Evropský parlament
2019-2024

Dokument ze zasedání

A9-0426/2023

8.12.2023

***I
ZPRÁVA

o návrhu 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
(COM(2023)0209 – C9-0136/2023 – 2023/0109(COD))

Výbor pro průmysl, výzkum a energetiku

Zpravodajka: Lina Gálvez Muñoz

Vysvětlivky

*	Postup konzultace
***	Postup souhlasu
***I	Řádný legislativní postup (první čtení)
***II	Řádný legislativní postup (druhé čtení)
***III	Řádný legislativní postup (třetí čtení)

(Druh postupu závisí na právním základu navrženém v návrhu aktu.)

Pozměňovací návrhy k návrhu aktu

Pozměňovacích návrhy Parlamentu předložené ve dvou sloupcích

Vypuštění textu je označeno ***tučnou kurzivou*** v levém sloupci. Nahrazení je označeno ***tučnou kurzivou*** v obou sloupcích. Nový text je označen ***tučnou kurzivou*** v pravém sloupci.

První a druhý řádek záhlaví každého pozměňovacího návrhu označují příslušnou část projednávaného návrhu aktu. Pokud se pozměňovací návrh týká existujícího aktu, který má být návrhem aktu pozměněn, je v záhlaví mimo to na třetím řádku uveden existující akt a na čtvrtém řádku ustanovení existujícího aktu, kterého se pozměňovací návrh týká.

Pozměňovací návrhy Parlamentu v podobě konsolidovaného textu

Nové části textu jsou označeny ***tučnou kurzivou***. Vypuštěné části textu jsou označeny symbolem ▌ nebo přeškrtnuty. Nahrazení se vyznačují tak, že nový text se označí ***tučnou kurzivou*** a nahrazený text se vymaže nebo přeškrtne. Výjimečně se neoznačují změny výlučně technické povahy, které provedly příslušné útvary za účelem vypracování konečného znění.

OBSAH

Strana

NÁVRH LEGISLATIVNÍHO USNESENÍ EVROPSKÉHO PARLAMENTU

o návrhu 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
(COM(2023)0209 – C9-0136/2023 – 2023/0109(COD))

(Řádný legislativní postup: první čtení)

Evropský parlament,

– s ohledem na návrh Komise předložený Evropskému parlamentu a Radě (COM(2023)0209),

– s ohledem na čl. 294 odst. 2 a čl. 173 odst. 3 a čl. 322 odst. 1 písm. a) Smlouvy o fungování Evropské unie, v souladu se kterými Komise předložila svůj návrh Parlamentu (C9-0136/2023),

– s ohledem na čl. 294 odst. 3 Smlouvy o fungování Evropské unie,

– s ohledem na stanovisko Evropského hospodářského a sociálního výboru ze dne 13. července 2023[1],

– s ohledem na článek 59 jednacího řádu,

– s ohledem na stanoviska Výboru pro zahraniční věci a Výboru pro dopravu a cestovní ruch,

– s ohledem na zprávu Výboru pro průmysl, výzkum a energetiku (A9-0426/2023),

1. přijímá níže uvedený postoj v prvním čtení;

2. schvaluje své prohlášení, které je přílohou tohoto usnesení;

3. vyzývá Komisi, aby věc znovu postoupila Parlamentu, jestliže svůj návrh nahradí jiným textem, podstatně jej změní nebo má v úmyslu jej podstatně změnit;

4. pověřuje svou předsedkyni, aby předala postoj Parlamentu Radě, Komisi, jakož i vnitrostátním parlamentům.

[1] Úř. věst. C 349, 29.9.2023, s. 167.

Pozměňovací návrh 1

POZMĚŇOVACÍ NÁVRHY EVROPSKÉHO PARLAMENTU*

k návrhu Komise

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 *a mění nařízení (EU) 2021/694*

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[2],

s ohledem na stanovisko Evropského hospodářského a sociálního výboru[3],

s ohledem na stanovisko Výboru regionů[4],

v souladu s řádným legislativním postupem,

vzhledem k těmto důvodům:

(1) Používání informačních a komunikačních technologií a závislost na nich je dnes základním aspektem***, ale současně přineslo možné zranitelnosti*** ve všech odvětvích hospodářské činnosti ***a demokracie***, 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 ***z hlediska metod i dopadu v celé Unii i na světové úrovni***, včetně útoků na dodavatelský řetězec, a jejich cílem je kybernetická špionáž, ransomware nebo narušení provozu. Představují

---

* Pozměňovací návrhy: nový text či pozměněné znění je označeno tučnou kurzivou; vypuštění textu je označeno symbolem ▌.

2 Úř. věst. C […], […], s. […].

3 Úř. věst. C , , s. .

4 Úř. věst. C , , s. .

zásadní hrozbu pro fungování síťových a informačních systémů. 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 ***hospodářství a demokracii, pokud jde o kritické infrastruktury v celé Unii***, 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 ***a*** kriminálních ▌ 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. ***Proto je zapotřebí úzké a koordinované spolupráce mezi veřejným sektorem, soukromým sektorem, akademickou obcí, občanskou společností a sdělovacími prostředky. Kromě toho musí být reakce Unie koordinována s mezinárodními institucemi, jakož i s důvěryhodnými a podobně smýšlejícími mezinárodními partnery. Důvěryhodnými a podobně smýšlejícími partnery jsou země, které sdílejí hodnoty Unie, tedy demokracie, dodržování lidských práv, účinný multilateralismus a řád založený na pravidlech, a to v souladu s rámci mezinárodní spolupráce a dohodami o mezinárodní spolupráci. V zájmu zajištění spolupráce s důvěryhodnými a podobně smýšlejícími mezinárodními partnery a ochrany před systémovými konkurenty by subjektům usazeným ve třetích zemích, které nejsou stranou dohody o vládních zakázkách, nemělo být umožněno se účastnit zadávání zakázek podle tohoto nařízení.***

(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[5], je nutné zvýšit odolnost občanů, podniků***, zejména mikropodniků, malých a středních podniků (MSP), včetně začínajících podniků,*** a subjektů provozujících kritické infrastruktury***, včetně místních a regionálních orgánů,*** vůči rostoucím kybernetickým bezpečnostním hrozbám, které mohou mít ničivé společenské a hospodářské dopady. Proto je třeba investovat do infrastruktur a služeb ***a budování schopností pro rozvoj dovedností v oblasti kybernetické bezpečnosti***, 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.

(3a) Kybernetické útoky jsou často zaměřeny na místní, regionální nebo celostátní veřejné služby a infrastruktury. Místní orgány patří kvůli nedostatku finančních a lidských zdrojů k nejzranitelnějším cílům kybernetických útoků. Je proto obzvláště důležité, aby byly subjekty přijímající rozhodnutí na místní úrovni zpraveny o tom, že je třeba

[5] https://futureu.europa.eu/cs/.

zvýšit digitální odolnost, zlepšit svou schopnost omezit dopad kybernetických útoků a využívat příležitostí, které toto nařízení nabízí.

(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[6], doporučení Komise (EU) 2017/1584[7], směrnici Evropského parlamentu a Rady 2013/40/EU[8] a nařízení Evropského parlamentu a Rady (EU) 2019/881[9]. 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 ▌**,** reagovat na ně ***i se zotavit z jejich následků***. Členské státy rovněž v závěrech Rady o kybernetické pozici EU[10] vyzvaly Komisi, aby předložila návrh nového fondu pro reakci na mimořádné události v oblasti kybernetické bezpečnosti.

(6) Společné sdělení o politice kybernetické obrany EU[11] 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 ***sítě*** EU v podobě bezpečnostních operačních středisek, podporovat postupné vytváření rezervy pro kybernetickou bezpečnost na úrovni EU se službami 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 ***a předcházet jim***. Proto by měla být zavedena celoevropská ***síť*** bezpečnostních operačních středisek (evropský kybernetický štít) s cílem vybudovat a posílit společné

---

[6] 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).

[7] 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).

[8] 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*).

[9] 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).

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

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

schopnosti odhalování a situačního povědomí***, které zlepší schopnosti Unie odhalovat hrozby a sdílet informace***; 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[12]. 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 ▌ oblasti ***kybernetické bezpečnosti*** 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.

(9a) S ohledem na geopolitický vývoj a prostředí narůstajících kybernetických hrozeb (EPP 52) a s cílem zajistit kontinuitu a další rozvoj opatření stanovených v tomto nařízení po roce 2027, zejména evropského kybernetického štítu a mechanismu pro mimořádné události v oblasti kybernetické bezpečnosti, je nezbytné zajistit zvláštní rozpočtovou položku ve víceletém finančním rámci na období 2028–2034. Členské státy by se rovněž měly vynasnažit zavázat se k podpoře všech nezbytných opatření k omezení kybernetických hrozeb a incidentů v celé Unii a k posílení solidarity.

(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 ***v*** nařízení ***Evropského parlamentu a Rady (EU, Euratom) 2018/1046***[13] 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

---

[12] 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).

[13] ***Nařízení Evropského parlamentu a Rady (EU, Euratom) 2018/1046 ze dne 18. července 2018, kterým se stanoví finanční pravidla pro souhrnný rozpočet Unie, mění nařízení (EU) č. 1296/2013, (EU) č. 1301/2013, (EU) č. 1303/2013, (EU) č. 1304/2013, (EU) č. 1309/2013, (EU) č. 1316/2013, (EU) č. 223/2014 a (EU) č. 283/2014 a rozhodnutí č. 541/2014/EU a zrušuje nařízení (EU, Euratom) č. 966/2012 (Úř. věst. L 193, 30.7.2018, s. 1, ELI: http://data.europa.eu/eli/reg/2018/1046/oj).***

rozpočtu Unie, jak je stanoveno v nařízení Evropského parlamentu a Rady (EU, Euratom) 2020/2092.[14]

(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 ***v*** nařízení ***(EU, Euratom) 2018/1046***, čímž by se maximalizovala schopnost mechanismu pro mimořádné události v oblasti kybernetické bezpečnosti účinně podporovat členské státy v boji proti kybernetickým hrozbám.

(11a) Mechanismus pro mimořádné události v oblasti kybernetické bezpečnosti a rezerva EU pro kybernetickou bezpečnost zřízené tímto nařízením jsou nové iniciativy a nebyly plánovány při vytváření víceletého finančního rámce na období 2021–2027 a financování těchto iniciativ má zmenšit omezení financování jiných priorit v programu Digitální Evropa na minimum. Částka finančních zdrojů vyčleněných na rezervu EU pro kybernetickou bezpečnost by se proto měla snížit a měla by primárně čerpat z nepřiděleného rozpětí v rámci stropů víceletého finančního rámce nebo mobilizovaných prostřednictvím netematických zvláštních nástrojů víceletého finančního rámce. Veškeré vyčleněné finanční prostředky ze stávajících programů nebo jejich přerozdělení by se měly omezit na naprosté minimum, aby se ochránily stávající programy, zejména Erasmus+, před negativními dopady a zajistilo se, že tyto programy mohou dosáhnout svých stanovených cílů.

(12) Aby bylo možné účinněji předcházet kybernetickým hrozbám a incidentům, vyhodnocovat je***,*** reagovat na ně ***a zotavit se z jejich následků***, 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. ***Proaktivní přístup k identifikaci, zmírnění a předcházení potenciálním kybernetickým hrozbám zahrnuje zvýšení kapacity schopností pokročilého odhalování, které jsou nezbytné k zastavení pokročilých přetrvávajících hrozeb. Zpravodajskými informacemi o hrozbách se rozumí informace shromážděné, analyzované a vyložené s cílem porozumět možným hrozbám a rizikům. Díky analýze a usouvztažnění obrovského množství údajů umožňuje odhalit systematičnosti, trendy a ukazatele narušení bezpečnosti, které mohou upozornit na nekalé činnosti nebo zranitelnosti***. Měla by být zavedena ***síť*** 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. ***Národním bezpečnostním operačním střediskem se rozumí centralizovaná kapacita odpovědná za průběžné shromažďování zpravodajských informací o hrozbách a zlepšování kybernetické bezpečnosti subjektů spadajících pod národní jurisdikci prostřednictvím prevence, detekce a analýzy***

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

kybernetických hrozeb. 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[15].

(13) Pro účast na evropském kybernetickém štítu by měl každý členský stát určit veřejnoprávní subjekt na vnitrostátní úrovni, který by byl pověřen koordinací činnosti v oblasti odhalování kybernetických hrozeb a sdílení informací v daném členském státě. ***Členské státy se vyzývají, aby začlenily kapacitu národního bezpečnostního operačního střediska do své již existující kybernetické struktury a správy, aby se předešlo vytváření dalších vrstev správy a aby se sladilo toto nařízení s již existujícím právním aktem, včetně směrnice (EU) 2022/2555.*** Tato národní bezpečnostní operační střediska by měla na vnitrostátní úrovni fungovat jako referenční bod a brána pro účast ***soukromých a veřejných subjektů, zejména jejich národních bezpečnostních operačních středisek,*** 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. ***Národní bezpečnostní operační střediska by měla posílit spolupráci a sdílení informací mezi veřejnými a soukromými subjekty, aby se prolomily stávající uzavřené komunikační struktury. Přitom mohou podporovat vytváření modelů výměny dat a měla by usnadňovat a podporovat sdílení informací v důvěryhodném a bezpečném prostředí. K posílení odolnosti Unie v oblasti kybernetické bezpečnosti je zásadní úzká a koordinovaná spolupráce mezi veřejnými a soukromými subjekty.***

(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***, včetně shromažďování a sdílení údajů a informací o možném nekalém hackingu, nově vznikajících zlovolných hrozbách a zneužívání slabin, které se dosud nestaly příčinou kybernetických incidentů, a snah v oblasti analýzy,*** 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 ***a zabezpečeném*** prostředí ***s podporou agentury ENISA v záležitostech souvisejících s operativní spoluprací mezi členskými státy***. ***Přeshraniční bezpečnostní operační střediska by měla usnadnit sdílení informací v důvěryhodném a zabezpečeném prostředí a*** 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] 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).

(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 sítě CSIRT v souladu se směrnicí (EU) 2022/2555. Přeshraniční bezpečnostní operační střediska by měla představovat novou kapacitu, která ***se začlení do stávající infrastruktury kybernetické bezpečnosti, zejména do sítě*** týmů pro reakce na kybernetické bezpečnostní incidenty, neboť bude sdružovat a sdílet údaje o kybernetických bezpečnostních hrozbách od veřejných a soukromých subjektů***, zejména jejich bezpečnostních operačních středisek***, zvyšovat hodnotu těchto údajů prostřednictvím odborné analýzy a společně pořízené infrastruktury a nejmodernějších nástrojů a přispívat k ***technologické suverenitě Unie, její otevřené strategické autonomii, konkurenceschopnosti a odolnosti a k rozvoji významného ekosystému kybernetické bezpečnosti, mimo jiné i ve spolupráci s důvěryhodnými a podobně smýšlejícími mezinárodními partnery.***

(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) ***za účelem usnadnění rozbití v současnosti existujících komunikačních uzavřených struktur***. ***Přitom by přeshraniční bezpečnostní operační střediska mohla také podporovat vytváření vzorů pro výměny údajů v rámci celé Unie***. 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***, včetně shromažďování a sdílení údajů a informací o možném nekalém hackingu, nově vznikajících zlovolných hrozbách a zneužívání slabin, které se dosud nestaly příčinou kybernetických incidentů, a snah v oblasti analýzy***. 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[16], jakož i povinnost poskytování analytických zpráv pro opatření integrovaného mechanismu pro politickou reakci na krize podle prováděcího rozhodnutí ***Rady*** (EU) 2018/1993[17]. V situacích, kdy

---

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

[17] ***Prováděcí rozhodnutí Rady (EU) 2018/1993 ze dne 11. prosince 2018 o opatřeních pro integrovanou politickou reakci EU na krize (*****Úř. věst. L 320, 17.12.2018, s. 28,***

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***, a to v souladu se směrnicí (EU) 2022/2555***. 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 ***a zabezpečeném*** prostředí, měly by být subjekty zapojené do evropského kybernetického štítu vybaveny nejmodernějšími a vysoce bezpečnými nástroji, zařízeními a infrastrukturami ***a kvalifikovaným personálem***. 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, ***její otevřenou strategickou autonomii, konkurenceschopnost a odolnost a významný ekosystém kybernetické bezpečnosti EU***. Sdružování vysoce kvalitních kontrolovaných údajů by mělo rovněž přispět k rozvoji pokročilých technologií umělé inteligence a analýzy dat. ***Umělá inteligence je nejúčinnější ve spojení s lidskou analýzou. Proto jsou kvalifikovaní pracovníci i nadále zásadní pro shromažďování vysoce kvalitních údajů.*** Mělo by být usnadněno propojením evropského kybernetického štítu s celoevropskou infrastrukturou pro vysoce výkonnou výpočetní techniku zřízenou nařízením Rady (EU) 2021/1173[18].

(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 ***vstupní podmínky a bezpečnostní*** protokoly a normy, které umožní spolupráci s komunitou kybernetické obrany, včetně prověřování a bezpečnostních podmínek ***při respektování civilního charakteru institucí, a určení***

ELI: http://data.europa.eu/eli/dec_impl/2018/1993/oj).

[18] 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), ***ELI: http://data.europa.eu/eli/reg/2021/1173/oj***).

finančních prostředků, tedy s využitím prostředků, které má k dispozici komunita obrany. 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 ***a za plného respektování práv a svobod***.

(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 ***unijního*** nebo ***vnitrostátního práva*** 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 ***a účinné*** nasazení pomoci za vymezených okolností a jasných podmínek a umožnit pečlivé sledování a hodnocení toho, jak byly zdroje využity. Ačkoli primární odpovědnost za předcházení kybernetickým bezpečnostním incidentům a krizím i za připravenost a odezvu na ně nesou i nadále členské státy, mechanismus pro mimořádné události v ▌ oblasti ***kybernetické bezpečnosti*** podporuje solidaritu mezi členskými státy v souladu s čl. 3 odst. 3 Smlouvy o Evropské unii („dále jen „SEU“).

(25) Mechanismus pro mimořádné události v ▌ oblasti ***kybernetické bezpečnosti*** by měl členským státům poskytovat podporu doplňující jejich vlastní opatření a zdroje a další stávající možnosti podpory v případě reakce na významné 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[19] 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[20], integrovaná opatření EU pro

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

[20] Rozhodnutí Evropského parlamentu a Rady č. 1313/2013/EU ze dne 17. prosince 2013 o mechanismu

politickou reakci na krize[21] 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***, agenturou ENISA*** a dotčeným členským státem. Při žádosti o podporu v rámci mechanismu pro mimořádné události v ▌oblasti ***kybernetické bezpečnosti*** by měl členský stát poskytnout relevantní informace, které odůvodňují potřebu podpory.

(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 ▌oblasti ***kybernetické bezpečnosti*** by měl poskytovat pomoc při opatřeních zaměřených na posílení připravenosti, jakož i při opatřeních v reakci na incidenty s 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

civilní ochrany Unie (Úř. věst. L 347, 20.12.2013, s. 924).

[21] 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.

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[22]. Výběr odvětví by měl rovněž zohlednit doporučení Rady o celounijním koordinovaném přístupu za účelem posílení odolnosti kritické infrastruktury.

(30) Mechanismus pro mimořádné události v ▌oblasti ***kybernetické bezpečnosti*** 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 ▌oblasti ***kybernetické bezpečnosti*** 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 ▌oblasti ***kybernetické bezpečnosti*** 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 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 ***a zároveň posilovat odolnost Unie, včetně účasti evropských poskytovatelů řízených bezpečnostních služeb, které jsou malými a středními podniky, a zajistit vytvoření ekosystému kybernetické bezpečnosti, zejména mikropodniků, malých a středních podniků, včetně těch začínajících, prostřednictvím investic do výzkumu a inovací (VaI) za účelem vývoje nejmodernějších technologií, jako jsou technologie týkající se cloudu a umělé inteligence. Důvěryhodní poskytovatelé, včetně malých a středních podniků, by měli být schopni vzájemně spolupracovat, aby splnili výše uvedená kritéria.*** 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.

[22] 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.

Rezerva pro kybernetickou bezpečnost by proto měla motivovat k investicím do výzkumu a inovací, aby se podpořil vývoj těchto technologií. V případě potřeby by se mohla provádět společná cvičení s důvěryhodnými poskytovateli a potenciálními uživateli rezervy pro kybernetickou bezpečnost, aby se zajistilo účinné fungování rezervy v případě potřeby. 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. ***Komise by měla zajistit zapojení členských států a rozsáhlé výměny informací s nimi s cílem předejít zdvojování činnosti s podobnými iniciativami, mimo jiné i v rámci Organizace Severoatlantické smlouvy (NATO).***

(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. ***Je třeba podporovat účast menších poskytovatelů aktivních na regionální a místní úrovni.***

(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 ▌oblasti ***kybernetické bezpečnosti***. ***Aby mohla agentura ENISA plnit další úkoly vyplývající z tohoto ustanovení, měla by obdržet odpovídající dodatečné finanční prostředky.***

(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.

(37a) Třetí země by mohly využívat zdroje a podporu podle tohoto nařízení s využitím podpory při reakci na incidenty z rezervy EU pro kybernetickou bezpečnost. Kromě toho pro poskytování specifických služeb v rámci rezervy EU pro kybernetickou bezpečnost mohou být zapotřebí poskytovatelé služeb reakce na incidenty ze třetích zemí, včetně třetích zemí přidružených k programu Digitální Evropa nebo jiných partnerských zemí nebo členů NATO. Odchylně od nařízení (EU, Euratom) 2018/1046 s cílem posílit technologickou suverenitu Unie, její otevřenou strategickou autonomii, konkurenceschopnost a odolnost a ochránit strategická aktiva Unie, její zájmy nebo bezpečnost by subjektům usazeným ve třetích zemí, které nejsou stranou dohody o vládních zakázkách a které nepodléhají prověřování ve smyslu nařízení Evropského parlamentu a Rady (EU) 2019/452[23] a v nezbytných případech zmírňujícím opatřením, a to s ohledem na cíle stanovené v tomto nařízení, neměla být umožněna účast. Vnější rozměr tohoto nařízení by měl být v souladu s ustanoveními dohody o přidružení v rámci programu Digitální Evropa. Účast třetích zemí by měla podléhat veřejné kontrole se zapojením zákonodárné moci, aby bylo zaručeno, že se občané budou moci tohoto procesu účastnit.

(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.

---

* ***Nařízení Evropského parlamentu a Rady (EU) č. 182/2011 ze dne 16. února 2011, kterým se stanoví pravidla a obecné zásady způsobu, jakým členské státy kontrolují***

---

[23] Nařízení Evropského parlamentu a Rady (EU) 2019/452 ze dne 19. března 2019, kterým se stanoví rámec pro prověřování přímých zahraničních investic směřujících do Unie (Úř. věst. L 79I, 21.3.2019, s. 1), ELI: http://data.europa.eu/eli/reg/2019/452/oj.

Komisi při výkonu prováděcích pravomocí (Úř. věst. L 55, 28.2.2011, s. 13, ELI: http://data.europa.eu/eli/reg/2011/182/oj).

(38a) Kvalifikovaný personál, který je schopen spolehlivě poskytovat příslušné služby kybernetické bezpečnosti na nejvyšší úrovni, je nezbytný pro účinné provádění evropského kybernetického štítu a mechanismu pro mimořádné situace v oblasti kybernetické bezpečnosti. Je proto znepokojivé, že se Unie potýká s nedostatkem talentů v podobě nedostatku kvalifikovaných odborníků, a zároveň čelí rychle se vyvíjejícím hrozbám, jak je uvedeno ve sdělení Komise ze dne 18. dubna 2023 o Akademii kybernetických dovedností. Je důležité překlenout tento nedostatek talentů posílením spolupráce a koordinace mezi různými zúčastněnými stranami, včetně soukromého sektoru, akademické obce, členských států, Komise a agentury ENISA, s cílem na všech územích zvýšit a vytvořit synergie pro investice do vzdělávání a odborné přípravy, rozvoj partnerství veřejného a soukromého sektoru, podporu výzkumných a inovačních iniciativ, rozvoj a vzájemné uznávání společných norem a certifikaci dovedností v oblasti kybernetické bezpečnosti, mimo jiné prostřednictvím evropského rámce dovedností v oblasti kybernetické bezpečnosti. To by mělo rovněž usnadnit mobilitu odborníků na kybernetickou bezpečnost v rámci Unie. Cílem tohoto nařízení by měla být podpora rozmanitější pracovní síly v oblasti kybernetické bezpečnosti. Všechna opatření, která mají za cíl posílit dovednosti v oblasti kybernetické bezpečnosti, vyžadují záruky, aby se předešlo „odlivu mozků“ a riziku pro pracovní mobilitu.

(38b) Je třeba posílit specializované, interdisciplinární a obecné dovednosti a kompetence v celé Unii se zvláštním zaměřením na ženy, neboť v oblasti kybernetické bezpečnosti přetrvávají genderové rozdíly, přičemž ženy tvoří v průměru celosvětově jen 20 % pracovníků v tomto odvětví. Ženy musí být přítomny při utváření digitální budoucnosti a její správy a podílet se na něm.

(38c) Posílení výzkumu a inovací (VaI) v oblasti kybernetické bezpečnosti má za cíl zvýšit odolnost a otevřenou strategickou autonomii Unie. Obdobně je důležité vytvářet synergie s programy VaI a se stávajícími nástroji a institucemi a posilovat spolupráci a koordinaci mezi jednotlivými zúčastněnými stranami, včetně soukromého sektoru, občanské společnosti, akademické obce, členských států, Komise a agentury ENISA.

(38d) Cílem tohoto nařízení by mělo být přispět ke splnění závazku vyplývajícího z evropského prohlášení o digitálních právech a zásad pro digitální dekádu souvisejícího s ochranou zájmů našich demokracií, lidí, podniků a veřejných institucí před riziky v oblasti kybernetické bezpečnosti a před kyberkriminalitou, včetně narušení bezpečnosti údajů a krádeží identity nebo manipulace s ní. Uplatňování tohoto nařízení by mělo rovněž přispět k provádění jiných právních předpisů, například o umělé inteligenci, ochraně údajů a regulaci údajů, pokud jde o kybernetickou bezpečnost a kybernetickou odolnost.

(38e) Klíčem k úspěšnému provádění tohoto nařízení bude posílení kultury kybernetické bezpečnosti, která chápe bezpečnost, včetně bezpečnosti digitálního prostředí, jakožto veřejný statek. Dalším prostředkem k zajištění ochrany našich demokracií a základních hodnot by proto mělo být vypracování opatření k zapojení a zvýšení povědomí občanů.

(38f) Aby bylo možné doplnit některé prvky tohoto nařízení, které nejsou podstatné, měla by být na Komisi přenesena pravomoc přijímat akty v souladu s článkem 290 SFEU,

pokud jde o upřesnění podmínek pro interoperabilitu mezi přeshraničními bezpečnostními operačními středisky, stanovení procesních ujednání pro sdílení informací mezi přeshraničními bezpečnostními operačními středisky na jedné straně a sítí EU-CyCLONe, sítí CSIRT a Komisí na straně druhé, specifikování druhů a počtu služeb reakce požadovaných pro rezervu EU pro kybernetickou bezpečnost a další upřesnění podrobných ujednání pro přidělování podpůrných služeb z rezervy EU pro kybernetickou bezpečnost. Je obzvláště důležité, aby Komise v rámci přípravné činnosti vedla odpovídající konzultace, a to i na odborné úrovni, a aby tyto konzultace probíhaly v souladu se zásadami stanovenými v interinstitucionální dohodě o zdokonalení tvorby právních předpisů ze dne 13. dubna 2016*. Pro zajištění rovné účasti na vypracovávání aktů v přenesené pravomoci obdrží Evropský parlament a Rada veškeré dokumenty současně s odborníky z členských států a jejich odborníci mají automaticky přístup na setkání skupin odborníků Komise, jež se věnují přípravě aktů v přenesené pravomoci.

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

(39) ***Jelikož cílů*** tohoto nařízení***, konkrétně posílit prevenci, schopnosti odhalování, reakce a obnovy a vytvořit obecný rámec pro prolomení uzavřené komunikační infrastruktury, nemohou v dostatečné míře dosáhnout členské státy, ale naopak jich*** lze lépe dosáhnout na úrovni Unie. Unie proto může přijmout opatření v souladu se zásadami subsidiarity a proporcionality stanovenými v článku 5 Smlouvy o Evropské unii. ***V souladu se zásadou proporcionality stanovenou v uvedeném článku nepřekračuje*** toto nařízení 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 ***sítě*** 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 ***podpořit průmyslovou kapacitu Unie a členských států v odvětví kybernetické bezpečnosti a*** posílit konkurenceschopnost odvětví průmyslu***, zejména mikropodniků, malých a středních podniků, včetně těch začínajících,*** a služeb v Unii v celé digitální ekonomice a přispět k technologické suverenitě Unie***, její otevřené strategické autonomii, konkurenceschopnosti a odolnosti*** v ***tomto odvětví, posílení ekosystému kybernetické bezpečnosti s cílem zajistit silné schopnosti Unie, mimo jiné i ve spolupráci s mezinárodními partnery***;

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.

ca) rozvíjet koordinovaným způsobem dovednosti, know how, schopnosti a kompetence pracovníků s cílem zajistit kybernetickou bezpečnost a vytvářet synergie s Akademií kybernetických dovedností.

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:

-1a) „národním bezpečnostním operačním střediskem“ centralizovaná vnitrostátní schopnost průběžně shromažďovat a analyzovat zpravodajské informace o kybernetických hrozbách a zlepšovat pozici v oblasti kybernetické bezpečnosti v souladu s článkem 4;

1) **„přeshraničním bezpečnostním operačním střediskem“** platforma za účasti více zemí, která v koordinované síťové struktuře sdružuje národní bezpečnostní operační střediska ***v souladu s článkem 5***;

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

3) **„hostitelským konsorciem“** konsorcium složené ze zúčastněných států, zastoupených národními bezpečnostními operačními středisky ***v souladu s článkem 5***;

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

4a) „kritickým subjektem“ kritický subjekt ve smyslu definice uvedené v čl. 2 bodu 1 směrnice Evropského parlamentu a Rady (EU) 2022/2557[25].

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

5a) „řešením incidentu“ řešení incidentu ve smyslu čl. 6 odst. 8 směrnice (EU) 2022/2555;

5b) „rizikem“ se rozumí riziko ve smyslu čl. 6 bodu 9 směrnice (EU) 2022/2555;

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

6a) „významnou kybernetickou hrozbou“ významná kybernetická hrozba ve smyslu čl. 6 bodu 11 směrnice (EU) 2022/2555;

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;

10a) „poskytovatelem řízených bezpečnostních služeb“ poskytovatel řízených bezpečnostních služeb ve smyslu čl. 6 bodu 40 směrnice (EU) 2022/2555;

11) **„důvěryhodnými poskytovateli *řízených bezpečnostních služeb*“** poskytovatelé řízených bezpečnostních služeb ***zapojení do rezervy EU pro kybernetickou bezpečnost*** ve smyslu článku 16 tohoto nařízení.

---

[24] 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).

[25] Směrnice Evropského parlamentu a Rady (EU) 2022/2557 ze dne 14. prosince 2022 o odolnosti kritických subjektů a o zrušení směrnice Rady 2008/114/ES (Úř. věst. L 333, 27.12.2022, s. 164, ELI: http://data.europa.eu/eli/dir/2022/2557/oj).

Kapitola II

EVROPSKÝ KYBERNETICKÝ ŠTÍT

Článek 3

Zřízení evropského kybernetického štítu

1. Zřizuje se ***síť*** 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 ***a předcházet jim***. 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 ***a případně si vyměňuje informace se sítí CSIRT***;

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***, mimo jiné poskytováním konkrétních doporučení subjektům***;

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. ***Aby bylo možné se účastnit*** v evropském kybernetickém štítu***,*** určí každý členský stát alespoň jedno národní bezpečnostní operační středisko. Národní bezpečnostní operační středisko musí ***mít centralizovanou pravomoc ve*** veřejnoprávním ***subjektu***. ***Je-li to možné, zahrnuje národní bezpečnostní operační středisko týmy CSIRT a jiné stávající infrastruktury a orgány řízení v oblasti kybernetické bezpečnosti.***

Má kapacitu působit jako referenční bod a brána pro další veřejné a soukromé organizace na vnitrostátní úrovni, ***zejména jejich národní bezpečnostní operační střediska,*** která shromažďují a analyzují informace o kybernetických bezpečnostních hrozbách a incidentech ***a případně tyto informace sdílejí se členy sítě CSIRT daného členského státu*** a přispívají k přeshraničnímu bezpečnostnímu operačnímu středisku. Je vybaveno nejmodernějšími technologiemi schopnými zjišťovat, agregovat a analyzovat údaje týkající se kybernetických bezpečnostních hrozeb a incidentů ***a předcházet jim***.

Národní bezpečnostní operační středisko nebo tým CSIRT mohou požádat o údaje o telemetrii, z čidel nebo logů svých vnitrostátních kritických subjektů od poskytovatelů řízených bezpečnostních služeb, které nabízejí službu kritickému subjektu. Tyto údaje se sdílejí v souladu s právními předpisy Unie v oblasti ochrany údajů a výhradně za účelem podpory národního bezpečnostního operačního střediska nebo týmu CSIRT s cílem odhalit hrozby a incidenty v oblasti kybernetické bezpečnosti a předcházet jim.

2. Na základě výzvy k vyjádření zájmu ***může vybrat*** 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. ***Přeshraniční bezpečnostní operační střediska by měla být koncipována pro odhalování a analýzu hrozeb v oblasti kybernetické bezpečnosti, prevenci incidentů a podporu vytváření vysoce kvalitních zpravodajských informací, zejména prostřednictvím výměny údajů z různých zdrojů, ať už veřejných, nebo soukromých, jakož i prostřednictvím sdílení nejmodernějších nástrojů a společného rozvoje schopností kybernetického odhalování, analýzy, prevence a ochrany v důvěryhodném a zabezpečeném prostředí.***

2. Na základě výzvy k vyjádření zájmu ***může vybrat*** 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.

2a. Odchylně od článku 176 nařízení (EU, Euratom) 2018/1046 se subjekty usazené ve třetích zemích, které nejsou stranou dohody o vládních zakázkách, neúčastní společného zadávání veřejných zakázek na nástroje a infrastruktury.

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) ***zlepšuje výměnu zpravodajských informací o kybernetických hrozbách mezi***

národními a přeshraničními bezpečnostními operačními středisky a průmyslovými středisky ISAC s cílem předcházet hrozbám, odhalovat je nebo je zmírňovat;

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 ***údaje uvedené*** 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. ***V zájmu podpory výměny*** informací mezi přeshraničními bezpečnostními operačními operačními středisky ***a s průmyslovými středisky ISAC*** zajistí přeshraniční bezpečnostní operační střediska vysokou úroveň vzájemné interoperability ***a pokud možno i s průmyslovými středisky ISAC***. Aby ***se*** usnadnila ***interoperabilita*** mezi přeshraničními bezpečnostními operačními středisky ***a s průmyslovými ISAC, mohou být normy a protokoly pro sdílení informací harmonizovány s mezinárodními normami a osvědčenými postupy v daném odvětví***. ***Rovněž je třeba podpořit společné zadávání zakázek na kybernetické infrastruktury, služby a nástroje. Navíc*** po konzultaci s centrem ECCC ***a agenturou ENISA je Komise zmocněna do ... [šesti měsíců ode dne vstupu tohoto nařízení v platnost] přijmout akty v přenesené pravomoci v souladu s článkem 20a, kterým doplní toto nařízení tím, že upřesní*** podmínky této interoperability ***v těsné koordinaci s přeshraničními bezpečnostními operačními středisky a na základě mezinárodních norem a odvětvových osvědčených postupů***.

4. Přeshraniční bezpečnostní operační střediska mezi sebou ***a případně s průmyslovými středisky ISAC*** uzavřou dohody o spolupráci, v nichž stanoví zásady sdílení informací ***a interoperability*** mezi přeshraničními platformami***, přičemž zohlední již existující příslušné mechanismy sdílení informací podle směrnice (EU) 2022/2555***. ***Ve vhodných případech přeshraniční bezpečnostní operační střediska uzavřou dohody o spolupráci s průmyslovými středisky ISAC. V souvislosti s potenciálním nebo probíhajícím rozsáhlým kybernetickým bezpečnostním incidentem musí být mechanismy sdílení informací v souladu s příslušnými ustanoveními směrnice (EU) 2022/2555.***

Článek 7

Spolupráce a sdílení informací se *sítí CSIRT*

1. Pokud přeshraniční bezpečnostní operační střediska získají informace týkající se potenciálního nebo probíhajícího rozsáhlého kybernetického bezpečnostního incidentu ***za účelem sdílení situačního povědomí, koordinační bezpečnostní operační středisko poskytne*** příslušné informace ***svému týmu CSIRT nebo příslušnému orgánu, který je bez zbytečného odkladu oznámí*** EU-CyCLONe, síti CSIRT a Komisi ***a agentuře ENISA*** s ohledem na jejich

příslušné úlohy ***a postupy*** v oblasti řešení krizí v souladu se směrnicí (EU) 2022/2555. ***Tento odstavec neukládá veřejným ani soukromým subjektům další povinnosti oznamovat případný nebo probíhající rozsáhlý kybernetický bezpečnostní incident, pokud jde o plnění povinností stanovených ve směrnici (EU) 2022/2555.***

2. Komisi ***je svěřena pravomoc přijímat akty v přenesené pravomoci v souladu s článkem 20a po konzultaci se sítí CSIRT za účelem doplnění tohoto nařízení stanovením procesních*** opatření pro sdílení informací podle odstavce 1 ***tohoto článku a v souladu se směrnicí (EU) 2022/2555***.

Článek 8

Zabezpečení

1. Členské státy, které se účastní evropského kybernetického štítu, zajistí vysokou úroveň ***důvěrnosti a*** 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. ***Řídí se směrnicemi (EU) 2022/2555 a (EU) 2022/2557***. Komise ***ve svých prováděcích aktech*** za podpory vysokého představitele zohlední příslušné normy zabezpečení na úrovni obrany, aby usnadnila spolupráci s vojenskými subjekty.

Kapitola III

MECHANISMUS PRO MIMOŘÁDNÉ UDÁLOSTI V ▌OBLASTI KYBERNETICKÉ BEZPEČNOSTI

Článek 9

Zřízení mechanismu pro mimořádné události v ▌oblasti *kybernetické bezpečnosti*

1. Zřizuje se mechanismus pro mimořádné události v ▌oblasti ***kybernetické bezpečnosti*** 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 ▌, 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 ***řízených bezpečnostních služeb*** 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.

1a. Po spuštění mechanismu Komise každý rok posoudí a zveřejní zprávu o pozitivních i negativních aspektech fungování mechanismu, včetně toho, zda jsou zapotřebí další požadavky na spolupráci nebo odbornou přípravu.

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 ***v souladu s opatřeními zavedenými pro subjekty z vysoce kritických odvětví vyjmenovaných v příloze I směrnice (EU) 2022/2555***.

2. Skupina pro spolupráci v oblasti bezpečnosti sítí a informací ve spolupráci s Komisí, agenturou ENISA a vysokým představitelem ***a subjekty, které se podrobují koordinovanému testování připravenosti podle odstavce 1,*** vypracuje společné rizikové scénáře a metodiky pro koordinované testování ***připravenosti, což vyvrcholí pracovním plánem vypracovaným po vzájemné dohodě***. ***Subjekty podrobované koordinovanému testování připravenosti vypracují a provedou plán nápravy, kterým se provádí doporučení vyplývající z testování připravenosti.***

Skupina pro spolupráci v oblasti bezpečnosti sítí a informací může přispět k určování priorit odvětví nebo pododvětví pro koordinované testování připravenosti.

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.

Pokud je zjevné, že pořízené služby nemohou být plně využity pro účely poskytování podpory pro reakci na významné nebo rozsáhlé incidenty, lze tyto služby výjimečně využít v podobě cvičení nebo školení pro vypořádání se s incidenty a na požádání je může veřejný zadavatel poskytnout uživatelům.

2. Rezerva EU pro kybernetickou bezpečnost se skládá ze služeb reakce na incidenty od důvěryhodných poskytovatelů ***řízených bezpečnostních služeb*** vybraných v souladu s kritérii stanovenými v článku 16. Rezerva ***EU pro kybernetickou bezpečnost*** zahrnuje předem přislíbené služby. Služby musí být možné provádět ve všech členských státech***, musí posilovat technologickou suverenitu Unie, její otevřenou strategickou autonomii, konkurenceschopnost a odolnost v odvětví kybernetické bezpečnosti, mimo jiné i prostřednictvím podpory inovací na jednotném digitálním trhu v rámci celé Unie***.

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 ***ve smyslu čl. 3 odst. 1 nařízení Evropského parlamentu a Rady (EU) .../2023[26] a CERT-EU***.

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 ***ve spolupráci se skupinou pro spolupráci v oblasti bezpečnosti sítí a informací a*** 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 ***pověří*** provozem a správou rezervy EU pro kybernetickou bezpečnost plně nebo zčásti 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***, včetně***

---

[26] ***Nařízení (EU) .../2023, kterým se stanoví opatření k zajištění vysoké společné úrovně kybernetické bezpečnosti v orgánech, institucích a jiných subjektech Unie (Úř. věst. C , , s. , ELI: ...).***

potřebných dovedností a kapacity pracovníků v oblasti kybernetické bezpečnosti a případně poskytovatelů řízených bezpečnostních služeb a jiných zástupců odvětví kybernetické bezpečnosti. Agentura ENISA po konzultaci s Komisí***, poskytovateli řízených bezpečnostních služeb a případně jiných zástupců odvětví kybernetické bezpečnosti*** 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 ***a informuje Radu o potřebách třetích zemí***.

8. ***Komisi je svěřena pravomoc přijímat akty v přenesené pravomoci v souladu s článkem 20a za účelem doplnění tohoto nařízení upřesněním druhů a počtu*** služeb reakce požadovaných pro rezervu EU pro kybernetickou bezpečnost. ▌

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. ***Komisi je svěřena pravomoc přijímat akty v přenesené pravomoci v souladu s článkem 20a za účelem doplnění tohoto nařízení upřesněním podrobných*** opatření pro přidělování podpůrných služeb z rezervy EU pro kybernetickou bezpečnost. ▌

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 ***bez zbytečného prodlení a v každém případě do 24 hodin*** 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) ***rozsah a*** 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 ***a veškerá další ustanovení, která strany dohody považují za nezbytné pro poskytování příslušné služby***.

4. Dohody uvedené v odstavci 3 ***vycházejí*** ze vzorů, které vypracuje agentura ENISA po konzultaci s členskými státy ***a případně dalšími uživateli rezervy EU pro kybernetickou bezpečnost***.

5. Komise a agentura ENISA nenesou žádnou smluvní odpovědnost za škody způsobené třetím osobám službami poskytovanými v rámci provádění rezervy EU pro kybernetickou bezpečnost***, s výjimkou případů hrubé nedbalosti při hodnocení žádosti poskytovatele služeb nebo v případě, že jsou Komise nebo agentura ENISA uživateli rezervy EU pro kybernetickou bezpečnost podle čl. 14 odst. 3***.

6. Do jednoho měsíce od ukončení podpůrné akce předloží uživatelé Komisi a agentuře ENISA***, síti CSIRT a případně síti EU-CyCLONe*** 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.
Zpráva dodržuje unijní a vnitrostátní právní předpisy týkající se ochrany citlivých nebo utajovaných informací.

7. Komise ***pravidelně a nejméně dvakrát ročně*** podává skupině pro spolupráci v oblasti bezpečnosti sítí a informací pravidelné zprávy o využívání podpory a jejích výsledcích. ***Chrání důvěrné informace v souladu s právem Unie a vnitrostátním právem týkajícím se ochrany citlivých nebo utajovaných údajů.***

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[27], 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 ▌ oblasti ***kybernetické bezpečnosti*** 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 ***SFEU*** nebo k této pomoci přispívat.

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

Článek 16

Důvěryhodní poskytovatelé

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 ***a dosažení genderové vyváženosti v tomto odvětví a posílení technologické suverenity, otevřené strategické autonomie, konkurenceschopnosti a odolnosti Unie.***

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

[27] 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).

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 ***aktuálním*** hardwarovým a softwarovým technickým zařízením nezbytným pro podporu požadované služby ***a případně jedná v souladu s nařízením Evropského parlamentu a Rady (EU) .../...[28] (2022/0272(COD))***;

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 ***nebo v jednom z pracovních jazyků orgánů Unie***, v němž/nichž může službu poskytovat;

j) jakmile bude zaveden ***evropský*** systém ***certifikace kybernetické bezpečnosti*** pro řízené bezpečnostní služby podle nařízení (EU) 2019/881, bude poskytovatel certifikován v souladu s tímto systémem ***do dvou let od přijetí tohoto systému;***

ja) poskytovatel musí být schopen poskytnout službu nezávisle a ne jako součást balíčku, a tím zachovat možnost uživatelů přejít k jinému poskytovateli služeb;

jb) pro účely čl. 12 odst. 1 poskytovatel začlení do návrhu předloženého v rámci výzvy možnost přeměny nepoužívaných služeb reakce na incidenty do podoby cvičení nebo školení;

jc) poskytovatel musí být usazen a musí mít své struktury výkonného vedení v Unii, v přidružené zemi nebo ve třetí zemi, která je stranou dohody o vládních zakázkách v kontextu Světové obchodní organizace;

jd) poskytovatel nepodléhá kontrole ze strany nepřidružené třetí země nebo subjektu nepřidružené třetí země, která není stranou dohody o vládních zakázkách, nebo případně musí být nejprve podroben prověřování ve smyslu nařízení (EU) 2019/452 a v nezbytných případech podléhá zmírňujícím opatřením, a to s přihlédnutím k cílům uvedeným v tomto nařízení.

---

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

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 ***bez zbytečného odkladu informuje Radu o*** obdržených ***žádostech*** a provádění podpory poskytované třetím zemím z rezervy EU pro kybernetickou bezpečnost ***a koordinuje tuto činnost s vysokým představitelem***.

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 ***a shromažďuje od nich zpětnou vazbu***, včetně zástupců členských států, Komise, dalších příslušných orgánů, institucí a jiných subjektů EU, poskytovatelů řízených bezpečnostních služeb a uživatelů služeb kybernetické bezpečnosti ***v národních a přeshraničních bezpečnostních operačních střediscích doplněné zárukami a***

monitorováním, které je přiměřené k zajištění toho, aby získané poznatky a zjištěné osvědčené postupy podpořili aktéři v odvětví 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. ***Nesmí obsahovat žádné podrobnosti o aktivně zneužívaných zranitelnostech, které zůstávají neopravené.***

3a. Zpráva uvedená v odstavci 1 tohoto článku uvádí poznatky získané ze vzájemných hodnocení provedených podle článku 19 směrnice (EU) 2022/2555.

4. Dle potřeby zpráva uvádí doporučení***, a to i pro všechny příslušné zúčastněné strany,*** 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:

i) 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“;

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

„g) zřídit a provozovat mechanismus pro mimořádné události v ▌oblasti ***kybernetické bezpečnosti*** 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“;

b) odstavec 2 se nahrazuje tímto:

„2. Akce v rámci specifického cíle č. 3 jsou prováděny především prostřednictvím Evropského průmyslového, technologického a výzkumného centra kompetencí pro kybernetickou bezpečnost a sítě národních koordinačních center v souladu s nařízením Evropského parlamentu a Rady (EU) 2021/887*, s výjimkou opatření, kterými se provádí rezerva EU pro kybernetickou bezpečnost, jež provádí Komise a agentura ENISA.

_____

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

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) ***1 620 566 000*** EUR pro specifický cíl č. 3 Kybernetická bezpečnost a důvěra;

d) ***500 347 000*** EUR pro specifický cíl č. 4 Pokročilé digitální dovednosti“;

aa) vkládá se nový odstavec 2a, který zní:

„2a. Částka uvedená v odst. 2 písm. c) se primárně využije na dosažení operačních cílů uvedených v čl. 6 odst. 1 písm. a) až f) programu.“;

ab) doplňuje se nový odstavec 2b, který zní:

„2b. Částka pro zřízení a provedení rezervy EU pro kybernetickou bezpečnost nepřekročí 27 milionů EUR po zamýšlenou dobu trvání nařízení, 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.“;

b) doplňuje se nový odstavec 8, který zní:

„8. Odchylně od čl. 12 odst. 4 nařízení (EU, Euratom) 2018/1046 se ***v souvislosti s prováděním rezervy EU pro kybernetickou bezpečnost*** 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.“;

Komise informuje Parlament a Rady o prostředcích přenesených v souladu s čl. 12 odst. 6 nařízení (EU, Euratom) 2018/1046.

3) V článku 14 se odstavec 2 nahrazuje tímto:

„2. Program může poskytovat financování kteroukoli z forem stanovených ***v*** nařízení ***(EU, Euratom) 2018/1046***, 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***/…*** 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 služby pro tyto třetí země, včetně pronájmu. Odchylně od čl. 169 odst. 3 nařízení (EU) ***…/…*** 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) ***…/…*** 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:

„***Článek 16a***

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/**…**. V případě rozporu mezi ustanoveními tohoto nařízení a články 4 a 5 nařízení (EU) 2023/**…** 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 ▌nařízení ***(EU, Euratom) 2018/1046*** a mohou pokrývat až 100 % způsobilých nákladů, aniž je dotčena zásada spolufinancování stanovená v článku 190 ▌nařízení ***(EU, Euratom) 2018/1046***. 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) ▌nařízení ***(EU, Euratom) 2018/1046*** udělovat národním bezpečnostním operačním střediskům podle článku 4 nařízení ***(EU) .../...*** a hostitelskému konsorciu podle článku 5 nařízení ***(EU) .../...*** přímo centrum ECCC bez výzvy k předkládání návrhů.

Podporu v podobě grantů pro mechanismus pro mimořádné události v ▌oblasti ***kybernetické bezpečnosti*** podle článku 10 nařízení ***(EU) .../...*** může v souladu s čl. 195 odst. 1 písm. d) ▌nařízení ***(EU, Euratom) 2018/1046*** udělovat členským státům přímo centrum ECCC bez výzvy k předkládání návrhů.

U akcí uvedených v čl. 10 odst. 1 písm. c) nařízení ***(EU) .../...*** 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 ***(EU) .../...*** a v souladu s čl. 193 odst. 2 druhým pododstavcem písm. a) ▌nařízení ***(EU, Euratom) 2018/1046*** lze v řádně odůvodněných případech považovat náklady za způsobilé i tehdy, pokud vznikly před podáním žádosti o grant.“;

6) Přílohy I a II nařízení (EU) 2021/694 se mění v souladu s přílohou tohoto nařízení.

Článek 19a
Dodatečné zdroje pro agenturu ENISA

Agentura ENISA obdrží dodatečné zdroje na plnění svých dodatečných úkolů stanovených v tomto nařízení. Tato dodatečná podpora, včetně financování, neohrozí dosažení cílů jiných programů Unie, zejména programu Digitální Evropa.

Článek 20

Hodnocení *a přezkum*

1. Do [***dvou*** let ode dne použitelnosti tohoto nařízení] ***a poté každé dva roky provede*** Komise ***hodnocení fungování opatření stanovených v tomto nařízení a předloží*** zprávu ▌ Evropskému parlamentu a Radě.

2. Hodnocení posoudí zejména:

a) používání a přidanou hodnotu přeshraničních bezpečnostních operačních středisek a míru, v jaké přispívají k podpoře odhalování kybernetických hrozeb a situačního povědomí a k reakci na ně; aktivní účast národních bezpečnostních operačních středisek v rámci evropského kybernetického štítu, včetně počtu národních bezpečnostních operačních středisek a přeshraničních bezpečnostních operačních středisek, a míru, v jaké přispívá k vytvoření a výměně vysoce kvalitních použitelných informací a zpravodajských informací o kybernetických hrozbách; počet infrastruktur nebo nástrojů kybernetické bezpečnosti pořízených na základě společné veřejné zakázky a náklady na ně; počet dohod o spolupráci uzavřených mezi přeshraničními bezpečnostními operačními středisky a s odvětvovými středisky ISAC; počet incidentů oznámených síti CSIRT a dopad, který to má na činnost sítě CSIRT;

b) pozitivní i negativní aspekty fungování mechanismu pro mimořádné události v oblasti kybernetické bezpečnosti, včetně toho, zda jsou zapotřebí další požadavky na spolupráci nebo odbornou přípravu;

c) přínos tohoto nařízení k posílení odolnosti a otevřené strategické autonomie Unie, ke zlepšení konkurenceschopnosti příslušných průmyslových odvětví, mikropodniků, malých a středních podniků, včetně začínajících, a k rozvoji dovedností v oblasti kybernetické bezpečnosti v Unii;

d) používání a přidanou hodnotu rezervy EU pro kybernetickou bezpečnost, včetně počtu důvěryhodných poskytovatelů bezpečnosti, které jsou součástí rezervy EU pro kybernetickou bezpečnost; počet, typ, náklad a dopad opatření provedených na podporu reakce na bezpečnostní incidenty, jakož i jejich uživatele a poskytovatele; průměrná doba, během které Komise potvrdí, že rezerva EU pro kybernetickou bezpečnost má být využita, a zareaguje a uživatelé se z incidentu zotaví; zda by oblast působnosti rezervy EU pro kybernetickou bezpečnost neměla být rozšířena na služby připravenosti na incidenty nebo společná cvičení s důvěryhodnými poskytovateli řízených bezpečnostních služeb a potenciálními uživateli rezervy EU pro kybernetickou bezpečnost, aby se v případě potřeby zajistilo účinné fungování rezervy EU pro kybernetickou bezpečnost;

e) příspěvek tohoto nařízení k rozvoji a zlepšování dovedností a kompetencí pracovní síly v odvětví kybernetické bezpečnosti, které jsou nezbytné k posílení schopnosti Unie odhalovat kybernetické hrozby a incidenty, předcházet jim, reagovat na ně a zotavovat se z nich;

f) příspěvek tohoto nařízení k zavádění a vývoji nejmodernějších technologií v Unii;

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

Článek 20a

Výkon přenesené pravomoci

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

2. Pravomoc přijímat akty v přenesené pravomoci uvedená v čl. 6 odst. 3, čl. 7 odst. 2, čl. 12 odst. 8, a čl. 13 odst. 7 je svěřena Komisi na dobu ... let od … [datum vstupu základního legislativního aktu v platnost či jiný datum stanovený spolunormotvůrci]. Komise vypracuje zprávu o výkonu přenesení pravomoci nejpozději devět měsíců před koncem tohoto ... období. Přenesení pravomoci se automaticky prodlužuje o stejně dlouhá období, pokud Evropský parlament ani Rada nevysloví proti tomuto prodloužení námitku nejpozději tři měsíce před koncem každého z těchto období.

3. Evropský parlament nebo Rada mohou přenesení pravomoci uvedené v čl. 6 odst. 3, čl. 7 odst. 2, čl. 12 odst. 8 a čl. 13 odst. 7 kdykoli zrušit. Rozhodnutím o zrušení se ukončuje přenesení pravomoci v něm určené. Rozhodnutí nabývá účinku prvním dnem po zveřejnění v Úředním věstníku Evropské unie nebo k pozdějšímu dni, který je v něm upřesněn. Nedotýká se platnosti žádných již platných aktů v přenesené pravomoci.

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

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

6. Akt v přenesené pravomoci přijatý podle čl. 6 odst. 3, čl. 7 odst. 2, čl. 12 odst. 8 a čl. 13 odst. 7 vstoupí v platnost, pouze pokud proti němu Evropský parlament nebo Rada nevysloví námitky ve lhůtě dvou měsíců ode dne, kdy jim byl tento akt oznámen, nebo pokud Evropský parlament i Rada před uplynutím této lhůty informují Komisi o tom, že námitky nevysloví. Z podnětu Evropského parlamentu nebo Rady se tato lhůta prodlouží o [dva měsíce].

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*

PŘÍLOHA

Nařízení (EU) 2021/694 se mění takto:

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

„Specifický cíl č. 3 – Kybernetická bezpečnost a důvěra

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

Počáteční a případně následné akce v rámci tohoto cíle zahrnují:

1. Společné investování spolu s členskými státy do vyspělého zařízení, infrastruktury

a know-how v oblasti kybernetické bezpečnosti, jež jsou zásadní pro ochranu klíčových infrastruktur a jednotného digitálního trhu jako takového. Toto společné investování by mohlo zahrnovat investice do kvantových zařízení a datových zdrojů pro kybernetickou bezpečnost, povědomí o situaci v kyberprostoru, ***včetně národních bezpečnostních operačních středisek a přeshraničních bezpečnostních operačních středisek tvořících evropský kybernetický štít,*** jakož i dalších nástrojů, které budou zpřístupněny veřejnému i soukromému sektoru v celé Evropě.

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

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

4. Podpora odstraňování nedostatků v dovednostech v oblasti kybernetické bezpečnosti***, se zvláštním zaměřením na dosažení genderové vyváženosti v odvětví***, např. slaďováním vzdělávacích programů v oblasti kybernetické bezpečnosti, jejich přizpůsobováním potřebám konkrétních odvětví***, včetně interdisciplinárního a obecného zaměření,*** a usnadňováním přístupu ke specializované odborné přípravě***, která zlepší postavení všech osob a území, aniž je dotčena možnost využívat příležitostí, které toto nařízení poskytuje***.

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

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

„Specifický cíl č. 3 – Kybernetická bezpečnost a důvěra

3.1. Počet infrastruktur nebo nástrojů kybernetické bezpečnosti pořízených na základě společné veřejné zakázky ***jako součást štítu pro kybernetickou bezpečnost.***

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

3.3. Počet***, typ, náklady a dopad*** opatření ***provedených*** na podporu připravenosti a reakce na kybernetické bezpečnostní incidenty v rámci mechanismu pro mimořádné situace v oblasti ***kybernetické bezpečnosti***. ***Rozsah, v jakém byla doporučení vyplývající z testování připravenosti provedena a zavedena uživatelem, jakož i průměrná doba, během které Komise potvrdí, že rezerva EU pro kybernetickou bezpečnost má být využita, a zareaguje a uživatel se z incidentu zotaví.“***

VYSVĚTLUJÍCÍ PROHLÁŠENÍ

SOUVISLOSTI

Kybernetická bezpečnost je a měla by být středobodem našich demokracií. Hrozby pro kybernetickou bezpečnost souvisejí se šířením nejistoty mezi obyvatelstvem a společnostmi, jakož i s nárůstem dezinformací, což zpochybňuje demokratické zásady, které chrání dodržování lidských práv. Aby se tomu zabránilo, má pro naše demokracie zásadní význam bezpečné digitální prostředí podléhající veřejné kontrole.

Kybernetické útoky v EU jsou na vzestupu, pokud jde o metody a dopad. Kromě toho útok Ruska na Ukrajinu přinesl hluboké změny, a to už před invazí, a podle zprávy agentury ENISA o stavu hrozeb z roku 2022 zahájil novou éru **kybernetického softwaru**.[1] Prioritami vycházejícími z tohoto konfliktu v oblasti kybernetiky jsou potřeba **budovat kapacity** v **mnohostranných programech** a projektech a potřeba rychle **rozvíjet dovednosti**. V zájmu větší odolnosti je naléhavě zapotřebí společná evropská reakce založená na posílené spolupráci na evropské úrovni nad rámec spolupráce na vnitrostátní úrovni.

Klíčem k úspěšnému provádění tohoto nařízení bude posílení kultury kybernetické bezpečnosti, která chápe bezpečnost, včetně bezpečnosti digitálního prostředí, jakožto veřejný statek.

Kybernetické útoky jsou navíc často zaměřeny na **místní, regionální nebo vnitrostátní veřejné služby** a infrastruktury (např. zdravotnictví, které zůstává hlavním cílem kybernetických útoků[2]). Důkazy rovněž poukazují na to, že **místní orgány** patří k nejzranitelnějším cílům z důvodu nedostatku finančních a lidských zdrojů a že je obzvláště důležité, aby vedoucí představitelé na místní úrovni měli povědomí o zvyšování digitální odolnosti[3]. Útoky se primárně a přímo dotýkají občanů, a ohrožují tak naše demokracie, a to i prostřednictvím dezinformačních kampaní. Pocit nejistoty, který tyto situace mohou vyvolat u obyvatelstva, může vést k politickým preferencím, které se řídí radikálním závazkem k bezpečnosti na úkor dodržování základních práv. Nicméně spíše opak je pravdou: bezpečnost je nezbytnou součástí našich demokracií, která je slučitelná se všemi ostatními právy a je pro ně nezbytná.

Kromě toho **společnosti a malé a střední podniky** v EU zažívají kyberkriminalitu a vzhledem k rostoucímu využívání digitální sféry k řízení podniků panují větší obavy o kybernetickou bezpečnost. Malé a střední podniky jsou méně připravené, mají méně zdrojů na svou ochranu a ještě méně si uvědomují, že mohou být předmětem takových útoků.

Očekává se, že tyto útoky budou v budoucnu pokračovat a budou se zvyšovat. Zejména v situacích politické nestability a zejména v souvislosti s válkou. Vzhledem k tomu, že digitální

[1] Zpráva agentury ENISA o typech ohrožení 2022, říjen 2022. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022/@@download/fullReport
[2] Zpráva agentury ENISA o typech ohrožení: Odvětví zdravotnictví, červenec 2023. https://www.enisa.europa.eu/publications/health-threat-landscape/@@download/fullReport
[3] Evropský výbor regionů, Digital Resilience (Digitální odolnost), 2023. https://cor.europa.eu/en/engage/studies/Documents/Digital%20resilience.pdf.

transformace každý den pokračuje, je digitální odolnost stále důležitější pro náš každodenní život a pro **otevřenou strategickou autonomii EU**.

NÁVRH ZPRAVODAJKY

Zpravodajka se domnívá, že EU musí být lépe připravena na budoucnost, a vítá tento naléhavý právní předpis, který spočívá ve sdílení opravných prostředků, informací a znalostí s cílem zajistit solidaritu mezi členskými státy, zvýšit průmyslovou kapacitu v EU, **koordinovaně** rozvíjet **dovednosti a schopnosti**, které zajistí kybernetickou bezpečnost, zvýšit odolnost vůči budoucím útokům a chránit naše demokracie před svévolným využíváním bezpečnostních potřeb. Kromě toho je důležité chránit integritu našich volebních procesů. Tento právní předpis je zásadním závazkem k dosažení cíle **otevřené strategické autonomie**.

Z těchto důvodů potřebuje EU silnou a **koordinovanou správu** v EU a strukturovanou spolupráci se soukromým sektorem na podporu rozvoje evropského kybernetického průmyslu, a to vedle spolupráce s podobně smýšlejícími mezinárodními partnery, ale také s dalšími zeměmi, které nemají stejné možnosti a mohou potřebovat pomoc, pokud se stanou oběťmi kybernetických útoků. Akt EU o kybernetické solidaritě musí dobře definovat svou správu a nesmí se překrývat s již existujícími iniciativami a právními předpisy, jako je směrnice NIS2.

Návrh je do značné míry založen na dobrovolné výměně informací mezi členskými státy. Z tohoto důvodu zpravodajka navrhuje posílit záruky pro budování důvěry mezi členskými státy s cílem zvýšit jejich účast a spolupráci, například pokud jde o společné pořizování infrastruktury, jakož i zapojení orgánů moci zákonodárné s cílem zajistit důvěru občanů a **demokratické záruky**.

Zadruhé zpravodajka navrhuje **zajistit rozpočet** z nadcházejících VFR pro tuto iniciativu, a to i se závazkem členských států, aby byla zaručena kontinuita činností vyvíjených v rámci aktu EU o kybernetické solidaritě po roce 2027.

Zatřetí zpravodajka navrhuje zlepšit **strukturu správy**, stanovit jasnou definici správy a propojit ji se stávajícími právními předpisy.

Zpravodajka rovněž navrhuje lepší **koordinaci** mezi různými subjekty členských států odpovědnými za kybernetickou bezpečnost s cílem nabídnout společný počítačový štít. Kromě toho navrhuje zvýšit příspěvek agentury ENISA ke koordinaci a interakci mezi různými aktéry vnitrostátních komunit.

V souvislosti s **novou rezervou pro kybernetickou bezpečnost** se zpravodajka domnívá, že by mohla přispět k rozvoji průmyslových kapacit v EU, a to i pro malé a střední podniky, prostřednictvím investic do výzkumu a inovací za účelem vývoje nejmodernějších technologií, jako jsou cloudové technologie a technologie umělé inteligence. Zpravodajka dále navrhuje, aby byla zachována účast průmyslu, posílila se kritéria a důvěra v jeho účast (tj. došlo k propojení jeho účasti s celostátní nebo místní společností) vyjasněním **kritérií** a definice **technologické suverenity** a aby byla zaručena rovnováha mezi subjekty z EU a ze třetích zemí. Rovněž navrhuje, aby **mechanismus pro mimořádné události v kybernetické oblasti**

používal **systém certifikace** pro soukromé poskytovatele za účelem budování dlouhodobého a důvěryhodného partnerství.

Pokud se týká **mechanismu přezkumu incidentů**, zpravodajka navrhuje posílit úlohu agentury ENISA a soukromého sektoru v rámci bezpečnostních operačních středisek, a to pomocí správných záruk a monitorování, aby bylo možné ověřit, zda zjištěné poznatky podporují i subjekty působící v tomto odvětví. Zpravodajka dále navrhuje zohlednit poznatky získané na základě vzájemných hodnocení podle směrnice NIS2 a zvýšit finanční prostředky poskytované agentuře ENISA s cílem zajistit účinné uplatňování právních předpisů a odpovídající ochranu při řešení kybernetických bezpečnostních hrozeb.

Kromě toho má tento návrh ze své podstaty velmi významný **vnější rozměr**, protože třetí země mohou získat přístup ke zdrojům a podpoře z aktu EU o kybernetické solidaritě prostřednictvím podpory při reakci na incidenty z rezervy EU pro kybernetickou bezpečnost a protože pro kybernetickou rezervu jsou stále zapotřebí aktéři ze soukromého sektoru pocházející ze třetích zemí. Vnější rozměr musí rovněž podléhat veřejné kontrole, na které se podílí i moc zákonodárná, aby bylo zaručeno, že se občané budou moci tohoto procesu účastnit. Kybernetická bezpečnost by měla být považována za veřejný statek.

Ústředním pilířem tohoto návrhu je navíc rozvoj dovedností a kompetencí, který by se neměl omezovat na pouhé investice do rozvoje znalostí, ale měl by se zaměřit na investice do přístupu pro všechny občany, aby si mohli tyto dovednosti osvojit. Zpravodajka navrhuje posílit vazbu na **Akademii dovedností EU v oblasti kybernetické bezpečnosti**, přičemž jejím záměrem je řešit nedostatek talentů v oblasti kybernetické bezpečnosti propojením soukromých a veřejných iniciativ a poskytováním odborné přípravy a certifikace občanům. Posílení této vazby si vyžádá záruky, aby se předešlo odlivu mozků, a nemělo by být na úkor mobility pracovních sil.

Podle návrhu zpravodajky je rovněž třeba investovat a začlenit aktivní opatření na rozvoj dovedností v tomto odvětví vzhledem k tomu, že rok 2023 je Evropským rokem dovedností, a zvýšit povědomí občanů. Opatření budou navržena tak, aby investice nezpůsobovaly nerovnováhu mezi členskými státy, neboť stávající vysoká poptávka a vysoké mzdy v tomto odvětví mohou vést k určitému druhu „odlivu mozků“ směrem k nejlépe placeným příležitostem.

Z těchto důvodů zpravodajka navrhuje posílit specializované, interdisciplinární a obecné dovednosti v celé EU se zvláštním zaměřením na ženy, neboť v oblasti kybernetické bezpečnosti přetrvávají genderové rozdíly, kdy ženy tvoří v průměru celosvětově jen 20 % pracovníků v tomto odvětví.[4] Ženy musí být přítomny při utváření digitální budoucnosti a její správy a podílet se na něm.

Zpravodajka dále navrhuje posílit při rozvoji dovedností a kompetencí trojúhelník mezi národními kompetenčními centry, Evropským centrem kompetencí pro kybernetickou bezpečnost (ECCC) a agenturou ENISA. Je třeba zvětšit úlohu **průmyslu** při **rozvoji dovedností** a navazovat partnerství s **akademickou obcí** a subjekty občanské společnosti, s

[4] Usnesení Evropského parlamentu ze dne 10. června 2021 o prosazování rovnosti žen a mužů ve vzdělávání a zaměstnání v oblasti přírodních věd, technologií, inženýrství a matematiky (obory STEM) (2019/2164(INI)) https://www.europarl.europa.eu/doceo/document/TA-9-2021-0296_CS.html#def_1_22

přihlédnutím k regionálním zkušenostem, znalostem a specializaci a spojenectvím jednotlivých zemí, s podobně smýšlejícími partnery za účelem intenzivnějších kontaktů a zajištění globálního přístupu na podporu občanů, podniků a institucí.

Zpravodajka rovněž navrhuje spolupracovat v oblasti talentů a měření škod způsobených kybernetickými útoky lidem (např. dopad ransomwarového útoku na zdravotnictví).

Jako další opatření ochrany našich demokracií a základních hodnot předkládá zpravodajka opatření k zapojení a zvýšení povědomí občanů bez vzbuzování paniky. Také je třeba posílit **kulturu kybernetické bezpečnosti**, která chápe bezpečnost, včetně bezpečnosti digitálního prostředí, jakožto veřejný statek. Tímto způsobem budeme schopni zaručit model digitální demokracie, na rozdíl od digitálního autoritářství, založený na transparentnosti, demokracii a jistotě, kterou může přinést vypracování právních předpisů ex ante.

Zpravodajka se dále domnívá, že posílení **výzkumu a inovací** v oblasti kybernetické bezpečnosti zvýší odolnost a otevřenou strategickou autonomii EU. Rovněž je třeba zajistit součinnost s programy v oblasti výzkumu a inovací a se stávajícími nástroji a institucemi, jakož i posílit trojúhelník znalostí s cílem překlenout nedostatek dovedností v celé EU.

Kromě toho toto nařízení zvýší odolnost EU a jejích členských států, a to nejen přímo prostřednictvím právních předpisů v oblasti kybernetické bezpečnosti a kybernetické odolnosti, ale také prostřednictvím dopadu, který může mít na exponenciální rozvoj umělé inteligence, a dopadu, který může mít regulace a ochrana údajů na kybernetickou bezpečnost.

Tento právní předpis dále přispěje ke splnění závazku vyplývajícího z **evropského prohlášení o digitálních právech a zásadách pro digitální dekádu**, který souvisí s ochranou zájmů lidí, podniků a veřejných institucí před riziky v oblasti kybernetické bezpečnosti a před kyberkriminalitou, včetně narušení bezpečnosti údajů a krádeží identity nebo manipulace s ní.

V této souvislosti se zpravodajka domnívá, že tento návrh, včetně evropského štítu pro kybernetickou bezpečnost a mechanismu pro mimořádné události v kybernetické oblasti, by měl být funkční co nejdříve, abychom měli k dispozici obecný rámec a nevznikaly uzavřené struktury, neboť kybernetický prostor nezná hranice.

PŘÍLOHA: SUBJEKTY NEBO OSOBY, OD NICHŽ ZPRAVODAJKA OBDRŽELA PODNĚTY

Zpravodajka v souladu s článkem 8 přílohy I jednacího řádu prohlašuje, že při vypracovávání zprávy až do okamžiku jejího přijetí ve výboru obdržela podněty od těchto subjektů nebo osob:

Subjekt nebo osoba
CorwdStrike
CyberPeace institute
Microsoft Corporation
Romanian National Cyber Security Directorate
ENISA
Centro Criptológico Nacional
Permanent Representation of Spain
Trellix
Palo Alto Networks Inc
Committee of the regions rapporteur

Výše uvedený seznam je sestaven na výhradní odpovědnost zpravodajky.

27.10.2023

STANOVISKO VÝBORU PRO ZAHRANIČNÍ VĚCI

pro Výbor pro průmysl, výzkum a energetiku

k návrhu 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
(COM(2023)0209 – C9-0136/2023 – 2023/0109(COD))

Zpravodaj: Dragoş Tudorache

Pozměňovací návrh 1

Návrh nařízení
Bod odůvodnění 1

Znění navržené Komisí	*Pozměňovací návrh*
(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.	(1) Používání informačních a komunikačních technologií a závislost na nich je dnes základním aspektem ve všech odvětvích hospodářské ***a vojenské*** činnosti, neboť naše orgány státní správy, společnosti a občané ***a také subjekty ve vojenské a obranné oblasti*** jsou více než kdykoli předtím vzájemně propojení a závislí, a to napříč odvětvími i hranicemi.

Pozměňovací návrh 2

Návrh nařízení
Bod odůvodnění 2

Znění navržené Komisí	*Pozměňovací návrh*
(2) Rozsah, četnost a dopad kybernetických bezpečnostních incidentů se zvyšuje, včetně útoků na dodavatelský řetězec, a jejich cílem je kybernetická špionáž, ransomware nebo narušení	(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.

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. ***Závažnost těchto hrozeb se stala ještě aktuálnější v souvislosti s návratem války na náš kontinent. Tyto hrozby přesahují*** rámec ruské vojenské agrese vůči Ukrajině a pravděpodobně ***budou*** 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 ***a bezpečnosti*** Unie a mohou mít i zdraví nebo životy ohrožující následky***, neboť by mohly narušit činnost místních či celostátních zařízení spojených s bezpečností***. 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. ***Kybernetická bezpečnost je důležitá pro ochranu našich evropských hodnot a zajišťuje fungování našich demokracií tím, že chrání naši volební infrastrukturu a demokratické postupy před veškerým zahraničním vměšováním.***

Pozměňovací návrh 3

Návrh nařízení
Bod odůvodnění 2 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	(2a) Kybernetická bezpečnost má zásadní význam pro zachování bezpečnosti naší Unie a pro zamezení tomu, aby státní i nestátní subjekty s nekalými úmysly podkopávaly naši demokracii, hospodářství a bezpečnost. Je nezbytné zabránit nejednotnosti, neboť taková situace by nebyla vhodným přístupem, zejména pokud bychom čelili hrozbě budoucího rozsáhlého kybernetického útoku zaměřeného na několik členských států současně nebo na nadnárodní kritickou infrastrukturu. Proto je zapotřebí orgán Unie, který by fungoval jako koordinační platforma pro všechny stávající i budoucí nástroje, fondy a mechanismy v oblasti kybernetické bezpečnosti.

Pozměňovací návrh 4

Návrh nařízení
Bod odůvodnění 3

Znění navržené Komisí	*Pozměňovací návrh*
(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[16], 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	(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[16], 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.	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***, a zlepšit svou schopnost proaktivního jednání a rozhodné reakce na kybernetické bezpečnostní hrozby a incidenty***.
[16] https://futureu.europa.eu/cs/	[16] https://futureu.europa.eu/cs/

Pozměňovací návrh 5

Návrh nařízení
Bod odůvodnění 4

Znění navržené Komisí	*Pozměňovací návrh*
(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[17], doporučení Komise (EU) 2017/1584[18], směrnici Evropského parlamentu a Rady 2013/40/EU[19] a nařízení Evropského parlamentu a Rady (EU) 2019/881[20]. 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.	(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[17], doporučení Komise (EU) 2017/1584[18], směrnici Evropského parlamentu a Rady 2013/40/EU[19] a nařízení Evropského parlamentu a Rady (EU) 2019/881[20]. 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, ***proaktivně,*** 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. ***Kromě toho Unie v březnu 2022 schválila a spustila Strategický kompas pro bezpečnost a obranu, který se mimo jiné zaměřuje na posílení kybernetické bezpečnosti a prohloubení mezinárodní***

spolupráce s podobně smýšlejícími spojenci a demokratickými partnery, zejména v této oblasti. Kybernetická bezpečnost kromě toho tvoří ústřední bod nedávného třetího společného prohlášení o spolupráci mezi EU a NATO z ledna 2023. Zejména v závěrečné hodnotící zprávě vypracované pracovní skupinou EU-NATO se doporučuje plně využívat součinnosti mezi EU a NATO[1], včetně výměny osvědčených postupů mezi civilními a vojenskými subjekty při provádění příslušných politik a právních předpisů souvisejících s kybernetickou bezpečností.

[1] https://commission.europa.eu/document/34209534-3c59-4b01-b4f0-b2c6ee2df736_en

---

[17] 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).

[18] 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).

[19] 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).

[20] 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

[17] 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).

[18] 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).

[19] 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).

[20] 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).	o kybernetické bezpečnosti“) (Úř. věst. L 151, 7.6.2019, s. 15).

Pozměňovací návrh 6

Návrh nařízení
Bod odůvodnění 6

Znění navržené Komisí	*Pozměňovací návrh*
(6) Společné sdělení o politice kybernetické obrany EU[22] 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 důvěryhodných soukromých poskytovatelů a testování kritických subjektů na potenciální zranitelnost na základě posouzení rizik v EU.	(6) Společné sdělení o politice kybernetické obrany EU[22] 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 důvěryhodných soukromých poskytovatelů a testování kritických subjektů na potenciální zranitelnost na základě posouzení rizik v EU. ***Rychle se vyvíjející oblast kybernetických hrozeb a překotný technologický vývoj navíc ukazují, že je zapotřebí posílené civilně-vojenské koordinace a spolupráce, jak zdůraznila Rada ve svých závěrech o politice EU pro kybernetickou obranu[1].***
	[1] Závěry Rady o politice EU pro kybernetickou obranu schválené Radou na zasedání dne 22. května 2023 (9618/23).
[22] Společné sdělení Evropskému parlamentu a Radě, Politika kybernetické obrany EU, JOIN/2022/49 final.	[22] Společné sdělení Evropskému parlamentu a Radě, Politika kybernetické obrany EU, JOIN/2022/49 final.

Pozměňovací návrh 7

Návrh nařízení
Bod odůvodnění 6 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	(6a) Vzhledem k nejasným hranicím mezi oblastí civilních a vojenských záležitosti a dvojímu využití kybernetických nástrojů a technologií je třeba, aby byl v digitální oblasti uplatňován komplexní a celostní přístup. V případě rozsáhlého kybernetického bezpečnostního incidentu a krize zahrnující více než jeden členský stát by mělo být zavedeno odpovídající řešení a řízení krize. Tyto struktury by měly organizovat výměnu informací, koordinaci a spolupráci se strukturami Unie v oblasti vnější bezpečnosti a řízení vojenských krizí a se subjekty členských států odpovědnými za bezpečnost a obranu (komunitou kybernetické obrany). To by se mělo vztahovat i na operace a mise v rámci společné bezpečnostní a obranné politiky, které provádí Unie s cílem zajistit mír a stabilitu ve svém sousedství i mimo něj.

Pozměňovací návrh 8

Návrh nařízení
Bod odůvodnění 7

Znění navržené Komisí	*Pozměňovací návrh*
(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	(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“).	přípravě na významné a rozsáhlé incidenty v oblasti kybernetické bezpečnosti, při reakci na ně a při okamžité obnově po nich***, včetně incidentů zahrnujících více než jeden členský stát. Je-li to proveditelné a nezbytné, měl by mechanismus pro mimořádné situace v oblasti kybernetické bezpečnosti organizovat výměnu informací a spolupráci s obrannými orgány členských států a měl by být podporován orgány, institucemi a jinými subjekty EU (společenství EU v oblasti kybernetické obrany)***; měl by být zřízen mechanismus přezkumu kybernetických bezpečnostních incidentů, který by přezkoumával a posuzoval konkrétní významné nebo rozsáhlé incidenty***. Tyto nové struktury by rovněž měly podporovat operace a mise SBOP EU***. Těmito opatřeními nejsou dotčeny články 107 a 108 Smlouvy o fungování Evropské unie (dále jen „SFEU“).

Pozměňovací návrh 9

Návrh nařízení
Bod odůvodnění 11

Znění navržené Komisí	*Pozměňovací návrh*
(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 mechanismu pro mimořádné události v oblasti kybernetické bezpečnosti účinně podporovat členské státy v boji proti kybernetickým hrozbám.	(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 mechanismu pro mimořádné události v oblasti kybernetické bezpečnosti účinně podporovat členské státy v boji proti kybernetickým hrozbám. ***Tato zvláštní pravidla by rovněž umožnila dlouhodobější finanční podporu pro***

	společné zadávání zakázek na vysoce bezpečné nástroje a infrastrukturu nové generace, aby se zlepšily schopnosti kolektivního odhalování s využitím nejnovějších technologií umělé inteligence a analýzy dat.

Pozměňovací návrh 10

Návrh nařízení
Bod odůvodnění 13

Znění navržené Komisí	*Pozměňovací návrh*
(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.	(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. ***Je-li to proveditelné a nezbytné, měla by bezpečnostní operační střediska rovněž umožnit účast obranných subjektů vytvořením „obranného pilíře“, pokud jde o správu a druh sdílených informací, jak je uvedeno ve společném sdělení o politice kybernetické obrany EU[1] a jak jej podpořil vysoký představitel.*** ***[1] Společné sdělení Evropskému parlamentu a Radě, Politika kybernetické obrany EU, JOIN/2022/49 final***

Pozměňovací návrh 11

Návrh nařízení
Bod odůvodnění 14

Znění navržené Komisí	*Pozměňovací návrh*
(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.	(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, ***včetně „obranného pilíře“,*** 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, ***a je-li to proveditelné a nezbytné, z vojenských zdrojů s dostatečnými pokyny ohledně sdílení informací,*** 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.

Pozměňovací návrh 12

Návrh nařízení
Bod odůvodnění 15

Znění navržené Komisí	*Pozměňovací návrh*
(15) Na vnitrostátní úrovni zajišťují monitorování, odhalování a analýzu	(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 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.

kybernetických hrozeb obvykle bezpečnostní operační střediska veřejných a soukromých subjektů v kombinaci s týmy CSIRT. Kromě toho si týmy CSIRT vyměňují informace v rámci 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 ***odolnosti*** Unie.

Pozměňovací návrh 13

Návrh nařízení
Bod odůvodnění 16

Znění navržené Komisí	*Pozměňovací návrh*
(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	(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***, jakož i komunita kybernetické obrany***). 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

dohody o spolupráci s jinými přeshraničními bezpečnostními operačními středisky.	operační střediska by také měla uzavírat dohody o spolupráci s jinými přeshraničními bezpečnostními operačními středisky ***a s operační sítí pro vojenské týmy pro reakci na počítačové hrozby (vojenské týmy CERT) – sítí MICNET, až bude vytvořena***.

Pozměňovací návrh 14

Návrh nařízení
Bod odůvodnění 17

Znění navržené Komisí	*Pozměňovací návrh*
(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	(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***, komunitě***

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.	***kybernetické obrany*** 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.

Pozměňovací návrh 15

Návrh nařízení
Bod odůvodnění 19

Znění navržené Komisí	*Pozměňovací návrh*
(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.	(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***, s výjimkou vysoce rizikových dodavatelů kritických produktů s digitálními prvky,*** 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. ***Při používání umělé inteligence by měl být zajištěn lidský dohled a dostatečná úroveň gramotnosti v oblasti umělé inteligence, nezbytná podpora a pravomoc k výkonu této funkce.***

Pozměňovací návrh 16

Návrh nařízení
Bod odůvodnění 19 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	(19 a) V souladu s nařízením [XX/XXXX (akt o kybernetické odolnosti)] by subjekty zapojené do evropského kybernetického štítu měly požadavky stanovené v tomto nařízení splnit také u všech produktů s digitálními prvky. Vzhledem k rostoucím rizikům plynoucím z ekonomických závislostí je nutné minimalizovat vystavení vysoce rizikovým dodavatelům kritických produktů prostřednictvím společného strategického rámce pro hospodářskou bezpečnost EU. Závislost na vysoce rizikových dodavatelích kritických produktů s digitálními prvky představuje strategické riziko, které je třeba řešit na úrovni Unie, zejména pokud se určitá země dopouští hospodářské špionáže nebo vyvíjí ekonomický nátlak a její právní předpisy zavazují ke svévolnému přístupu k jakémukoli druhu operací nebo údajů společností, zejména pokud jsou kritické produkty určeny k použití základními subjekty ve smyslu směrnice (EU) 2022/2555.

Pozměňovací návrh 17

Návrh nařízení
Bod odůvodnění 20

Znění navržené Komisí	*Pozměňovací návrh*
(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[25].	(20) Prostřednictvím shromažďování, sdílení a výměny údajů by měl evropský kybernetický štít posílit technologickou suverenitu Unie***, její strategickou autonomii, konkurenceschopnost a odolnost***. 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[25].

[25] 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).

[25]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).

Pozměňovací návrh 18

Návrh nařízení
Bod odůvodnění 25

Znění navržené Komisí	*Pozměňovací návrh*
(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 ***spolupráce26*** 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.	(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[1], nový projekt PESCO Koordinační středisko pro kybernetický a informační prostor (CIDCC) a navrhované koordinační středisko EU pro kybernetickou obranu (EUCDCC), které jej má nahradit,*** 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***, zejména v těchkandidátských zemích EU, které dosáhly souladu se společnou zahraniční***

a bezpečnostní politikou a společnou bezpečnostní a obrannou politikou EU, a bylo možné je podpořit v úsilí o budování vlastních kapacit kybernetické obrany a posílit přeshraniční a regionální spolupráci mezi těmito kandidátskými zeměmi v kybernetické oblasti.

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

---

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

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

Pozměňovací návrh 19

Návrh nařízení
Bod odůvodnění 26

Znění navržené Komisí	*Pozměňovací návrh*
(26) Tímto nástrojem nejsou dotčeny postupy a rámce pro koordinaci reakce na krize na úrovni Unie, zejména mechanismus civilní ochrany Unie[27], integrovaná opatření EU pro politickou reakci na krize[28], 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***.	(26) Tímto nástrojem nejsou dotčeny postupy a rámce pro koordinaci reakce na krize na úrovni Unie, zejména mechanismus civilní ochrany Unie[27], integrovaná opatření EU pro politickou reakci na krize[28], 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 ***rovněž*** koordinováno s prováděním opatření souboru nástrojů ***kybernetické diplomacie, čímž se posílí spolupráce na strategické, operační a technické úrovni mezi komunitou kybernetické obrany a dalšími komunitami v kybernetické oblasti, zejména za účelem posílení schopnosti bojovat proti kybernetickým hrozbám ze***

***zemí mimo Unii, včetně restriktivních opatření, která lze využít k předcházení nepřátelské činnosti v kyberprostoru a k reakci na ni*.**

[27] 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).

[28] 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.

[27] 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).

[28] 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.

Pozměňovací návrh 20

Návrh nařízení
Bod odůvodnění 28

Znění navržené Komisí	*Pozměňovací návrh*
(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	(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 cílem zmírnit dopady významných a rozsáhlých kybernetických bezpečnostních incidentů, podpořit okamžitou obnovu a/nebo obnovit fungování základních služeb.

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 cílem zmírnit dopady významných a rozsáhlých kybernetických bezpečnostních incidentů, podpořit okamžitou obnovu a/nebo obnovit fungování základních služeb***, přičemž by měl vhodným způsobem využívat celé řady možností obrany dostupných civilním a vojenským komunitám***.

Pozměňovací návrh 21

Návrh nařízení
Bod odůvodnění 29

Znění navržené Komisí	*Pozměňovací návrh*
(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	(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. ***Evropská služba pro vnější činnost (ESVČ), zejména prostřednictvím Zpravodajského a informačního centra EU (EU INTCEN) a jeho střediska pro hybridní hrozby, by se v případě potřeby měla s podporou***

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/***255429***. Výběr odvětví by měl rovněž zohlednit doporučení Rady o celounijním koordinovaném přístupu za účelem posílení odolnosti kritické infrastruktury.

zpravodajského ředitelství Vojenského štábu EU (EUMS) v rámci společné zpravodajsko-analytické složky (SIAC) rovněž zapojit do zajištění aktuálních posouzení, a přispět tak k určení odvětví nebo pododvětví***, která*** 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***. Tato testování by také měla hrát důležitou roli ve zlepšování spolupráce mezi civilními a vojenskými subjekty. Při organizování testování by proto Komise, ESVČ a agentura ENISA měly systematicky zvažovat zapojení účastníků z jiných kybernetických komunit, jako je Evropská obranná agentura (EDA) a další příslušné subjekty.*** 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[1]***. Výběr odvětví by měl rovněž zohlednit doporučení Rady o celounijním koordinovaném přístupu za

účelem posílení odolnosti kritické infrastruktury.

[1] 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.

---

[29] 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.

---

[29] 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.

Pozměňovací návrh 22

Návrh nařízení
Bod odůvodnění 32

Znění navržené Komisí	*Pozměňovací návrh*
(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 odborníků v rámci vzájemné pomoci. Způsobilé náklady mohou zahrnovat cestovní výdaje, výdaje na ubytování a denní příspěvky pro odborníky na kybernetickou bezpečnost.	(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 odborníků v rámci vzájemné pomoci***, což by mělo zajistit účinnou koordinaci mezi příslušnými programy a nástroji EU, včetně Evropského mírového nástroje, SZBP a nástroje NDICI, při poskytování pomoci třetím zemím, zejména Ukrajině a Moldavsku***. Způsobilé náklady mohou zahrnovat cestovní výdaje, výdaje na ubytování a denní příspěvky pro odborníky na kybernetickou bezpečnost.

Pozměňovací návrh 23

Návrh nařízení
Bod odůvodnění 33

Znění navržené Komisí	*Pozměňovací návrh*
(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.	(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***, včetně misí SBOP***.

Pozměňovací návrh 24

Návrh nařízení
Bod odůvodnění 34

Znění navržené Komisí	*Pozměňovací návrh*
(34) Pro účely výběru soukromých poskytovatelů služeb, kteří budou poskytovat služby v rámci rezervy EU pro kybernetickou bezpečnost, je nezbytné	(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.	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***, přičemž je rovněž nezbytné zohlednit rizika spojená s účastí poskytovatelů ze zemí konkurenčních ze strategického hlediska, neboť může způsobit hospodářská bezpečnostní rizika, jakož i důsledky pro strategickou bezpečnost Unie***.

Pozměňovací návrh 25

Návrh nařízení
Bod odůvodnění 36

Znění navržené Komisí	*Pozměňovací návrh*
(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	(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. ***S ohledem na rozvoj bezpečného systému propojení vycházejícího z evropské kvantové komunikační infrastruktury (EuroQCI) a družicové komunikace Evropské unie v rámci státní správy (GOVSATCOM), zejména zavedení systému GALILEO GNSS pro uživatele obrany, by měl jakýkoli budoucí vývoj zohlednit nástup „hyperwaru“, který slučuje rychlost a sofistikovanost kvantové výpočetní techniky s vysoce autonomními vojenskými systémy, které mají schopnost devastovat společnost, a členské státy musí jako prioritu zajistit, aby byla upřednostněna ochrana celé***

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.

elektronické komunikační sítě, jako jsou vzdušné, pozemní a podmořské systémy. 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***, ESVČ a všem misím SBOP v zemi, které se incident týká, prostřednictvím jejich velitelství***.

Pozměňovací návrh 26

Návrh nařízení
Bod odůvodnění 37

Znění navržené Komisí	*Pozměňovací návrh*
(37) S ohledem na nepředvídatelnou povahu kybernetických bezpečnostních	(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.

útoků a skutečnost, že se často neomezují na určitou zeměpisnou oblast a představují vysoké riziko přelévání, přispívá posílení odolnosti sousedních zemí***, zejména Ukrajiny a Moldavska,*** a jejich schopnosti účinně reagovat na významné a rozsáhlé kybernetické bezpečnostní incidenty k ochraně Unie jako celku. Třetí země přidružené k programu Digitální Evropa ***by*** proto ***měly*** být podpořeny z rezervy EU pro kybernetickou bezpečnost***. Podpora by se měla vztahovat i na třetí země***, ***v nichž je nasazena mise SBOP se zvláštním mandátem k posílení odolnosti vůči hybridním hrozbám, včetně kybernetických hrozeb, nebo v nichž bylo přijato opatření pomoci*** v ***rámci Evropského mírového nástroje*** k ***posílení kybernetické odolnosti země***. 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.

Pozměňovací návrh 27

Návrh nařízení
Čl. 1 – odst. 1 – písm. c

Znění navržené Komisí	*Pozměňovací návrh*
c) zřízení evropského mechanismu pro kybernetické bezpečnostní incidenty, který bude přezkoumávat a posuzovat významné nebo rozsáhlé incidenty.	c) zřízení evropského mechanismu pro kybernetické bezpečnostní incidenty, který bude přezkoumávat a posuzovat významné nebo rozsáhlé incidenty ***či hrozby***.

Pozměňovací návrh 28

Návrh nařízení
Čl. 1 – odst. 2 – písm. a

Znění navržené Komisí	*Pozměňovací návrh*
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;	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 ***odolnosti*** Unie v oblasti kybernetické bezpečnosti;

Pozměňovací návrh 29

Návrh nařízení
Čl. 1 – odst. 2 – písm. b

Znění navržené Komisí	*Pozměňovací návrh*
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;	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 ***nebo třetím zemím, které jsou kandidáty na přistoupení k Unii a nejsou v rozporu s bezpečnostními a obrannými zájmy Unie a jejích členských států stanovenými v rámci SZBP podle hlavy V Smlouvy o EU; Členské státy by měly považovat aktivní program kybernetické obrany za součást své vnitrostátní strategie kybernetické bezpečnosti, která zahrnuje pravidelná společná cvičení odborné přípravy mezi členskými státy a napříč mezinárodními organizacemi. Takovýto program by měl zajišťovat synchronizovanou kapacitu pro zjišťování, odhalování, analýzu a zmírňování hrozeb v reálném čase***;

Pozměňovací návrh 30

Návrh nařízení
Čl. 1 – odst. 2 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	2a. snížit systémová kybernetická rizika spojená se závislostí na kritickém vybavení ze zemí, které by byly v rozporu s bezpečnostními a obrannými zájmy Unie a jejích členských států, jak je stanoveno v rámci SZBP podle hlavy V Smlouvy o EU;

Pozměňovací návrh 31

Návrh nařízení
Čl. 2 – odst. 2 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	„komunitou kybernetické obrany“ orgány členských států v oblasti obrany s podporou orgánů, institucí a jiných subjektů EU, jak je uvedeno ve společném sdělení Politika kybernetické obrany EU[1]
	[1] Společné sdělení Evropskému parlamentu a Radě, Politika kybernetické obrany EU, JOIN/2022/49 final

Pozměňovací návrh 32

Návrh nařízení
Čl. 3 – odst. 2 – pododstavec 1 – písm. b a (nové)

Znění navržené Komisí	*Pozměňovací návrh*
	ba) pomoci modernizovat celé systémy kybernetické obrany, zvýšit kvalitu schopností kybernetické obrany zaváděním systémů UI a urychlit výměnu informací mezi národními bezpečnostními operačními středisky a přeshraničními

bezpečnostními operačními středisky;

Pozměňovací návrh 33

Návrh nařízení
Čl. 3 – odst. 2 – pododstavec 1 – písm. d a (nové)

Znění navržené Komisí	*Pozměňovací návrh*
	da) provádět přezkum a hodnocení kritických technologií a zařízení v oblasti kybernetické bezpečnosti používaných bezpečnostními operačními středisky v reakci na kybernetické bezpečnostní incidenty u systémových rizik vyplývajících z kontroly vysoce rizikových poskytovatelů ze strany zemí, které by byly v rozporu s bezpečnostními a obrannými zájmy Unie a jejích členských států, jak je stanoveno v rámci SZBP podle hlavy V Smlouvy o EU.

Pozměňovací návrh 34

Návrh nařízení
Čl. 4 – odst. 1 – pododstavec 2

Znění navržené Komisí	*Pozměňovací návrh*
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.	Má kapacitu působit jako referenční bod a brána pro další veřejné a soukromé organizace na vnitrostátní úrovni, ***a případně vojenské subjekty,*** 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.

Pozměňovací návrh 35

Návrh nařízení
Čl. 4 – odst. 2

Znění navržené Komisí	*Pozměňovací návrh*
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.	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 ***za přísné podmínky, že tyto nástroje a infrastruktura jsou poskytovány důvěryhodnými poskytovateli v souladu s článkem 16***. 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.

Pozměňovací návrh 36

Návrh nařízení
Čl. 5 – odst. 2

Znění navržené Komisí	*Pozměňovací návrh*
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 %	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 ***za přísné podmínky, že tyto nástroje a***

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.	***infrastruktura jsou poskytovány důvěryhodnými poskytovateli v souladu s článkem 16***. 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.

Pozměňovací návrh 37

Návrh nařízení
Čl. 5 – odst. 2 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	2a. Každá infrastruktura nebo poskytovatel pocházející z vysoce rizikové třetí země jsou automaticky vyloučeny.

Pozměňovací návrh 38

Návrh nařízení
Čl. 6 – odst. 1 – písm. b a (nové)

Znění navržené Komisí	*Pozměňovací návrh*
	ba) přímo podporuje posílení vojenských a obranných schopností zúčastněných členů nebo brání přímému a bezprostřednímu ohrožení jejich bezpečnosti. Vzhledem k tomu, že využití zranitelných míst v odvětví obrany může způsobit závažné narušení a škodu, vyžaduje kybernetická bezpečnost v obranném průmyslu zvláštní opatření k zajištění bezpečnosti dodavatelských řetězců, zejména pokud jde o subjekty, které jsou v dodavatelském řetězci na nižším místě a nevyžadují přístup k utajovaným informacím, ale mohly by představovat závažné riziko pro celé odvětví. Zvláštní pozornost by měla být

	věnována dopadu, který by jakékoli porušení mohlo mít, a hrozbě jakékoli potenciální manipulace se síťovými daty, která by mohla vést k tomu, že by kritické obranné prostředky byly zbytečné nebo by dokonce převažovaly nad příslušnými operačními systémy, což by je činilo zranitelnými vůči "únosu".

Pozměňovací návrh 39

Návrh nařízení
Čl. 6 – odst. 1 – písm. b a (nové)

Znění navržené Komisí	*Pozměňovací návrh*
	bb) podporuje posílení obranných schopností zúčastněných členů nebo předchází přímému a bezprostřednímu ohrožení jejich bezpečnosti, přičemž zajišťuje bezpečnost dodavatelských řetězců, zejména pokud jde o subjekty, které jsou v dodavatelském řetězci na nižším místě a nevyžadují přístup k utajovaným informacím, ale mohly by představovat závažné riziko pro celé odvětví.

Pozměňovací návrh 40

Návrh nařízení
Čl. 7 – odst. 1

Znění navržené Komisí	*Pozměňovací návrh*
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.	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***, mimo jiné vysokému představiteli a ESVČ v případě, že jde o třetí zemi,*** s ohledem na jejich příslušné úlohy v oblasti řešení krizí v souladu se směrnicí (EU) 2022/2555.

Pozměňovací návrh 41

Návrh nařízení
Čl. 8 – odst. 1

Znění navržené Komisí	*Pozměňovací návrh*
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.	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, ***jakož i snížení rizik a podpora technologického náskoku EU v kritických odvětvích,*** včetně ***opatření k omezení či vyloučení vysoce rizikových dodavatelů a rovněž k ochraně*** bezpečnosti údajů vyměňovaných prostřednictvím této infrastruktury.

Pozměňovací návrh 42

Návrh nařízení
Čl. 8 – odst. 2

Znění navržené Komisí	*Pozměňovací návrh*
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.	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 ***a aby jakékoli sdílení informací s vysoce rizikovými poskytovateli bylo svým rozsahem omezeno a nebyla jím dotčena bezpečnost a strategické zájmy Unie***.

Pozměňovací návrh 43

Návrh nařízení
Čl. 8 – odst. 3

Znění navržené Komisí	*Pozměňovací návrh*
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.	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***, přičemž vhodným způsobem využívá celé řady možností obrany dostupných civilním a vojenským komunitám v zájmu širší bezpečnosti a obrany EU a informuje Evropský parlament***.

Pozměňovací návrh 44

Návrh nařízení
Čl. 9 – odst. 2

Znění navržené Komisí	*Pozměňovací návrh*
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**.**	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***, a dále jsou podporovány Evropským mírovým nástrojem při zajišťování opatření pomoci třetím zemím, zejména Ukrajině a Moldavsku;***

Pozměňovací návrh 45

Návrh nařízení
Čl. 10 – odst. 1 – písm. a

Znění navržené Komisí	*Pozměňovací návrh*
a) opatření v oblasti připravenosti, včetně koordinovaného testování připravenosti subjektů působících ve vysoce kritických odvětvích v celé Unii;	a) opatření v oblasti připravenosti, včetně koordinovaného testování připravenosti subjektů působících ve vysoce kritických odvětvích***, jako je veřejná infrastruktura, volební infrastruktura, doprava, finanční, telekomunikační, zdravotní péče, dodávky potravin a bezpečnost*** v celé Unii;

Pozměňovací návrh 46

Návrh nařízení
Čl. 10 – odst. 1 – písm. c

Znění navržené Komisí	*Pozměňovací návrh*
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.	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 ***a v kontextu čl. 42 odst. 7 SEU a článku 222 SFEU;***

Pozměňovací návrh 47

Návrh nařízení
Čl. 10 – odst. 1 – písm. c a (nové)

Znění navržené Komisí	*Pozměňovací návrh*
	ca) nahrazení a postupné vyřazení kritického zařízení od vysoce rizikových dodavatelů, kteří by byli v rozporu s bezpečnostními a obrannými zájmy Unie a jejích členských států, jak je stanoveno v rámci SZBP podle hlavy V Smlouvy o EU.

Pozměňovací návrh 48

Návrh nařízení
Čl. 11 – odst. 2

Znění navržené Komisí	*Pozměňovací návrh*
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.	2. Skupina pro spolupráci v oblasti bezpečnosti sítí a informací ve spolupráci s Komisí, agenturou ENISA***,*** vysokým představitelem***, ESVČ a případně Evropskou obrannou agenturou*** vypracuje společné rizikové scénáře a metodiky pro koordinované testování.

Pozměňovací návrh 49

Návrh nařízení
Čl. 12 – odst. 2

Znění navržené Komisí	*Pozměňovací návrh*
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.	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 ***a třetích zemích, které splňují příslušné požadavky tohoto nařízení***.

Pozměňovací návrh 50

Návrh nařízení
Čl. 12 – odst. 3 – písm. b

Znění navržené Komisí	*Pozměňovací návrh*
b) orgány, instituce nebo jiné subjekty Unie.	b) orgány, instituce nebo jiné subjekty Unie***, včetně misí SBOP***.

Pozměňovací návrh 51

Návrh nařízení
Čl. 12 – odst. 4

Znění navržené Komisí	*Pozměňovací návrh*
4. Uživatelé uvedení v odst. 3 písm. a)	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.

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, ***jako je veřejná infrastruktura, volební infrastruktura, doprava, zdravotnictví, finance, telekomunikace, dodávky potravin a bezpečnost,*** a k okamžité obnově po těchto incidentech.

Pozměňovací návrh 52

Návrh nařízení
Čl. 12 – odst. 5

Znění navržené Komisí	*Pozměňovací návrh*
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.	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 ***a cíli*** Unie***, zejména se strategickým cílem snížit závislosti na vysoce rizikových dodavatelích, kteří by byli v rozporu s bezpečnostními a obrannými zájmy Unie a jejích členských států, jak je stanoveno v rámci SZBP podle hlavy V Smlouvy o EU***.

Pozměňovací návrh 53

Návrh nařízení
Čl. 12 – odst. 7

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

Pozměňovací návrh 54

Návrh nařízení
Čl. 14 – odst. 2 – písm. a a (nové)

Znění navržené Komisí	*Pozměňovací návrh*
	aa) dopad incidentu na bezpečnost a obranu Unie;

Pozměňovací návrh 55

Návrh nařízení
Čl. 15 – odst. 3

Znění navržené Komisí	*Pozměňovací návrh*
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.	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 ***(CRRT), s cílem lépe podpořit členské státy EU, mise a operace SBOP a třetí země, které dosáhly souladu se společnou zahraniční a bezpečnostní politikou a společnou bezpečnostní a obrannou politikou EU, v jejich úsilí o budování kapacit kybernetické obrany, zejména Ukrajinu a Moldavsko***. 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.

Pozměňovací návrh 56

Návrh nařízení
Čl. 16 – odst. 2 – písm. a a (nové)

Znění navržené Komisí	*Pozměňovací návrh*
	aa) poskytovatel prokáže, že jeho rozhodovací a řídící struktury nepodléhají jakémukoli nepatřičnému ovlivňování ze strany vlád států, které by byly v rozporu s bezpečnostními a obrannými zájmy Unie a jejích členských států, jak je stanoveno v rámci SZBP podle hlavy V SEU;

Pozměňovací návrh 57

Návrh nařízení
Čl. 16 – odst. 2 – písm. f

Znění navržené Komisí	*Pozměňovací návrh*
f) poskytovatel je vybaven hardwarovým a softwarovým technickým zařízením nezbytným pro podporu požadované služby;	f) poskytovatel je vybaven hardwarovým a softwarovým technickým zařízením nezbytným pro podporu požadované služby ***a splňuje požadavky stanovené v článku X nařízení XX/XXXX (akt o kybernetické odolnosti)***;

Pozměňovací návrh 58

Návrh nařízení
Čl. 16 – odst. 2 – písm. j a (nové)

Znění navržené Komisí	*Pozměňovací návrh*
	ja) není přípustný žádný poskytovatel pocházející z vysoce rizikové třetí země.

Pozměňovací návrh 59

Návrh nařízení

Čl. 16 – odst. 2 – písm. j b (nové)

Znění navržené Komisí	*Pozměňovací návrh*
	jb) poskytovatel pokud možno úzce spolupracuje s příslušnými malými a středními podniky;

Pozměňovací návrh 60

Návrh nařízení
Čl. 17 – odst. 1

Znění navržené Komisí	*Pozměňovací návrh*
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.***	1. Třetí země mohou požádat o podporu z rezervy EU pro kybernetickou bezpečnost, pokud***:***
	a) to stanoví dohody o přidružení týkající se jejich účasti v programu Digitální Evropa;
	b) třetí země, v nichž je nasazena mise SBOP se zvláštním mandátem k posílení odolnosti vůči hybridním hrozbám, včetně kybernetických hrozeb, nebo v nichž bylo přijato opatření pomoci v rámci Evropského mírového nástroje k posílení kybernetické odolnosti země.

Pozměňovací návrh 61

Návrh nařízení
Čl. 17 – odst. 2

Znění navržené Komisí	*Pozměňovací návrh*
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.	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 ***s výjimkou třetích zemí, na něž se vztahují ustanovení odst.*** 1 ***písm. b)***.

Pozměňovací návrh 62

Návrh nařízení
Čl. 18 – odst. 1

Znění navržené Komisí	*Pozměňovací návrh*
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.	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***, zejména pokud se incident týká třetí země,*** Komise sdílí zprávu s vysokým představitelem ***a ESVČ***.

Pozměňovací návrh 63

Návrh nařízení
Čl. 18 – odst. 3 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	3a. Zpráva se sdílí s Evropským parlamentem v souladu s právními předpisy Unie nebo vnitrostátními právními předpisy o ochraně citlivých utajovaných informací.

Pozměňovací návrh 64

Návrh nařízení
Čl. 19 – odst. 1 – bod 1 – písm. a – bod 1
Nařízení (EU) 2021/694
Čl. 6 – odst. 1

Znění navržené Komisí	*Pozměňovací návrh*
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“***;	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 a ke snížení závislosti Unie na vysoce rizikových poskytovatelích kritického zařízení nebo součástí v oblasti kybernetické bezpečnosti, kteří by byli v rozporu s bezpečnostními a obrannými zájmy Unie a jejích členských států, jak je stanoveno v rámci SZBP podle hlavy V SEU***;

Pozměňovací návrh 65

Návrh nařízení
Čl. 20 – odst. 1

Znění navržené Komisí	*Pozměňovací návrh*
Do ***[čtyř*** let ode dne použitelnosti tohoto ***nařízení]*** předloží Komise Evropskému parlamentu a Radě zprávu o hodnocení a přezkumu tohoto nařízení.	Do ***[tří*** let ode dne použitelnosti tohoto ***nařízení a poté každé dva roky]*** předloží Komise Evropskému parlamentu a Radě zprávu o hodnocení a přezkumu tohoto nařízení.

POSTUP VE VÝBORU POŽÁDANÉM O STANOVISKO

Název	Stanovení opatření k posílení solidarity Unie a jejích kapacit v oblasti odhalování kybernetických bezpečnostních hrozeb a incidentů a přípravy a reakce na ně
Referenční údaje	COM(2023)0209 – C9-0136/2023 – 2023/0109(COD)
Příslušný výbor Datum oznámení na zasedání	ITRE 1.6.2023
Výbor, který vypracoval stanovisko Datum oznámení na zasedání	AFET 1.6.2023
Zpravodaj(ka) Datum jmenování	Dragoş Tudorache 16.6.2023
Projednání ve výboru	18.9.2023
Datum přijetí	24.10.2023
Výsledek konečného hlasování	+: 39 –: 4 0: 0
Členové přítomní při konečném hlasování	Alexander Alexandrov Yordanov, Petras Auštrevičius, Traian Băsescu, Anna Bonfrisco, Włodzimierz Cimoszewicz, Katalin Cseh, Michael Gahler, Giorgos Georgiou, Sunčana Glavak, Bernard Guetta, Sandra Kalniete, Dietmar Köster, Andrius Kubilius, David Lega, Leopoldo López Gil, Jaak Madison, Pedro Marques, David McAllister, Vangelis Meimarakis, Sven Mikser, Francisco José Millán Mon, Matjaž Nemec, Demetris Papadakis, Kostas Papadakis, Tonino Picula, Thijs Reuten, Nacho Sánchez Amor, Andreas Schieder, Jordi Solé, Sergei Stanishev, Tineke Strik, Dominik Tarczyński, Dragoş Tudorache, Thomas Waitz, Bernhard Zimniok, Željana Zovko
Náhradníci přítomní při konečném hlasování	Attila Ara-Kovács, Lars Patrick Berg, Andrey Kovatchev, Georgios Kyrtsos, Sergey Lagodinsky, Giuliano Pisapia, Mick Wallace

JMENOVITÉ KONEČNÉ HLASOVÁNÍ
VE VÝBORU POŽÁDANÉM O STANOVISKO

39	+
ECR	Lars Patrick Berg, Dominik Tarczyński
ID	Anna Bonfrisco, Jaak Madison
PPE	Alexander Alexandrov Yordanov, Traian Băsescu, Michael Gahler, Sunčana Glavak, Sandra Kalniete, Andrey Kovatchev, Andrius Kubilius, David Lega, Leopoldo López Gil, David McAllister, Vangelis Meimarakis, Francisco José Millán Mon, Željana Zovko
Renew	Petras Auštrevičius, Katalin Cseh, Bernard Guetta, Georgios Kyrtsos, Dragoş Tudorache
S&D	Attila Ara-Kovács, Włodzimierz Cimoszewicz, Dietmar Köster, Pedro Marques, Sven Mikser, Matjaž Nemec, Demetris Papadakis, Tonino Picula, Giuliano Pisapia, Thijs Reuten, Nacho Sánchez Amor, Andreas Schieder, Sergei Stanishev
Verts/ALE	Sergey Lagodinsky, Jordi Solé, Tineke Strik, Thomas Waitz

4	-
ID	Bernhard Zimniok
NI	Kostas Papadakis
The Left	Giorgos Georgiou, Mick Wallace

0	0

Význam zkratek:
+ : pro
- : proti
0 : zdrželi se

25.10.2023

STANOVISKO VÝBORU PRO DOPRAVU A CESTOVNÍ RUCH

pro Výbor pro průmysl, výzkum a energetiku

k návrhu 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
(COM(2023)0209 – C9-0136/2023 – 2023/0109(COD))

Zpravodaj: Gheorghe Falcă

STRUČNÉ ODŮVODNĚNÍ

Organizace postižené kybernetickými útoky, a to i v odvětví dopravy, tyto útoky zřídkakdy nahlásí – a to zejména společnosti v oblasti soukromého sektoru, neboť je považují za „špatnou reklamu“. Většina organizací se s nimi raději vypořádává interně. A tak jsou to často útočníci, kteří útoky zveřejňují. Dobrou zprávou v EU je to, že vstup v platnost směrnice 2022/2555 o bezpečnosti sítí (tzv. „směrnice NIS2“), na jejíž provedení mají členské státy čas do října 2024, harmonizuje povinnosti týkající se hlášení incidentů ve všech členských státech.. Proto je pravděpodobné, že v nadcházejících letech dojde k lepšímu pochopení povahy a rozsahu problému.

Agentura Evropské unie pro kybernetickou bezpečnost (ENISA) zveřejnila nedávnou zprávu[1], která poskytuje informace o kybernetických bezpečnostních hrozbách v odvětví dopravy a v níž zdůrazňuje, že pachatelé kybernetických trestných činů byli odpovědní za více než polovinu incidentů zaznamenaných ve vykazovaném období 2022 (55 %) a že hlavní motivací těchto útoků byl finanční zisk. Konstatuje rovněž, že většina kybernetických útoků v odvětví dopravy se zaměřuje na informační systémy, což způsobuje narušení provozu.

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 května 2022 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 provádí **strategie kybernetické bezpečnosti EU** přijatá v prosinci 2020, v níž bylo oznámeno vytvoření **evropského kybernetického štítu**, jenž posílí schopnosti zjišťování kybernetických hrozeb a sdílení informací v Evropské unii prostřednictvím sítě

[1] „Porozumění kybernetickým hrozbám v dopravě“, , ENISA, zveřejněná 21. března 2023.
[2] Závěry Rady o rozvoji kybernetické pozice Evropské unie, 23. května 2022, dokument 9364/22.

národních a přeshraničních bezpečnostních operačních středisek. Opatření tohoto nařízení budou podporována z **finančních prostředků rámci strategického cíle programu Digitální Evropa „Kybernetická bezpečnost“.**

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 centrum kompetencí pro kybernetickou bezpečnost (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.

Postoj zpravodaje

Zpravodaj vítá nový návrh a domnívá se, že přinese značné výhody různým zúčastněným stranám. Zpravodaj zdůrazňuje, že je nezbytné lépe porozumět potřebám a požadavkům v oblasti kybernetické bezpečnosti v oblasti dopravy, jakož i poskytnout kritickým subjektům v oblasti dopravy přístup k řádnému financování připravenosti, reakce a řešení incidentů.

Zpravodaj podporuje „soubor nástrojů pro kybernetickou bezpečnost dopravy“, jehož cílem je přispět k vyšší úrovni kybernetické informovanosti a kybernetické hygieny se zvláštním zaměřením na odvětví dopravy. Zabývá se dopravními organizacemi bez ohledu na jejich velikost a oblast činnosti, jakož i s ohledem na kritickou dopravní infrastrukturu a vojenskou mobilitu, zejména s ohledem na válku na Ukrajině, zejména:

- Letečtí dopravci, řídící orgány letišť, hlavní letiště, uspořádání letového provozu a střediska řízení letového provozu, Agentura Evropské unie pro bezpečnost letectví a Eurocontrol;
- Provozovatelé infrastruktury, železniční podniky a evropský systém řízení železničního provozu (ERTMS);
- Společnosti vnitrozemské, námořní a pobřežní osobní a nákladní vodní dopravy, řídící orgány přístavů, včetně jejich přístavních zařízení, subjekty provozující práce a vybavení v přístavech, provozovatelé služeb lodní dopravy;
- Silniční orgány odpovědné za kontrolu řízení dopravy, provozovatelé inteligentních dopravních systémů;
- Komunikační služby – Poštovní a kurýrní služby.

Zpravodaj je přesvědčen, že výše rozpočtu na fungování **Fondu pro reakci na mimořádné situace pro kybernetickou bezpečnost (ERFC)** bude určující pro jeho úspěch; proto by měla být dostatečně rozsáhlá na to, aby podporovala členské státy ***při přípravě*** na významné

a rozsáhlé kybernetické bezpečnostní incidenty, ***reakci na ně a zotavení se z nic***h. Podpora reakce na incidenty bude zpřístupněna i orgánům, institucím a jiným subjektům Unie.

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.

POZMĚŇOVACÍ NÁVRH

Výbor pro dopravu a cestovní ruch vyzývá Výbor pro průmysl, výzkum a energetiku jako příslušný výbor, aby zohlednil následující pozměňovací návrhy:

Pozměňovací návrh 1

Návrh nařízení
Bod odůvodnění 2

Znění navržené Komisí	*Pozměňovací návrh*
(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.	(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***, jakož i kritické infrastruktury IT a fyzické infrastruktury***. 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***, veřejné a soukromé dopravy*** 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 i mobilitě v rámci*** 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.

Pozměňovací návrh 2

Návrh nařízení
Bod odůvodnění 2 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	(2a) Státem podporovaní aktéři, pachatelé kybernetické trestné činnosti a „hacktivisté“, kteří útočí na veřejné orgány a provozovatele, výrobce, dodavatele a poskytovatele služeb v letecké, námořní, železniční a silniční dopravě, představují pro odvětví dopravy stále závažnější hrozbu. Agentura Evropské unie pro kybernetickou bezpečnost (ENISA) zaznamenala v roce 2022 nárůst průměrného měsíčního počtu nahlášených incidentů postihujících odvětví dopravy o 25 % ve srovnání s úrovněmi v roce 2021. Většina útoků na odvětví dopravy se zaměřuje na systémy informačních technologií (IT), což může vést k narušení provozu[14a].
	[14b] ENISA (2023), Zpráva agentury ENISA o typech ohrožení: Odvětví dopravy, s. 7 a 17.

Pozměňovací návrh 3

Návrh nařízení
Bod odůvodnění 2 b (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	(2b) Nevyprovokovaná invaze Ruska na Ukrajinu vedla k výraznému nárůstu kybernetických bezpečnostních incidentů, včetně útoků distribuovaným odmítnutím služby (DDoS), které cílí na odvětví dopravy v EU a na oblasti v blízkosti EU, zejména na letiště, železnice a dopravní podniky[14b]. Tento nárůst útoků bude s

velkou pravděpodobností pokračovat.

---

*[14b] **ENISA (2023), Zpráva agentury ENISA o typech ohrožení: Odvětví dopravy, s. 9.***

Pozměňovací návrh 4

Návrh nařízení
Bod odůvodnění 2 c (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	(2c) Kybernetické útoky se zaměřují na orgány a subjekty ve všech pododvětvích dopravy, přičemž jsou dotčeny železniční podniky a provozovatelé infrastruktury, jakož i provozovatelé přístavů. Pokud jde o odvětví silniční dopravy, útoky se zaměřily na výrobce původního vybavení, dodavatele a poskytovatele služeb spolu s provozovateli veřejné dopravy. V odvětví letectví byly hlavními cíli letecké společnosti a provozovatelé letišť, následovaní poskytovateli služeb, provozovateli povrchové dopravy a dodavatelským řetězcem[14c].

---

*[14c] **ENISA (2023), Zpráva agentury ENISA o typech ohrožení: Odvětví dopravy, s. 17.***

Pozměňovací návrh 5

Návrh nařízení
Bod odůvodnění 3

Znění navržené Komisí	*Pozměňovací návrh*
(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	(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[16], 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.

digitálním trhu. Jak je doporučeno ve třech různých návrzích konference o budoucnosti Evropy[16], je nutné zvýšit odolnost občanů, podniků***, provozovatelů dopravy*** 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***, jakož i o stavu a vývoji trhu práce v oblasti kybernetické bezpečnosti, neboť ten hraje zásadní úlohu při poskytování nezbytných služeb detekce a reakce***.

[16] https://futureu.europa.eu/cs/

[16] https://futureu.europa.eu/cs/

Pozměňovací návrh 6

Návrh nařízení
Bod odůvodnění 4

Znění navržené Komisí	*Pozměňovací návrh*
(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[17], doporučení Komise (EU) 2017/1584[18], směrnici Evropského parlamentu a Rady 2013/40/EU[19] a nařízení Evropského parlamentu a Rady (EU) 2019/881[20] . Doporučení Rady o celounijním koordinovaném přístupu za účelem	(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[17] , doporučení Komise (EU) 2017/1584[18] , směrnici Evropského parlamentu a Rady 2013/40/EU[19] a nařízení Evropského parlamentu a Rady (EU) 2019/881[20]***, jakož i návrh nařízení o hlavních směrech pro rozvoj transevropské dopravní sítě a návrh***

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.

nařízení o horizontálních požadavcích na kybernetickou bezpečnost produktů s digitálními prvky (akt o kybernetické odolnosti). 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.

---

[17] 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).

[18] 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).

[19] 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).

[20] 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).

[17] 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).

[18] 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).

[19] 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).

[20] 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).

Pozměňovací návrh 7

Návrh nařízení
Bod odůvodnění 4 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	(4a) Přestože vítá soubor nástrojů Evropské komise pro kybernetickou bezpečnost v dopravě[2a], který obsahuje základní informace o hrozbách, které mohou mít dopad na dopravní organizace (šíření malwaru, odepření služby, neoprávněný přístup a krádež a manipulace se softwarem), a obsahuje seznam osvědčených postupů pro zmírňování rizik, měli by být provozovatelé dopravy vybaveni řádnou odbornou přípravou v oblasti kybernetické bezpečnosti a vhodnými nástroji pro předcházení kybernetickým hrozbám. Rozpočet Unie by měl rovněž pokrývat podporu, jako je odborná příprava, kterou poskytuje agentura ENISA, aby provozovatelé dopravy mohli účinně uplatňovat osvědčené postupy pro zmírňování rizik obsažené v souboru nástrojů.
	[1a] Zpráva agentury ENISA o typech ohrožení: odvětví dopravy/ENISA, březen 2023
	[2a] Evropská komise (2021). Soubor nástrojů pro kybernetickou bezpečnost v dopravě, k dispozici na adrese https://transport.ec.europa.eu/transport-themes/security-safety/cybersecurity_en.

Pozměňovací návrh 8

Návrh nařízení
Bod odůvodnění 4 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	(4a) Celounijní koordinovaný přístup k posílení připravenosti a odolnosti kritické

infrastruktury, jako je dopravní infrastruktura, je založen na budování kapacit členských států. Jak uznala Komise v nedávném sdělení Evropskému parlamentu a Radě o řešení nedostatku talentů v oblasti kybernetické bezpečnosti za účelem posílení konkurenceschopnosti, růstu a odolnosti EU[19a], bezpečnost EU nelze zaručit bez nejcennějšího aktiva EU: lidí.

[19a] Sdělení Komise Evropskému parlamentu a Radě – Řešení nedostatku talentů v oblasti kybernetické bezpečnosti za účelem posílení konkurenceschopnosti, růstu a odolnosti EU („Akademie dovedností v oblasti kybernetické bezpečnosti“), COM(2023) 207 final

Pozměňovací návrh 9

Návrh nařízení
Bod odůvodnění 12

Znění navržené Komisí	*Pozměňovací návrh*
(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	(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. ***Mezi tato kritická aktiva a infrastruktury patří inteligentní dopravní systémy, které jsou sice nezbytné pro automatizovanou a multimodální mobilitu, ale fungují na základě zásadních změn citlivých údajů.*** 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

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[24].

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[24].

[24] 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).

[24] 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).

Pozměňovací návrh 10

Návrh nařízení
Bod odůvodnění 14 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	(14a) Odvětví dopravy se stále více stává jedním z nejlukrativnějších oborů podnikání pro kyberzločince, přičemž údaje o zákaznících jsou považovány za vysoce cennou komoditu a dodavatelský řetězec v dopravě je stále více jejich cílem. Z tohoto důvodu by dopravní infrastruktura charakterizovaná přeshraniční povahou nebo výměnou dat prostřednictvím bezdrátových technologií

měla být považována za klíčový předmět analýzy a monitorování jak pro vnitrostátní, tak zejména pro přeshraniční bezpečnostní operační střediska. Například nedávný návrh na revizi nařízení o TEN-T vyžaduje větší solidaritu a spolupráci při sdílení informací o přeshraničních kybernetických hrozbách, kterým by tato nadnárodní síť mohla čelit. Stejně tak mají inteligentní dopravní systémy (ITS) zásadní význam pro zvýšení bezpečnosti, účinnosti a udržitelnosti dopravy, avšak zvyšují zranitelnost dopravních systémů vůči kybernetickým útokům, které mohou způsobit nehody, dopravní zácpy nebo způsobit hospodářské ztráty soukromým i veřejným provozovatelům. V zájmu zajištění bezpečnosti cestujících, ochrany údajů uživatelů a poskytovatelů a zabránění finančním škodám je nezbytné, aby prováděcí program revidované směrnice o inteligentních dopravních systémech obsahoval ustanovení a nástroje k posílení spolupráce mezi členskými státy při odhalování kybernetických bezpečnostních hrozeb a incidentů, přípravě na ně a reakci na ně.

Pozměňovací návrh 11

Návrh nařízení
Bod odůvodnění 15

Znění navržené Komisí	*Pozměňovací návrh*
(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 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,	(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 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.	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. ***V tomto ohledu je v zájmu posílení autonomie Unie v kybernetické oblasti a s odkazem na čl. 47 odst. 4 návrhu nařízení o hlavních směrech pro rozvoj transevropské dopravní sítě (COM(2021)0812) rovněž nezbytné zabránit přístupu k údajům vedoucím ke kybernetickým hrozbám prosazováním pevného regulačního rámce, který upravuje zahraniční vlastnictví a investice do kritické infrastruktury, jako je doprava.***

Pozměňovací návrh 12

Návrh nařízení
Bod odůvodnění 21

Znění navržené Komisí	*Pozměňovací návrh*
(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	(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.	platformami, které jsou odpovědné za sdílení informací v komunitě kybernetické obrany, a to v úzké spolupráci s vysokým představitelem. ***Měl by rovněž umožnit součinnost s akčním plánem pro vojenskou mobilitu 2.0. Dobře fungující síť vojenské mobility musí být odolná, a to i v souvislosti s kybernetickými a jinými hybridními hrozbami, které by mohly mít dopad na kritické uzly v dopravním systému, které jsou dvojího užití. Závažné důsledky by mohl mít například kybernetický útok na systémy používané na letištích, přístavech nebo železnicích nebo kybernetický útok na vojenské prostředky. Digitalizace procesů a postupů, a to i pro nezbytnou civilní a vojenskou spolupráci, proto bude vyžadovat posílení počítačových informačních systémů (CIS) proti kybernetickým hrozbám.***

Pozměňovací návrh 13

Návrh nařízení
Bod odůvodnění 21 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	(21a) V případě krize kybernetické bezpečnosti je pro zajištění situačního povědomí mezi vojenským a civilním odvětvím dopravy klíčová účinná výměna informací. Tato výměna informací by měla rovněž podnítit spolupráci mezi příslušnými odvětvovými orgány odpovědnými za dopravu, příslušnými orgány pro kybernetickou bezpečnost, bezpečnostními operačními středisky a týmy CSIRT.

Pozměňovací návrh 14

Návrh nařízení
Bod odůvodnění 29

Znění navržené Komisí	*Pozměňovací návrh*
(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	(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“). ***Zvláštní pozornost by měla být věnována odvětví dopravy a jeho pododvětvím (letecké, železniční, vodní, silniční), neboť zahrnují kritickou infrastrukturu, kde by kybernetické incidenty a útoky mohly vážně ohrozit bezpečnost cestujících a provozovatelů.*** 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

prováděno podle článku 22 směrnice (EU) 2022/2555, a testování digitální provozní odolnosti podle nařízení Evropského parlamentu a Rady (EU) 2022/2554[29]. Výběr odvětví by měl rovněž zohlednit doporučení Rady o celounijním koordinovaném přístupu za účelem posílení odolnosti kritické infrastruktury.

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[29]. Výběr odvětví by měl rovněž zohlednit doporučení Rady o celounijním koordinovaném přístupu za účelem posílení odolnosti kritické infrastruktury.

[29] 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.

[29] 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.

Pozměňovací návrh 15

Návrh nařízení
Bod odůvodnění 30 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	(30a) S ohledem na kritičnost tohoto odvětví a na dopady kybernetických hrozeb na mobilitu a v důsledku toho i na lidské životy cestujících a chodců by odvětví dopravy mělo být upřednostněno, pokud jde o koordinované testování připravenosti subjektů.

Pozměňovací návrh 16

Návrh nařízení
Bod odůvodnění 35 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	(35a) Vzhledem k větším úkolům a

	povinnostem, které agentuře ENISA ukládá tento návrh, jakož i návrh aktu o kybernetické odolnosti, je nezbytné přijmout opravný rozpočet agentury ENISA č. 1/2022 pro pilotní provádění opatření na podporu kybernetické bezpečnosti. Kromě toho by s ohledem na zájmy Unie měly být agentuře ENISA přiděleny dodatečné finanční a lidské zdroje.

Pozměňovací návrh 17

Návrh nařízení
Bod odůvodnění 38 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	(38a) Rozvoj dovedností a kompetencí by proto měl být středem pozornosti ve všech odvětvích, v neposlední řadě ve vztahu k těm, která jsou zranitelná vůči kybernetickým hrozbám, jako jsou zaměstnanci pracující na hromadném tranzitu nebo kritické infrastruktuře, včetně systémů řízení vlaků a nástrojů digitálního plánování dopravy pro všechny druhy dopravy. Zavedení a další rozvoj kultury kybernetické bezpečnosti má proto zásadní význam pro úspěch provádění tohoto nařízení, pokud jde o informovanost občanů i znalosti odborníků ve všech odvětvích kritické infrastruktury.

Pozměňovací návrh 18

Návrh nařízení
Čl. 1 – odst. 2 – písm. a

Znění navržené Komisí	*Pozměňovací návrh*
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	a) posílit společné odhalování kybernetických hrozeb a incidentů v Unii a situační povědomí v této oblasti, což umožní posílit konkurenceschopnost odvětví průmyslu***, dopravní infrastruktury***

digitální ekonomice a přispět k technologické suverenitě Unie v oblasti kybernetické bezpečnosti;	a ***odvětví*** služeb v Unii v celé digitální ekonomice a přispět k technologické suverenitě Unie v oblasti kybernetické bezpečnosti;

Pozměňovací návrh 19

Návrh nařízení
Čl. 1 – odst. 2 – písm. b

Znění navržené Komisí	*Pozměňovací návrh*
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;	b) posílit připravenost ***subjektů*** 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***, se zvláštním důrazem na kritickou IT a fyzickou infrastrukturu***, včetně zpřístupnění podpory Unie při reakci na kybernetické bezpečnostní incidenty třetím zemím přidruženým k programu Digitální Evropa;

Pozměňovací návrh 20

Návrh nařízení
Čl. 1 – odst. 2 – písm. c a (nové)

Znění navržené Komisí	*Pozměňovací návrh*
	ca) posílit připravenost, spolupráci a účinnost Unie při ochraně dopravní infrastruktury a služeb v členských státech před kybernetickými bezpečnostními incidenty s cílem zajistit nepřetržité fungování odvětví dopravy, integritu dodavatelských řetězců a mobilitu v celé Unii.

Pozměňovací návrh 21

Návrh nařízení
Čl. 3 – odst. 2 – pododstavec 1 – písm. c

Znění navržené Komisí	*Pozměňovací návrh*
c) ***přispívá*** k lepší ochraně a reakci na kybernetické hrozby***;***	c) ***přispívá*** k lepší ochraně a reakci na kybernetické hrozby***, a to i v případě dopravní infrastruktury vyznačující se přeshraniční povahou, jako je síť TEN-T, nebo pomocí výměny dat prostřednictvím bezdrátových technologií, jako jsou inteligentní dopravní systémy.***

Pozměňovací návrh 22

Návrh nařízení
Čl. 3 – odst. 2 – pododstavec 2

Znění navržené Komisí	*Pozměňovací návrh*
Je vyvíjen ve spolupráci s celoevropskou infrastrukturou pro vysoce výkonnou výpočetní techniku zřízenou podle nařízení (EU) 2021/1173.	Je vyvíjen ve spolupráci s celoevropskou infrastrukturou pro vysoce výkonnou výpočetní techniku zřízenou podle nařízení (EU) 2021/1173. ***Umožňuje spolupráci s komunitou kybernetické obrany prostřednictvím specializovaných protokolů a norem s cílem zajistit rozvoj silnějších schopností civilního odhalování a získávání poznatků o situaci v zájmu ochrany kritické infrastruktury. V tomto ohledu se rovněž rozvíjí součinnost s akčním plánem pro vojenskou mobilitu 2.0 a zajistí se účinná výměna informací s cílem zajistit informovanost o situaci mezi vojenským a civilním odvětvím dopravy.***

Pozměňovací návrh 23

Návrh nařízení
Čl. 8 – odst. 2 a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	2a. Komise zapojí evropský kybernetický štít, zejména přeshraniční bezpečnostní operační střediska, do svého stanoviska pro členské státy v rámci návrhu nařízení o transevropské dopravní síti (COM(2021)0812), kdykoli bude pravděpodobné, že účast fyzické osoby ze

	třetí země nebo podniku třetí země nebo jakýkoli příspěvek jakékoli povahy ovlivní kybernetickou bezpečnost přeshraniční kritické infrastruktury, jako je síť TEN-T.

Pozměňovací návrh 24

Návrh nařízení
Čl. 10 – odst. 1 – písm. a

Znění navržené Komisí	*Pozměňovací návrh*
a) opatření v oblasti připravenosti, včetně koordinovaného testování připravenosti subjektů působících ve vysoce kritických odvětvích v celé Unii;	a) opatření v oblasti připravenosti, včetně koordinovaného testování připravenosti subjektů působících ve vysoce kritických odvětvích v celé Unii***, se zvláštním důrazem na dopravní infrastrukturu a její pododvětví uvedená v příloze I směrnice (EU) 2022/255***;

Pozměňovací návrh 25

Návrh nařízení
Čl. 18 – odst. 2

Znění navržené Komisí	*Pozměňovací návrh*
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.	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***, včetně provozovatelů dopravy***. Na podporu přezkumu může agentura ENISA konzultovat i další typy zúčastněných stran. Konzultovaní zástupci oznámí jakýkoli případný střet zájmů.

Pozměňovací návrh 26

Návrh nařízení
Čl. 19 – odst. 1 – bod 1 – písm. b
Nařízení (EU) 2021/694
Čl. 6 – odst. 2a (nový)

Znění navržené Komisí	*Pozměňovací návrh*
	2a. S ohledem na dotčené zájmy Unie, pokud jde o její odpovědnost za přípravu návrhů systémů certifikace podle nařízení (EU) 2019/881, její povinnosti přezkoumávat a posuzovat kybernetické hrozby, zranitelnost a zmírňování, vypracovat zprávu o přezkumu incidentů pro mechanismus pro přezkum kybernetických bezpečnostních incidentů, jakož i poskytovat provozovatelům kritické infrastruktury odbornou přípravu v boji proti kybernetickým útokům a incidentům a s ohledem na nově přidělené povinnosti v rámci návrhu aktu o kybernetické odolnosti, musí být agentuře ENISA poskytovány nezbytné zdroje z rozpočtu Unie v souladu s platnými právními předpisy.

Pozměňovací návrh 27

Návrh nařízení
Čl. 19 – odst. 1 – bod 1 a (nový)
Nařízení (EU) 2021/694
Čl. 7 – odst. 1 – písm. ca (nové)

Znění navržené Komisí	*Pozměňovací návrh*
	1a) Článek 7 se mění takto:
	a) odstavec 1 se mění takto:
	1) vkládá se nové písmeno (ca), které zní:
	ca) podporovat vysoce kvalitní odbornou přípravu provozovatelů dopravy a správců a pracovníků kritické dopravní infrastruktury, a to i s cílem účinně sdílet a provádět zmírňující postupy v souvislosti s kybernetickými útoky nebo incidenty kritické infrastruktury, jako jsou ty, které

poskytuje soubor nástrojů pro kybernetickou bezpečnost v dopravě.

POSTUP VE VÝBORU POŽÁDANÉM O STANOVISKO

Název	Stanovení opatření k posílení solidarity Unie a jejích kapacit v oblasti odhalování kybernetických bezpečnostních hrozeb a incidentů a přípravy a reakce na ně
Referenční údaje	COM(2023)0209 – C9-0136/2023 – 2023/0109(COD)
Příslušný výbor Datum oznámení na zasedání	ITRE 1.6.2023
Výbor, který vypracoval stanovisko Datum oznámení na zasedání	TRAN 1.6.2023
Zpravodaj(ka) Datum jmenování	Gheorghe Falcă 7.7.2023
Datum přijetí	25.10.2023
Výsledek konečného hlasování	+: 38 –: 0 0: 0
Členové přítomní při konečném hlasování	Magdalena Adamowicz, Andris Ameriks, José Ramón Bauzá Díaz, Izaskun Bilbao Barandica, Karolin Braunsberger-Reinhold, Karima Delli, Anna Deparnay-Grunenberg, Gheorghe Falcă, Carlo Fidanza, Jens Gieseke, Elsi Katainen, Elena Kountoura, Bogusław Liberadzki, Peter Lundgren, Elżbieta Katarzyna Łukacijewska, Marian-Jean Marinescu, Tilly Metz, Cláudia Monteiro de Aguiar, Caroline Nagtegaal, Jan-Christoph Oetjen, Rovana Plumb, Thomas Rudner, Massimiliano Salini, Vera Tax, Barbara Thaler, István Ujhelyi, Achille Variati, Petar Vitanov, Elissavet Vozemberg-Vrionidi, Lucia Vuolo
Náhradníci přítomní při konečném hlasování	Sara Cerdas, Josianne Cutajar, Roman Haider, Pär Holmgren, Pierre Karleskind, Colm Markey, Ljudmila Novak, Dorien Rookmaker

JMENOVITÉ KONEČNÉ HLASOVÁNÍ
VE VÝBORU POŽÁDANÉM O STANOVISKO

38	+
ECR	Carlo Fidanza, Peter Lundgren, Dorien Rookmaker
ID	Roman Haider
PPE	Magdalena Adamowicz, Karolin Braunsberger-Reinhold, Gheorghe Falcă, Jens Gieseke, Elżbieta Katarzyna Łukacijewska, Marian-Jean Marinescu, Colm Markey, Cláudia Monteiro de Aguiar, Ljudmila Novak, Massimiliano Salini, Barbara Thaler, Elissavet Vozemberg-Vrionidi, Lucia Vuolo
Renew	José Ramón Bauzá Díaz, Izaskun Bilbao Barandica, Pierre Karleskind, Elsi Katainen, Caroline Nagtegaal, Jan-Christoph Oetjen
S&D	Andris Ameriks, Sara Cerdas, Josianne Cutajar, Bogusław Liberadzki, Rovana Plumb, Thomas Rudner, Vera Tax, István Ujhelyi, Achille Variati, Petar Vitanov
The Left	Elena Kountoura
Verts/ALE	Karima Delli, Anna Deparnay-Grunenberg, Pär Holmgren, Tilly Metz

0	-

0	0

Význam zkratek:
+ : pro
- : proti
0 : zdrželi se

POSTUP V PŘÍSLUŠNÉM VÝBORU

Název	Stanovení opatření k posílení solidarity Unie a jejích kapacit v oblasti odhalování kybernetických bezpečnostních hrozeb a incidentů a přípravy a reakce na ně			
Referenční údaje	COM(2023)0209 – C9-0136/2023 – 2023/0109(COD)			
Datum předložení Parlamentu	19.4.2023			
Příslušný výbor Datum oznámení na zasedání	ITRE 1.6.2023			
Výbory požádané o stanovisko Datum oznámení na zasedání	AFET 1.6.2023	BUDG 1.6.2023	CONT 1.6.2023	IMCO 1.6.2023
	TRAN 1.6.2023	LIBE 1.6.2023		
Nezaujetí stanoviska Datum rozhodnutí	BUDG 26.4.2023	CONT 24.5.2023	IMCO 23.5.2023	LIBE 30.5.2023
Zpravodajové Datum jmenování	Lina Gálvez Muñoz 2.5.2023			
Projednání ve výboru	19.9.2023			
Datum přijetí	7.12.2023			
Výsledek konečného hlasování	+: –: 0:	43 10 1		
Členové přítomní při konečném hlasování	Nicola Beer, Hildegard Bentele, Vasile Blaga, Michael Bloss, Marc Botenga, Martin Buschmann, Jerzy Buzek, Maria da Graça Carvalho, Josianne Cutajar, Nicola Danti, Marie Dauchy, Pilar del Castillo Vera, Martina Dlabajová, Christian Ehler, Valter Flego, Niels Fuglsang, Nicolás González Casares, Henrike Hahn, Ivo Hristov, Ivars Ijabs, Romana Jerković, Seán Kelly, Izabela-Helena Kloc, Andrius Kubilius, Miapetra Kumpula-Natri, Iskra Mihaylova, Angelika Niebler, Niklas Nienaß, Johan Nissinen, Mikuláš Peksa, Tsvetelina Penkova, Morten Petersen, Markus Pieper, Manuela Ripa, Robert Roos, Sara Skyttedal, Riho Terras, Pernille Weiss, Carlos Zorrinho			
Náhradníci přítomní při konečném hlasování	Andrus Ansip, Laura Ballarín Cereza, Cornelia Ernst, Alexis Georgoulis, Ladislav Ilčić, Elena Kountoura, Alin Mituța, Günther Sidl, Jordi Solé, Susana Solís Pérez			
Náhradníci (čl. 209 odst. 7) přítomní při konečném hlasování	Alexander Alexandrov Yordanov, Jonás Fernández, Virginie Joron, Radan Kanev, Karin Karlsbro			
Datum předložení	8.12.2023			

JMENOVITÉ KONEČNÉ HLASOVÁNÍ V PŘÍSLUŠNÉM VÝBORU

43	+
ECR	Ladislav Ilčić, Izabela-Helena Kloc
ID	Marie Dauchy, Virginie Joron
NI	Alexis Georgoulis
PPE	Alexander Alexandrov Yordanov, Hildegard Bentele, Vasile Blaga, Jerzy Buzek, Maria da Graça Carvalho, Pilar del Castillo Vera, Christian Ehler, Radan Kanev, Seán Kelly, Andrius Kubilius, Angelika Niebler, Markus Pieper, Sara Skyttedal, Riho Terras, Pernille Weiss
Renew	Andrus Ansip, Nicola Beer, Nicola Danti, Martina Dlabajová, Valter Flego, Ivars Ijabs, Karin Karlsbro, Iskra Mihaylova, Alin Mituța, Morten Petersen, Susana Solís Pérez
S&D	Laura Ballarín Cereza, Josianne Cutajar, Jonás Fernández, Niels Fuglsang, Nicolás González Casares, Ivo Hristov, Romana Jerković, Miapetra Kumpula-Natri, Tsvetelina Penkova, Günther Sidl, Carlos Zorrinho
The Left	Elena Kountoura

10	-
ECR	Johan Nissinen, Robert Roos
The Left	Marc Botenga, Cornelia Ernst
Verts/ALE	Michael Bloss, Henrike Hahn, Niklas Nienaß, Mikuláš Peksa, Manuela Ripa, Jordi Solé

1	0
NI	Martin Buschmann

Význam zkratek:
+ : pro
- : proti
0 : zdrželi se