centrum je platforma, které se účastní více zemí, zřízená písemnou dohodou o konsorciu uvedenou v odstavci 3. V koordinované síťové struktuře sdružuje národní kybernetická centra členských států hostitelského konsorcia. Je určeno pro zdokonalení monitorování, odhalování a analýzy kybernetických hrozeb, předcházení incidentům a podporu získávání poznatků o kybernetických hrozeb, zejména prostřednictvím sdílení relevantních a případně anonymizovaných dat a informací a také prostřednictvím sdílení nejmodernějších nástrojů a společným rozvojem schopností odhalování, analýzy, prevence a ochrany v oblasti kybernetické bezpečnosti v důvěryhodném prostředí.

5. Přeshraniční kybernetické centrum je pro právní účely zastoupeno členem příslušného hostitelského konsorcia, který působí jako koordinátor, nebo hostitelským konsorciem, má-li právní osobnost. Odpovědnost za to, že přeshraniční kybernetické centrum dodržuje toto nařízení a dohodu o hostování a užívání, se určí v písemné dohodě o konsorciu uvedené v odstavci 3.

6. Členský stát se může připojit ke stávajícímu hostitelskému konsorciu se souhlasem členů hostitelského konsorcia. Písemná dohoda o konsorciu uvedená v odstavci 3 a dohoda o hostování a užívání se odpovídajícím způsobem upraví. Tím nejsou dotčena vlastnická práva Evropského průmyslového, technologického a výzkumného centra kompetencí pro kybernetickou bezpečnost (dále jen „centrum ECCC“) k nástrojům, infrastruktuře nebo službám, které již byly pořízeny společně s tímto hostitelským konsorciem.

Článek 6

Spolupráce a sdílení informací v rámci přeshraničních kybernetických center a mezi nimi

1. Členové hostitelského konsorcia zajistí, aby jejich národní kybernetická centra v souladu s písemnou dohodou o konsorciu podle čl. 5 odst. 3 mezi sebou v rámci přeshraničního kybernetického centra sdílela relevantní a, tam kde je to vhodné, anonymizované informace, jako jsou informace týkající se kybernetických hrozeb, významných událostí, zranitelností, technik a postupů, indikátorů narušení, nepřátelských taktik, informací specifických pro daný subjekt a danou hrozbu, varování v oblasti kybernetické bezpečnosti a doporučení týkající se konfigurace nástrojů kybernetické bezpečnosti, které slouží k odhalování kybernetických útoků, pokud toto sdílení informací:

   a) podporuje a zlepšuje odhalování kybernetických hrozeb a posiluje schopnosti sítě CSIRT předcházet incidentům a reagovat na ně nebo zmírňovat jejich dopad,

   b) zvyšuje úroveň kybernetické bezpečnosti, například zvyšováním informovanosti o kybernetických hrozbách, omezováním nebo bráněním schopnosti těchto hrozeb šířit se, podporou obranných schopností, nápravou a zveřejňováním zranitelností, odhalováním hrozeb, technikami na zamezení šíření hrozeb a předcházení jim, strategií zmírňování, fází reakce a obnovy nebo podporou společného výzkumu hrozeb ze strany subjektů veřejného a soukromého sektoru.

2. V písemné dohodě o konsorciu podle čl. 5 odst. 3 se stanoví:

a) závazek sdílet mezi členy hostitelského konsorcia informace uvedené v odstavci 1 a podmínky, za nichž mají být tyto informace sdíleny;

b) rámec řízení, který objasňuje sdílení relevantních a případně anonymizovaných informací uvedených v odstavci 1 všemi účastníky a který účastníky k jejich sdílení motivuje,

c) cíle pro přispění k vývoji pokročilých nástrojů a technologií, jako je umělá inteligence a nástroje analýzy dat.

Písemná dohoda o konsorciu může upřesnit, že informace uvedené v odstavci 1 mají být sdíleny v souladu s unijním a vnitrostátním právem.

3. Přeshraniční kybernetická centra mezi sebou uzavírají dohody o spolupráci, v nichž stanoví zásady interoperability a sdílení informací mezi přeshraničními kybernetickými centry. Přeshraniční kybernetická centra informují Komisi o uzavřených dohodách o spolupráci.

4. Sdílení informací podle odstavce 1 mezi přeshraničními kybernetickými centry je zajištěno prostřednictvím vysoké úrovně interoperability. Na podporu této interoperability vydá agentura ENISA v úzké spolupráci s Komisí bez zbytečného odkladu a v každém případě do ... [12 měsíců ode dne vstupu tohoto nařízení v platnost] pokyny k interoperabilitě, v nichž upřesní zejména formáty a protokoly pro sdílení informací, přičemž zohlední mezinárodní normy, osvědčené postupy a fungování již zřízených přeshraničních kybernetických center. Požadavky na interoperabilitu stanovené v dohodách o spolupráci přeshraničních kybernetických center vycházejí z pokynů vydaných agenturou ENISA.

Článek 7

Spolupráce a sdílení informací se sítěmi na úrovni Unie

1. Přeshraniční kybernetická centra a síť CSIRT úzce spolupracují, zejména za účelem sdílení informací. Za tímto účelem se dohodnou na procesních ujednáních o spolupráci a sdílení relevantních informací, a aniž je dotčen odstavec 2, také na druzích informací, které mají být sdíleny.

2. Pokud přeshraniční kybernetická centra získají informace týkající se potenciálního nebo probíhajícího rozsáhlého kybernetického bezpečnostního incidentu, zajistí pro účely získání společného situačního povědomí, aby byly orgánům členských států a Komisi prostřednictvím sítě EU-CyCLONe a sítě CSIRT neprodleně poskytnuty relevantní informace a včasná varování.

Článek 8

Zabezpečení

1. Členské státy, které se účastní Evropského systému varování v oblasti kybernetické bezpečnosti, zajistí vysokou úroveň kybernetické bezpečnosti, včetně důvěrnosti a bezpečnosti dat a fyzické bezpečnosti Evropského systému varování v oblasti kybernetické bezpečnosti, a zabezpečí, aby byla síť přiměřeně spravována a kontrolována, tak aby byla chráněna před hrozbami a aby byla zajištěna její bezpečnost a bezpečnost systémů, včetně bezpečnosti dat a informací sdílených prostřednictvím této sítě.

2. Členské státy, které se účastní Evropského systému varování v oblasti kybernetické bezpečnosti, zajistí, aby sdílení informací podle čl. 6 odst. 1 v rámci Evropského systému varování v oblasti kybernetické bezpečnosti s jakýmkoli jiným subjektem, než je orgán veřejné moci nebo orgán členského státu, nemělo negativní dopad na bezpečnostní zájmy Unie nebo členských států.

Článek 9

Financování Evropského systému varování v oblasti kybernetické bezpečnosti

1. Na základě výzvy k vyjádření zájmu pro členské státy, které se hodlají účastnit Evropského systému varování v oblasti kybernetické bezpečnosti, vybere centrum ECCC členské státy, aby se společně s tímto centrem zúčastnily společného zadávání veřejných zakázek na nástroje, infrastrukturu nebo služby za účelem zřízení národních kybernetických center, jak je uvedeno v čl. 4 odst. 1, nebo za účelem rozšíření schopností takových center. Centrum ECCC může vybraným členským státům udělit granty na financování provozu těchto nástrojů, infrastruktury a služeb. Finanční příspěvek Unie pokrývá až 50 % nákladů na pořízení nástrojů, infrastruktury nebo služeb a až 50 % nákladů na provoz. Zbývající náklady hradí vybrané členské státy. Před zahájením řízení za účelem pořízení nástrojů, infrastruktury nebo služeb uzavře centrum ECCC s vybranými členskými státy dohodu o hostingu a užívání, která upravuje používání příslušných nástrojů, infrastruktury nebo služeb.

2. Pokud se národní kybernetické centrum členského státu nestane účastníkem přeshraničního kybernetického centra do dvou let ode dne, kdy byly nástroje, infrastruktura nebo služby pořízeny nebo kdy obdrželo grantové financování, podle toho, co nastane dříve, nemá členský stát nárok na dodatečnou podporu Unie podle této kapitoly, dokud se nepřipojí k přeshraničnímu kybernetickému centru.

3. Na základě výzvy k vyjádření zájmu vybere centrum ECCC hostitelské konsorcium, které se bude spolu s centrem ECCC podílet na společném zadávání veřejných zakázek týkajících se nástrojů, infrastruktury nebo služeb. Centrum ECCC může hostitelskému konsorciu udělit grant na financování provozu těchto nástrojů, infrastruktury nebo služeb. Finanční příspěvek Unie pokrývá až 75 % nákladů na pořízení nástrojů, infrastruktury nebo služeb a až 50 % nákladů na provoz. Zbývající náklady hradí hostitelské konsorcium. Před zahájením řízení za účelem pořízení nástrojů, infrastruktury nebo služeb uzavře centrum ECCC s hostitelským konsorciem dohodu o hostování a užívání, která upravuje používání příslušných nástrojů, infrastruktury nebo služeb.

4. Centrum ECCC provede alespoň každé dva roky mapování nástrojů, infrastruktury nebo služeb, které jsou nezbytné a mají odpovídající kvalitu pro zřízení národních kybernetických center a přeshraničních kybernetických center a rozšíření jejich schopností a pro zlepšení jejich dostupnosti, mimo jiné od právních subjektů usazených v členských státech nebo považovaných za usazené v členských státech a řízenými členskými státy nebo státními příslušníky členských států. Při provádění tohoto mapování provádí centrum ECCC konzultace se sítí CSIRT, s veškerými stávajícími přeshraničními kybernetickými centry, agenturou ENISA a Komisí.

Kapitola III
Mechanismus pro mimořádné události v oblasti kybernetické bezpečnosti

Článek 10

Zřízení mechanismu pro mimořádné události v oblasti kybernetické bezpečnosti

1. Zřizuje se mechanismus pro mimořádné události v oblasti kybernetické bezpečnosti s cílem podporovat posilování odolnosti Unie vůči kybernetickým hrozbám a, v duchu solidarity, na přípravu na krátkodobý dopad významných kybernetických bezpečnostních incidentů, rozsáhlých kybernetických bezpečnostních incidentů a incidentů obdobných rozsáhlým kybernetickým bezpečnostním incidentům a jeho zmírňování.

2. V případě členských států se akce podle mechanismu pro mimořádné události v oblasti kybernetické bezpečnosti provádějí na jejich žádost a doplňují úsilí a akce členských států s cílem připravit se na incidenty, reagovat na ně a zotavit se z nich.

3. Akce, kterými se provádí mechanismus pro mimořádné události v oblasti kybernetické bezpečnosti, jsou podporovány z finančních prostředků programu Digitální Evropa a prováděny v souladu s nařízením (EU) 2021/694, zejména s jeho specifickým cílem č. 3.

4. Akce v rámci mechanismu pro mimořádné události v oblasti kybernetické bezpečnosti jsou prováděny především prostřednictvím centra ECCC v souladu s nařízením (EU) 2021/887. Akce zaměřené na provádění rezervy EU pro kybernetickou bezpečnost podle čl. 11 písm. b) tohoto nařízení však provádí Komise a agentura ENISA.

Článek 11

Druhy akcí

Mechanismus pro mimořádné události v oblasti kybernetické bezpečnosti podporuje tyto druhy akcí:

a) akce v oblasti připravenosti, konkrétně:

   i) koordinované testování připravenosti subjektů působících ve vysoce kritických odvětvích v celé Unii, jak je uvedeno v článku 12,

   ii) další akce v oblasti připravenosti pro subjekty působící ve vysoce kritických odvětvích nebo v dalších kritických odvětvích, jak je uvedeno v článku 13,

b) akce, které podporují reakci na významné kybernetické bezpečnostní incidenty, rozsáhlé kybernetické bezpečnostní incidenty a incidenty obdobné rozsáhlým bezpečnostním incidentům a zahajování obnovy po nich a která mají poskytovat důvěryhodní poskytovatelé řízených bezpečnostních služeb zapojení do rezervy EU pro kybernetickou bezpečnost zřízené podle článku 14,

c) akce podporující vzájemnou pomoc podle článku 18.

Článek 12

Koordinované testování připravenosti subjektů

1. Mechanismus pro mimořádné události v oblasti kybernetické bezpečnosti podporuje dobrovolné koordinované testování připravenosti subjektů působících ve vysoce kritických odvětvích.

2. Koordinované testování připravenosti může sestávat z činností v oblasti připravenosti, jako je penetrační testování, a z posuzování hrozeb.

3. Podpora akcí v oblasti připravenosti podle tohoto článku se poskytuje členským státům především ve formě grantů a za podmínek stanovených v příslušných pracovních programech, jak je uvedeno v článku 24 nařízení (EU) 2021/694.

4. Za účelem podpory koordinovaného testování připravenosti subjektů uvedených v čl. 11 písm. a) bodu i) tohoto nařízení v celé Unii určí Komise po konzultaci se skupinou pro spolupráci NIS, sítí EU-CyCLONe a agenturou ENISA dotčená odvětví nebo pododvětví z vysoce kritických odvětví vyjmenovaných v příloze I směrnice (EU) 2022/2555, v nichž může být zahájena výzva k podávání návrhů pro účely udělení grantu. Účast členských států na těchto výzvách k podávání návrhů je dobrovolná.

5. Při určování odvětví nebo pododvětví podle odstavce 4 zohlední Komise koordinovaná posouzení rizik a testování odolnosti na úrovni Unie a jejich výsledky.

6. Skupina pro spolupráci NIS vypracuje ve spolupráci s Komisí, vysokým představitelem Unie pro zahraniční věci a bezpečnostní politiku (dále jen „vysoký představitel“) a agenturou ENISA a v rámci jejího mandátu i se sítí EU-CyCLONe společné rizikové scénáře a metodiku pro koordinované testování připravenosti podle čl. 11 odst. 1 písm. a) bodu i) a případně pro další akce v oblasti připravenosti podle písm. a) bodu ii) uvedeného článku.

7. Pokud se subjekt působící ve vysoce kritickém odvětví dobrovolně účastní koordinovaného testování připravenosti a výsledkem tohoto testování jsou doporučení týkající se konkrétních opatření, která by zúčastněný subjekt mohl začlenit do plánu nápravy, orgán členského státu odpovědný za koordinované testování připravenosti přezkoumá, tam kde je to vhodné, následné plnění těchto opatření ze strany zúčastněných subjektů s cílem zlepšit připravenost.

Článek 13

Další akce v oblasti připravenosti

1. Mechanismus pro mimořádné události v oblasti kybernetické bezpečnosti podporuje akce v oblasti připravenosti, na něž se nevztahuje článek 12. Tyto akce zahrnují koordinované akce v oblasti připravenosti pro subjekty v odvětvích, která nejsou určena pro koordinované testování podle článku 12. Tyto akce mohou podporovat monitorování zranitelností a rizik, cvičení a školení.

2. Podpora opatření v oblasti připravenosti podle tohoto článku se členským státům poskytuje na jejich žádost, především ve formě grantů a za podmínek stanovených v příslušných pracovních programech podle článku 24 nařízení (EU) 2021/694.

Článek 14

Zřízení rezervy EU pro kybernetickou bezpečnost

1. Zřizuje se rezerva EU pro kybernetickou bezpečnost, která má uživatelům uvedeným v odstavci 3 pomáhat na jejich žádost při reakci nebo při poskytování podpory reakci na významné kybernetické bezpečnostní incidenty, rozsáhlé kybernetické bezpečnostní incidenty a incidenty obdobné rozsáhlým kybernetickým bezpečnostním incidentům a při zahajování obnovy po těchto incidentech.

2. Rezerva EU pro kybernetickou bezpečnost se skládá ze služeb určených k reakci od důvěryhodných poskytovatelů řízených bezpečnostních služeb vybraných v souladu s kritérii stanovenými v čl. 17 odst. 2. Rezerva EU pro kybernetickou bezpečnost může zahrnovat předem přislíbené služby. Předem přislíbené služby důvěryhodného poskytovatele řízených bezpečnostních služeb lze v případech, kdy tyto služby nejsou využívány k reakci na incidenty po dobu, na kterou jsou tyto služby předem přislíbeny, přeměnit na služby připravenosti související s předcházením incidentům a reakcí na ně. Rezervu EU pro kybernetickou bezpečnost lze použít na žádost ve všech členských státech, orgánech, institucích a jiných subjektech Unie a ve třetích zemích přidružených k programu Digitální Evropa uvedených v čl. 19 odst. 1.

3. Uživateli služeb poskytovaných z rezervy EU pro kybernetickou bezpečnost jsou:

a) orgány členských států pro řešení kybernetických krizí a týmy CSIRT ve smyslu čl. 9 odst. 1 a 2 a článku 10 směrnice (EU) 2022/2555;

b) CERT-EU v souladu s článkem 13 nařízení (EU, Euratom) 2023/2841;

c) příslušné orgány, jako jsou týmy pro reakce na počítačové bezpečnostní incidenty a orgány třetích zemí přidružených k programu Digitální Evropa pro řešení kybernetických krizí v souladu s čl. 19 odst. 8.

4. Celkovou odpovědnost za provádění rezervy EU pro kybernetickou bezpečnost nese Komise. Komise určí v koordinaci se skupinou NIS priority a vývoj rezervy EU pro kybernetickou bezpečnost v souladu s požadavky uživatelů uvedených v odstavci 3, dohlíží na její provádění a zajišťuje doplňkovost, jednotnost, součinnost a vazby s dalšími podpůrnými akcemi podle tohoto nařízení, jakož i s jinými opatřeními a programy Unie. Tyto priority se přezkoumávají a případně revidují každé dva roky. Komise o těchto prioritách a jejich revizi informuje Evropský parlament a Radu.

5. Aniž je dotčena celková odpovědnost Komise za provádění rezervy EU pro kybernetickou bezpečnost uvedená v odstavci 4 tohoto článku a s výhradou dohody o přiznání příspěvku ve smyslu čl. 2 bodu 19 nařízení (EU, Euratom) 2024/2509, svěří Komise zcela nebo zčásti provoz a správu rezervy EU pro kybernetickou bezpečnost agentuře ENISA. Aspekty, které nejsou svěřeny agentuře ENISA, podléhají i nadále přímému řízení ze strany Komise.

6. Agentura ENISA provádí alespoň každé dva roky mapování služeb, které uživatelé uvedení v odst. 3 písm. a) a b) tohoto článku potřebují. Mapování zahrnuje také dostupnost těchto služeb, a to i od právnických osob usazených nebo považovaných za usazené v členských státech a řízenými členskými státy nebo státními příslušníky členských států. Při mapování jejich dostupnosti posuzuje agentura ENISA dovednosti a kapacity pracovníků v oblasti kybernetické bezpečnosti v Unii, které jsou relevantní pro cíle rezervy EU pro kybernetickou bezpečnost. Při provádění mapování provádí agentura ENISA konzultace se skupinou pro spolupráci NIS, sítí EU-CyCLONe, s Komisí a případně s interinstitucionálním výborem pro kybernetickou bezpečnost zřízeným podle článku 10 nařízení (EU, Euratom) 2023/2841. Při mapování dostupnosti služeb provádí agentura ENISA konzultace rovněž s příslušnými relevantními stranami z průmyslového odvětví zaměřující se na kybernetickou bezpečnost, včetně poskytovatelů řízených bezpečnostních služeb. Poté, co informuje Radu a provede konzultace se sítí EU-CyCLONe, s Komisí a případně s vysokým představitelem, vypracuje agentura ENISA podobné mapování s cílem zjistit potřeby uživatelů uvedených v odst. 3 písm. c) tohoto článku.

7. Komisi je svěřena pravomoc přijímat akty v přenesené pravomoci v souladu s článkem 23 za účelem doplnění tohoto nařízení upřesněním druhů a počtu služeb určených k reakci požadovaných pro rezervu EU pro kybernetickou bezpečnost. Při přípravě těchto aktů v přenesené pravomoci zohlední Komise mapování uvedené v odstavci 6 tohoto článku a může si vyměňovat rady a spolupracovat se skupinou pro spolupráci NIS a s agenturou ENISA.

Článek 15

Žádosti o podporu z rezervy EU pro kybernetickou bezpečnost

1. Uživatelé uvedení v čl. 14 odst. 3 mohou požádat o služby z rezervy EU pro kybernetickou bezpečnost za účelem podpory reakce na významné kybernetické bezpečnostní incidenty, rozsáhlé kybernetické bezpečnostní incidenty nebo incidenty obdobné rozsáhlým kybernetickým bezpečnostním incidentům a za účelem zahájení obnovy po nich.

2. Aby mohli uživatelé uvedení v čl. 14 odst. 3 získat podporu z rezervy EU pro kybernetickou bezpečnost, musí přijmout veškerá vhodná opatření ke zmírnění dopadů incidentu, pro nějž je podpora požadována, včetně případného poskytnutí přímé technické pomoci a dalších prostředků na pomoc při reakci na incident a při obnově po něm.

3. Žádosti o podporu se veřejnému zadavateli předávají takto:

   a) v případě uživatelů uvedených v čl. 14 odst. 3 písm. a) tohoto nařízení prostřednictvím jednotného kontaktního místa určeného nebo zřízeného členským státem podle čl. 8 odst. 3 směrnice (EU) 2022/2555;

b) v případě uživatele uvedeného v čl. 14 odst. 3 písm. b) uvedeným uživatelem;

c) v případě uživatelů uvedených v čl. 14 odst. 3 písm. c) prostřednictvím jednotného kontaktního místa uvedeného v čl. 19 odst. 9.

4. V případě žádostí uživatelů uvedených v čl. 14 odst. 3 písm. a) informují členské státy síť CSIRT, a případně síť EU-CyCLONe, o žádostech svých uživatelů o podporu pro reakci na incidenty a počáteční obnovy podle tohoto článku.

5. V žádostech o podporu pro reakci na incident a počáteční obnovy se uvádějí:

a) příslušné informace týkající se zasaženého subjektu a možného dopadu incidentu:

i) v případě uživatelů uvedených v čl. 14 odst. 3 písm. a) na dotčené členské státy a uživatele, včetně rizika rozšíření do jiného členského státu;

ii) v případě uživatele uvedeného v čl. 14 odst. 3 písm. b) na dotčené orgány, instituce nebo jiné subjekty Unie;

iii) v případě uživatelů uvedených v čl. 14 odst. 3 písm. c) na dotčené země přidružené k programu Digitální Evropa;

b) informace o požadované službě spolu s plánovaným využitím požadované podpory, včetně odhadovaných potřeb,

c) příslušné informace o opatřeních přijatých ke zmírnění následků incidentu, pro který je podpora požadována, jak je uvedeno v odstavci 2,

d) případně dostupné informace o dalších formách podpory, které má zasažený subjekt k dispozici.

6. Agentura ENISA ve spolupráci s Komisí a sítí EU-CyCLONe vypracuje vzor, který usnadní podávání žádostí o podporu z rezervy EU pro kybernetickou bezpečnost.

7. Komise může prostřednictvím prováděcích aktů dále upřesnit podrobná procesní opatření týkající se toho, jakým způsobem je třeba o podporu z rezervy EU pro kybernetickou bezpečnost požádat a jak se na tyto žádosti reaguje podle tohoto článku, čl. 16 odst. 1 a čl. 19 odst. 10, včetně ujednání o podávání takových žádostí a poskytování odpovědí a vzorů pro zprávy uvedené v čl. 16 odst. 9. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 24 odst. 2.

Článek 16

Poskytování podpory z rezervy EU pro kybernetickou bezpečnost

1. V případě žádostí uživatelů uvedených v čl. 14 odst. 3 písm. a) a b) posuzuje žádosti o podporu z rezervy EU pro kybernetickou bezpečnost veřejný zadavatel. Aby byla zajištěna účinnost podpory, předá se odpověď uživatelům uvedeným v čl. 14 odst. 3 písm. a) a b) neprodleně a v každém případě nejpozději do 48 hodin od podání žádosti. Veřejný zadavatel informuje o výsledcích tohoto postupu Radu a Komisi.

2. Pokud jde o informace sdílené v průběhu podávání žádostí o služby v rámci rezervy EU pro kybernetickou bezpečnost a poskytování těchto služeb, všechny strany zapojené do uplatňování tohoto nařízení musí:

   a) omezit používání a sdílení těchto informací na to, co je nezbytné pro plnění jejich povinností nebo funkcí podle tohoto nařízení,

   b) používat a sdílet veškeré informace, které jsou podle unijního a vnitrostátního práva důvěrné nebo utajované, pouze v souladu s tímto právem, a

   c) zajistit účinnou, účelnou a bezpečnou výměnu informací, případně využíváním a dodržováním příslušných protokolů pro sdílení informací, včetně protokolu TLP (Traffic Light Protocol).

3. Při posuzování jednotlivých žádostí podle čl. 16 odst. 1 a čl. 19 odst. 10 veřejný zadavatel nebo případně Komise nejprve posoudí, zda jsou splněna kritéria uvedená v čl. 15 odst. 1 a 2. Je-li tomu tak, posoudí dobu trvání a povahu vhodné podpory s ohledem na cíl uvedený v čl. 1 odst. 3 písm. b) a případně na tato kritéria:

a) rozsah a závažnost incidentu,

b) druh zasaženého subjektu, přičemž vyšší prioritu mají incidenty, které mají vliv na základní subjekty podle čl. 3 odst. 1 směrnice (EU) 2022/2555;

c) potenciální dopad incidentu na zasažené členské státy, orgány, instituce nebo jiné subjekty Unie nebo třetí země přidružené k programu Digitální Evropa;

d) potenciální přeshraniční povahu incidentu a riziko rozšíření do jiných členských států, orgánů, institucí nebo jiných subjektů Unie nebo do třetích zemí přidružených k programu Digitální Evropa;

e) opatření přijatá uživatelem na pomoc při reakci a počáteční obnově podle čl. 15 odst. 2.

4. Za účelem stanovení priority žádostí v případě souběžných žádostí uživatelů uvedených v čl. 14 odst. 3 se případně zohlední kritéria uvedená v odstavci 3 tohoto článku, aniž je dotčena zásada loajální spolupráce mezi členskými státy a orgány, institucemi a jinými subjekty Unie. Pokud jsou podle kritérií posouzeny dvě nebo více žádostí jako rovnocenné, mají vyšší prioritu žádosti uživatelů z členských států. Pokud je provoz a správa rezervy EU pro kybernetickou bezpečnost svěřena podle čl. 14 odst. 5 zcela nebo zčásti agentuře ENISA, úzce spolupracuje na stanovení priority žádostí v souladu s tímto odstavcem s Komisí.

5. Služby v rámci rezervy EU pro kybernetickou bezpečnost se poskytují v souladu se zvláštními dohodami mezi důvěryhodným poskytovatelem řízených bezpečnostních služeb a uživatelem, kterému je poskytnuta podpora z rezervy EU pro kybernetickou bezpečnost. Tyto služby mohou být poskytovány v souladu se zvláštními dohodami mezi důvěryhodným poskytovatelem řízených bezpečnostních služeb, uživatelem a zasaženým subjektem. Všechny dohody uvedené v tomto odstavci musí obsahovat mimo jiné podmínky odpovědnosti.

6. Dohody uvedené v odstavci 5 vycházejí ze vzorů, které vypracuje agentura ENISA po konzultaci s členskými státy a případně dalšími uživateli rezervy EU pro kybernetickou bezpečnost.

7. Komise, agentura ENISA a uživatelé rezervy EU pro kybernetickou bezpečnost nenesou žádnou smluvní odpovědnost za škody způsobené třetím osobám službami poskytovanými v rámci provádění rezervy EU pro kybernetickou bezpečnost.

8. Uživatelé mohou využívat služby rezervy EU pro kybernetickou bezpečnost poskytnuté v reakci na žádost podle čl. 15 odst. 1 pouze za účelem podpory reakce na významné kybernetické bezpečnostní incidenty, rozsáhlé kybernetické bezpečnostní incidenty nebo incidenty obdobné rozsáhlým kybernetickým bezpečnostním incidentům a za účelem zahájení obnovy po nich. Uživatelé mohou tyto služby využívat pouze s ohledem na:

   a) subjekty působící ve vysoce kritických odvětvích nebo subjekty působící v dalších kritických odvětvích v případě uživatelů uvedených v čl. 14 odst. 3 písm. a) a na rovnocenné subjekty v případě uživatelů uvedených v čl. 14 odst. 3 písm. c) a

   b) orgány, instituce a jiné subjekty Unie v případě uživatele uvedeného v čl. 14 odst. 3 písm. b).

9. Do dvou měsíců od ukončení podpory předloží uživatelé, kteří obdrželi podporu, souhrnnou zprávu o poskytnuté službě, dosažených výsledcích a vyvozených poučení, a to takto:

   a) uživatelé uvedení v čl. 14 odst. 3 písm. a) předloží souhrnnou zprávu Komisi, agentuře ENISA, síti CSIRT a síti EU-CyCLONe,

   b) uživatel uvedený v čl. 14 odst. 3 písm. b) předloží souhrnnou zprávu Komisi, agentuře ENISA a interinstitucionálnímu výboru pro kybernetickou bezpečnost,

c) uživatelé uvedení v čl. 14 odst. 3 písm. c) předloží tuto zprávu Komisi.

Komise předá souhrnnou zprávu, již obdržela od uživatelů uvedených v čl. 14 odst. 3 podle prvního pododstavce písm. c) tohoto odstavce Radě a vysokému představiteli.

10. Pokud je provoz a správa rezervy EU pro kybernetickou bezpečnost svěřena podle čl. 14 odst. 5 tohoto nařízení zcela nebo zčásti agentuře ENISA, podává tato agentura v tomto ohledu pravidelně zprávy Komisi a konzultuje s ní. V této souvislosti agentura ENISA neprodleně zašle Komisi veškeré žádosti, které obdrží od uživatelů uvedených v čl. 14 odst. 3 písm. c) tohoto nařízení, a je-li to nezbytné pro účely stanovení priority podle tohoto článku, veškeré žádosti, které obdržela od uživatelů uvedených v čl. 14 odst. 3 písm. a) nebo b) tohoto nařízení. Povinnostmi uvedenými v tomto odstavci není dotčen článek 14 nařízení (EU) 2019/881.

11. V případě uživatelů uvedených v čl. 14 odst. 3 písm. a) a b) podává veřejný zadavatel skupině pro spolupráci NIS pravidelně, nejméně však dvakrát ročně zprávy o využívání podpory a jejích výsledcích.

12. V případě uživatelů uvedených v čl. 14 odst. 3 písm. c) podává Komise Radě a vysokému představiteli pravidelně, nejméně však dvakrát ročně zprávy o využívání podpory a jejích výsledcích.

Článek 17

Důvěryhodní poskytovatelé řízených bezpečnostních služeb

1. Při zadávacích řízeních za účelem zřízení rezervy EU pro kybernetickou bezpečnost postupuje veřejný zadavatel v souladu se zásadami stanovenými v nařízení (EU, Euratom) 2024/2509 a v souladu s těmito zásadami:

   a) zajistit, aby služby zahrnuté do rezervy EU pro kybernetickou bezpečnost byly jako celek takové, aby rezerva EU pro kybernetickou bezpečnost zahrnovala služby, které mohou být využívány ve všech členských státech, zejména s ohledem na vnitrostátní požadavky na poskytování takových služeb, včetně požadavků na jazyky, certifikaci nebo akreditaci,

   b) zajistit ochranu základních bezpečnostních zájmů Unie a jejích členských států,

   c) zajistit, aby rezerva EU pro kybernetickou bezpečnost přinášela Unii přidanou hodnotu tím, že přispěje k dosažení cílů stanovených v článku 3 nařízení (EU) 2021/694, včetně podpory rozvoje dovedností v oblasti kybernetické bezpečnosti v Unii.

2. Při zadávání zakázek na služby pro rezervu EU pro kybernetickou bezpečnost uvede veřejný zadavatel v zadávací dokumentaci tato kritéria a požadavky:

a) poskytovatel prokáže, že jeho zaměstnanci mají nejvyšší stupeň profesní bezúhonnosti, nezávislosti, zodpovědnosti a požadované technické způsobilosti k výkonu činnosti v jejich konkrétním oboru a zajistí trvalost a kontinuitu odborných znalostí i potřebných technických zdrojů;

b) poskytovatel a veškeré příslušné dceřiné společnosti a subdodavatelé dodržují příslušná pravidla na ochranu utajovaných informací a mají zavedena vhodná opatření, včetně případných vzájemných dohod, na ochranu důvěrných informací týkajících se služby, a zejména důkazů, zjištění a zpráv;

c) poskytovatel předloží dostatečný důkaz o tom, že jeho řídicí struktura je transparentní a neohrozí jeho nestrannost a kvalitu jeho služeb ani nezpůsobí střet zájmů;

d) poskytovatel má odpovídající bezpečnostní prověrku, alespoň v případě pracovníků určených k nasazení v rámci dané služby, pokud to vyžaduje členský stát;

e) poskytovatel má odpovídající úroveň zabezpečení svých IT systémů;

f) poskytovatel je vybaven hardwarem a softwarem nezbytným pro podporu požadované služby, které neobsahují známé zneužitelné zranitelnosti, zahrnují nejnovější bezpečnostní aktualizace a v každém případě splňují veškerá použitelná ustanovení nařízení Evropského parlamentu a Rady (EU) 2024/…[23+];

g) poskytovatel je schopen prokázat, že má zkušenosti s poskytováním podobných služeb příslušným vnitrostátním orgánům, subjektům působícím ve vysoce kritických odvětvích nebo subjektům působícím v dalších kritických odvětvích;

h) poskytovatel je schopen poskytnout službu v krátkém časovém rámci v členských státech, v nichž může službu poskytovat;

i) poskytovatel je schopen poskytnout službu v jednom nebo ve více úředních jazycích orgánů Unie nebo v jazyce členského státu, pokud to členské státy, v nichž může poskytovatel službu poskytovat, nebo uživatelé uvedení v čl. 14 odst. 3 písm. b) a c) vyžadují;

j) jakmile budou zavedena evropská schémata certifikace kybernetické bezpečnosti pro řízené bezpečnostní služby podle nařízení (EU) 2019/881, bude poskytovatel certifikován v souladu s těmito schématy do dvou let ode dne začátku uplatňování těchto schémat;

---

[23] Nařízení Evropského parlamentu a Rady (EU) 2024/... ze dne... o ... (Úř. věst. L, …, ELI: …).

[+] Pro Úř. věst.: vložte prosím do textu číslo nařízení obsaženého v dokumentu PE-CONS 100/23 (2022/0272(COD)) a do poznámky pod čarou číslo, datum, odkaz na vyhlášení uvedeného nařízení v Úředním věstníku a odkaz ELI.

k) poskytovatel musí do nabídky zahrnout pro jakékoliv nevyužité služby určené k reakci na incidenty, které by mohly být přeměněny na služby připravenosti úzce související s reakcí na incidenty, jako jsou cvičení nebo školení, podmínky takové přeměny.

3. Pro účely zadávání zakázek na služby pro rezervu EU pro kybernetickou bezpečnost může veřejný zadavatel v úzké spolupráci s členskými státy případně vypracovat kritéria a požadavky nad rámec kritérií uvedených v odstavci 2.

Článek 18

Akce na podporu vzájemné pomoci

1. Mechanismus pro mimořádné události v oblasti kybernetické bezpečnosti podporuje technickou pomoc poskytovanou jedním členským státem jinému členskému státu, který je zasažen významným kybernetickým bezpečnostním incidentem nebo rozsáhlým kybernetickým bezpečnostním incidentem, a to i v případech uvedených v čl. 11 odst. 3 písm. f) směrnice (EU) 2022/2555.

2. Podpora vzájemné technické pomoci uvedená v odstavci 1 tohoto článku se poskytuje ve formě grantů za podmínek stanovených v příslušných pracovních programech uvedených v článku 24 nařízení (EU) 2021/694.

Článek 19

Podpora pro třetí země přidružené k programu Digitální Evropa

1. Třetí země přidružená k programu Digitální Evropa může požádat o podporu z rezervy EU pro kybernetickou bezpečnost, pokud je v dohodě, jejímž prostřednictvím je k programu Digitální Evropa přidružena, stanovena účast v této rezervě. Tato dohoda obsahuje ustanovení, která vyžadují, aby dotčená třetí země přidružená k programu Digitální Evropa plnila povinnosti stanovené v odstavcích 2 a 9 tohoto článku. Pro účely účasti třetí země v rezervě EU pro kybernetickou bezpečnost může částečné přidružení třetí země k programu Digitální Evropa zahrnovat přidružení, jež se omezuje na operační cíl uvedený v čl. 6 odst. 1 písm. g) nařízení (EU) 2021/694.

2. Do tří měsíců od uzavření dohody uvedené v odstavci 1 a v každém případě před získáním jakékoli podpory z rezervy EU pro kybernetickou bezpečnost poskytne třetí země přidružená k programu Digitální Evropa Komisi informace o svých schopnostech v oblasti kybernetické odolnosti a řízení rizik, alespoň včetně informací o vnitrostátních opatřeních přijatých za účelem přípravy na významné kybernetické bezpečnostní incidenty nebo incidenty obdobné rozsáhlým kybernetickým bezpečnostním incidentům, jakož i informací o odpovědných vnitrostátních subjektech, včetně týmů pro reakce na počítačové bezpečnostní incidenty nebo obdobných subjektů, jejich schopnostech a zdrojích, které jim byly přiděleny. Třetí země přidružená k programu Digitální Evropa tyto informace pravidelně, nejméně však jednou ročně aktualizuje. K usnadnění uplatňování odstavce 11 poskytne Komise tyto informace vysokému představiteli a agentuře ENISA.

3. Komise pravidelně, nejméně však jednou ročně posuzuje v případě každé třetí země přidružené k programu Digitální Evropa uvedené v odstavci 1 tato kritéria:

a) zda tato země dodržuje podmínky dohody uvedené v odstavci 1, pokud se týkají účasti v rezervě EU pro kybernetickou bezpečnost,

b) zda tato země přijala odpovídající kroky k přípravě na významné kybernetické bezpečnostní incidenty nebo incidenty obdobné rozsáhlým kybernetickým bezpečnostním incidentům na základě informací uvedených v odstavci 2 a

c) zda je poskytování podpory v souladu s politikou Unie vůči této zemi a s celkovými vztahy Unie s touto zemí a zda je v souladu s ostatními politickými opatřeními Unie v oblasti bezpečnosti.

Komise při provádění posouzení podle prvního pododstavce konzultuje plnění kritéria uvedeného v písmenu c) uvedeného pododstavce s vysokým představitelem.

Pokud Komise dospěje k závěru, že třetí země přidružená k programu Digitální Evropa splňuje všechny podmínky uvedené v prvním pododstavci, předloží Radě návrh na přijetí prováděcího aktu v souladu s odstavcem 4, kterým se povolí poskytnutí podpory z rezervy EU pro kybernetickou bezpečnost této zemi.

4. Rada může přijmout prováděcí akty uvedené v odstavci 3. Tyto prováděcí akty se použijí nejvýše po dobu jednoho roku. Jejich platnost lze prodloužit. Mohou obsahovat limit stanovující počet dnů, po které je možné podporu na základě jediné žádosti poskytovat, přičemž tento limit nesmí být kratší než 75 dnů.

Pro účely tohoto článku Rada jedná urychleně a zpravidla přijme prováděcí akty uvedené v tomto odstavci do osmi týdnů od přijetí příslušného návrhu Komise podle odstavce 3 třetího pododstavce.

5. Na návrh Komise může Rada prováděcí akt přijatý podle odstavce 4 kdykoli změnit nebo zrušit.

Pokud se Rada domnívá, že došlo k významné změně ve věci kritéria uvedeného v odst. 3 prvním pododstavci písm. c), může na základě řádně odůvodněného podnětu jednoho nebo více členských států prováděcí akt uvedený v odstavci 4 změnit nebo zrušit.

6. Při výkonu svých prováděcích pravomocí podle tohoto článku použije Rada kritéria uvedená v odstavci 3 prvním pododstavci a vysvětlí své posouzení uvedených kritérií. Pokud Rada jedná z vlastního podnětu podle odst. 5 druhého pododstavce, vysvětlí zejména významnou změnu uvedenou v uvedeném pododstavci.

7. Podpora třetí země přidružené k programu Digitální Evropa z rezervy EU pro kybernetickou bezpečnost musí splňovat veškeré zvláštní podmínky stanovené v dohodě uvedené v odstavci 1.

8. K uživatelům z třetích zemí přidružených k programu Digitální Evropa, kteří jsou způsobilí získat služby z rezervy EU pro kybernetickou bezpečnost, patří příslušné orgány, jako jsou týmy pro reakce na počítačové bezpečnostní incidenty nebo obdobné subjekty a orgány pro řešení kybernetických krizí.

9. Každá třetí země přidružená k programu Digitální Evropa, která je způsobilá k podpoře z rezervy EU pro kybernetickou bezpečnost, určí orgán, který bude pro účely tohoto nařízení působit jako jednotné kontaktní místo.

10. Žádosti o podporu z rezervy EU pro kybernetickou bezpečnost podle tohoto článku posuzuje Komise. Veřejný zadavatel může poskytnout podporu třetí zemi pouze tehdy, pokud a dokud je v platnosti prováděcí akt Rady přijatý podle odstavce 4 tohoto článku, který takovou podporu ve vztahu k této zemi povoluje. Odpověď se předá uživatelům uvedeným v čl. 14 odst. 3 písm. c) bez zbytečného odkladu.

11. Po obdržení žádosti o podporu podle tohoto článku o tom Komise neprodleně informuje Radu. Komise Radu průběžně informuje o posuzování žádosti. Komise na obdržených žádostech a na poskytování podpory z rezervy EU pro kybernetickou bezpečnost třetím zemím přidruženým k programu Digitální Evropa spolupracuje rovněž s vysokým představitelem. Dále Komise zohlední také veškerá stanoviska, která k těmto žádostem poskytla agentura ENISA.

Článek 20

Koordinace s mechanismy Unie pro řešení krizí

1. Pokud významný kybernetický bezpečnostní incident, rozsáhlý kybernetický bezpečnostní incident nebo incident obdobný rozsáhlému kybernetickému bezpečnostnímu incidentu vznikl v důsledku katastrofy ve smyslu čl. 4 bodu 1 rozhodnutí č. 1313/2013/EU nebo má za následek katastrofu v tomto smyslu, doplňuje podpora pro reakci na tento incident poskytovaná podle tohoto nařízení akce podle uvedeného rozhodnutí a není jím dotčena.

2. V případě rozsáhlého kybernetického bezpečnostního incidentu nebo incidentu obdobného rozsáhlému kybernetickému bezpečnostnímu incidentu, kdy jsou aktivována opatření pro integrovanou politickou reakci EU na krize podle prováděcího rozhodnutí (EU) 2018/1993 (dále jen „opatření IPCR“), se podpora pro reakci na tento incident poskytovaná podle tohoto nařízení řídí příslušnými postupy v souladu s opatřeními IPCR.

Kapitola IV
Evropský mechanismus přezkumu kybernetických bezpečnostních incidentů

Článek 21

Evropský mechanismus přezkumu kybernetických bezpečnostních incidentů

1. Na žádost Komise nebo sítě EU-CyCLONe agentura ENISA s podporou sítě CSIRT a se souhlasem dotčených členských států přezkoumá a posoudí kybernetické hrozby, známé zneužitelné zranitelnosti a opatření ke zmírnění dopadů v souvislosti s konkrétním významným kybernetickým bezpečnostním incidentem nebo rozsáhlým kybernetickým bezpečnostním incidentem. Po dokončení přezkumu a posouzení incidentu předá agentura ENISA síti EU-CyCLONe, síti CSIRT, dotčeným členským státům a Komisi zprávu o přezkumu incidentu s cílem vyvodit poučení, a zabránit tak budoucím incidentům nebo je zmírnit, aby je podpořila při plnění jejich úkolů, zejména s ohledem na úkoly stanovené v článcích 15 a 16 směrnice (EU) 2022/2555. Má-li incident dopad na třetí zemi přidruženou k programu Digitální Evropa, poskytne agentura ENISA tuto zprávu Radě. V takových případech Komise poskytne dotčenou zprávu vysokému představiteli.

2. Při přípravě zprávy o přezkumu incidentu podle odstavce 1 tohoto článku spolupracuje agentura ENISA se všemi příslušnými zúčastněnými stranami, včetně zástupců členských států, Komise, dalších příslušných orgánů, institucí a jiných subjektů Unie, průmyslu, *včetně* poskytovatelů řízených bezpečnostních služeb a uživatelů služeb kybernetické bezpečnosti, a získává od nich zpětnou vazbu. Ve vhodných případech agentura ENISA ve spolupráci s týmy CSIRT a případně s příslušnými orgány určenými nebo zřízenými podle čl. 8 odst. 1 směrnice (EU) 2022/2555 spolupracuje také se subjekty zasaženými významnými kybernetickými bezpečnostními incidenty nebo rozsáhlými kybernetickými bezpečnostními incidenty. Konzultovaní zástupci oznámí jakýkoli případný střet zájmů.

3. Zpráva o přezkumu incidentu podle odstavce 1 tohoto článku zahrnuje přezkum a analýzu konkrétního významného kybernetického bezpečnostního incidentu nebo rozsáhlého kybernetického bezpečnostního incidentu, včetně hlavních příčin, známých zneužitelných zranitelností a vyvozených poučení. Agentura ENISA zajistí, aby byla zpráva v souladu s právem Unie nebo vnitrostátním právem týkajícím se ochrany citlivých či utajovaných informací. Pokud o to příslušné členské státy nebo jiní uživatelé uvedení v čl. 14 odst. 3, jež byli zasaženi incidentem, požádají, údaje a informace obsažené ve zprávě se anonymizují. Nesmí obsahovat žádné podrobnosti o aktivně zneužívaných zranitelnostech, které zůstávají neopravené.

4. Dle potřeby se ve zprávě o přezkumu incidentu uvedou doporučení ke zlepšení pozice Unie v oblasti kybernetické bezpečnosti a mohou v ní být uvedeny osvědčené postupy a poučení získané od příslušných zúčastněných stran.

5. Agentura ENISA může vydat veřejně přístupnou verzi zprávy o přezkumu incidentu. Tato verze zprávy obsahuje výhradně spolehlivé veřejné informace, nebo i další spolehlivé informace, pokud s tím souhlasily dotčené členské státy, a pokud jde o informace týkající se uživatele podle čl. 14 odst. 3 písm. b) nebo c), pokud s tím souhlasil tento uživatel.

Kapitola V
Závěrečná ustanovení

Článek 22

Změny nařízení (EU) 2021/694

Nařízení (EU) 2021/694 se mění takto:

1) Článek 6 se mění takto:

a) odstavec 1 se mění takto:

i) vkládá se nové písmeno, které zní:

„aa) podporovat rozvoj Evropského systému varování v oblasti kybernetické bezpečnosti, zřízeného článkem 3 nařízení Evropského parlamentu a Rady (EU) …/…[*+] (dále jen „Evropský systém varování v oblasti kybernetické bezpečnosti“), včetně vývoje, zavádění a provozu národních kybernetických center a přeshraničních kybernetických center, která přispívají k povědomí o situaci v Unii a k posílení kapacit Unie v oblasti získávání poznatků o kybernetických hrozbách (tzv. cyber threat intelligence);

---

[*] Nařízení Evropského parlamentu a Rady (EU) …/... ze dne ..., kterým se stanovují opatření k posílení solidarity a kapacit v Unii pro odhalování kybernetických hrozeb a incidentů a pro připravenost a reakci na ně a mění nařízení (EU) 2021/694 (nařízení o kybernetické solidaritě) (Úř. věst. L ..., ELI: ...).“

[+] Pro Úř. věst.: vložte prosím do textu číslo nařízení obsaženého v dokumentu PE-CONS 94/24 (2023/0109(COD)) a do poznámky pod čarou číslo, datum, odkaz na vyhlášení uvedeného nařízení v Úředním věstníku a odkaz ELI.

ii) doplňuje se nové písmeno, které zní:

„g) zřídit a provozovat mechanismus pro mimořádné události v oblasti kybernetické bezpečnosti, zřízený článkem 10 nařízení Evropského parlamentu a Rady (EU) …/…[+], včetně rezervy EU pro kybernetickou bezpečnost, zřízené článkem 14 uvedeného nařízení (dále jen „rezerva EU pro kybernetickou bezpečnost“), na podporu členských států při přípravě na významné kybernetické bezpečnostní incidenty a rozsáhlé kybernetické bezpečnostní incidenty a při reakci na ně, který doplní vnitrostátní zdroje a schopnosti a další formy podpory dostupné na úrovni Unie, a na podporu dalších uživatelů při reakci na významné kybernetické bezpečnostní incidenty a incidenty obdobné rozsáhlým kybernetickým bezpečnostním incidentům;“

b) odstavec 2 se nahrazuje tímto:

„2. Akce v rámci specifického cíle č. 3 jsou prováděny především prostřednictvím Evropského průmyslového, technologického a výzkumného centra kompetencí pro kybernetickou bezpečnost a sítě národních koordinačních center v souladu s nařízením Evropského parlamentu a Rady (EU) 2021/887[*]. Rezervu EU pro kybernetickou bezpečnost však provádí Komise a v souladu s čl. 14 odst. 6 nařízení (EU) …/…[+] agentura ENISA.

---

[*] Nařízení Evropského parlamentu a Rady (EU) 2021/887 ze dne 20. května 2021, kterým se zřizuje Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost a síť národních koordinačních center (Úř. věst. L 202, 8.6.2021, s. 1).“

[+] Pro Úř. věst.: vložte prosím do textu číslo nařízení obsaženého v dokumentu PE-CONS 94/24 (2023/0109(COD)).

2) Článek 9 se mění takto:

a) v odstavci 2 se písmena b), c) a d) nahrazují tímto:

„b) 1 760 806 000 EUR pro specifický cíl č. 2 Umělá inteligence,

c) 1 372 020 000 EUR pro specifický cíl č. 3 Kybernetická bezpečnost a důvěra,

d) 482 640 000 EUR pro specifický cíl č. 4 Pokročilé digitální dovednosti,“;

b) doplňuje se nový odstavec, který zní:

„8. Odchylně od čl. 12 odst. 1 finančního nařízení se nevyužité prostředky na závazky a platby na akce související s prováděním rezervy EU pro kybernetickou bezpečnost a na akce na podporu vzájemné pomoci podle nařízení (EU) …/…[+], která sledují cíle stanovené v čl. 6 odst. 1 písm. g) tohoto nařízení, automaticky přenášejí a mohou být přiděleny a vyplaceny do 31. prosince následujícího rozpočtového roku. O prostředcích přenesených podle čl. 12 odst. 6 finančního nařízení jsou informovány Evropský parlament a Rada.“

[+] Pro Úř. věst.: vložte prosím do textu číslo nařízení obsaženého v dokumentu PE-CONS 94/24 (2023/0109(COD)).

3) Článek 12 se mění takto:

a) vkládají se nové odstavce, které znějí:

„5a. Jedná-li se o právní subjekty usazené v Unii, ale řízené ze třetích zemí, nepoužije se odstavec 5 na žádné opatření zavádějící Evropský systém varování v oblasti kybernetické bezpečnosti, pokud jsou v souvislosti s dotčeným opatřením splněny obě tyto podmínky:

a) s přihlédnutím k výsledkům mapování provedeného podle čl. 9 odst. 4 nařízení (EU) .../...[+] existuje skutečné riziko, že od právních subjektů usazených nebo považovaných za usazené v členských státech a řízených členskými státy nebo státními příslušníky členských států nebudou k dispozici nástroje, infrastruktura nebo služby nezbytné a postačující k tomu, aby toto opatření odpovídajícím způsobem přispělo k cíli Evropského systému varování v oblasti kybernetické bezpečnosti;

b) bezpečnostní riziko zadávání zakázek v rámci Evropského systému varování v oblasti kybernetické bezpečnosti těmto právním subjektům je úměrné přínosům a nepodkopává základní bezpečnostní zájmy Unie a jejích členských států.

[+] Pro Úř. věst.: vložte prosím do textu číslo nařízení obsaženého v dokumentu PE-CONS 94/24 (2023/0109(COD)).

5b. Jedná-li se o právní subjekty usazené v Unii, ale řízené ze třetích zemí, nepoužije se odstavec 5 na žádné opatření provádějící rezervu EU pro kybernetickou bezpečnost, pokud jsou v souvislosti s dotčeným opatřením splněny obě tyto podmínky:

a) s přihlédnutím k výsledkům mapování provedeného podle čl. 14 odst. 6 nařízení (EU)…/…[+] existuje skutečné riziko, že od právních subjektů usazených nebo považovaných za usazené v členských státech a řízených členskými státy nebo státními příslušníky členských států nebudou k dispozici technologie, odborné znalosti nebo kapacita nezbytné a postačující k tomu, aby rezerva EU pro kybernetickou bezpečnost odpovídajícím způsobem plnila své funkce;

b) bezpečnostní riziko začlenění těchto právních subjektů do rezervy EU pro kybernetickou bezpečnost je úměrné přínosům a nepodkopává základní bezpečnostní zájmy Unie a jejích členských států.“;

[+] Pro Úř. věst.: vložte prosím do textu číslo nařízení obsaženého v dokumentu PE-CONS 94/24 (2023/0109(COD)).

b) odstavec 6 se nahrazuje tímto:

„6. Pracovní program může rovněž stanovit, že právní subjekty usazené v přidružených zemích a právní subjekty usazené v Unii, ale řízené ze třetích zemí mohou být z řádně odůvodněných bezpečnostních důvodů způsobilé k účasti na všech nebo některých akcích v rámci specifických cílů č. 1 a 2 pouze tehdy, pokud splňují požadavky, které jsou na tyto právní subjekty kladeny s cílem zaručit ochranu základních bezpečnostních zájmů Unie a členských států a zajistit ochranu utajovaných informací. Uvedené požadavky musí být stanoveny v pracovním programu.

Jedná-li se o právní subjekty usazené v Unii, ale řízené ze třetích zemí, použije se první pododstavec rovněž na akce v rámci specifického cíle č. 3:

a) za účelem zavedení Evropského systému varování v oblasti kybernetické bezpečnosti, pokud se použije odst. 5a, a

b) za účelem provádění rezervy EU pro kybernetickou bezpečnost, pokud se použije odst. 5b.“

4) V článku 14 se odstavec 2 nahrazuje tímto:

„2. Program může poskytovat financování kteroukoli z forem stanovených ve finančním nařízení, včetně zejména zadávání veřejných zakázek jako základní formy, jakož i grantů a cen.

Pokud dosažení cíle akce vyžaduje zadávání zakázek na inovační zboží a služby, mohou být granty uděleny pouze příjemcům, kteří jsou veřejnými zadavateli nebo zadavateli, jak jsou vymezeni ve směrnicích Evropského parlamentu a Rady 2014/24/EU* a 2014/25/EU**.

Pokud je pro dosažení cílů akce nezbytné dodání inovačního zboží nebo služeb, které dosud nejsou ve velkém rozsahu dostupné na trhu, veřejní zadavatelé a zadavatelé mohou schválit zadání několika zakázek v rámci jednoho zadávacího řízení.

V řádně odůvodněných případech týkajících se veřejné bezpečnosti může veřejný zadavatel nebo zadavatel vyžadovat, aby se místo plnění smlouvy nacházelo na území Unie.

Při provádění zadávacích řízení na rezervu EU pro kybernetickou bezpečnost mohou Komise a agentura ENISA jednat jako centrální zadavatel a zadávat zakázky v zastoupení nebo jménem třetích zemí přidružených k programu v souladu s článkem 10 tohoto nařízení. Komise a agentura ENISA mohou rovněž působit jako velkoobchodníci a nakupovat, skladovat a dále prodávat nebo darovat dodávky a služby těmto třetím zemím, včetně pronájmu. Odchylně od čl. 168 odst. 3 nařízení Evropského parlamentu a Rady (EU, Euratom)2024/2509*** postačuje k pověření Komise nebo agentury ENISA jednáním žádost jediné třetí země.

Při provádění zadávacích řízení na rezervu EU pro kybernetickou bezpečnost mohou Komise a agentura ENISA jednat jako centrální zadavatel a zadávat zakázky v zastoupení nebo jménem orgánů, institucí nebo jiných subjektů Unie. Komise a agentura ENISA mohou rovněž působit jako velkoobchodníci a nakupovat, skladovat, dále prodávat nebo darovat dodávky a služby orgánům, institucím nebo jiným subjektům Unie, včetně pronájmu. Odchylně od čl. 168 odst. 3 nařízení (EU, Euratom) 2024/2059 postačuje k pověření Komise nebo agentury ENISA jednáním žádost jediného orgánu, instituce nebo jiného subjektu Unie.

Program může také poskytovat financování formou finančních nástrojů v rámci operací kombinování zdrojů.

---

* Směrnice Evropského parlamentu a Rady 2014/24/EU ze dne 26. února 2014 o zadávání veřejných zakázek a o zrušení směrnice 2004/18/ES (Úř. věst. L 94, 28.3.2014, s. 65).

** Směrnice Evropského parlamentu a Rady 2014/25/EU ze dne 26. února 2014 o zadávání zakázek subjekty působícími v odvětví vodního hospodářství, energetiky, dopravy a poštovních služeb a o zrušení směrnice 2004/17/ES (Úř. věst. L 94, 28.3.2014, s. 243).

*** Nařízení Evropského parlamentu a Rady 2024/2509 (EU, Euratom) 2024/2509 ze dne 23. září 2024, kterým se stanoví finanční pravidla pro souhrnný rozpočet Unie (přepracované znění) (Úř. věst. L, 2024/2509, 26.9.2024, ELI: http://data.europa.eu/eli/reg/2024/2509/oj).“

5) Vkládá se nový článek, který zní:

„*Článek 16a*

Rozpory mezi pravidly

V případě akcí, kterými se zavádí Evropský systém varování v oblasti kybernetické bezpečnosti, se použijí pravidla stanovená v článcích 4, 5 a 9 nařízení (EU) .../...+.

V případě rozporu mezi ustanoveními tohoto nařízení a články 4, 5 a 9 nařízení (EU) .../...+ jsou pro tyto konkrétní akce rozhodné články 4 a 5 uvedeného nařízení, které se použijí.

+ Pro Úř. věst.: vložte prosím do textu číslo nařízení obsaženého v dokumentu PE-CONS 94/24 (2023/0109(COD)).

V případě rezervy EU pro kybernetickou bezpečnost jsou zvláštní pravidla pro účast třetích zemí přidružených k programu stanovena v článku 19 nařízení (EU) .../...[+]. V případě rozporu mezi ustanoveními tohoto nařízení a článkem 19 nařízení (EU) .../... + se na tyto konkrétní akce použije článek 19 uvedeného nařízení.“

6) Článek 19 se nahrazuje tímto:

„*Článek 19*
Granty

Granty v rámci programu se udělují a spravují v souladu s hlavou VIII finančního nařízení a mohou pokrývat až 100 % způsobilých nákladů, aniž je dotčena zásada spolufinancování stanovená v článku 190 finančního nařízení. Tyto granty se udělují a spravují, jak je stanoveno pro každý specifický cíl.

Podporu v podobě grantů může v souladu s čl. 195 odst. 1 písm. d) finančního nařízení udělovat členským státům vybraným podle článku 9 nařízení (EU) .../...[+] a hostitelskému konsorciu uvedenému v článku 5 nařízení (EU) .../...[+] přímo centrum ECCC bez výzvy k podávání návrhů.

Podporu v podobě grantů pro mechanismus pro mimořádné události v oblasti kybernetické bezpečnosti může v souladu s čl. 195 odst. 1 písm. d) finančního nařízení udělovat členským státům přímo centrum ECCC bez výzvy k podávání návrhů.

[+] Pro Úř. věst.: vložte prosím do textu číslo nařízení obsaženého v dokumentu PE-CONS 94/24 (2023/0109(COD)).

U akcí na podporu vzájemné pomoci uvedených v článku 18 nařízení (EU) .../...[+] informuje centrum ECCC Komisi a agenturu ENISA o žádostech členských států o přímé granty bez výzvy k podávání návrhů.

U akcí na podporu vzájemné pomoci uvedené v článku 18 nařízení (EU) .../...[+] a v souladu s čl. 193 odst. 2 druhým pododstavcem písm. a) finančního nařízení lze v řádně odůvodněných případech považovat náklady za způsobilé i tehdy, pokud vznikly před podáním žádosti o grant.“

7) Přílohy I a II se mění v souladu s přílohou tohoto nařízení.

Článek 23

Výkon přenesené pravomoci

1. Pravomoc přijímat akty v přenesené pravomoci je svěřena Komisi za podmínek stanovených v tomto článku.

2. Pravomoc přijímat akty v přenesené pravomoci uvedená v čl. 12 odst. 8 je svěřena Komisi na dobu pěti let od ... [den vstupu tohoto nařízení v platnost]. Komise vypracuje zprávu o přenesené pravomoci nejpozději devět měsíců před koncem tohoto pětiletého období. Přenesení pravomoci se automaticky prodlužuje o stejně dlouhá období, pokud Evropský parlament ani Rada nevysloví proti tomuto prodloužení námitku nejpozději tři měsíce před koncem každého z těchto období.

[+] Pro Úř. věst.: vložte prosím do textu číslo nařízení obsaženého v dokumentu PE-CONS 94/24 (2023/0109(COD)).

3. Evropský parlament nebo Rada mohou přenesení pravomoci uvedené v čl. 14 odst. 7 kdykoli zrušit. Rozhodnutím o zrušení se ukončuje přenesení pravomoci v něm určené. Rozhodnutí nabývá účinku prvním dnem po zveřejnění v *Úředním věstníku Evropské unie* nebo k pozdějšímu dni, který je v něm upřesněn. Nedotýká se platnosti již platných aktů v přenesené pravomoci.

4. Před přijetím aktu v přenesené pravomoci Komise vede konzultace s odborníky jmenovanými jednotlivými členskými státy v souladu se zásadami stanovenými v interinstitucionální dohodě ze dne 13. dubna 2016 o zdokonalení tvorby právních předpisů.

5. Přijetí aktu v přenesené pravomoci Komise neprodleně oznámí současně Evropskému parlamentu a Radě.

6. Akt v přenesené pravomoci přijatý podle čl. 14 odst. 7 vstoupí v platnost pouze tehdy, pokud proti němu Evropský parlament ani Rada nevysloví námitky ve lhůtě dvou měsíců ode dne, kdy jim byl tento akt oznámen, nebo pokud Evropský parlament i Rada před uplynutím této lhůty informují Komisi o tom, že námitku nevysloví. Z podnětu Evropského parlamentu nebo Rady se tato lhůta prodlouží o dva měsíce.

Článek 24

Postup projednávání ve výborech

1. Komisi je nápomocen koordinační výbor programu Digitální Evropa uvedený v čl. 31 odst. 1 nařízení (EU) 2021/694. Tento výbor je výborem ve smyslu nařízení (EU) č. 182/2011.

2. Odkazuje-li se na tento odstavec, použije se článek 5 nařízení (EU) č. 182/2011.

Článek 25

Hodnocení a přezkum

1. Do ... [dva roky ode dne vstupu tohoto nařízení v platnost] a poté alespoň každé čtyři roky provede Komise hodnocení fungování opatření stanovených v tomto nařízení a předloží zprávu Evropskému parlamentu a Radě.

2. V rámci hodnocení uvedeného v odstavci 1 posoudí zejména:

a) počet zřízených národních kybernetických center a přeshraničních kybernetických center, rozsah sdílených informací, pokud možno včetně dopadu na činnost sítě CSIRT, a do jaké míry přispěla tato centra k posílení společného odhalování kybernetických hrozeb a incidentů v Unii a situačního povědomí o nich a k rozvoji nejmodernějších technologií; využívání financování programu Digitální Evropa na nástroje, infrastrukturu nebo služby v oblasti kybernetické bezpečnosti, které byly společně pořízeny, a pokud jsou k dispozici příslušné informace, úroveň spolupráce mezi národními kybernetickými centry a odvětvovými a meziodvětvovými komunitami základních a důležitých subjektů podle článku 3 směrnice (EU) 2022/2555;

b) využívání a účinnost akcí v rámci mechanismu pro mimořádné události v oblasti kybernetické bezpečnosti na podporu připravenosti, včetně školení, reakce na významné kybernetické bezpečnostní incidenty, rozsáhlé kybernetické bezpečnostní incidenty a na incidenty obdobné rozsáhlým kybernetickým bezpečnostním incidentům a počáteční obnovy, včetně využití financování programu Digitální Evropa a poučení a doporučení získaných při uplatňování mechanismu pro mimořádné události v oblasti kybernetické bezpečnosti;

c) využívání a účinnost rezervy EU pro kybernetickou bezpečnost ve vztahu k druhu uživatelů, včetně využívání financování programu Digitální Evropa, využívání služeb, včetně jejich druhu, průměrné doby potřebné k reakci na žádosti a k využití rezervy EU pro kybernetickou bezpečnost, procentního podílu služeb přeměněných na služby připravenosti související s předcházením incidentům a reakcí na ně a poučení a doporučení získaných při provádění rezervy EU pro kybernetickou bezpečnost;

d) příspěvek tohoto nařízení k posílení konkurenčního postavení průmyslu a služeb v Unii v celé digitální ekonomice, včetně mikropodniků, malých a středních podniků a začínajících podniků, a příspěvek k dosažení celkového cíle, jímž je posílit dovednosti a kapacity pracovníků týkající se kybernetické bezpečnosti.

3. Komise na základě zpráv uvedených v odstavci 1 případně předloží Evropskému parlamentu a Radě legislativní návrh na změnu tohoto nařízení.

Článek 26

Vstup v platnost

Toto nařízení vstupuje v platnost dvacátým dnem po vyhlášení v *Úředním věstníku Evropské unie*.

Toto nařízení je závazné v celém rozsahu a přímo použitelné ve všech členských státech.

V … dne ...

Za Evropský parlament	*Za Radu*
předsedkyně	*předseda/předsedkyně*

PŘÍLOHA

Přílohy nařízení (EU) 2021/694 se mění takto:

1) V příloze I se oddíl „Specifický cíl č. 3 – Kybernetická bezpečnost a důvěra“ nahrazuje tímto:

„Specifický cíl č. 3 – Kybernetická bezpečnost a důvěra

Program podpoří posilování, budování a pořizování základní kapacity potřebné k zabezpečení digitálního hospodářství, společnosti a demokracie v Unii tím, že bude zvyšovat průmyslový potenciál a konkurenceschopnost Unie v oblasti kybernetické bezpečnosti a prohlubovat schopnost soukromého i veřejného sektoru chránit občany a podniky před kybernetickými hrozbami, mimo jiné podporou uplatňování směrnice (EU) 2016/1148.

Počáteční a případné následné akce v rámci tohoto cíle zahrnují:

1. společné investování spolu s členskými státy do vyspělého zařízení, infrastruktury a know-how v oblasti kybernetické bezpečnosti, jež mají zásadní význam pro ochranu klíčové infrastruktury a jednotného digitálního trhu jako takového. Toto společné investování by mohlo zahrnovat investice do kvantových zařízení a datových zdrojů pro kybernetickou bezpečnost, povědomí o situaci v kyberprostoru, včetně národních kybernetických center a přeshraničních kybernetických center tvořících Evropský systém varování v oblasti kybernetické bezpečnosti, jakož i dalších nástrojů, které budou zpřístupněny veřejnému i soukromému sektoru v celé Evropě;

2. rozšiřování stávajících technologických kapacit a propojování odborných středisek v členských státech a zajištění toho, aby tyto kapacity odpovídaly potřebám veřejného sektoru a výrobního odvětví, a to i u produktů a služeb, jež upevňují kybernetickou bezpečnost a důvěru v rámci jednotného digitálního trhu;

3. široké zavádění účinných nejmodernějších řešení v oblasti kybernetické bezpečnosti a důvěry ve všech členských státech. Toto zavádění zahrnuje posílení bezpečnosti produktů již od fáze jejich návrhu až po jejich uvedení na trh,

4. podporu odstraňování nedostatků v dovednostech v oblasti kybernetické bezpečnosti s přihlédnutím k vyváženému genderovému zastoupení, např. slaďováním vzdělávacích programů v oblasti kybernetické bezpečnosti, jejich přizpůsobováním potřebám konkrétních odvětví a usnadňováním přístupu ke specializovaným školením,

5. podporu solidarity mezi členskými státy při přípravě na významné kybernetické bezpečnostní incidenty a rozsáhlé kybernetické bezpečnostní incidenty a reakci na ně prostřednictvím přeshraničního zavádění služeb kybernetické bezpečnosti, včetně podpory vzájemné pomoci mezi orgány veřejné moci a vytvoření rezervy důvěryhodných poskytovatelů řízených bezpečnostních služeb na úrovni Unie.“

2) V příloze II se oddíl „Specifický cíl č. 3 – Kybernetická bezpečnost a důvěra“ nahrazuje tímto:

„Specifický cíl č. 3 – Kybernetická bezpečnost a důvěra

3.1. Počet infrastruktur nebo nástrojů kybernetické bezpečnosti pořízených v rámci společné veřejné zakázky, a to i v souvislosti s Evropským systémem varování v oblasti kybernetické bezpečnosti

3.2. Počet uživatelů a uživatelských skupin s přístupem k evropským zařízením kybernetické bezpečnosti

3.3 Počet akcí na podporu připravenosti a reakce na kybernetické bezpečnostní incidenty v rámci mechanismu pro mimořádné události v oblasti kybernetické bezpečnosti“.

K tomuto aktu [bylo učiněno/byla učiněna] prohlášení, [které/která] lze nalézt v ... [Pro Úřední věstník: Úř. věst. C XXX, XX.XX.2024, s. XX] a na této internetové adrese: … [Pro Úřední věstník: vložte prosím odkaz na prohlášení]