Rada
Evropské unie

Brusel 20. dubna 2023
(OR. en)

8512/23

Interinstitucionální spis:
2023/0109(COD)

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

NÁVRH

Odesílatel:	Martine DEPREZOVÁ, ředitelka, za generální tajemnici Evropské komise
Datum přijetí:	19. dubna 2023
Příjemce:	Thérèse BLANCHETOVÁ, generální tajemnice Rady Evropské unie
Č. dok. Komise:	COM(2023) 209 final
Předmět:	Návrh NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY, kterým se stanoví opatření k posílení solidarity a kapacit v Unii pro odhalování kybernetických bezpečnostních hrozeb a incidentů a pro připravenost a reakci na ně

Delegace naleznou v příloze dokument COM(2023) 209 final.

Příloha: COM(2023) 209 final

EVROPSKÁ
KOMISE

Ve Štrasburku dne 18.4.2023
COM(2023) 209 final

2023/0109 (COD)

Návrh

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY,

kterým se stanoví opatření k posílení solidarity a kapacit v Unii pro odhalování kybernetických bezpečnostních hrozeb a incidentů a pro připravenost a reakci na ně

DŮVODOVÁ ZPRÁVA

1. SOUVISLOSTI NÁVRHU

• Odůvodnění a cíle návrhu

Tato důvodová zpráva je připojena k návrhu aktu o kybernetické solidaritě. Používání informačních a komunikačních technologií a závislost na nich je dnes základním aspektem ve všech odvětvích hospodářské činnosti, neboť naše orgány státní správy, společnosti a občané jsou více než kdykoli předtím vzájemně propojení a závislí, a to napříč odvětvími i hranicemi. Toto intenzivnější využívání digitálních technologií znamená vyšší vystavení kybernetickým bezpečnostním incidentům a zvyšuje jejich možné dopady. Členské státy zároveň čelí rostoucím rizikům v oblasti kybernetické bezpečnosti a celkově složitému prostředí hrozeb s jasným rizikem rychlého přelévání kybernetických incidentů z jednoho členského státu do ostatních.

Kybernetické operace jsou navíc stále více začleňovány do hybridních a válečných strategií, a to s významným dopadem na cíl. Konkrétně vojenské agresi Ruska proti Ukrajině předcházela strategie nepřátelských kybernetických operací, které i nadále uvedenou agresi doprovázejí. To zásadně mění vnímání a hodnocení připravenosti EU na kolektivní řešení kybernetických krizí a znamená to i výzvu k neodkladným krokům. Hrozba možného rozsáhlého incidentu, který by způsobil významné narušení a poškození kritických infrastruktur, vyžaduje zvýšenou připravenost na všech úrovních ekosystému kybernetické bezpečnosti EU. Tato hrozba přesahuje rámec ruské vojenské agrese vůči Ukrajině a zahrnuje neustálé kybernetické hrozby ze strany státních i nestátních subjektů, které budou pravděpodobně trvat i nadále vzhledem k množství se státem spojených, kriminálních a aktivistických hackerských subjektů, které se podílejí na stávajícím geopolitickém napětí. V posledních letech se výrazně zvýšil počet kybernetických útoků, včetně útoků na dodavatelské řetězce zaměřených na kybernetickou špionáž, ransomware nebo narušení. V roce 2020 zasáhl útok na dodavatelský řetězec společnosti SolarWinds více než 18 000 organizací po celém světě, včetně vládních agentur a velkých společností. Významné kybernetické bezpečnostní incidenty mohou být pro jeden nebo několik zasažených členských států natolik disruptivní, že je nemohou řešit samy. Z toho důvodu je třeba posílit solidaritu na úrovni Unie, aby bylo možné lépe odhalovat kybernetické bezpečnostní hrozby a incidenty, připravovat se a reagovat na ně.

Pokud jde o odhalování kybernetických hrozeb a incidentů, je naléhavě nutné zvýšit výměnu informací a zlepšit naše společné kapacity, aby se výrazně zkrátila doba potřebná k odhalení kybernetických hrozeb dříve, než budou moci způsobit rozsáhlé škody a náklady[1]. Přestože mnoho kybernetických bezpečnostních hrozeb a incidentů má potenciální přeshraniční rozměr, kvůli propojení digitálních infrastruktur je sdílení příslušných informací mezi členskými státy stále omezené. K řešení tohoto problému má přispět vybudování sítě

[1] Podle zprávy Ponemon Institute a IBM Security činila v roce 2022 průměrná doba identifikace narušení 207 dní a dalších 70 dní bylo zapotřebí na jeho zvládnutí. Zároveň v roce 2022 činily průměrné náklady na porušení zabezpečení údajů s životním cyklem delším než 200 dní 4,86 milionu EUR oproti 3,74 milionu EUR v případě narušení údajů s životním cyklem do 200 dní. („Cost of a data breach 2022“ (Náklady na porušení zabezpečení údajů v roce 2022), https://www.ibm.com/reports/data-breach).

přeshraničních bezpečnostních operačních středisek, která posílí kapacity pro odhalování a reakci.

Pokud jde o připravenost a reakci na kybernetické bezpečnostní incidenty, podpora na úrovni Unie a solidarita mezi členskými státy jsou v současné době omezené. V závěrech Rady z října 2021 byla zdůrazněna potřeba tyto nedostatky řešit a Komise byla vyzvána, aby předložila návrh nového fondu pro reakci na mimořádné události v oblasti kybernetické bezpečnosti[2].

Tímto nařízením se rovněž provádí strategie kybernetické bezpečnosti EU přijatá v prosinci 2020[3], v níž bylo oznámeno vytvoření evropského kybernetického štítu, jenž posílí schopnosti zjišťování kybernetických hrozeb a sdílení informací v Evropské unii prostřednictvím sítě národních a přeshraničních bezpečnostních operačních středisek.

Toto nařízení vychází z prvních kroků, které již proběhly v úzké spolupráci s hlavními zúčastněnými stranami a podpořeny programem Digitální Evropa. Konkrétně pokud jde o bezpečnostní operační střediska, byla v rámci pracovního programu pro kybernetickou bezpečnost na období 2021–2022, který je součástí programu Digitální Evropa, vyhlášena výzva k vyjádření zájmu týkající se společného nákupu nástrojů a infrastruktury pro zřízení přeshraničních bezpečnostních operačních středisek a výzva k předkládání žádostí o granty, které umožní budování kapacit bezpečnostních operačních středisek sloužících veřejným a soukromým organizacím. Pokud jde o připravenost a reakci na kybernetické incidenty, Komise zřídila krátkodobý program na podporu členských států prostřednictvím dodatečných finančních prostředků přidělených Agentuře Evropské unie pro kybernetickou bezpečnost (ENISA) s cílem okamžitě posílit připravenost a schopnost reakce na závažné kybernetické incidenty. Obě akce byly připraveny v úzké koordinaci s členskými státy. Toto nařízení řeší nedostatky a začleňuje poznatky z uvedených akcí.

V neposlední řadě tento návrh naplňuje závazek v souladu se společným sdělením o kybernetické obraně[4], které bylo přijato dne 10. listopadu, a to připravit návrh iniciativy EU pro kybernetickou solidaritu s těmito cíli: posílit společné schopnosti EU v oblasti odhalování, situačního povědomí a reakce, postupně vytvářet rezervu pro kybernetickou bezpečnost na úrovni EU se službami od důvěryhodných soukromých poskytovatelů a podporovat testování kritických subjektů.

Za uvedené situace Komise předkládá tento akt o kybernetické solidaritě s cílem posílit solidaritu na úrovni Unie, aby bylo možné lépe odhalovat kybernetické bezpečnostní hrozby a incidenty, připravovat se na ně a reagovat na ně prostřednictvím těchto specifických cílů:

---

[2] Závěry Rady o vývoji kybernetické pozice Evropské unie schválené Radou na zasedání dne 23. května 2022 (9364/22).

[3] Společné sdělení Evropskému parlamentu a Radě, Strategie kybernetické bezpečnosti EU pro digitální dekádu, JOIN(2020) 18 final.

[4] Společné sdělení Evropskému parlamentu a Radě, Politika kybernetické obrany EU, JOIN(2022) 49 final.

- posílit společné odhalování kybernetických hrozeb a incidentů a situační povědomí o těchto hrozbách a incidentech v EU, a tím přispět k evropské technologické suverenitě v oblasti kybernetické bezpečnosti,
- posílit připravenost kritických subjektů v celé EU a upevnit solidaritu vytvořením společných kapacit pro reakci na významné nebo rozsáhlé kybernetické bezpečnostní incidenty, včetně zpřístupnění podpory při reakci na incidenty třetím zemím přidruženým k programu Digitální Evropa,
- zvýšit odolnost Unie a přispět k účinné reakci přezkumem a posouzením významných nebo rozsáhlých incidentů, včetně vyvození poučení a případných doporučení.

Uvedené cíle se provádějí prostřednictvím těchto opatření:

- Zavedení celoevropské infrastruktury bezpečnostních operačních středisek (evropský kybernetický štít) s cílem vybudovat a posílit společné schopnosti odhalování a situačního povědomí.
- Vytvoření mechanismu pro mimořádné události v kybernetické oblasti, který by podporoval členské státy při přípravě na významné a rozsáhlé kybernetické bezpečnostní incidenty, při reakci na ně a při okamžité obnově po takových incidentech. Podpora reakce na incidenty bude zpřístupněna i evropským orgánům, institucím a jiným subjektům Unie.
- Zřízení evropského mechanismu pro přezkum kybernetických bezpečnostních incidentů, který bude přezkoumávat a posuzovat konkrétní významné nebo rozsáhlé incidenty.

Evropský kybernetický štít a mechanismus pro mimořádné události v kybernetické oblasti budou podporovány z prostředků programu Digitální Evropa, který tento legislativním nástroj pozmění s cílem zavést výše uvedená opatření, poskytnout finanční podporu na jejich rozvoj a vyjasnit podmínky pro čerpání finanční podpory.

•Soulad s platnými předpisy v této oblasti politiky

Rámec EU zahrnuje několik právních předpisů, které jsou již přijaty nebo navrženy na úrovni Unie s cílem snížit zranitelnost, zvýšit odolnost kritických subjektů vůči rizikům v oblasti kybernetické bezpečnosti a podpořit koordinované zvládání rozsáhlých incidentů a krizí v oblasti kybernetické bezpečnosti, zejména směrnici o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (NIS 2)[5], akt o kybernetické

[5] 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).

bezpečnosti[6], směrnici o útocích na informační systémy[7], doporučení Komise (EU) 2017/1584 o koordinované reakci na rozsáhlé kybernetické bezpečnostní incidenty a krize[8].

Opatření navrhovaná v rámci aktu o kybernetické solidaritě se týkají situačního povědomí, sdílení informací, jakož i podpory připravenosti na kybernetické incidenty a reakce na ně. Tato opatření jsou v souladu s cíli regulačního rámce existujícího na úrovni Unie a tyto cíle podporují, zejména na základě směrnice (EU) 2022/2555 („směrnice NIS 2“). Akt o kybernetické solidaritě bude vycházet zejména ze stávajících rámců pro operativní spolupráci v oblasti kybernetické bezpečnosti a pro řešení krizí, zejména Evropské sítě styčných organizací pro řešení kybernetických krizí (EU-CyCLONe) a sítě týmů pro reakce na počítačové bezpečnostní incidenty (týmů CSIRT), a bude tyto rámce podporovat.

Přeshraniční platformy bezpečnostních operačních středisek by měly představovat novou kapacitu, která doplní síť týmů pro reakce na kybernetické bezpečnostní incidenty, neboť bude sdružovat a sdílet údaje o kybernetických bezpečnostních hrozbách od veřejných a soukromých subjektů, zvyšovat hodnotu těchto údajů prostřednictvím odborné analýzy a nejmodernějších nástrojů a přispívat k rozvoji schopností a technologické suverenity Unie.

A v neposlední řadě je tento návrh v souladu s doporučením Rady o celounijním koordinovaném přístupu za účelem posílení odolnosti kritické infrastruktury[9], které vyzývá členské státy, aby přijaly naléhavá a účinná opatření a aby loajálně, efektivně, solidárně a koordinovaně 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.

- **Soulad s ostatními politikami Unie**

Návrh je v souladu s dalšími mechanismy a protokoly pro řešení krizových situací, jako je například mechanismus integrovaných opatření EU pro politickou reakci na krize (IPCR). Akt o kybernetické solidaritě doplní tyto rámce a protokoly řešení krizí, neboť poskytne specializovanou podporu pro připravenost a reakci na kybernetické bezpečnostní incidenty. Návrh bude rovněž v souladu s vnější činností EU v reakci na rozsáhlé incidenty v rámci společné zahraniční a bezpečnostní politiky (SZBP), mimo jiné prostřednictvím souboru nástrojů kybernetické diplomacie EU. Návrh doplní opatření prováděná v souvislosti s čl. 42

[6] 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“).

[7] 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.

[8] Návrh nařízení Evropského parlamentu a Rady o horizontálních požadavcích na kybernetickou bezpečnost produktů s digitálními prvky a o změně nařízení (EU) 2019/1020, COM(2022) 454 final.

[9] Doporučení Rady ze dne 8. prosince 2022 o celounijním koordinovaném přístupu za účelem posílení odolnosti kritické infrastruktury (Text s významem pro EHP) 2023/C 20/01.

odst. 7 Smlouvy o Evropské unii nebo v situacích vymezených v článku 222 Smlouvy o fungování Evropské unie.

Doplňuje také mechanismus civilní ochrany Unie (UCPM)[10] zřízený v prosinci 2013 a dovršený novým právním předpisem přijatým v květnu 2021[11], který posiluje pilíře prevence, připravenosti a reakce mechanismu UCPM a poskytuje EU další kapacity pro reakci na nová rizika v Evropě a ve světě a posiluje rezervu rescEU.

2. PRÁVNÍ ZÁKLAD, SUBSIDIARITA A PROPORCIONALITA

• Právní základ

Právním základem tohoto návrhu je čl. 173 odst. 3 a čl. 322 odst. 1 písm. a) Smlouvy o fungování Evropské unie (dále jen „SFEU“). Podle článku 173 SFEU Unie a členské státy zajistí, aby existovaly podmínky nezbytné pro konkurenceschopnost průmyslu Unie. Cílem tohoto nařízení je posílit konkurenceschopnost odvětví průmyslu a služeb v Evropě v rámci digitalizované ekonomiky a podpořit jejich digitální transformaci posílením úrovně kybernetické bezpečnosti na jednotném digitálním trhu. Nařízení si klade za cíl zejména zvýšit odolnost občanů, podniků a subjektů působících v kritických a vysoce kritických odvětvích vůči rostoucím kybernetickým bezpečnostním hrozbám, které mohou mít ničivé společenské a hospodářské dopady.

Návrh vychází rovněž z čl. 322 odst. 1 písm. a) SFEU, neboť obsahuje zvláštní pravidla pro přenos prostředků odchylující se od zásady ročního rozpočtu stanovené v nařízení Evropského parlamentu a Rady (EU, Euratom) 2018/1046 (dále jen „finanční nařízení“)[12]. V zájmu řádného finančního řízení a s ohledem na nepředvídatelnou, výjimečnou a specifickou povahu prostředí kybernetické bezpečnosti a kybernetických hrozeb by měl mechanismus pro mimořádné události v oblasti kybernetické bezpečnosti využívat určitou míru flexibility ve vztahu k rozpočtovému řízení, a to zejména tím, že nevyužité prostředky na závazky a platby na akce sledující cíle stanovené v nařízení budou automaticky přeneseny do následujícího rozpočtového roku. Vzhledem k tomu, že toto nové pravidlo vyvolává problémy ve vztahu k finančnímu nařízení, mohla by být tato otázka řešena v rámci probíhajících jednání o přepracovaném znění finančního nařízení.

• Subsidiarita (v případě nevýlučné pravomoci)

Silná přeshraniční povaha kybernetických bezpečnostních hrozeb a rostoucí počet rizik a incidentů, které se přelévají přes hranice a mezi odvětvími a produkty, znamená, že cílů

---

[10] Rozhodnutí Evropského parlamentu a Rady č. 1313/2013/EU ze dne 17. prosince 2013 o mechanismu civilní ochrany Unie (Text s významem pro EHP).

[11] Nařízení Evropského parlamentu a Rady (EU) 2021/836 ze dne 20. května 2021, kterým se mění rozhodnutí č. 1313/2013/EU o mechanismu civilní ochrany Unie (Text s významem pro EHP).

[12] Nařízení Evropského parlamentu a Rady (EU, Euratom) 2018/1046 ze dne 18. července 2018, kterým se stanoví finanční pravidla pro souhrnný rozpočet Unie (Úř. věst. L 193, 30.7.2018, s. 1).

tohoto zásahu nemohou členské státy účinně dosáhnout samy a je zapotřebí společného postupu a solidarity na úrovni Unie.

Zkušenosti s bojem proti kybernetickým hrozbám vyplývajícím z války proti Ukrajině spolu s poznatky získanými z cvičení v oblasti kybernetické bezpečnosti, které proběhlo během francouzského předsednictví (EU CyCLES), ukázaly, že pro dosažení solidarity na úrovni EU je třeba vytvořit konkrétní mechanismy vzájemné podpory, zejména spolupráce se soukromým sektorem. V této souvislosti závěry Rady ze dne 23. května 2022 o vývoji kybernetické pozice Evropské unie vyzývají Komisi, aby předložila návrh nového fondu pro reakci na mimořádné události v oblasti kybernetické bezpečnosti.

Podpora a opatření na úrovni Unie s cílem lépe odhalovat kybernetické bezpečnostní hrozby a zvyšovat připravenost a schopnost reakce představují přidanou hodnotu, neboť zabraňují zdvojování úsilí v Unii a členských státech. Vedly by k lepšímu využívání stávajících prostředků a k větší koordinaci a výměně informací o získaných poznatcích. Mechanismus pro mimořádné události v kybernetické oblasti rovněž počítá s poskytováním podpory třetím zemím přidruženým k programu Digitální Evropa z rezervy EU pro kybernetickou bezpečnost.

Podpora poskytovaná prostřednictvím různých iniciativ, které mají být zřízeny a financovány na úrovni Unie, bude doplňovat a nebude zdvojovat vnitrostátní kapacity, pokud jde o odhalování, situační povědomí, připravenost a reakci na kybernetické hrozby a incidenty.

• Proporcionalita

Opatření nepřekračují rámec toho, co je nezbytné pro dosažení obecných a specifických cílů nařízení. Opatřeními tohoto nařízení nejsou dotčeny povinnosti členských států v oblasti národní bezpečnosti, veřejné bezpečnosti, prevence, vyšetřování, odhalování a stíhání trestných činů. Opatření nemají vliv ani na právní povinnosti subjektů působících v kritických a vysoce kritických odvětvích přijmout opatření v oblasti kybernetické bezpečnosti v souladu se směrnicí NIS 2.

Opatření, na něž se vztahuje toto nařízení, doplňují tyto činnosti a opatření tím, že podporují vytváření infrastruktur pro lepší odhalování a analýzu hrozeb a poskytují podporu pro připravenost a opatření reakce v případě významných nebo rozsáhlých incidentů.

• Volba nástroje

Návrh má podobu nařízení Evropského parlamentu a Rady. Jedná se o nejvhodnější právní nástroj, neboť pouze nařízení s přímo použitelnými právními předpisy může zajistit nezbytnou míru jednotnosti potřebnou pro zřízení a fungování evropského kybernetického štítu a mechanismu pro mimořádné události v kybernetické oblasti stanovením podpory pro jejich zřízení z programu Digitální Evropa i jasných podmínek pro využívání a přidělování této podpory.

3. VÝSLEDKY HODNOCENÍ *EX POST*, KONZULTACÍ SE ZÚČASTNĚNÝMI STRANAMI A POSOUZENÍ DOPADŮ

- **Konzultace se zúčastněnými stranami**

Opatření tohoto nařízení budou podporována programem Digitální Evropa, který byl předmětem rozsáhlých konzultací. Kromě toho se budou opírat o první kroky, které byly připraveny v úzké spolupráci s hlavními zúčastněnými stranami. Pokud jde o bezpečnostní operační střediska, Komise v úzké spolupráci s členskými státy v rámci Evropského centra kompetencí pro kybernetickou bezpečnost (ECCC) vypracovala koncepční dokument o rozvoji přeshraničních platforem bezpečnostních operačních středisek a výzvu k vyjádření zájmu. V této souvislosti byl proveden průzkum kapacit národních bezpečnostních operačních středisek a v rámci technické pracovní skupiny centra ECCC, která sdružuje zástupce členských států, byly projednány společné přístupy a technické požadavky. Kromě toho probíhaly diskuze s příslušným odvětvím, zejména prostřednictvím skupiny odborníků pro bezpečnostní operační střediska, kterou zřídily agentura ENISA a Evropská organizace pro kybernetickou bezpečnost (ECSO).

Za druhé, pokud jde o připravenost a reakci na kybernetické incidenty, Komise zřídila krátkodobý program na podporu členských států prostřednictvím dodatečných finančních prostředků přidělených agentuře ENISA z programu Digitální Evropa s cílem okamžitě posílit připravenost a schopnosti reagovat na závažné kybernetické incidenty. Zpětná vazba členských států a příslušného odvětví získaná během provádění tohoto krátkodobého programu již poskytuje cenné poznatky, které byly využity při přípravě navrhovaného nařízení s cílem odstranit zjištěné nedostatky. Jednalo se o první krok v souladu se závěry Rady o kybernetické pozici, v nichž byla Komise vyzvána, aby předložila návrh nového fondu pro reakci na mimořádné události v oblasti kybernetické bezpečnosti.

Kromě toho se 16. února 2023 na základě diskusního dokumentu uskutečnilo pracovní setkání s odborníky z členských států na téma mechanismu pro mimořádné události v kybernetické oblasti. Tohoto semináře se zúčastnily všechny členské státy a jedenáct členských států poskytlo ještě písemné příspěvky.

- **Posouzení dopadů**

Vzhledem k naléhavé povaze návrhu nebylo posouzení dopadů provedeno. Opatření tohoto nařízení budou podpořena programem Digitální Evropa a jsou v souladu s opatřeními stanovenými v nařízení o programu Digitální Evropa, které bylo podrobeno zvláštnímu posouzení dopadů. Toto nařízení nebude mít žádné významné administrativní dopady ani dopady na životní prostředí nad rámec těch, které již byly posouzeny v posouzení dopadů nařízení o programu Digitální Evropa.

Dále navazuje na první opatření vypracovaná v uzavřené spolupráci s hlavními zúčastněnými stranami, jak je uvedeno výše, a na výzvu členských států, aby Komise do konce třetího čtvrtletí roku 2022 předložila návrh nového fondu pro reakci na mimořádné události v oblasti kybernetické bezpečnosti.

Konkrétně pokud jde o situační povědomí a odhalování hrozeb v rámci evropského kybernetického štítu, byla v rámci pracovního programu pro kybernetickou bezpečnost na období 2021–2022, který je součástí programu Digitální Evropa, vyhlášena výzva k vyjádření zájmu týkající se společného nákupu nástrojů a infrastruktury pro zřízení přeshraničních bezpečnostních operačních středisek a výzva k předkládání žádostí o granty, které umožní budování kapacit bezpečnostních operačních středisek sloužících veřejným a soukromým organizacím.

Jak je uvedeno výše, v oblasti připravenosti a reakce na incidenty Komise vytvořila krátkodobý program na podporu členských států z programu Digitální Evropa, který provádí agentura ENISA. Poskytované služby zahrnují opatření v oblasti připravenosti, jako je penetrační testování kritických subjektů s cílem identifikovat zranitelná místa. Rovněž jsou posíleny možnosti pomoci členským státům v případě závažného incidentu s dopadem na kritické subjekty. Agentura ENISA tento krátkodobý program právě provádí a již poskytla relevantní poznatky, které byly zohledněny při přípravě tohoto nařízení.

- **Základní práva**

Tím, že tento návrh přispěje k bezpečnosti digitálních údajů, přispěje k ochraně práva na svobodu a bezpečnost v souladu s článkem 6 Listiny základních práv EU a práva na respektování soukromého a rodinného života v souladu s článkem 7 Listiny základních práv EU. Ochranou podniků před hospodářsky škodlivými kybernetickými útoky návrh rovněž přispěje ke svobodě podnikání podle článku 16 Listiny základních práv EU a k právu na vlastnictví podle článku 17 Listiny základních práv EU. A konečně, díky ochraně integrity kritické infrastruktury před kybernetickými útoky návrh přispěje k právu na zdravotní péči v souladu s článkem 35 Listiny základních práv EU a k právu na přístup ke službám obecného hospodářského zájmu v souladu s článkem 36 Listiny základních práv EU.

4. ROZPOČTOVÉ DŮSLEDKY

Opatření tohoto nařízení budou podporována z finančních prostředků v rámci strategického cíle „Kybernetická bezpečnost“ programu Digitální Evropa.

Celkový rozpočet zahrnuje navýšení o 100 milionů EUR, které toto nařízení navrhuje přerozdělit z jiných strategických cílů programu Digitální Evropa. Tím se celková částka, která je k dispozici na akce v oblasti kybernetické bezpečnosti v rámci programu Digitální Evropa, zvýší na 842,8 milionu EUR.

Část z dodatečných 100 milionů EUR posílí rozpočet spravovaný centrem ECCC na provádění opatření týkajících se bezpečnostních operačních středisek a připravenosti v rámci jejich pracovního programu / pracovních programů. Dodatečné financování navíc poslouží na podporu zřízení rezervy EU pro kybernetickou bezpečnost.

Doplňuje rozpočet, který se již plánuje pro podobná opatření v hlavním programu Digitální Evropa a v jeho pracovním programu pro kybernetickou bezpečnost na období 2023–2027, což by mohlo přinést celkovou částku 551 milionů na období 2023–2027, zatímco 115 milionů již bylo vyčleněno ve formě pilotních projektů na období 2021–2022. Včetně příspěvků členských států by celkový rozpočet mohl dosáhnout až 1,109 miliardy EUR.

Přehled souvisejících nákladů je uveden v „legislativním finančním výkazu“, který je připojen k tomuto návrhu.

5. OSTATNÍ PRVKY

• Plány provádění a způsoby sledování, hodnocení a podávání zpráv

Komise bude monitorovat provádění, použití a dodržování těchto nových ustanovení s cílem posoudit jejich účinnost. Komise předloží Evropskému parlamentu a Radě zprávu o hodnocení a přezkumu tohoto nařízení do čtyř let ode dne jeho použitelnosti.

• Podrobné vysvětlení konkrétních ustanovení návrhu

Obecné cíle, předmět a definice (kapitola I)

Kapitola I stanoví cíle nařízení, tedy posílit solidaritu na úrovni Unie, aby bylo možné lépe odhalovat kybernetické bezpečnostní hrozby a incidenty, připravovat se na ně a reagovat na ně, a zejména posílit společné odhalování kybernetických hrozeb a incidentů v Unii a situační povědomí v této oblasti, upevnit připravenost subjektů působících v kritických a vysoce kritických odvětvích v celé Unii a posílit solidaritu vytvořením společných kapacit pro reakci na významné nebo rozsáhlé kybernetické bezpečnostní incidenty a zvýšit odolnost Unie přezkumem a hodnocením významných nebo rozsáhlých incidentů. Tato kapitola rovněž stanoví opatření, jejichž prostřednictvím bude těchto cílů dosaženo: zavedení evropského kybernetického štítu, vytvoření mechanismu pro mimořádné události v kybernetické oblasti a zřízení mechanismu pro přezkum kybernetických bezpečnostních incidentů. Vymezuje rovněž definice používané v rámci celého nástroje.

Evropský kybernetický štít (kapitola II)

Kapitola II zřizuje evropský kybernetický štít a stanoví jeho jednotlivé prvky a podmínky účasti. Nejprve oznamuje celkový cíl evropského kybernetického štítu, kterým je rozvoj pokročilých schopností Unie odhalovat, analyzovat a zpracovávat údaje o kybernetických hrozbách a incidentech v Unii, jakož i konkrétní operační cíle. Stanoví, že financování evropského kybernetického štítu ze strany Unie se provádí v souladu s nařízením o programu Digitální Evropa.

Kapitola dále popisuje typy subjektů, které tvoří evropský kybernetický štít. Štít se skládá z národních bezpečnostních operačních středisek a přeshraničních bezpečnostních operačních středisek. Každý zúčastněný členský stát určí národní bezpečnostní operační středisko. To bude fungovat jako referenční bod a brána k dalším veřejným a soukromým organizacím na

vnitrostátní úrovni, které budou shromažďovat a analyzovat informace o kybernetických bezpečnostních hrozbách a incidentech a přispívat k přeshraničnímu bezpečnostnímu operačnímu středisku. Na základě výzvy k vyjádření zájmu může centrum ECCC vybrat národní bezpečnostní operační středisko, aby podílelo na společném zadávání zakázek týkajících se nástrojů a infrastruktur s centrem ECCC a získalo grant na provozování nástrojů a infrastruktur. Pokud národní bezpečnostní operační středisko využívá podpory Unie, zaváže se, že do dvou let požádá o účast v přeshraničním bezpečnostním operačním středisku.

Přeshraniční bezpečnostní operační střediska tvoří konsorcium nejméně tří členských států zastoupených národními bezpečnostními operačními středisky, která se zavázala spolupracovat na koordinaci svých činností v oblasti odhalování a sledování kybernetických hrozeb. Po první výzvě k vyjádření zájmu může centrum ECCC vybrat hostitelské konsorcium, aby se podílelo na společném zadávání zakázek týkajících se nástrojů a infrastruktur s centrem ECCC a obdrželo grant na provozování nástrojů a infrastruktur. Členové hostitelského konsorcia uzavřou písemnou dohodu o konsorciu, která stanoví jejich vnitřní ujednání. Tato kapitola dále podrobně popisuje požadavky na sdílení informací mezi účastníky přeshraničního bezpečnostního operačního střediska a na sdílení informací mezi přeshraničním bezpečnostním operačním střediskem a ostatními přeshraničními bezpečnostními operačními středisky, jakož i s příslušnými subjekty EU. Národní bezpečnostní operační střediska, která se účastní přeshraničního bezpečnostního operačního střediska, si vzájemně vyměňují relevantní informace týkající se kybernetických hrozeb, přičemž podrobnosti, včetně závazku sdílet významné množství údajů a jeho podmínek, by měly být definovány v dohodě o konsorciu. Přeshraniční bezpečnostní operační střediska zajistí vysokou úroveň vzájemné interoperability. Přeshraniční bezpečnostní operační střediska by měla rovněž uzavírat dohody o spolupráci s ostatními přeshraničními bezpečnostními operačními středisky, které stanoví zásady sdílení informací. Pokud přeshraniční bezpečnostní operační střediska získají informace týkající se potenciálního nebo probíhajícího rozsáhlého kybernetického bezpečnostního incidentu, poskytnou příslušné informace síti EU CyCLONe, síti CSIRT a Komisi s ohledem na jejich příslušné úlohy v oblasti řešení krizí v souladu se směrnicí (EU) 2022/2555. V závěru kapitoly II jsou upřesněny bezpečnostní podmínky pro účast v evropském kybernetickém štítu.

Mechanismus pro mimořádné události v oblasti kybernetické bezpečnosti (kapitola III)

Kapitola III zřizuje mechanismus pro mimořádné události v kybernetické oblasti s cílem zlepšit odolnost Unie vůči zásadním kybernetickým bezpečnostním hrozbám a připravit se na krátkodobé dopady významných a rozsáhlých incidentů nebo krizí v oblasti kybernetické bezpečnosti a v duchu solidarity je zmírňovat. Akce, kterými se provádí mechanismus pro mimořádné události v kybernetické oblasti, jsou podporovány z finančních prostředků programu Digitální Evropa. Mechanismus stanoví opatření na podporu připravenosti, včetně koordinovaného testování subjektů působících ve vysoce kritických odvětvích, reakce na významné nebo rozsáhlé kybernetické bezpečnostní incidenty a okamžité obnovy po nich nebo zmírňování významných kybernetických hrozeb a opatření vzájemné pomoci.

Opatření mechanismu pro mimořádné události v kybernetické oblasti zahrnují koordinované testování připravenosti subjektů působících ve vysoce kritických odvětvích. Komise by měla po konzultaci s agenturou ENISA a skupinou pro spolupráci v oblasti bezpečnosti sítí a informací pravidelně určovat příslušná odvětví nebo pododvětví v rámci vysoce kritických odvětví vyjmenovaných v příloze I směrnice (EU) 2022/2555, v nichž mohou být subjekty podrobeny koordinovanému testování připravenosti na úrovni EU.

Pro účely provádění navrhovaných opatření pro reakci na incidenty se tímto nařízením zřizuje rezerva EU pro kybernetickou bezpečnost, kterou tvoří služby reakce na incidenty ze strany důvěryhodných poskytovatelů vybraných v souladu s kritérii stanovenými v tomto nařízení. Uživateli služeb rezervy EU pro kybernetickou bezpečnost jsou orgány členských států pro řešení kybernetických krizí, týmy CSIRT a orgány, instituce nebo jiné subjekty Unie. Komise nese celkovou odpovědnost za provádění rezervy EU pro kybernetickou bezpečnost a může agenturu ENISA zcela nebo částečně pověřit provozováním a správou rezervy EU pro kybernetickou bezpečnost.

Aby uživatelé mohli získat podporu z rezervy EU pro kybernetickou bezpečnost, měli by přijmout vlastní opatření ke zmírnění dopadů incidentu, pro který je podpora požadována. Žádosti o podporu z rezervy EU pro kybernetickou bezpečnost by měly obsahovat nezbytné příslušné informace o incidentu a opatřeních, která již uživatelé přijali. V kapitole jsou popsány i způsoby provádění, včetně posuzování žádostí podaných k rezervě EU pro kybernetickou bezpečnost.

Nařízení rovněž stanoví zásady zadávání veřejných zakázek a kritéria výběru důvěryhodných poskytovatelů rezervy EU pro kybernetickou bezpečnost.

Třetí země mohou požádat o podporu z rezervy EU pro kybernetickou bezpečnost, pokud to stanoví dohody o přidružení týkající se jejich účasti v programu Digitální Evropa. Tato kapitola popisuje další podmínky a způsoby této účasti.

Mechanismus přezkumu kybernetických bezpečnostních incidentů (kapitola IV)

Na žádost Komise, sítě EU-CyCLONe nebo sítě CSIRT by agentura ENISA měla přezkoumat a posoudit hrozby, zranitelná místa a opatření ke zmírnění dopadů v souvislosti s konkrétním významným nebo rozsáhlým kybernetickým bezpečnostním incidentem. Přezkum a posouzení by měla agentura ENISA předat ve formě zprávy o přezkumu incidentu síti CSIRT, síti EU-CyCLONe a Komisi, aby je podpořila při plnění jejich úkolů. Pokud se incident týká třetí země, měla by Komise zprávu předat vysokému představiteli. Zpráva by měla obsahovat získané poznatky a případně doporučení ke zlepšení kybernetické pozice Unie.

Závěrečná ustanovení (kapitola V)

Kapitola V obsahuje změny nařízení o programu Digitální Evropa a povinnost Komise vypracovávat pravidelné zprávy o hodnocení a přezkumu nařízení pro Evropský parlament a Radu. Komisi je svěřena pravomoc přijímat přezkumným postupem podle článku 21 prováděcí akty, které: specifikují podmínky této interoperability mezi přeshraničními

bezpečnostními operačními středisky; určí procesní režim pro sdílení informací souvisejících s potenciálním nebo probíhajícím rozsáhlým kybernetickým bezpečnostním incidentem mezi přeshraničními bezpečnostními operačními středisky a subjekty Unie; stanoví technické požadavky na zajištění vysoké úrovně bezpečnosti dat a fyzické bezpečnosti infrastruktury a na ochranu bezpečnostních zájmů Unie při sdílení informací se subjekty, které nejsou veřejnoprávními subjekty členských států; specifikují druhy a počet služeb reakce požadovaných pro rezervu EU pro kybernetickou bezpečnost a upřesní podrobná opatření pro přidělování podpůrných služeb z rezervy EU pro kybernetickou bezpečnost.

2023/0109 (COD)

Návrh

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY,

kterým se stanoví opatření k posílení solidarity a kapacit v Unii pro odhalování kybernetických bezpečnostních hrozeb a incidentů a pro připravenost a reakci na ně

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,

vzhledem k těmto důvodům:

(1) Používání informačních a komunikačních technologií a závislost na nich je dnes základním aspektem ve všech odvětvích hospodářské činnosti, neboť naše orgány státní správy, společnosti a občané jsou více než kdykoli předtím vzájemně propojení a závislí, a to napříč odvětvími i hranicemi.

(2) Rozsah, četnost a dopad kybernetických bezpečnostních incidentů se zvyšuje, včetně útoků na dodavatelský řetězec, a jejich cílem je kybernetická špionáž, ransomware nebo narušení provozu. Představují zásadní hrozbu pro fungování síťových a informačních systémů. Vzhledem k rychle se vyvíjejícímu prostředí hrozeb vyžaduje hrozba možných rozsáhlých incidentů, které mohou způsobit významné narušení a poškození kritických infrastruktur, zvýšenou připravenost na všech úrovních rámce kybernetické bezpečnosti Unie. Tato hrozba přesahuje rámec ruské vojenské agrese vůči Ukrajině a pravděpodobně bude trvat i nadále vzhledem k množství se státem spojených, kriminálních a aktivistických hackerských subjektů, které se podílejí na stávajícím geopolitickém napětí. Takové incidenty mohou narušit poskytování veřejných služeb a výkon hospodářských činností, a to i v kritických nebo vysoce kritických odvětvích, způsobit značné finanční ztráty, podkopat důvěru uživatelů, způsobit velké škody hospodářství Unie a mohou mít i zdraví nebo životy ohrožující následky. Kybernetické bezpečnostní incidenty jsou navíc nepředvídatelné, protože se často objevují a vyvíjejí ve velmi krátkém časovém období, nejsou omezeny na konkrétní zeměpisnou oblast a vyskytují se současně nebo se okamžitě šíří v mnoha zemích.

---

1 Úř. věst. C […], […], s. […].
2 Úř. věst. C , , s. .
3 Úř. věst. C , , s. .

(3) Je nezbytné posílit konkurenceschopnost odvětví průmyslu a služeb v Unii v rámci celé digitalizované ekonomiky a podpořit jejich digitální transformaci zvýšením úrovně kybernetické bezpečnosti na jednotném digitálním trhu. Jak je doporučeno ve třech různých návrzích konference o budoucnosti Evropy[4], je nutné zvýšit odolnost občanů, podniků a subjektů provozujících kritické infrastruktury vůči rostoucím kybernetickým bezpečnostním hrozbám, které mohou mít ničivé společenské a hospodářské dopady. Proto je třeba investovat do infrastruktur a služeb, které podpoří rychlejší odhalování kybernetických bezpečnostních hrozeb a incidentů a reakci na ně, přičemž členské státy potřebují pomoc při lepší přípravě na významné a rozsáhlé incidenty v oblasti kybernetické bezpečnosti a při reakci na ně. Unie by rovněž měla zvýšit své kapacity v těchto oblastech, zejména pokud jde o shromažďování a analýzu údajů o kybernetických bezpečnostních hrozbách a incidentech.

(4) Unie již přijala řadu opatření ke snížení zranitelnosti a zvýšení odolnosti kritických infrastruktur a subjektů vůči rizikům v oblasti kybernetické bezpečnosti, zejména směrnici Evropského parlamentu a Rady (EU) 2022/2555[5], doporučení Komise (EU) 2017/1584[6], směrnici Evropského parlamentu a Rady 2013/40/EU[7] a nařízení Evropského parlamentu a Rady (EU) 2019/881[8]. Doporučení Rady o celounijním koordinovaném přístupu za účelem posílení odolnosti kritické infrastruktury navíc vyzývá členské státy, aby přijaly naléhavá a účinná opatření a aby loajálně, efektivně, solidárně a koordinovaně 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) Narůstající rizika v oblasti kybernetické bezpečnosti a celkově složité prostředí hrozeb s jasným rizikem rychlého přelévání kybernetických incidentů z jednoho členského státu do ostatních a ze třetí země do Unie vyžadují posílenou solidaritu na úrovni Unie, aby bylo možné lépe odhalovat kybernetické bezpečnostní hrozby a incidenty, připravovat se na ně a reagovat na ně. Členské státy rovněž v závěrech Rady o kybernetické pozici EU[9] vyzvaly Komisi, aby předložila návrh nového fondu pro reakci na mimořádné události v oblasti kybernetické bezpečnosti.

(6) Společné sdělení o politice kybernetické obrany EU[10] přijaté 10. listopadu 2022 oznámilo iniciativu EU pro kybernetickou solidaritu s těmito cíli: posílit společné schopnosti EU v oblasti odhalování, situačního povědomí a reakce podporou zavádění infrastruktury EU v podobě bezpečnostních operačních středisek, podporovat postupné vytváření rezervy pro kybernetickou bezpečnost na úrovni EU se službami

---

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

5 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 (Úř. věst. L 333, 27.12.2022).

6 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).

7 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).

8 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).

9 Závěry Rady o rozvoji kybernetické pozice Evropské unie, schválené Radou na zasedání dne 23. května 2022 (9364/22).

10 Společné sdělení Evropskému parlamentu a Radě, Politika kybernetické obrany EU, JOIN/2022/49 final.

důvěryhodných soukromých poskytovatelů a testování kritických subjektů na potenciální zranitelnost na základě posouzení rizik v EU.

(7) Je nezbytné posílit odhalování kybernetických hrozeb a incidentů a situační povědomí v celé Unii a posílit solidaritu tím, že se zvýší připravenost a schopnost členských států a Unie reagovat na významné a rozsáhlé kybernetické bezpečnostní incidenty. Proto by měla být zavedena celoevropská infrastruktura bezpečnostních operačních středisek (evropský kybernetický štít) s cílem vybudovat a posílit společné schopnosti odhalování a situačního povědomí; měl by být zřízen mechanismus pro mimořádné události v oblasti kybernetické bezpečnosti, který by podporoval členské státy při přípravě na významné a rozsáhlé incidenty v oblasti kybernetické bezpečnosti, při reakci na ně a při okamžité obnově po nich; měl by být zřízen mechanismus přezkumu kybernetických bezpečnostních incidentů, který by přezkoumával a posuzoval konkrétní významné nebo rozsáhlé incidenty. Těmito opatřeními nejsou dotčeny články 107 a 108 Smlouvy o fungování Evropské unie (dále jen „SFEU“).

(8) K dosažení těchto cílů je rovněž nezbytné v některých oblastech změnit nařízení Evropského parlamentu a Rady (EU) 2021/694[11]. Tímto nařízením by mělo být změněno nařízení (EU) 2021/694, zejména pokud jde o doplnění nových operačních cílů týkajících se evropského kybernetického štítu a mechanismu pro mimořádné události v kybernetické oblasti v rámci specifického cíle 3 programu Digitální Evropa, který má zajistit odolnost, integritu a důvěryhodnost jednotného digitálního trhu, posílit kapacity pro monitorování kybernetických útoků a hrozeb a pro reakci na ně a posílit přeshraniční spolupráci v oblasti kybernetické bezpečnosti. To bude doplněno stanovením konkrétních podmínek, za nichž může být na tyto akce poskytnuta finanční podpora, a vymezením mechanismů řízení a koordinace nezbytných k dosažení zamýšlených cílů. Další změny nařízení (EU) 2021/694 by měly zahrnovat popisy navrhovaných opatření v rámci nových operačních cílů, jakož i měřitelné ukazatele, kterými se bude sledovat provádění těchto nových operačních cílů.

(9) Financování akcí podle tohoto nařízení by mělo být stanoveno v nařízení (EU) 2021/694, které by mělo zůstat příslušným základním aktem pro tyto akce zakotvené ve specifickém cíli 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.

(10) 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 ve finančním nařízení 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) Pro účely řádného finančního řízení by měla být stanovena zvláštní pravidla pro přenos nevyužitých prostředků na závazky a platby. Při respektování zásady, že rozpočet Unie je stanovován na ročním základě, by toto nařízení mělo vzhledem k nepředvídatelné, výjimečné a specifické povaze prostředí kybernetické bezpečnosti stanovit možnosti přenosu nevyužitých finančních prostředků nad rámec prostředků stanovených ve finančním nařízení, čímž by se maximalizovala schopnost

[11] 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).

mechanismu pro mimořádné události v oblasti kybernetické bezpečnosti účinně podporovat členské státy v boji proti kybernetickým hrozbám.

(12) Aby bylo možné účinněji předcházet kybernetickým hrozbám a incidentům, vyhodnocovat je a reagovat na ně, je nutné získat komplexnější znalosti o hrozbách pro kritická aktiva a infrastruktury na území Unie, včetně jejich zeměpisného rozložení, vzájemného propojení a možných dopadů v případě kybernetických útoků na tyto infrastruktury. Měla by být zavedena rozsáhlá unijní infrastruktura bezpečnostních operačních středisek („evropský kybernetický štít“), která by se skládala z několika interoperabilních přeshraničních platforem, z nichž každá by sdružovala několik národních bezpečnostních operačních středisek. Tato infrastruktura by měla sloužit zájmům členských států a potřebám Unie v oblasti kybernetické bezpečnosti a využívat nejmodernější technologie pro pokročilé nástroje shromažďování údajů a analýzy, zlepšovat schopnosti odhalování a řízení kybernetických útoků a poskytovat přehled o situaci v reálném čase. Tato infrastruktura by měla sloužit k lepšímu odhalování kybernetických bezpečnostních hrozeb a incidentů, a tím doplňovat a podporovat subjekty a sítě Unie odpovědné za řešení krizí v Unii, zejména Evropskou síť styčných organizací pro řešení kybernetických krizí (dále jen „EU-CyCLONe“), jak je definována ve směrnici Evropského parlamentu a Rady (EU) 2022/2555[12].

(13) Každý členský stát by měl určit veřejnoprávní subjekt na vnitrostátní úrovni, který bude pověřen koordinací činností v oblasti odhalování kybernetických hrozeb v daném členském státě. Tato národní bezpečnostní operační střediska by měla na vnitrostátní úrovni fungovat jako referenční bod a brána pro účast v evropském kybernetickém štítu a měla by zajistit, aby informace o kybernetických hrozbách od veřejných a soukromých subjektů byly na vnitrostátní úrovni sdíleny a shromažďovány účinně a efektivně.

(14) V rámci evropského kybernetického štítu by měla být zřízena řada přeshraničních operačních středisek v oblasti kybernetické bezpečnosti (dále jen „přeshraniční bezpečnostní operační střediska“). Ta by měla sdružovat národní bezpečnostní operační střediska alespoň ze tří členských států, aby bylo možné plně využít výhod přeshraničního odhalování hrozeb a sdílení a správy informací. Obecným cílem přeshraničních bezpečnostních operačních středisek by mělo být posílení kapacit pro analýzu, prevenci a odhalování kybernetických bezpečnostních hrozeb a podpora vytváření vysoce kvalitních zpravodajských informací o kybernetických bezpečnostních hrozbách, zejména prostřednictvím sdílení údajů z různých zdrojů, ať už veřejných nebo soukromých, jakož i prostřednictvím sdílení a společného využívání nejmodernějších nástrojů a společným rozvojem schopností odhalování, analýzy a prevence v důvěryhodném prostředí. Měla by poskytnout nové dodatečné kapacity, které budou vycházet ze stávajících bezpečnostních operačních středisek a týmů pro reakce na počítačové bezpečnostní incidenty (dále jen „týmy CSIRT“) a dalších příslušných subjektů a budou je doplňovat.

(15) Na vnitrostátní úrovni zajišťují monitorování, odhalování a analýzu kybernetických hrozeb obvykle bezpečnostní operační střediska veřejných a soukromých subjektů v kombinaci s týmy CSIRT. Kromě toho si týmy CSIRT vyměňují informace v rámci

[12] 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).

sítě CSIRT v souladu se směrnicí (EU) 2022/2555. Přeshraniční bezpečnostní operační střediska by měla představovat novou kapacitu, která doplní síť týmů pro reakce na kybernetické bezpečnostní incidenty, neboť bude sdružovat a sdílet údaje o kybernetických bezpečnostních hrozbách od veřejných a soukromých subjektů, zvyšovat hodnotu těchto údajů prostřednictvím odborné analýzy a společně pořízené infrastruktury a nejmodernějších nástrojů a přispívat k rozvoji schopností a technologické suverenity Unie.

(16) Přeshraniční bezpečnostní operační střediska by měla fungovat jako ústřední bod umožňující široké sdružování příslušných údajů a zpravodajských informací o kybernetických hrozbách, umožňovat šíření informací o hrozbách mezi velkým a různorodým souborem subjektů (např. týmy pro reakci na počítačové hrozby (dále jen „týmy CERT“), týmy CSIRT, střediska pro sdílení a analýzu informací (dále jen „střediska ISAC“), provozovatelé kritických infrastruktur). Informace vyměňované mezi účastníky přeshraničního bezpečnostního operačního střediska mohou zahrnovat údaje ze sítí a čidel, zpravodajské informace o hrozbách, indikátory narušení a kontextualizované informace o incidentech, hrozbách a zranitelnostech. Přeshraniční bezpečnostní operační střediska by také měla uzavírat dohody o spolupráci s jinými přeshraničními bezpečnostními operačními středisky.

(17) Sdílené situační povědomí mezi příslušnými orgány je nezbytným předpokladem připravenosti a koordinace v celé Unii, pokud jde o významné 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. Doporučení (EU) 2017/1584 o koordinované reakci na rozsáhlé kybernetické bezpečnostní incidenty a krize se zabývá úlohou všech příslušných aktérů. Směrnice (EU) 2022/2555 rovněž připomíná povinnosti Komise v rámci mechanismu civilní ochrany Unie zřízeného rozhodnutím Evropského parlamentu a Rady 1313/2013/EU, jakož i povinnost poskytování analytických zpráv pro opatření integrovaného mechanismu pro politickou reakci na krize podle prováděcího rozhodnutí (EU) 2018/1993. V situacích, kdy přeshraniční bezpečnostní operační střediska získají informace týkající se potenciálního nebo probíhajícího rozsáhlého kybernetického bezpečnostního incidentu, by proto měla poskytnout příslušné informace síti EU-CyCLONe, síti CSIRT a Komisi. V závislosti na situaci mohou informace, které mají být sdíleny, zahrnovat zejména technické údaje, 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 sdílených informací.

(18) Subjekty, které se účastní evropského kybernetického štítu, by měly zajistit vysokou úroveň vzájemné interoperability, dle potřeby včetně interoperability týkající se formátů dat, taxonomie, nástrojů pro zpracování a analýzu dat a bezpečných komunikačních kanálů, minimální úrovně zabezpečení aplikační vrstvy, přehledu situačního povědomí a ukazatelů. Přijetí společné taxonomie a vypracování vzoru situačních zpráv pro popis technických příčin a dopadů kybernetických bezpečnostních incidentů by mělo zohlednit probíhající práce týkající se oznamování incidentů v souvislosti s prováděním směrnice (EU) 2022/2555.

(19) Aby byla umožněna rozsáhlá výměna údajů o kybernetických bezpečnostních hrozbách z různých zdrojů v důvěryhodném prostředí, měly by být subjekty zapojené

do evropského kybernetického štítu vybaveny nejmodernějšími a vysoce bezpečnými nástroji, zařízeními a infrastrukturami. Díky tomu by mělo být možné zlepšit schopnost kolektivního odhalování a včasného varování orgánů a příslušných subjektů, zejména s využitím nejnovějších technologií umělé inteligence a analýzy dat.

(20) Prostřednictvím shromažďování, sdílení a výměny údajů by měl evropský kybernetický štít posílit technologickou suverenitu Unie. Sdružování vysoce kvalitních kontrolovaných údajů by mělo rovněž přispět k rozvoji pokročilých technologií umělé inteligence a analýzy dat. Mělo by být usnadněno propojením evropského kybernetického štítu s celoevropskou infrastrukturou pro vysoce výkonnou výpočetní techniku zřízenou nařízením Rady (EU) 2021/1173[13].

(21) Evropský kybernetický štít je sice civilní projekt, pro komunitu kybernetické obrany by však mohly být přínosem větší civilní schopnosti v oblasti detekce a situačního povědomí vyvinuté k ochraně kritické infrastruktury. Přeshraniční bezpečnostní operační střediska by měla s podporou Komise a Evropského centra kompetencí pro kybernetickou bezpečnost (dále jen „ECCC“) a ve spolupráci s vysokým představitelem Unie pro zahraniční věci a bezpečnostní politiku (dále jen „vysoký představitel“) postupně vypracovat specializované protokoly a normy, které umožní spolupráci s komunitou kybernetické obrany, včetně prověřování a bezpečnostních podmínek. Vývoj evropského kybernetického štítu by měl být doprovázen úvahami umožňujícími budoucí spolupráci se sítěmi a platformami, které jsou odpovědné za sdílení informací v komunitě kybernetické obrany, a to v úzké spolupráci s vysokým představitelem.

(22) Sdílení informací mezi účastníky evropského kybernetického štítu by mělo být v souladu se stávajícími právními požadavky, zejména s právními předpisy Unie a vnitrostátními právními předpisy 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 nezbytné zpracování osobních údajů, 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.

(23) Aniž je dotčen článek 346 SFEU, měla by být výměna informací, které mají podle unijních nebo vnitrostátních předpisů důvěrnou povahu, omezena na údaje, které jsou relevantní a přiměřené účelu této výměny. Při výměnách informací by se měla zachovávat důvěrnost předmětných informací a chránit bezpečnost a obchodní zájmy dotčených subjektů, při plném respektování obchodního a podnikatelského tajemství.

(24) Vzhledem k rostoucím rizikům a počtu kybernetických incidentů, které postihují členské státy, je nezbytné zřídit nástroj krizové podpory, který zlepší odolnost Unie vůči významným a rozsáhlým kybernetickým bezpečnostním incidentům a doplní opatření členských států prostřednictvím mimořádné finanční podpory pro připravenost, reakci a okamžité obnovení základních služeb. Tento nástroj by měl umožnit rychlé nasazení pomoci za vymezených okolností a jasných podmínek a umožnit pečlivé sledování a hodnocení toho, jak byly zdroje využity. Ačkoli primární odpovědnost za předcházení kybernetickým bezpečnostním incidentům a krizím i za připravenost a odezvu na ně nesou i nadále členské státy, mechanismus pro

[13] Nařízení Rady (EU) 2021/1173 ze dne 13. července 2021, kterým se zřizuje společný podnik pro evropskou vysoce výkonnou výpočetní techniku a zrušuje nařízení (EU) 2018/1488 (Úř. věst. L 256, 19.7.2021, s. 3).

mimořádné události v kybernetické oblasti podporuje solidaritu mezi členskými státy v souladu s čl. 3 odst. 3 Smlouvy o Evropské unii („dále jen „SEU“).

(25) Mechanismus pro mimořádné události v kybernetické oblasti by měl členským státům poskytovat podporu doplňující jejich vlastní opatření a zdroje a další stávající možnosti podpory v případě reakce na významné a rozsáhlé kybernetické bezpečnostní incidenty a okamžité obnovy po nich, jako jsou služby poskytované Agenturou Evropské unie pro bezpečnost sítí a informací (dále jen „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 SEU, týmy rychlé reakce v kybernetickém prostoru v rámci stálé strukturované spolupráce[14] a hybridní týmy rychlé reakce. 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.

(26) Tímto nástrojem nejsou dotčeny postupy a rámce pro koordinaci reakce na krize na úrovni Unie, zejména mechanismus civilní ochrany Unie[15], integrovaná opatření EU pro politickou reakci na krize[16,] a směrnice (EU) 2022/2555. Může přispívat k opatřením prováděným v souvislosti s čl. 42 odst. 7 SEU nebo v situacích vymezených v článku 222 SFEU nebo tato opatření doplňovat. Používání tohoto nástroje by mělo být v případě potřeby koordinováno s prováděním opatření souboru nástrojů kybernetické diplomacie.

(27) Pomoc poskytovaná podle tohoto nařízení by měla podporovat a doplňovat opatření přijatá členskými státy na vnitrostátní úrovni. Za tímto účelem by měla být zajištěna úzká spolupráce a konzultace mezi Komisí a dotčeným členským státem. Při žádosti o podporu v rámci mechanismu pro mimořádné události v kybernetické oblasti by měl členský stát poskytnout relevantní informace, které odůvodňují potřebu podpory.

(28) 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 kapacity, 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 pověřeny odpovědností 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 kybernetické oblasti by měl poskytovat pomoc při opatřeních zaměřených na posílení připravenosti, jakož i při opatřeních v reakci na incidenty s

---

14 ROZHODNUTÍ RADY (SZBP) 2017/2315 ze dne 11. prosince 2017, kterým se zřizuje stálá strukturovaná spolupráce a stanoví seznam zúčastněných členských států.

15 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).

16 Integrovaná opatření EU pro politickou reakci na krize (IPCR) a v souladu s doporučením Komise (EU) 2017/1584 ze dne 13. září 2017 o koordinované reakci na rozsáhlé kybernetické bezpečnostní incidenty a krize.

cílem zmírnit dopady významných a rozsáhlých kybernetických bezpečnostních incidentů, podpořit okamžitou obnovu a/nebo obnovit fungování základních služeb.

(29) V rámci opatření v oblasti připravenosti by měla být v zájmu 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. Za tímto účelem by měla Komise s podporou agentury ENISA a ve spolupráci se skupinou pro spolupráci v oblasti bezpečnosti sítí a informací zřízenou směrnicí (EU) 2022/2555 pravidelně určovat příslušná odvětví nebo pododvětví, která by měla být způsobilá pro získání finanční podpory na koordinované testování na úrovni Unie. Odvětví nebo pododvětví by měla být vybrána z přílohy I směrnice (EU) 2022/2555 (dále jen „vysoce kritická odvětví“). Koordinované testování by mělo být založeno na společných scénářích a metodikách týkajících se rizik. Výběr odvětví a vypracování rizikových scénářů by měly zohlednit příslušná hodnocení rizik a scénáře rizik pro celou Unii, včetně potřeby vyhnout se zdvojování, jako jsou hodnocení rizik a rizikové scénáře, které požaduje Rada v závěrech o rozvoji kybernetické pozice Evropské unie, které mají provádět Komise, vysoký představitel a skupina pro spolupráci v oblasti bezpečnosti sítí a informací 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 v oblasti bezpečnosti sítí a informací za podpory Komise a agentury ENISA a ve spolupráci se Sdružením evropských regulačních orgánů v oblasti elektronických komunikací (dále jen „BEREC“), koordinované posouzení rizik, 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[17]. Výběr odvětví by měl rovněž zohlednit doporučení Rady o celounijním koordinovaném přístupu za účelem posílení odolnosti kritické infrastruktury.

(30) Mechanismus pro mimořádné události v kybernetické oblasti by měl navíc nabízet podporu pro další opatření v oblasti připravenosti a podporovat připravenost v jiných odvětvích, na něž se nevztahuje koordinované testování subjektů působících ve vysoce kritických odvětvích. Tato opatření by mohla zahrnovat různé typy činností v oblasti vnitrostátní připravenosti.

(31) Mechanismus pro mimořádné události v kybernetické oblasti by měl poskytovat podporu pro opatření v reakci na incidenty s cílem zmírnit dopady významných a rozsáhlých kybernetických bezpečnostních incidentů, podpořit okamžitou 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 kybernetických incidentů na občany.

(32) Mechanismus pro mimořádné události v kybernetické oblasti by měl podporovat pomoc poskytovanou členskými státy členskému státu, který je postižen významným nebo rozsáhlým kybernetickým bezpečnostním incidentem, a to i prostřednictvím sítě CSIRT podle článku 15 směrnice (EU) 2022/2555. Členské státy poskytující pomoc by měly mít možnost předkládat žádosti o úhradu nákladů spojených s vysláním týmů

[17] 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.

odborníků v rámci vzájemné pomoci. Způsobilé náklady mohou zahrnovat cestovní výdaje, výdaje na ubytování a denní příspěvky pro odborníky na kybernetickou bezpečnost.

(33) Postupně by měla být zřízena rezerva pro kybernetickou bezpečnost na úrovni Unie, která by se skládala ze služeb soukromých poskytovatelů řízených bezpečnostních služeb na podporu reakce a okamžité obnovy v případě významných nebo rozsáhlých kybernetických bezpečnostních incidentů. Rezerva EU pro kybernetickou bezpečnost by měla zajistit dostupnost a připravenost služeb. Služby rezervy EU pro kybernetickou bezpečnost by měly sloužit jako podpora vnitrostátním orgánům při poskytování pomoci postiženým subjektům působícím v kritických nebo vysoce kritických odvětvích jako doplněk jejich vlastních opatření na vnitrostátní úrovni. Při žádosti o podporu z rezervy EU pro kybernetickou bezpečnost by členské státy měly upřesnit, jaká podpora byla dotčenému subjektu poskytnuta na vnitrostátní úrovni, a tato podpora by měla být zohledněna při posuzování žádosti členského státu. Služby rezervy EU pro kybernetickou bezpečnost mohou za podobných podmínek sloužit také na podporu orgánů, institucí nebo jiných subjektů Unie.

(34) Pro účely výběru soukromých poskytovatelů služeb, kteří budou poskytovat služby v rámci rezervy EU pro kybernetickou bezpečnost, je nezbytné stanovit soubor minimálních kritérií, která by měla být zahrnuta do výzvy k podávání nabídek za účelem výběru těchto poskytovatelů, aby bylo zajištěno naplnění potřeb orgánů členských států a subjektů působících v kritických nebo vysoce kritických odvětvích.

(35) Na podporu zřízení rezervy EU pro kybernetickou bezpečnost by Komise mohla zvážit možnost požádat agenturu ENISA, aby připravila systém certifikace podle nařízení (EU) 2019/881 pro řízené bezpečnostní služby v oblastech, na které se vztahuje mechanismus pro mimořádné události v kybernetické oblasti.

(36) V zájmu podpory cílů tohoto nařízení, kterými jsou podpora sdíleného situačního povědomí, zvýšení odolnosti Unie a umožnění účinné reakce na významné a rozsáhlé kybernetické bezpečnostní incidenty, měly by mít síť EU-CyCLONe, síť CSIRT nebo Komise možnost požádat agenturu ENISA o přezkum a posouzení hrozeb, zranitelností a opatření ke zmírnění dopadů v souvislosti s konkrétním významným nebo rozsáhlým kybernetickým bezpečnostním incidentem. Po dokončení přezkumu a posouzení incidentu by agentura ENISA měla ve spolupráci s příslušnými zúčastněnými stranami, včetně zástupců soukromého sektoru, členských států, Komise a dalších příslušných orgánů, institucí a jiných subjektů EU, vypracovat zprávu o přezkumu incidentu. Pokud jde o soukromý sektor, agentura ENISA buduje cesty pro výměnu informací se specializovanými poskytovateli, včetně poskytovatelů řízených bezpečnostních řešení a prodejců, s cílem přispět k poslání agentury ENISA, kterým je dosáhnout vysoké společné úrovně kybernetické bezpečnosti v celé Unii. Na základě spolupráce se zúčastněnými stranami, včetně soukromého sektoru, by se zpráva o přezkumu konkrétních incidentů měla zaměřit na posouzení příčin, dopadů 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 dle požadavků tohoto nařízení. Zpráva by měla být předložena síti EU-CyCLONe, síti CSIRT a Komisi a měla by být využita při jejich činnosti. Pokud se incident týká třetí země, předá Komise zprávu také vysokému představiteli.

(37) S ohledem na nepředvídatelnou povahu kybernetických bezpečnostních útoků a skutečnost, že se často neomezují na určitou zeměpisnou oblast a představují vysoké

riziko přelévání, přispívá posílení odolnosti sousedních zemí a jejich schopnosti účinně reagovat na významné a rozsáhlé kybernetické bezpečnostní incidenty k ochraně Unie jako celku. Třetí země přidružené k programu Digitální Evropa proto mohou být podpořeny z rezervy EU pro kybernetickou bezpečnost, je-li to stanoveno v příslušné dohodě o přidružení k programu Digitální Evropa. Financování přidružených třetích zemí 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 nebo rozsáhlé kybernetické bezpečnostní incidenty a okamžité obnovy po těchto incidentech. 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.

(38) Za účelem zajištění jednotných podmínek k provedení tohoto nařízení by měly být Komisi svěřeny prováděcí pravomoci, pokud jde o upřesnění podmínek interoperability mezi přeshraničními bezpečnostními operačními středisky; určení procesního režimu pro sdílení informací souvisejících s potenciálním nebo probíhajícím rozsáhlým kybernetickým bezpečnostním incidentem mezi přeshraničními bezpečnostními operačními středisky a subjekty Unie; stanovení technických požadavků na zajištění bezpečnosti evropského kybernetického štítu; specifikaci druhů a počtu služeb reakce požadovaných pro rezervu EU pro kybernetickou bezpečnost a další upřesnění podrobných 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.

(39) Cíle tohoto nařízení lze lépe dosáhnout na úrovni Unie než na úrovni členských států. Unie proto může přijmout opatření v souladu se zásadami subsidiarity a proporcionality stanovenými v článku 5 Smlouvy o Evropské unii. Toto nařízení nepřekračuje rámec toho, co je nezbytné pro dosažení tohoto cíle,

PŘIJALY TOTO NAŘÍZENÍ:

Kapitola I

OBECNÉ CÍLE, PŘEDMĚT A DEFINICE

Článek 1

Předmět a cíle

1. Tímto nařízením se stanoví opatření k posílení kapacit Unie pro odhalování kybernetických bezpečnostních hrozeb a incidentů, přípravu na ně a reakci na ně, zejména prostřednictvím těchto kroků:

a) zavedení celoevropské infrastruktury bezpečnostních operačních středisek („evropského kybernetického štítu“) s cílem vybudovat a posílit společné schopnosti odhalování a situačního povědomí;

b) vytvoření mechanismu pro mimořádné události v oblasti kybernetické bezpečnosti, který bude podporovat členské státy při přípravě na významné a rozsáhlé kybernetické bezpečnostní incidenty, při reakci na ně a při okamžité obnově po takových incidentech;

c) zřízení evropského mechanismu pro kybernetické bezpečnostní incidenty, který bude přezkoumávat a posuzovat významné nebo rozsáhlé incidenty.

2. Cílem tohoto nařízení je posílit solidaritu na úrovni Unie prostřednictvím těchto specifických cílů:

a) posílit společné odhalování kybernetických hrozeb a incidentů v Unii a situační povědomí v této oblasti, což umožní posílit konkurenceschopnost odvětví průmyslu a služeb v Unii v celé digitální ekonomice a přispět k technologické suverenitě Unie v oblasti kybernetické bezpečnosti;

b) posílit připravenost působících v kritických a vysoce kritických odvětvích v celé Unii a upevnit solidaritu vytvořením společných kapacit pro reakci na významné nebo rozsáhlé kybernetické bezpečnostní incidenty, včetně zpřístupnění podpory Unie při reakci na kybernetické bezpečnostní incidenty třetím zemím přidruženým k programu Digitální Evropa;

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

3. Tímto nařízením není dotčena prvořadá odpovědnost členských států v oblasti národní bezpečnosti, veřejné bezpečnosti a prevence, vyšetřování, odhalování a stíhání trestných činů.

Článek 2

Definice

Pro účely tohoto nařízení se rozumí:

(1) „**přeshraničním bezpečnostním operačním střediskem**“ platforma za účasti více zemí, která v koordinované síťové struktuře sdružuje národní bezpečnostní operační střediska z nejméně tří členských států, jež tvoří hostitelské konsorcium, a která je určena k předcházení kybernetickým hrozbám a incidentům a k podpoře vytváření vysoce kvalitních zpravodajských informací, zejména prostřednictvím výměny údajů z různých zdrojů, veřejných i soukromých, jakož i sdílením nejmodernějších nástrojů a společným vývojem schopností detekce, analýzy a prevence a ochrany v kybernetické oblasti v důvěryhodném prostředí;

(2) „**veřejnoprávním subjektem**“ veřejnoprávní subjekt ve smyslu čl. 2 odst. 1 bodu 4 směrnice Evropského parlamentu a Rady 2014/24/EU[18];

(3) **„hostitelským konsorciem**“ konsorcium složené ze zúčastněných států, zastoupených národními bezpečnostními operačními středisky, které souhlasily se

[18] 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).

zřízením nástrojů a infrastruktury pro přeshraniční bezpečnostní operační střediska a jejich provoz a s poskytnutím příspěvku na pořízení těchto nástrojů a infrastruktury;

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

(5) „**subjekty působícími v kritických nebo vysoce kritických odvětvích**“ druhy subjektů vyjmenované v příloze I a II směrnice (EU) 2022/2555;

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

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

(8) „**rozsáhlým kybernetickým bezpečnostním incidentem**“ incident ve smyslu čl. 6 bodu 7 směrnice (EU) 2022/2555;

(9) „**připraveností**“ stav připravenosti a schopnosti zajistit účinnou rychlou reakci na významný nebo rozsáhlý kybernetický bezpečnostní incident, který je výsledkem posouzení rizik a předem přijatých monitorovacích opatření;

(10) „**reakcí**“ opatření v případě významného nebo rozsáhlého kybernetického bezpečnostního incidentu nebo v průběhu takového incidentu či po něm, jehož cílem je řešit jeho okamžité a krátkodobé nepříznivé důsledky;

(11) „**důvěryhodnými poskytovateli**“ poskytovatelé řízených bezpečnostních služeb ve smyslu čl. 6 bodu 40 směrnice (EU) 2022/2555, kteří byli vybráni v souladu s článkem 16 tohoto nařízení.

Kapitola II

EVROPSKÝ KYBERNETICKÝ ŠTÍT

Článek 3

Zřízení evropského kybernetického štítu

1. Zřizuje se propojená celoevropská infrastruktura bezpečnostních operačních středisek (dále jen „evropský kybernetický štít“), která bude rozvíjet pokročilé schopnosti Unie odhalovat, analyzovat a zpracovávat údaje o kybernetických hrozbách a incidentech v Unii. Evropský kybernetický štít se skládá z národních bezpečnostních operačních středisek a přeshraničních bezpečnostních operačních středisek.

Akce, kterými se provádí evropský kybernetický štít, jsou podporovány z finančních prostředků programu Digitální Evropa a prováděny v souladu s nařízením (EU) 2021/694, a zejména s jeho specifickým cílem č. 3.

2. Evropský kybernetický štít:

a) shromažďuje a sdílí údaje o kybernetických hrozbách a incidentech z různých zdrojů prostřednictvím přeshraničních bezpečnostních operačních středisek;

b) vytváří vysoce kvalitní a použitelné informace a zpravodajské informace o kybernetických hrozbách s využitím nejmodernějších nástrojů, zejména technologie umělé inteligence a analýzy dat;

c) přispívá k lepší ochraně a reakci na kybernetické hrozby;

d) přispívá k rychlejšímu odhalování kybernetických hrozeb a k situačnímu povědomí v celé Unii;

e) poskytuje služby a činnosti pro komunitu kybernetické bezpečnosti v Unii, včetně přínosu k vývoji pokročilých nástrojů umělé inteligence a analýzy dat.

Je vyvíjen ve spolupráci s celoevropskou infrastrukturou pro vysoce výkonnou výpočetní techniku zřízenou podle nařízení (EU) 2021/1173.

Článek 4

Národní bezpečnostní operační střediska

1. Pro účast v evropském kybernetickém štítu určí každý členský stát alespoň jedno národní bezpečnostní operační středisko. Národní bezpečnostní operační středisko musí být veřejnoprávním subjektem.

Má kapacitu působit jako referenční bod a brána pro další veřejné a soukromé organizace na vnitrostátní úrovni, které shromažďují a analyzují informace o kybernetických bezpečnostních hrozbách a incidentech a přispívají k přeshraničnímu bezpečnostnímu operačnímu středisku. Je vybaveno nejmodernějšími technologiemi schopnými zjišťovat, agregovat a analyzovat údaje týkající se kybernetických bezpečnostních hrozeb a incidentů.

2. Na základě výzvy k vyjádření zájmu vybere Evropské centrum kompetencí pro kybernetickou bezpečnost (dále jen „ECCC“) národní bezpečnostní operační střediska, která se budou podílet na společném zadávání zakázek týkajících se nástrojů a infrastruktury s centrem ECCC. Centrum ECCC může vybraným národním bezpečnostním operačním střediskům udělit granty na financování provozu těchto nástrojů a infrastruktur. Finanční příspěvek Unie pokrývá až 50 % nákladů na pořízení nástrojů a infrastruktury a až 50 % nákladů na provoz, přičemž zbývající náklady hradí členský stát. Před zahájením řízení za účelem pořízení nástrojů a infrastruktur uzavřou centrum ECCC a národní bezpečnostní operační středisko dohodu o hostingu a užívání, která upravuje používání nástrojů a infrastruktur.

3. Národní bezpečnostní operační středisko vybrané podle odstavce 2 se zavazuje podat žádost o účast v přeshraničním bezpečnostním operačním středisku do dvou let ode dne, kdy získá nástroje a infrastrukturu, nebo kdy obdrží grantové financování, podle toho, co nastane dříve. Pokud se národní bezpečnostní operační středisko do té doby nestane účastníkem přeshraničního bezpečnostního operačního střediska, není způsobilé k další podpoře z Unie podle tohoto nařízení.

Článek 5

Přeshraniční bezpečnostní operační střediska

1. Hostitelské konsorcium složené z nejméně tří členských států zastoupených národními bezpečnostními operačními středisky, která se zavázala spolupracovat na koordinaci svých činností v oblasti detekce a monitorování kybernetických hrozeb, je způsobilé účastnit se činností za účelem zřízení přeshraničního bezpečnostního operačního střediska.

2. Na základě výzvy k vyjádření zájmu vybere centrum ECCC hostitelské konsorcium, které se bude podílet na společném zadávání zakázek týkajících se nástrojů a infrastruktury s centrem ECCC. Centrum ECCC může hostitelskému konsorciu udělit grant na financování provozu těchto nástrojů a infrastruktur. Finanční příspěvek Unie pokrývá až 75 % nákladů na pořízení nástrojů a infrastruktury a až 50 % nákladů na provoz, přičemž zbývající náklady hradí hostitelské konsorcium. Před zahájením řízení za účelem pořízení nástrojů a infrastruktur uzavřou centrum ECCC a hostitelské konsorcium dohodu o hostingu a užívání, která upravuje používání nástrojů a infrastruktur.

3. Členové hostitelského konsorcia uzavřou písemnou dohodu o konsorciu, která stanoví jejich vnitřní ujednání k provádění dohody o hostingu a užívání.

4. Přeshraniční bezpečnostní operační středisko je pro právní účely zastoupeno národním bezpečnostním operačním střediskem, které působí jako koordinující bezpečnostní operační středisko, nebo hostitelským konsorciem, má-li právní subjektivitu. Koordinující bezpečnostní operační středisko odpovídá za dodržování požadavků dohody o hostingu a užívání a tohoto nařízení.

Článek 6

Spolupráce a sdílení informací v rámci přeshraničních bezpečnostních operačních středisek a mezi nimi

1. Členové hostitelského konsorcia si v rámci přeshraničního bezpečnostního operačního střediska mezi sebou vyměňují relevantní informace, včetně informací týkajících se kybernetických hrozeb, případů, kdy téměř došlo k incidentu, zranitelností, technik a postupů, indikátorů narušení, nepřátelských taktik, informací specifických pro daný subjekt a danou hrozbu, varování při ohrožení kybernetické bezpečnosti a doporučení týkající se konfigurace nástrojů kybernetické bezpečnosti, které slouží k odhalování kybernetických útoků, pokud toto sdílení informací:

a) má za cíl předcházet incidentům, odhalovat je, reagovat na ně, zajišťovat následnou obnovu nebo zmírňovat jejich dopad;

b) zvyšuje úroveň kybernetické bezpečnosti, zejména 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 nebo fází reakce a obnovy nebo podporou společného výzkumu hrozeb ze strany subjektů veřejného a soukromého sektoru.

2. Písemná dohoda o konsorciu podle čl. 5 odst. 3 stanoví:

a) závazek sdílet významné množství údajů uvedených v odstavci 1 a podmínky, za nichž mají být tyto informace vyměňovány;

b) rámec řízení, který všechny účastníky motivuje ke sdílení informací;

c) cíle pro přispění k vývoji pokročilých nástrojů umělé inteligence a analýzy dat.

3. S cílem povzbudit výměnu informací mezi přeshraničními bezpečnostními operačními středisky zajistí přeshraniční bezpečnostní operační střediska vysokou úroveň vzájemné interoperability. Aby usnadnila interoperabilitu mezi přeshraničními bezpečnostními operačními středisky, může Komise prostřednictvím prováděcích aktů po konzultaci s centrem ECCC stanovit podmínky této interoperability. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 21 odst. 2 tohoto nařízení.

4. Přeshraniční bezpečnostní operační střediska mezi sebou uzavřou dohody o spolupráci, v nichž stanoví zásady sdílení informací mezi přeshraničními platformami.

Článek 7

Spolupráce a sdílení informací se subjekty Unie

1. Pokud přeshraniční bezpečnostní operační střediska získají informace týkající se potenciálního nebo probíhajícího rozsáhlého kybernetického bezpečnostního incidentu, poskytnou neprodleně příslušné informace síti EU-CyCLONe, síti CSIRT a Komisi s ohledem na jejich příslušné úlohy v oblasti řešení krizí v souladu se směrnicí (EU) 2022/2555.

2. Komise může prostřednictvím prováděcích aktů stanovit procesní opatření pro sdílení informací podle odstavce 1. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 21 odst. 2 tohoto nařízení.

Článek 8

Zabezpečení

1. Členské státy, které se účastní evropského kybernetického štítu, zajistí vysokou úroveň bezpečnosti údajů a fyzické bezpečnosti infrastruktury evropského kybernetického štítu a zabezpečí, aby byla infrastruktura přiměřeně spravována a kontrolována tak, aby byla chráněna před hrozbami a aby byla zajištěna její bezpečnost a bezpečnost systémů, včetně bezpečnosti údajů vyměňovaných prostřednictvím této infrastruktury.

2. Členské státy, které se účastní evropského kybernetického štítu, zajistí, aby sdílení informací v rámci evropského kybernetického štítu se subjekty, které nejsou veřejnoprávními subjekty členského státu, nemělo negativní dopad na bezpečnostní zájmy Unie.

3. Komise může přijmout prováděcí akty, kterými stanoví technické požadavky na členské státy při plnění jejich povinností podle odstavců 1 a 2. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 21 odst. 2 tohoto nařízení. Komise přitom za podpory vysokého představitele zohlední příslušné normy zabezpečení na úrovni obrany, aby usnadnila spolupráci s vojenskými subjekty.

Kapitola III

MECHANISMUS PRO MIMOŘÁDNÉ UDÁLOSTI V KYBERNETICKÉ OBLASTI

Článek 9

Zřízení mechanismu pro mimořádné události v kybernetické oblasti

1. Zřizuje se mechanismus pro mimořádné události v kybernetické oblasti s cílem zlepšit odolnost Unie vůči zásadním hrozbám v oblasti kybernetické bezpečnosti, připravit se na krátkodobé dopady významných a rozsáhlých kybernetických bezpečnostních incidentů nebo krizí a v duchu solidarity je zmírňovat (dále jen „mechanismus“).

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

Článek 10

Druhy opatření

1. Mechanismus podporuje tyto druhy opatření:

a) opatření v oblasti připravenosti, včetně koordinovaného testování připravenosti subjektů působících ve vysoce kritických odvětvích v celé Unii;

b) opatření reakce, která podporují reakci na významné a rozsáhlé kybernetické bezpečnostní incidenty a okamžitou obnovu po nich a která mají poskytovat důvěryhodní poskytovatelé zapojení do rezervy EU pro kybernetickou bezpečnost zřízené podle článku 12;

c) opatření vzájemné pomoci spočívající v poskytování pomoci vnitrostátními orgány jednoho členského státu jinému členskému státu, zejména podle čl. 11 odst. 3 písm. f) směrnice (EU) 2022/2555.

Článek 11

Koordinované testování připravenosti subjektů

1. Za účelem podpory koordinovaného testování připravenosti subjektů uvedených v čl. 10 odst. 1 písm. a) v celé Unii určí Komise po konzultaci se skupinou pro spolupráci v oblasti bezpečnosti sítí a informací a agenturou ENISA dotčená odvětví nebo pododvětví z vysoce kritických odvětví vyjmenovaných v příloze I směrnice (EU) 2022/2555, v nichž mohou být subjekty podrobeny koordinovanému testování připravenosti, přičemž zohlední stávající a plánovaná koordinovaná posouzení rizik a testování odolnosti na úrovni Unie.

2. Skupina pro spolupráci v oblasti bezpečnosti sítí a informací ve spolupráci s Komisí, agenturou ENISA a vysokým představitelem vypracuje společné rizikové scénáře a metodiky pro koordinované testování.

Článek 12

Zřízení rezervy EU pro kybernetickou bezpečnost

1. Zřizuje se rezerva EU pro kybernetickou bezpečnost, která má uživatelům uvedeným v odstavci 3 pomáhat při reakci nebo při poskytování podpory reakci na významné nebo rozsáhlé kybernetické bezpečnostní incidenty a při okamžité obnově po těchto incidentech.

2. Rezerva EU pro kybernetickou bezpečnost se skládá ze služeb reakce na incidenty od důvěryhodných poskytovatelů vybraných v souladu s kritérii stanovenými v článku 16. Rezerva zahrnuje předem přislíbené služby. Služby musí být možné provádět ve všech členských státech.

3. K uživatelům služeb z rezervy EU pro kybernetickou bezpečnost patří:

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) orgány, instituce nebo jiné subjekty Unie.

4. Uživatelé uvedení v odst. 3 písm. a) využívají služby rezervy EU pro kybernetickou bezpečnost k reakci nebo k podpoře reakce na významné nebo rozsáhlé incidenty, které postihují subjekty působící v kritických nebo vysoce kritických odvětvích, a k okamžité obnově po těchto incidentech.

5. Komise nese celkovou odpovědnost za provádění rezervy EU pro kybernetickou bezpečnost. Komise určí priority a vývoj rezervy EU pro kybernetickou bezpečnost v souladu s požadavky uživatelů uvedenými v odstavci 3, dohlíží na její provádění a zajišťuje doplňkovost, jednotnost, synergie a vazby s dalšími podpůrnými opatřeními podle tohoto nařízení i s jinými opatřeními a programy Unie.

6. Komise může provozem a správou rezervy EU pro kybernetickou bezpečnost plně nebo zčásti pověřit agenturu ENISA, a to prostřednictvím dohod o příspěvcích.

7. S cílem podpořit Komisi při zřizování rezervy EU pro kybernetickou bezpečnost vypracuje agentura ENISA po konzultaci s členskými státy a Komisí mapování potřebných služeb. Agentura ENISA po konzultaci s Komisí připraví podobné mapování, aby určila potřeby třetích zemí způsobilých pro podporu z rezervy EU pro kybernetickou bezpečnost podle článku 17. Komise dle potřeby konzultuje s vysokým představitelem.

8. Komise může prostřednictvím prováděcích aktů specifikovat druhy a počet služeb reakce požadovaných pro rezervu EU pro kybernetickou bezpečnost. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 21 odst. 2.

Článek 13

Žádosti o podporu z rezervy EU pro kybernetickou bezpečnost

1. Uživatelé uvedení v čl. 12 odst. 3 mohou požádat o služby z rezervy EU pro kybernetickou bezpečnost na podporu reakce na významné nebo rozsáhlé kybernetické bezpečnostní incidenty a okamžité obnovy po nich.

2. Aby uživatelé uvedení v čl. 12 odst. 3 mohli získat podporu z rezervy EU pro kybernetickou bezpečnost, musí přijmout opatření ke zmírnění dopadů incidentu, pro který je podpora požadována, včetně poskytnutí přímé technické pomoci a dalších zdrojů na pomoc při reakci na incident a při okamžité obnově.

3. Žádosti o podporu podané uživateli uvedenými v čl. 12 odst. 3 písm. a) tohoto nařízení se předávají Komisi a agentuře ENISA prostřednictvím jednotného kontaktního místa určeného nebo zřízeného členským státem v souladu s čl. 8 odst. 3 směrnice (EU) 2022/2555.

4. Členské státy informují síť CSIRT, případně síť EU-CyCLONe o svých žádostech o podporu reakce na incidenty a okamžité obnovy podle tohoto článku.

5. Žádosti o podporu reakce na incident a okamžité obnovy uvádějí:

a) příslušné informace týkající se dotčeného subjektu a možných dopadů incidentu a plánovaného využití požadované podpory, včetně uvedení odhadovaných potřeb;

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

c) informace o dalších formách podpory, které má postižený subjekt k dispozici, včetně existujících smluvních ujednání o službách reakce na incident a okamžité obnovy, jakož i o pojistných smlouvách, které by mohly pokrývat tento druh incidentu.

6. Agentura ENISA ve spolupráci s Komisí a skupinou pro spolupráci v oblasti bezpečnosti sítí a informací vypracuje šablonu, která usnadní podávání žádostí o podporu z rezervy EU pro kybernetickou bezpečnost.

7. Komise může prostřednictvím prováděcích aktů dále upřesnit podrobná opatření pro přidělování podpůrných služeb z rezervy EU pro kybernetickou bezpečnost. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 21 odst. 2.

Článek 14

Provádění podpory z rezervy EU pro kybernetickou bezpečnost

1. Komise za pomoci agentury ENISA nebo jak je stanoveno v dohodách o příspěvku podle čl. 12 odst. 6 posoudí žádosti o podporu z rezervy EU pro kybernetickou bezpečnost a odpověď neprodleně předá uživatelům uvedeným v čl. 12 odst. 3.

2. Při určování pořadí přednosti žádostí se v případě více souběžných žádostí zohlední případně tato kritéria:

a) závažnost kybernetického bezpečnostního incidentu;

b) druh dotčeného subjektu, přičemž vyšší přednost mají incidenty, které mají vliv na základní subjekty ve smyslu čl. 3 odst. 1 směrnice (EU) 2022/2555;

c) potenciální dopad na dotčený členský stát (dotčené členské státy) nebo uživatele;

d) potenciální přeshraniční povaha incidentu a riziko přelévání do jiných členských států nebo k jiným uživatelům;

e) opatření přijatá uživatelem na pomoc při reakci a okamžité obnově podle čl. 13 odst. 2 a čl. 13 odst. 5 písm. b).

3. Služby rezervy EU pro kybernetickou bezpečnost se poskytují v souladu se zvláštními dohodami mezi poskytovatelem služeb a uživatelem, kterému je poskytnuta podpora z rezervy EU pro kybernetickou bezpečnost. Tyto dohody musí obsahovat podmínky odpovědnosti.

4. Dohody uvedené v odstavci 3 mohou vycházet ze vzorů, které vypracuje agentura ENISA po konzultaci s členskými státy.

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

6. Do jednoho měsíce od ukončení podpůrné akce předloží uživatelé Komisi a agentuře ENISA souhrnnou zprávu o poskytnuté službě, dosažených výsledcích a získaných poznatcích. Je-li uživatel ze třetí země podle článku 17, je tato zpráva sdílena s vysokým představitelem.

7. Komise podává skupině pro spolupráci v oblasti bezpečnosti sítí a informací pravidelné zprávy o využívání podpory a jejích výsledcích.

Článek 15

Koordinace s mechanismy pro řešení krizí

1. V případech, kdy významné nebo rozsáhlé incidenty v oblasti kybernetické bezpečnosti vzniknou v důsledku katastrof nebo vedou ke katastrofám ve smyslu rozhodnutí 1313/2013/EU[19], podpora podle tohoto nařízení pro reakci na takové incidenty doplňuje činnosti podle rozhodnutí 1313/2013/EU a tyto činností jí nejsou dotčeny.

2. V případě rozsáhlého přeshraničního kybernetického bezpečnostního incidentu, kdy jsou spuštěna integrovaná opatření EU pro politickou reakci na krize (dále jen „IPCR“), se podpora podle tohoto nařízení pro reakci na takový incident řeší v souladu s příslušnými protokoly a postupy podle IPCR.

3. Po konzultaci s vysokým představitelem může podpora v rámci mechanismu pro mimořádné události v kybernetické oblasti doplňovat pomoc poskytovanou v rámci společné zahraniční a bezpečnostní politiky a společné bezpečnostní a obranné politiky, a to i prostřednictvím týmů rychlé kybernetické reakce. Může rovněž doplňovat pomoc poskytovanou jedním členským státem jinému členskému státu na základě čl. 42 odst. 7 Smlouvy o Evropské unii nebo k této pomoci přispívat.

4. Podpora v rámci mechanismu pro mimořádné události v kybernetické oblasti může být součástí společné reakce Unie a členských států v situacích podle článku 222 Smlouvy o fungování Evropské unie.

Článek 16

Důvěryhodní poskytovatelé

[19] 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).

1. Při zadávání veřejných zakázek za účelem zřízení rezervy EU pro kybernetickou bezpečnost postupuje veřejný zadavatel v souladu se zásadami stanovenými v nařízení (EU, Euratom) 2018/1046 a v souladu s těmito zásadami:

a) zajistit, 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 certifikace nebo akreditace;

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

c) zajistit, aby rezerva EU pro kybernetickou bezpečnost přinášela EU 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 EU.

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

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

b) poskytovatel, jeho dceřiné společnosti a subdodavatelé mají zaveden rámec pro ochranu citlivých informací týkajících se služby, zejména důkazů, zjištění a zpráv, a dodržují bezpečnostní předpisy Unie týkající se ochrany utajovaných informací EU;

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

d) poskytovatel má odpovídající bezpečnostní prověrku, alespoň pro pracovníky určené k nasazení v dané službě;

e) poskytovatel má odpovídající úroveň zabezpečení svých IT systémů;

f) poskytovatel je vybaven hardwarovým a softwarovým technickým zařízením nezbytným pro podporu požadované služby;

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

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

i) poskytovatel je schopen poskytnout službu v místním jazyce členského státu / členských států, v němž/nichž může službu poskytovat;

j) jakmile bude zaveden systém certifikace EU pro řízené bezpečnostní služby podle nařízení (EU) 2019/881, bude poskytovatel certifikován v souladu s tímto systémem.

Článek 17

Podpora pro třetí země

1. Třetí země mohou požádat o podporu z rezervy EU pro kybernetickou bezpečnost, pokud to stanoví dohody o přidružení týkající se jejich účasti v programu Digitální Evropa.

2. Podpora z rezervy EU pro kybernetickou bezpečnost musí být v souladu s tímto nařízením a musí splňovat veškeré zvláštní podmínky stanovené v dohodách o přidružení uvedených v odstavci 1.

3. K uživatelům z přidružených třetích zemí, kteří jsou způsobilí získat služby z rezervy EU pro kybernetickou bezpečnost, patří příslušné orgány, jako jsou týmy CSIRT a orgány pro řešení kybernetických krizí.

4. Každá třetí země způsobilá k podpoře z rezervy EU pro kybernetickou bezpečnost určí orgán, který bude pro účely tohoto nařízení působit jako jednotné kontaktní místo.

5. Před obdržením jakékoli podpory z rezervy EU pro kybernetickou bezpečnost poskytnou třetí země Komisi a vysokému představiteli informace o svých schopnostech v oblasti kybernetické odolnosti a řízení rizik, alespoň včetně informací o vnitrostátních opatřeních přijatých za účelem přípravy na významné nebo rozsáhlé kybernetické bezpečnostní incidenty, jakož i informací o odpovědných vnitrostátních subjektech, včetně týmů CSIRT nebo rovnocenných subjektů, jejich schopnostech a zdrojích, které jim byly přiděleny. Pokud ustanovení článků 13 a 14 tohoto nařízení odkazují na členské státy, vztahují se na třetí země podle odstavce 1.

6. Komise s vysokým představitelem koordinuje činnost týkající se obdržených žádostí a provádění podpory poskytované třetím zemím z rezervy EU pro kybernetickou bezpečnost.

Kapitola IV

MECHANISMUS PŘEZKUMU KYBERNETICKÝCH BEZPEČNOSTNÍCH INCIDENTŮ

Článek 18

Mechanismus přezkumu kybernetických bezpečnostních incidentů

1. Na žádost Komise, sítě EU-CyCLONe nebo sítě CSIRT agentura ENISA přezkoumá a posoudí hrozby, zranitelná místa a opatření ke zmírnění dopadů v souvislosti s konkrétním významným nebo rozsáhlým kybernetickým bezpečnostním incidentem. Po dokončení přezkumu a posouzení incidentu předá agentura ENISA síti CSIRT, síti EU-CyCLONe a Komisi zprávu o přezkumu incidentu, aby je podpořila při plnění jejich úkolů, zejména s ohledem na úkoly stanovené v článcích 15 a 16 směrnice (EU) 2022/2555. V případě potřeby Komise sdílí zprávu s vysokým představitelem.

2. Při přípravě zprávy o přezkumu incidentů podle odstavce 1 agentura ENISA spolupracuje se všemi příslušnými zúčastněnými stranami, včetně zástupců členských států, Komise, dalších příslušných orgánů, institucí a jiných subjektů EU, poskytovatelů řízených bezpečnostních služeb a uživatelů služeb kybernetické bezpečnosti. Agentura ENISA v případě potřeby spolupracuje také se subjekty, které byly zasaženy významnými nebo rozsáhlými kybernetickými bezpečnostními incidenty. Na podporu přezkumu může agentura ENISA konzultovat i další typy zúčastněných stran. Konzultovaní zástupci oznámí jakýkoli případný střet zájmů.

3. Zpráva zahrnuje přezkum a analýzu konkrétního významného nebo rozsáhlého kybernetického bezpečnostního incidentu, včetně hlavních příčin, zranitelností a získaných

zkušeností. Chrání důvěrné informace v souladu s právem Unie nebo vnitrostátním právem týkajícím se ochrany citlivých nebo utajovaných údajů.

4. Dle potřeby zpráva uvádí doporučení ke zlepšení kybernetické pozice Unie.

5. Pokud je to možné, zpřístupní se určitá verze zprávy veřejnosti. Tato verze obsahuje pouze veřejné informace.

Kapitola V

ZÁVĚREČNÁ USTANOVENÍ

Článek 19

Změny nařízení (EU) 2021/694

Nařízení (EU) 2021/694 se mění takto:

1) článek 6 se mění takto:

a) odstavec 1 se mění takto:

1) vkládá se nové písmeno aa), které zní:

„aa) podporovat rozvoj kybernetického štítu EU, včetně vývoje, zavádění a provozu národních a přeshraničních platforem bezpečnostních operačních středisek, které přispívají k situačnímu povědomí v Unii a k posílení zpravodajských kapacit Unie v oblasti kybernetických hrozeb“;

2) doplňuje se nové písmeno g), které zní:

„g) zřídit a provozovat mechanismus pro mimořádné události v kybernetické oblasti na podporu členských států při přípravě na významné kybernetické bezpečnostní incidenty a při reakci na ně, který doplní vnitrostátní zdroje a kapacity a další formy podpory dostupné na úrovni Unie, včetně zřízení rezervy EU pro kybernetickou bezpečnost“;

a) 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[20], s výjimkou opatření, kterými se provádí rezerva EU pro kybernetickou bezpečnost, jež provádí Komise a agentura ENISA.“;

2) článek 9 se mění takto:

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

„b) 1 776 956 000 EUR pro specifický cíl č. 2 Umělá inteligence;

c) 1 629 566 000 EUR pro specifický cíl č. 3 Kybernetická bezpečnost a důvěra;

d) 482 347 000 EUR pro specifický cíl č. 4 Pokročilé digitální dovednosti“;

b) doplňuje se nový odstavec 8, který zní:

„8. Odchylně od čl. 12 odst. 4 nařízení (EU, Euratom) 2018/1046 se nevyužité prostředky na závazky a platby na akce sledující 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.“;

3) 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[27] a 2014/25/EU[28].

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 pro rezervu EU pro kybernetickou bezpečnost zřízenou článkem 12 nařízení (EU) 2023/XX 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. Komise a agentura ENISA mohou rovněž působit jako velkoobchodníci a nakupovat, skladovat nebo darovat dodávky a

[20] 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).

služby pro tyto třetí země, včetně pronájmu. Odchylně od čl. 169 odst. 3 nařízení (EU) XXX/XXXX [přepracované znění] postačuje k pověření Komise nebo agentury ENISA jednáním žádost jediné třetí země.

Při provádění zadávacích řízení pro rezervu EU pro kybernetickou bezpečnost zřízenou článkem 12 nařízení (EU) 2023/XX 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 nebo darovat dodávky a služby pro orgány, instituce nebo jiné subjekty Unie, včetně pronájmu. Odchylně od čl. 169 odst. 3 nařízení (EU) XXX/XXXX [přepracované znění] 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.“;

4) vkládá se nový článek 16a, který zní:

„V případě opatření, kterými se provádí evropský kybernetický štít zřízený článkem 3 nařízení (EU) 2023/XX, se použijí pravidla stanovená v článcích 4 a 5 nařízení (EU) 2023/XX. V případě rozporu mezi ustanoveními tohoto nařízení a články 4 a 5 nařízení (EU) 2023/XX jsou tato jiná pravidla pro tyto konkrétní akce rozhodná a použijí se.“;

5) článek 19 se nahrazuje tímto:

„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 národním bezpečnostním operačním střediskům podle článku 4 nařízení XXXX a hostitelskému konsorciu podle článku 5 nařízení XXXX přímo centrum ECCC bez výzvy k předkládání návrhů.

Podporu v podobě grantů pro mechanismus pro mimořádné události v kybernetické oblasti podle článku 10 nařízení XXXX může v souladu s čl. 195 odst. 1 písm. d) finančního nařízení udělovat členským státům přímo centrum ECCC bez výzvy k předkládání návrhů.

U akcí uvedených v čl. 10 odst. 1 písm. c) nařízení 202X/XXXX informuje centrum ECCC Komisi a agenturu ENISA o žádostech členských států o přímé granty bez výzvy k předkládání návrhů.

V případě podpory vzájemné pomoci při reakci na významný nebo rozsáhlý kybernetický bezpečnostní incident ve smyslu čl. 10 písm. c) nařízení XXXX 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.“;

6) přílohy I a II se mění v souladu s přílohou tohoto nařízení.

Článek 20

Hodnocení

Do [čtyř let ode dne použitelnosti tohoto nařízení] předloží Komise Evropskému parlamentu a Radě zprávu o hodnocení a přezkumu tohoto nařízení.

Článek 21

Postup projednávání ve výborech

1. Komisi je nápomocen koordinační výbor programu Digitální Evropa zřízený nařízením (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 22

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.

Ve Štrasburku dne

Za Evropský parlament
předseda/předsedkyně

Za Radu
předseda/předsedkyně

LEGISLATIVNÍ FINANČNÍ VÝKAZ

1. RÁMEC NÁVRHU/PODNĚTU

1.1. Název návrhu/podnětu

1.2. Příslušné oblasti politik

1.3. Návrh/podnět se týká:

1.4. Cíle

1.4.1. Obecné cíle

1.4.2. Specifické cíle

1.4.3. Očekávané výsledky a dopad

1.4.4. Ukazatele výkonnosti

1.5. Odůvodnění návrhu/podnětu

1.5.1. Požadavky, které mají být splněny v krátkodobém nebo dlouhodobém horizontu, včetně podrobného časového harmonogramu zavedení iniciativy

1.5.2. Přidaná hodnota ze zapojení Unie (může být důsledkem různých faktorů, např. přínosů z koordinace, právní jistoty, vyšší účinnosti nebo doplňkovosti). Pro účely tohoto bodu se „přidanou hodnotou ze zapojení Unie“ rozumí hodnota plynoucí ze zásahu Unie, jež doplňuje hodnotu, která by jinak vznikla činností samotných členských států.

1.5.3. Závěry vyvozené z podobných zkušeností v minulosti

1.5.4. Slučitelnost s víceletým finančním rámcem a možné synergie s dalšími vhodnými nástroji

1.5.5. Posouzení různých dostupných možností financování, včetně prostoru pro přerozdělení prostředků

1.6. Doba trvání a finanční dopad návrhu/podnětu

1.7. Předpokládaný způsob plnění rozpočtu

2. SPRÁVNÍ OPATŘENÍ

2.1. Pravidla pro sledování a podávání zpráv

2.2. Systémy řízení a kontroly

2.2.1. Odůvodnění navrhovaných způsobů řízení, mechanismů provádění financování, způsobů plateb a kontrolní strategie

2.2.2. Informace o zjištěných rizicích a systémech vnitřní kontroly zřízených k jejich zmírnění

2.2.3. Odhad a odůvodnění nákladové efektivnosti kontrol (poměr „náklady na kontroly ÷ hodnota souvisejících spravovaných finančních prostředků“) a posouzení očekávané míry rizika výskytu chyb (při platbě a při uzávěrce)

2.3. Opatření k zamezení podvodů a nesrovnalostí

3. ODHADOVANÝ FINANČNÍ DOPAD NÁVRHU/PODNĚTU

1. RÁMEC NÁVRHU/PODNĚTU

1.1. Název návrhu/podnětu

Nařízení Evropského parlamentu a Rady, kterým se stanoví opatření k posílení solidarity a kapacit v Unii pro odhalování hrozeb a incidentů v oblasti kybernetické bezpečnosti a pro připravenost a reakci na ně

1.2. Příslušné oblasti politik

Evropa připravená na digitální věk

Evropské strategické investice

Činnost: utváření digitální budoucnosti Evropy.

1.3. Návrh/podnět se týká:

☒ **nové akce**

☐ **nové akce následující po pilotním projektu / přípravné akci[33]**

☐ **prodloužení stávající akce**

☐ **sloučení jedné či více akcí v jinou/novou akci nebo přesměrování jedné či více akcí na jinou/novou akci**

1.4. Cíle

1.4.1. Obecné cíle

Akt o kybernetické solidaritě posílí solidaritu na úrovni Unie s cílem lépe odhalovat kybernetické bezpečnostní hrozby a incidenty, připravovat se a reagovat na ně. Jeho cílem je:

a) posílit společné odhalování kybernetických hrozeb a incidentů v EU a příslušné situační povědomí;

b) posílit připravenost kritických subjektů v celé EU a upevnit solidaritu vytvořením společných kapacit pro reakci na závažné nebo rozsáhlé kybernetické bezpečnostní incidenty, včetně zpřístupnění podpory při reakci na incidenty třetím zemím přidruženým k programu Digitální Evropa;

c) zvýšit odolnost Unie a přispět k účinné reakci přezkumem a posouzením závažných nebo rozsáhlých incidentů, včetně vyvození poučení a případných doporučení.

1.4.2. Specifické cíle

Akt o kybernetické solidaritě dosáhne souboru cílů prostřednictvím:

a) Zavedení celoevropské infrastruktury bezpečnostních operačních středisek (evropský kybernetický štít) s cílem vybudovat a posílit společné schopnosti odhalování a situačního povědomí.

[33] Uvedené v čl. 58 odst. 2 písm. a) nebo b) finančního nařízení.

b) Vytvoření mechanismu pro mimořádné události v oblasti kybernetické bezpečnosti, který bude podporovat členské státy při přípravě na významné a rozsáhlé kybernetické bezpečnostní incidenty, při reakci na ně a při okamžité obnově po takových incidentech. Podpora reakce na incidenty bude zpřístupněna i evropským orgánům, institucím a jiným subjektům Unie.

Tyto akce budou podporovány z prostředků programu Digitální Evropa, který tento legislativní nástroj pozmění s cílem zavést výše uvedená opatření, poskytnout finanční podporu na jejich rozvoj a vyjasnit podmínky pro čerpání finanční podpory.

c) Zřízení evropského mechanismu pro kybernetické bezpečnostní incidenty, který bude přezkoumávat a posuzovat významné nebo rozsáhlé incidenty.

1.4.3. Očekávané výsledky a dopad

Upřesněte účinky, které by návrh/podnět měl mít na příjemce / cílové skupiny.

Návrh by měl významné výhody pro různé zúčastněné strany. Evropský kybernetický štít zlepší schopnost členských států odhalovat kybernetické hrozby. Mechanismus pro mimořádné události v kybernetické oblasti bude doplňovat opatření členských států prostřednictvím mimořádné podpory pro připravenost, reakci a okamžitou obnovu / obnovení fungování základních služeb.

Tato opatření posílí konkurenceschopnost průmyslu a podniků v Evropě v rámci digitalizované ekonomiky a podpoří jejich digitální transformaci posílením úrovně kybernetické bezpečnosti na jednotném digitálním trhu. Cílem je zejména zvýšit odolnost občanů, podniků a subjektů působících v kritických nebo vysoce kritických odvětvích vůči rostoucím kybernetickým bezpečnostním hrozbám, které mohou mít ničivé společenské a hospodářské dopady. Tohoto cíle se dosáhne prostřednictvím investic do nástrojů, které podpoří rychlejší odhalování kybernetických bezpečnostních hrozeb a incidentů a reakci na ně, a pomoci členským státům při lepší přípravě na závažné a rozsáhlé kybernetické bezpečnostní incidenty a při reakci na ně. To by mělo rovněž podpořit zajištění větších kapacit Unie v těchto oblastech, zejména pokud jde o shromažďování a analýzu údajů o kybernetických bezpečnostních hrozbách a incidentech.

1.4.4. Ukazatele výkonnosti

Upřesněte ukazatele pro sledování pokroku a dosažených výsledků.

Za účelem podpory solidarity na úrovni Unie lze zohlednit několik ukazatelů:

(1) Počet infrastruktur nebo nástrojů kybernetické bezpečnosti pořízených na základě společné veřejné zakázky.

(2) Počet opatření na podporu připravenosti a reakce na kybernetické bezpečnostní incidenty v rámci mechanismu pro mimořádné události v kybernetické oblasti.

1.5. Odůvodnění návrhu/podnětu

1.5.1. Požadavky, které mají být splněny v krátkodobém nebo dlouhodobém horizontu, včetně podrobného časového harmonogramu zavedení iniciativy

Nařízení by mělo být plně použitelné krátce po svém přijetí, tj. dvacátým dnem po vyhlášení v *Úředním věstníku Evropské unie*.

1.5.2. Přidaná hodnota ze zapojení Unie (může být důsledkem různých faktorů, např. přínosů z koordinace, právní jistoty, vyšší účinnosti nebo doplňkovosti). Pro účely tohoto bodu se „přidanou hodnotou ze zapojení Unie“ rozumí hodnota plynoucí ze zásahu Unie, jež doplňuje hodnotu, která by jinak vznikla činností samotných členských států.

Silná přeshraniční povaha kybernetických bezpečnostních hrozeb obecně, jakož i rostoucí počet rizik a incidentů, které se přelévají přes hranice a mezi odvětvími a produkty, znamenají, že cílů tohoto zásahu nemohou členské státy účinně dosáhnout samy a je zapotřebí společného postupu a solidarity na úrovni Unie. Zkušenosti s bojem proti kybernetickým hrozbám vyplývajícím z války proti Ukrajině spolu s poznatky získanými z cvičení v oblasti kybernetické bezpečnosti, které proběhlo během francouzského předsednictví (EU CyCLES), ukázaly, že pro dosažení solidarity na úrovni EU je třeba vytvořit konkrétní mechanismy vzájemné podpory, zejména spolupráce se soukromým sektorem. V této souvislosti závěry Rady ze dne 23. května 2022 o vývoji kybernetické pozice Evropské unie vyzývají Komisi, aby předložila návrh nového fondu pro reakci na mimořádné události v oblasti kybernetické bezpečnosti. Podpora a opatření na úrovni Unie s cílem lépe odhalovat kybernetické bezpečnostní hrozby a zvyšovat připravenost a schopnost reakce představují přidanou hodnotu, neboť zabraňují zdvojování úsilí v Unii a členských státech. Vedly by k lepšímu využívání stávajících prostředků a k větší koordinaci a výměně informací o získaných poznatcích.

1.5.3. Závěry vyvozené z podobných zkušeností v minulosti

Pokud jde o situační povědomí a odhalování hrozeb v rámci evropského kybernetického štítu, byla v rámci pracovního programu pro kybernetickou bezpečnost na období 2021–2022, který je součástí programu Digitální Evropa, vyhlášena výzva k vyjádření zájmu týkající se společného nákupu nástrojů a infrastruktury pro zřízení přeshraničních bezpečnostních operačních středisek a výzva k předkládání žádostí o granty, které umožní budování kapacit bezpečnostních operačních středisek sloužících veřejným a soukromým organizacím.

Pokud jde o připravenost a reakci na kybernetické incidenty, Komise zřídila krátkodobý program na podporu členských států prostřednictvím dodatečných finančních prostředků přidělených agentuře ENISA s cílem okamžitě posílit připravenost a schopnosti reagovat na závažné kybernetické incidenty. Poskytované služby zahrnují opatření v oblasti připravenosti, jako je penetrační testování kritických subjektů s cílem identifikovat zranitelná místa. Rovněž jsou posíleny možnosti pomoci členským státům v případě závažného incidentu s dopadem na kritické subjekty. Agentura ENISA tento krátkodobý program právě provádí a již poskytla relevantní cenné poznatky, které byly zohledněny při přípravě tohoto nařízení.

1.5.4. Slučitelnost s víceletým finančním rámcem a možné synergie s dalšími vhodnými nástroji

Akt o kybernetické solidaritě bude vycházet z opatření, která Unie a členské státy v současné době podporují s cílem zlepšit situační povědomí a odhalování kybernetických hrozeb a reagovat na rozsáhlé a přeshraniční kybernetické bezpečnostní incidenty. Kromě toho je tento nástroj v souladu s dalšími rámci krizového řízení, včetně IPCR, společné bezpečnostní a obranné politiky, týmů rychlé kybernetické reakce a pomoci poskytované jedním členským státem jinému

členskému státu na základě s čl. 42 odst. 7 Smlouvy o Evropské unii. Nový návrh by rovněž doplnil a podpořil struktury vytvořené v rámci jiných nástrojů v oblasti kybernetické bezpečnosti, jako je směrnice (EU) 2022/2555 (směrnice NIS 2) nebo nařízení 2019/881 (akt o kybernetické bezpečnosti).

1.5.5. Posouzení různých dostupných možností financování, včetně prostoru pro přerozdělení prostředků

Řízení oblastí činnosti přidělených agentuře ENISA odpovídá jejímu stávajícímu mandátu a všeobecným úkolům. Tyto oblasti činnosti mohou vyžadovat specifické profily nebo nové úkoly, které by však mohly být zvládnuty pomocí stávajících zdrojů agentury ENISA a vyřešeny přerozdělením nebo propojením různých úkolů. Agentura ENISA v současné době provádí krátkodobý program, který Komise stanovila v roce 2022 s cílem okamžitě posílit připravenost a schopnosti reagovat na závažné kybernetické incidenty. Zahrnuté služby zahrnují možnosti pomoci členským státům v případě závažného incidentu s dopadem na kritické subjekty. Agentura ENISA tento krátkodobý program právě provádí a již poskytla relevantní cenné poznatky, které byly zohledněny při přípravě tohoto nařízení. Prostředky přidělené na krátkodobý program by mohly být využity i v souvislosti s tímto nařízením.

1.6. Doba trvání a finanční dopad návrhu/podnětu

☒ **Časově omezená doba trvání**

– ☒ s platností ode dne přijetí návrhu nařízení Evropského parlamentu a Rady k posílení solidarity a kapacit v Unii pro odhalování hrozeb a incidentů v oblasti kybernetické bezpečnosti a pro připravenost a reakci na ně („akt o kybernetické solidaritě“)

– ☒ Finanční dopad od roku 2023 do roku 2027 pro prostředky na závazky a od roku 2023 do roku 2031 pro prostředky na platby[34].

☐ **Časově neomezená doba trvání**

– Provádění s obdobím rozběhu od RRRR do RRRR,

– poté plné fungování.

1.7. Předpokládaný způsob plnění rozpočtu[35]

☒ **Přímé řízení** Komisí

– ☒ prostřednictvím jejích útvarů, včetně jejích zaměstnanců v delegacích Unie,

– ☐ prostřednictvím výkonných agentur.

☐ **Sdílené řízení** s členskými státy

☒ **Nepřímé řízení**, při kterém jsou úkoly souvisejícími s plněním rozpočtu pověřeny:

– ☐ třetí země nebo subjekty určené těmito zeměmi,

– ☐ mezinárodní organizace a jejich agentury (upřesněte),

– ☐ EIB a Evropský investiční fond,

– ☒ subjekty uvedené v článcích 70 a 71 finančního nařízení,

– ☐ veřejnoprávní subjekty,

– ☐ soukromoprávní subjekty pověřené výkonem veřejné služby v rozsahu, v jakém jim byly poskytnuty dostatečné finanční záruky,

– ☐ soukromoprávní subjekty členského státu pověřené uskutečňováním partnerství veřejného a soukromého sektoru a poskytující dostatečné finanční záruky,

– ☐ orgány nebo osoby pověřené prováděním specifických akcí v rámci společné zahraniční a bezpečnostní politiky podle hlavy V Smlouvy o EU a určené v příslušném základním právním aktu.

– *Pokud vyberete více způsobů řízení, upřesněte je v části „Poznámky“.*

Poznámky

Opatření související s evropským kybernetickým štítem bude provádět centrum ECCC. Dokud nebude centrum ECCC schopno plnit svůj vlastní rozpočet, bude Evropská komise provádět akce v rámci přímého řízení v zastoupení centra ECCC. Centrum ECCC může

[34] Opatření uvedená v aktu by měla být podpořena příštím víceletým finančním rámcem.

[35] Vysvětlení způsobů plnění rozpočtu spolu s odkazem na finanční nařízení jsou k dispozici na stránkách BUDGpedia: https://myintracomm.ec.europa.eu/corp/budget/financial-rules/budget-implementation/Pages/implementation-methods.aspx

vybrat subjekty na základě výzev k vyjádření zájmu o účast na společném zadávání veřejných zakázek na nástroje. Centrum ECCC může na provoz těchto nástrojů udělovat granty.

Kromě toho může centrum ECCC udělovat granty na opatření v oblasti připravenosti v rámci mechanismu pro mimořádné události v oblasti kybernetické bezpečnosti.

Komise nese celkovou odpovědnost za provádění rezervy EU pro kybernetickou bezpečnost. Komise může prostřednictvím dohod o příspěvcích plně nebo zčásti pověřit agenturu ENISA provozem a správou rezervy EU pro kybernetickou bezpečnost. Opatření, která jsou agentuře ENISA přidělena tímto nařízením, jsou v souladu s jejím stávajícím mandátem. Patří k nim: i) podpora skupiny pro spolupráci v oblasti bezpečnosti sítí a informací při vytváření opatření v oblasti připravenosti na základě posouzení rizik; ii) podpora Komise při zřizování rezervy EU pro kybernetickou bezpečnost a dohledu nad jejím prováděním, včetně přijímání a vyřizování žádostí o podporu; iii) vypracování šablon pro usnadnění podávání žádostí o podporu a konkrétních dohod, které mají být uzavřeny mezi poskytovatelem služeb a uživatelem, jemuž je poskytnuta podpora v rámci rezervy EU pro kybernetickou bezpečnost; iv) přezkum a posouzení hrozeb, zranitelností a opatření ke zmírnění dopadů konkrétních významných nebo rozsáhlých kybernetických bezpečnostních incidentů a vypracování zpráv o nich.

Všechny tyto úkoly se odhadují na přibližně 7 plných pracovních úvazků ze stávajících zdrojů agentury ENISA, přičemž se již vychází z odborných znalostí a přípravných prací, které agentura ENISA v současné době provádí v rámci pilotního projektu mimořádné podpory připravenosti a reakce na incidenty.

2. SPRÁVNÍ OPATŘENÍ

2.1. Pravidla pro sledování a podávání zpráv

Upřesněte četnost a podmínky.

Komise bude monitorovat provádění, použití a dodržování těchto nových ustanovení s cílem posoudit jejich účinnost. Komise předloží Evropskému parlamentu a Radě zprávu o hodnocení a přezkumu tohoto nařízení do čtyř let ode dne jeho použitelnosti.

2.2. Systémy řízení a kontroly

2.2.1. Odůvodnění navrhovaných způsobů řízení, mechanismů provádění financování, způsobů plateb a kontrolní strategie

Nařízení zavádí rámec pro provádění financování ze strany EU s cílem zvýšit odolnost v oblasti kybernetické bezpečnosti prostřednictvím opatření, která zvyšují schopnost odhalování, reakce a obnovy v případě významných a rozsáhlých kybernetických bezpečnostních incidentů. Provádění směrnice budou řídit útvary GŘ CNECT odpovědné za danou oblast politiky.

K plnění těchto nových úkolů je nutné poskytnout útvarům Komise náležité zdroje. Odhaduje se, že pro prosazování nového nařízení bude potřeba 6 plných pracovních úvazků (z toho 3 administrátoři (AD) a 3 smluvní zaměstnanci (SZ)) s cílem plnit tyto úkoly:

- určení opatření v oblasti připravenosti podle posouzení rizik,
- zajištění interoperability mezi platformami přeshraničních bezpečnostních operačních středisek,
- vypracování případných prováděcích aktů (dva pro bezpečnostní operační střediska a dva pro mechanismus kybernetické bezpečnosti),
- správa dohod o hostingu a užívání pro bezpečnostní operační střediska,
- zřízení a správa rezervy EU pro kybernetickou bezpečnost, a to přímo nebo prostřednictvím dohody o příspěvcích s agenturou ENISA. V případě dohody o příspěvcích s agenturou ENISA vypracování a dohled nad prováděním dohody o příspěvcích v souvislosti s úkoly přidělenými agentuře ENISA,
- účast v konzultačních skupinách svolaných agenturou ENISA za účelem přezkumu a posouzení významných a rozsáhlých kybernetických bezpečnostních incidentů a příprava zpráv.

2.2.2. Informace o zjištěných rizicích a systémech vnitřní kontroly zřízených k jejich zmírnění

Zjištěným rizikem pro evropský kybernetický štít je nesdílení dostatečného množství relevantních informací o kybernetických hrozbách členskými státy v rámci platforem přeshraničních bezpečnostních operačních středisek nebo mezi přeshraničními platformami a dalšími relevantními subjekty na úrovni EU. Aby se tato rizika zmírnila, bude přidělování finančních prostředků probíhat na základě výzvy k vyjádření zájmu, v níž se členské státy zaváží ke sdílení určitého množství informací s úrovní EU. Tento závazek bude následně formalizován v dohodě o hostingu a užívání, která centru ECCC poskytne pravomoc provádět audity, aby se zajistilo, že

společně pořízené nástroje a infrastruktura budou používány v souladu s dohodou. Závazky k vysoké úrovni sdílení informací v rámci přeshraničních bezpečnostních operačních středisek budou formalizovány v dohodě o konsorciu.

Zjištěným rizikem pro mechanismus pro mimořádné události v kybernetické oblasti je situace, kdy uživatelé účastnící se mechanismu nepřijmou dostatečná opatření k zajištění připravenosti na kybernetické útoky. Z tohoto důvodu jsou uživatelé povinni přijmout taková opatření, aby mohli získat podporu z rezervy EU pro kybernetickou bezpečnost. Při podávání žádostí o podporu z rezervy EU pro kybernetickou bezpečnost musí uživatelé vysvětlit, jaká opatření již byla v reakci na incident přijata, což bude zohledněno při posuzování žádostí o podporu z rezervy EU pro kybernetickou bezpečnost.

2.2.3. Odhad a odůvodnění nákladové efektivnosti kontrol (poměr „náklady na kontroly ÷ hodnota souvisejících spravovaných finančních prostředků“) a posouzení očekávané míry rizika výskytu chyb (při platbě a při uzávěrce)

Jelikož jsou pravidla pro účast v rámci programu Digitální Evropa vztahující se na podporu v rámci aktu o kybernetické solidaritě podobná pravidlům, která Komise použije ve svých pracovních programech, a skupina příjemců má podobný rizikový profil jako v případě programů v rámci přímého řízení, lze očekávat, že chybové rozpětí bude podobné, jaké Komise předpokládá u programu Digitální Evropa, tj. poskytnutí přiměřené jistoty, že riziko chyb v průběhu víceletého výdajového období je každoročně v rozmezí 2–5 %, přičemž konečným cílem je dosáhnout při uzavření víceletých programů míry zbytkových chyb blížící se co nejvíce 2 % po zohlednění finančního dopadu všech auditů, oprav a opatření ke zpětnému získání finančních prostředků.

2.3. Opatření k zamezení podvodů a nesrovnalostí

Upřesněte stávající či předpokládaná preventivní a ochranná opatření, např. opatření uvedená ve strategii pro boj proti podvodům.

V případě evropského kybernetického štítu bude mít centrum ECCC pravomoc provádět audit společně pořízených nástrojů a infrastruktur na základě přístupu k informacím a kontrol na místě v souladu s dohodou o hostingu a užívání, která bude podepsána mezi hostitelským konsorciem a centrem ECCC.

Stávající opatření k předcházení podvodům vztahující se na orgány, instituce nebo jiné subjekty Unie budou zahrnovat dodatečné prostředky potřebné pro toto nařízení.

3. ODHADOVANÝ FINANČNÍ DOPAD NÁVRHU/PODNĚTU

3.1. Okruhy víceletého finančního rámce a dotčené výdajové rozpočtové položky

- Stávající rozpočtové položky

V pořadí okruhů víceletého finančního rámce a rozpočtových položek.

Okruh víceletého finančního rámce	Rozpočtová položka	Druh výdaje	Příspěvek			
	Číslo	RP/NRP[36]	zemí ESVO[37]	z kandidátských zemí a potenciálních kandidátských zemí[38]	jiných třetích zemí	jiné účelově vázané příjmy
1	02 04 01 10 – Program Digitální Evropa – Kybernetická bezpečnost	RP	ANO	ANO	NE	NE
1	02 04 01 11 – Program Digitální Evropa – Evropské průmyslové, technologické a výzkumné centrum pro kybernetickou bezpečnost	RP	ANO	ANO	NE	NE
1	02 04 03 – Program Digitální Evropa – Umělá inteligence	RP	ANO	ANO	NE	NE
1	02 04 04 – Program Digitální Evropa – Dovednosti	RP	ANO	ANO	NE	NE
1	02 01 30 – Podpůrné výdaje pro program Digitální Evropa	NRP	ANO	ANO	NE	NE

[36] RP = rozlišené prostředky / NRP = nerozlišené prostředky.
[37] ESVO: Evropské sdružení volného obchodu.
[38] Kandidátské země a případně potenciální kandidátské země.

3.2. Odhadovaný finanční dopad návrhu na prostředky

3.2.1. Odhadovaný souhrnný dopad na operační prostředky

– ☐ Návrh/podnět nevyžaduje využití operačních prostředků.

– ☒ Návrh/podnět vyžaduje využití operačních prostředků, jak je vysvětleno dále:

v milionech EUR (zaokrouhleno na tři desetinná místa)

Okruh víceletého finančního rámce	Číslo	1 **Jednotný trh, inovace a digitální oblast**

Návrh nezvýší celkové závazky v rámci programu Digitální Evropa. Příspěvkem k této iniciativě je totiž přerozdělení závazků pocházejících z SC2 a SC4 na posílení rozpočtu SC3 a centra ECCC. Pro účely této iniciativy by mohlo být použito případné navýšení závazků v rámci programu Digitální Evropa vyplývající z revize víceletého finančního rámce.

GŘ CONNECT			Rok **2025**	Rok **2026**	Rok **2027**	Rok **2028+**	Vložit počet let podle trvání finančního dopadu (viz bod 1.6)			**CELKEM**
○ Operační prostředky										
Rozpočtová položka[39] 02.040110 (přerozdělení z 02.0403 a 02.0404)	Závazky	(1a)	15,000	15,000	6,000	p.m.				**36,000**
	Platby	(2a)	15,000	15,000	6,000					**36,000**
Rozpočtová položka 02.040111.02 (přerozdělení z 02.0403 a 02.0404)	Závazky	(1b)	13,000	23,000	28,000	p.m.				**64,000**
	Platby	(2b)	8,450	18,200	25,250	12,100				**64,000**
Prostředky správní povahy financované z rámce na zvláštní programy[40]										
Rozpočtová položka 02,0130		(3)	0,150	0,150	0,150	p.m.				0,450
Prostředky na GŘ CONNECT	Závazky	=1a+1b +3	**28,150**	**38,150**	**34,150**	**p.m.**				**100,450**

[39] Podle oficiální rozpočtové nomenklatury.

[40] Technická a/nebo administrativní pomoc a výdaje na podporu provádění programů a/nebo akcí EU (bývalé položky „BA“), nepřímý výzkum, přímý výzkum.

CELKEM	Platby	=2a+2b +3	**23,600**	**33,350**	**31,400**	**12,100**				**100,450**

○ Operační prostředky CELKEM	Závazky	(4)	28,000	38,000	34,000	p.m.				**100,000**
	Platby	(5)	23,450	33,200	31,250	12,100				**100,000**
○ Prostředky správní povahy financované z rámce na zvláštní programy CELKEM		(6)	0,150	0,150	0,150	p.m.				**0,450**
Prostředky z OKRUHU 1 víceletého finančního rámce **CELKEM**	Závazky	=4+6	**28,150**	**38,150**	**34,150**	**p.m.**				**100,450**
	Platby	=5+6	**23,600**	**33,350**	**31,400**	**12,100**				**100,450**

Pokud je návrhem/podnětem dotčen více než jeden operační okruh, zopakuje se výše uvedený oddíl:

○ Operační prostředky CELKEM (všechny operační okruhy)	Závazky	(4)	28,000	38,000	34,000	p.m.				**100,000**
	Platby	(5)	23,450	33,200	31,250	12,100				**100,000**
Prostředky správní povahy financované z rámce na zvláštní programy (všechny operační okruhy) CELKEM		(6)	0,150	0,150	0,150					**0,450**
Prostředky z OKRUHŮ 1 až 6 víceletého finančního rámce **CELKEM** (referenční částka)	Závazky	=4+6	**28,150**	**38,150**	**34,150**	**p.m.**				**100,450**
	Platby	=5+6	**23,600**	**33,350**	**31,400**	**12,100**				**100,450**

Okruh víceletého finančního rámce	7	Správní výdaje

Tento oddíl se vyplní pomocí „rozpočtových údajů správní povahy“, jež se nejprve uvedou v příloze legislativního finančního výkazu příloha 5 rozhodnutí Komise o interních pravidlech pro plnění oddílu Komise v souhrnném rozpočtu Evropské unie), která se pro účely konzultace mezi útvary vloží do aplikace DECIDE.

v milionech EUR (zaokrouhleno na tři desetinná místa)

		Rok **2025**	Rok **2026**	Rok **2027**	Rok **2028+**	Vložit počet let podle trvání finančního dopadu (viz bod 1.6)			**CELKEM**
GŘ: CONNECT									
○ Lidské zdroje		0,786	0,786	0,786	p.m.				**2,358**
○ Ostatní správní výdaje		0,035	0,035	0,035	p.m.				**0,105**
CELKEM GŘ CNECT	Prostředky	**0,821**	**0,821**	**0,821**					**2,463**

Prostředky z OKRUHU 7 víceletého finančního rámce CELKEM	(Závazky celkem = platby celkem)	**0,821**	**0,821**	**0,821**					**2,463**

v milionech EUR (zaokrouhleno na tři desetinná místa)

		Rok **2025**	Rok **2026**	Rok **2027**	Rok **2028+**	Vložit počet let podle trvání finančního dopadu (viz bod 1.6)			**CELKEM**
Prostředky z OKRUHŮ 1 až 7 víceletého finančního rámce **CELKEM**	Závazky	**28,971**	**38,971**	**34,971**	**p.m.**				**102,913**
	Platby	**24,421**	**34,171**	**32,221**	**12,100**				**102,913**

3.2.2. Odhadovaný výstup financovaný z operačních prostředků

Prostředky na závazky v milionech EUR (zaokrouhleno na tři desetinná místa)

Uveďte cíle a výstupy ⇩			Rok **N**		Rok **N+1**		Rok **N+2**		Rok **N+3**		Vložit počet let podle trvání finančního dopadu (viz bod 1.6)						**CELKEM**	
	VÝSTUPY																	
	Druh[41]	Průměrné náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Celkový počet	Náklady celkem
SPECIFICKÝ CÍL č. 1[42]…																		
– Výstup																		
– Výstup																		
– Výstup																		
Mezisoučet za specifický cíl č. 1																		
SPECIFICKÝ CÍL č. 2 …																		
– Výstup																		
Mezisoučet za specifický cíl č. 2																		
CELKEM																		

[41] Výstupy se rozumí produkty a služby, které mají být dodány (např. počet financovaných studentských výměn, počet vybudovaných kilometrů silnic atd.).

[42] Popsaný v bodě 1.4.2. „Specifické cíle…“

3.2.3. Odhadovaný souhrnný dopad na správní prostředky

– ☐ Návrh/podnět nevyžaduje využití prostředků správní povahy.

– ☒ Návrh/podnět vyžaduje využití prostředků správní povahy, jak je vysvětleno dále:

v milionech EUR (zaokrouhleno na tři desetinná místa)

	Rok 2025	Rok 2026	Rok 2027	Rok N+3	Vložit počet let podle trvání finančního dopadu (viz bod 1.6)			**OKRUH 7**
víceletého finančního rámce CELKEM								
Lidské zdroje	0,786	0,786	0,786					**2,358**
Ostatní správní výdaje	0,035	0,035	0,035					**0,105**
Mezisoučet za OKRUH 7 víceletého finančního rámce	**0,821**	**0,821**	**0,821**					**2,463**

Mimo OKRUH 7[43] víceletého finančního rámce								
Lidské zdroje								
Ostatní výdaje správní povahy	0,150	0,150	0,150					**0,450**
Mezisoučet mimo OKRUH 7 víceletého finančního rámce	**0,150**	**0,150**	**0,150**					**0,450**

CELKEM	**0,971**	**0,971**	**0,971**					**2,913**

Potřebné prostředky na oblast lidských zdrojů a na ostatní výdaje správní povahy budou pokryty z prostředků GŘ, které jsou již vyčleněny na řízení akce a/nebo byly vnitřně přerozděleny v rámci GŘ a případně doplněny z dodatečného přídělu, který lze řídícímu GŘ poskytnout v rámci ročního přidělování a s ohledem na rozpočtová omezení.

[43] Technická a/nebo administrativní pomoc a výdaje na podporu provádění programů a/nebo akcí EU (bývalé položky „BA“), nepřímý výzkum, přímý výzkum.

3.2.3.1. Odhadované potřeby v oblasti lidských zdrojů

– ☐ Návrh/podnět nevyžaduje využití lidských zdrojů.

– ☒ Návrh/podnět vyžaduje využití lidských zdrojů, jak je vysvětleno dále:

Odhad vyjádřete v přepočtu na plné pracovní úvazky

		Rok **2025**	Rok **2026**	Rok 2027	Rok **N+3**	Vložit počet let podle trvání finančního dopadu (viz bod 1.6)		
O Pracovní místa podle plánu pracovních míst (místa úředníků a dočasných zaměstnanců)								
20 01 02 01 (v ústředí a v zastoupeních Komise)		3	3	3				
20 01 02 03 (při delegacích)								
01 01 01 01 (v nepřímém výzkumu)								
01 01 01 11 (v přímém výzkumu)								
Jiné rozpočtové položky (upřesněte)								
O Externí zaměstnanci (v přepočtu na plné pracovní úvazky: FTE)[44]								
20 02 01 (SZ, VNO, ZAP z celkového rámce)		3	3	3				
20 02 03 (SZ, MZ, VNO, ZAP a MOD při delegacích)								
XX 01 xx **yy zz** [45]	– v ústředí							
	– při delegacích							
01 01 01 02 (SZ, VNO, ZAP v nepřímém výzkumu)								
01 01 01 12 (AC, END, INT v přímém výzkumu)								
Jiné rozpočtové položky (upřesněte)								
CELKEM		**6**	**6**	**6**				

XX je oblast politiky nebo dotčená hlava rozpočtu.

Potřeby v oblasti lidských zdrojů budou pokryty ze zdrojů GŘ, které jsou již vyčleněny na řízení akce a/nebo byly vnitřně přeobsazeny v rámci GŘ, a případně doplněny z dodatečného přídělu, který lze řídícímu GŘ poskytnout v rámci ročního přidělování a s ohledem na rozpočtová omezení.

Popis úkolů:

Úředníci a dočasní zaměstnanci	- stanovení opatření připravenosti podle posouzení rizik (článek 11) - vypracování případných prováděcích aktů (dva pro bezpečnostní operační střediska a dva pro mechanismus kybernetické bezpečnosti) - správa dohod o hostingu a užívání pro bezpečnostní operační střediska - zřízení a správa rezervy EU pro kybernetickou bezpečnost, a to přímo nebo prostřednictvím dohody o příspěvcích s agenturou ENISA
Externí zaměstnanci	Pod dohledem úředníka - stanovení opatření připravenosti podle posouzení rizik (článek 11) - vypracování případných prováděcích aktů (dva pro bezpečnostní operační střediska a dva pro mechanismus kybernetické bezpečnosti) - správa dohod o hostingu a užívání pro bezpečnostní operační střediska - zřízení a správa rezervy EU pro kybernetickou bezpečnost, a to přímo nebo prostřednictvím dohody o příspěvcích s agenturou ENISA

[44] SZ = smluvní zaměstnanec; MZ = místní zaměstnanec; VNO = vyslaný národní odborník; ZAP = zaměstnanec agentury práce; MOD = mladý odborník při delegaci.

[45] Dílčí strop na externí zaměstnance financované z operačních prostředků (bývalé položky „BA“).

3.2.4. *Slučitelnost se stávajícím víceletým finančním rámcem*

Návrh/podnět:

– [X] může být v plném rozsahu financován přerozdělením prostředků v rámci příslušného okruhu víceletého finančního rámce (VFR).

Upřesněte, jaká úprava se požaduje, příslušné rozpočtové položky a odpovídající částky. V případě zásadní úpravy přiložte excelovou tabulku.

	23	24	25	26	27	celkem
SC1	16 232 897	20 528 765	17 406 899	16 223 464	10 022 366	80 414 391
SC2 počáteční stav	226 316 819	295 067 000	195 649 000	221 809 000	246 608 000	1 185 449 819
Pro iniciativu CYBER			18 000 000	28 000 000	19 000 000	65 000 000
Nový stav SC2	**226 316 819**	**295 067 000**	**177 649 000**	**193 809 000**	**227 608 000**	**1 120 449 819**
SC3 NR 24	24 361 553	35 596 172	3 638 000	3 638 000	11 175 000	78 408 725
Z SC2–SC4			15 000 000	15 000 000	6 000 000	36 000 000
Nový stav SC3	**24 361 553**	**35 596 172**	**18 638 000**	**18 638 000**	**17 175 000**	**114 408 725**
ECCC počáteční stav	176 222 303	208 374 879	104 228 130	90 704 986	84 851 497	664 381 795
Z SC2–SC4			13 000 000	23 000 000	28 000 000	64 000 000
Nový stav ECCC	**176 222 303**	**208 374 879**	**117 228 130**	**113 704 986**	**112 851 497**	**728 381 795**
SC4 počáteční stav	66 902 708	64 892 032	56 577 977	70 477 245	72 107 201	330 957 163
Pro iniciativu CYBER			10 000 000	10 000 000	15 000 000	35 000 000
Nový stav SC4	**66 902 708**	**64 892 032**	**46 577 977**	**60 477 245**	**57 107 201**	**295 957 163**

– [ ] vyžaduje použití nepřiděleného rozpětí v rámci příslušného okruhu VFR a/nebo použití zvláštních nástrojů definovaných v nařízení o VFR.

Upřesněte, co se požaduje, příslušné okruhy a rozpočtové položky, odpovídající částky a navrhované nástroje, které mají být použity.

– [ ] vyžaduje revizi VFR.

Upřesněte, co se požaduje, příslušné okruhy a rozpočtové položky a odpovídající částky.

3.2.5. *Příspěvky třetích stran*

Návrh/podnět:

– [X] nepočítá se spolufinancováním od třetích stran

– [ ] počítá se spolufinancováním od třetích stran podle následujícího odhadu:

prostředky v milionech EUR (zaokrouhleno na tři desetinná místa)

	Rok **N**[46]	Rok **N+1**	Rok **N+2**	Rok **N+3**	Vložit počet let podle trvání finančního dopadu (viz bod 1.6)			Celkem
Upřesněte spolufinancující subjekt								
Spolufinancované prostředky CELKEM								

[46] Rokem N se rozumí rok, kdy se návrh/podnět začíná provádět. Výraz „N“ nahraďte předpokládaným prvním rokem provádění (například 2021). Totéž proveďte u let následujících.

3.3. Odhadovaný dopad na příjmy

– ☒ Návrh/podnět nemá žádný finanční dopad na příjmy.

– ☐ Návrh/podnět má tento finanční dopad:

  – ☐ na vlastní zdroje

  – ☐ na jiné příjmy

  – uveďte, zda je příjem účelově vázán na výdajové položky ☐

v milionech EUR (zaokrouhleno na tři desetinná místa)

Příjmová rozpočtová položka:	Prostředky dostupné v běžném rozpočtovém roce	Dopad návrhu/podnětu[47]						
		Rok **N**	Rok **N+1**	Rok **N+2**	Rok **N+3**	Vložit počet let podle trvání finančního dopadu (viz bod 1.6)		
Článek …….								

U účelově vázaných příjmů upřesněte dotčené výdajové rozpočtové položky.

[…]

Jiné poznámky (např. způsob/vzorec výpočtu dopadu na příjmy nebo jiné údaje).

[…]

[47] Pokud jde o tradiční vlastní zdroje (cla, dávky z cukru), je třeba uvést čisté částky, tj. hrubé částky po odečtení 20 % nákladů na výběr.