**Evropský parlament**
2019-2024

*Výbor pro průmysl, výzkum a energetiku*

**2023/0109(COD)**

22.9.2023

# POZMĚŇOVACÍ NÁVRHY 46 - 216

**Návrh zprávy**
**Lina Gálvez Muñoz**
(PE752.795v01-00)

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

Návrh nařízení
(COM(2023)0209 – C9-0136/2023 – 2023/0109(COD))

**Pozměňovací návrh 46**
**Evžen Tošenovský**

**Návrh nařízení**
**Název 1**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| NávrhNAŘÍZENÍ 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 | NávrhNAŘÍZENÍ 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 ***(Akt o kybernetické solidaritě)*** |

Or. en

**Pozměňovací návrh 47**
**Ville Niinistö**
za skupinu Verts/ALE

**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 činnosti***, který rovněž přináší zranitelnost***, neboť naše orgány státní správy, společnosti a občané jsou více než kdykoli předtím vzájemně propojení a závislí, a to napříč odvětvími i hranicemi. |

Or. en

*Odůvodnění*

*Potřeba tohoto právního textu vyplývá ze skutečnosti, že se základní závislosti přicházejí také zranitelnosti.*

**Pozměňovací návrh 48**
**Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu**

**Buşoi, Ioan-Rareş Bogdan**

**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. Vzhledem k rychle se vyvíjejícímu prostředí hrozeb vyžaduje hrozba možných rozsáhlých incidentů, které mohou způsobit významné narušení a poškození kritických infrastruktur ***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, 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. ***Ke zlepšení kybernetické bezpečnosti Unie je proto nezbytná úzká a koordinovaná spolupráce mezi veřejným sektorem, soukromým sektorem, členskými státy, orgány nebo agenturami Unie a akademickou sférou. Reakce Unie by měla probíhat ve spolupráci s důvěryhodnými a podobně smýšlejícími mezinárodními partnery a mezinárodními*** |

***institucemi a měla by být v souladu s mezinárodními rámci a dohodami o spolupráci.***

Or. en

**Pozměňovací návrh 49**
**Ville Niinistö**
za skupinu Verts/ALE

**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 | ***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 ***a kriminálních*** 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 |

současně nebo se okamžitě šíří v mnoha zemích.

v mnoha zemích.

Or. en

*Odůvodnění*

*Obecné zařazení hackerského aktivismu mezi trestnou činnost neodráží rozmanitost těchto aktivit, včetně legitimních protestů a whistleblowingu. Textu by prospělo, kdyby se vyhnul nejasnostem a chránil legitimní činnosti.*

**Pozměňovací návrh 50**
**Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Ioan-Rareş Bogdan, Cristian-Silviu Buşoi**

**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 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. | ***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 ***Evropy16***, je nutné zvýšit odolnost občanů, podniků***, včetně mikropodniků, malých a středních 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***, služeb a vysoce kvalifikovaných zaměstnanců, což*** 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***, a to i prostřednictvím aktivního shromažďování zpravodajských informací***. Unie by rovněž měla zvýšit své kapacity v těchto |

oblastech, zejména pokud jde o shromažďování a analýzu údajů o kybernetických bezpečnostních hrozbách a incidentech. ***[1]***
***https://futureu.europa.eu/en/***

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

Or. en

**Pozměňovací návrh 51**
**Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

**Návrh nařízení**
**Bod odůvodnění 5**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| (5) Narůstající rizika v oblasti kybernetické bezpečnosti a celkově složité prostředí hrozeb s jasným rizikem rychlého přelévání kybernetických incidentů z jednoho členského státu do ostatních a ze třetí země do Unie vyžadují posílenou solidaritu na úrovni Unie, aby bylo možné lépe odhalovat kybernetické bezpečnostní hrozby a incidenty, připravovat se na ně ***a*** reagovat na ně. Členské státy rovněž v závěrech Rady o kybernetické pozici EU[21]vyzvaly Komisi, aby předložila návrh nového fondu pro reakci na mimořádné události v oblasti kybernetické bezpečnosti. | (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[21] vyzvaly Komisi, aby předložila návrh nového fondu pro reakci na mimořádné události v oblasti kybernetické bezpečnosti. |
| [21] Závěry Rady o rozvoji kybernetické pozice Evropské unie, schválené Radou na zasedání dne 23. května 2022 (9364/22). | [21] Závěry Rady o rozvoji kybernetické pozice Evropské unie, schválené Radou na zasedání dne 23. května 2022 (9364/22). |

Or. en

**Pozměňovací návrh 52**
**Angelika Niebler, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

**Návrh nařízení**
**Bod odůvodnění 9 a (nový)**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| | ***(9a) Vzhledem ke geopolitickému vývoji a rostoucím kybernetickým hrozbám je důležité zajistit kontinuitu a další rozvoj opatření stanovených v tomto nařízení, zejména evropského kybernetického štítu a evropského mechanismu pro mimořádné události. Proto je nutné zajistit ve víceletém finančním rámci na roky 2028 až 2034 zvláštní rozpočtovou položku. Členské státy by se rovněž měly zavázat k podpoře všech nezbytných opatření k posílení solidarity v rámci Unie a ke snížení kybernetických hrozeb a incidentů v celé Unii.*** |

Or. en

**Pozměňovací návrh 53**
**Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

**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 | (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 ***proaktivního shromažďování zpravodajských informací***. Měla by být zavedena rozsáhlá unijní infrastruktura bezpečnostních operačních středisek („evropský kybernetický štít“), která by se skládala z několika interoperabilních přeshraničních |

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).

platforem, z nichž každá by sdružovala několik národních bezpečnostních operačních středisek***. Národní bezpečnostní operační středisko (SOC) je centralizovaná kapacita odpovědná za průběžné shromažďování zpravodajských informací o hrozbách a zlepšování kybernetické bezpečnosti subjektů spadajících pod národní jurisdikci prostřednictvím prevence, detekce a analýzy kybernetických hrozeb***. 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).

Or. en

**Pozměňovací návrh 54**
**Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

**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) ***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 důrazně vyzývají, aby začlenily kapacitu národního bezpečnostního operačního střediska do své již existující kybernetické struktury a správy, aby nevytvářely další vrstvy správy a aby sladily Akt o kybernetické solidaritě s již existujícími právními předpisy, včetně směrnice 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 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 SOC by měly posílit spolupráci a sdílení informací mezi veřejnými a soukromými subjekty, aby se prolomila stávající uzavřené komunikační struktury. Přitom mohou podporovat vytváření modelů výměny dat a měly by usnadňovat a podporovat sdílení informací v důvěryhodném a bezpečném prostředí. Pro posílení odolnosti Unie v oblasti kybernetické bezpečnosti je zásadní úzká a koordinovaná spolupráce mezi veřejnými a soukromými subjekty.*** |

Or. en

**Pozměňovací návrh 55**
**Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

**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, 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 ***a proaktivních*** 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. ***Přeshraniční bezpečnostní operační střediska by měla usnadňovat a podporovat sdílení informací v důvěryhodném a bezpečném prostředí. Agentura ENISA by měla podporovat přeshraniční bezpečnostní operační střediska v záležitostech týkajících se operativní spolupráce.*** Měla by poskytnout nové dodatečné kapacity ***a zároveň být začleněna do již existující infrastruktury kybernetické bezpečnosti, včetně*** bezpečnostních operačních středisek a týmů reakce na počítačové bezpečnostní incidenty (dále jen „týmy CSIRT“) a dalších příslušných subjektů. |

Or. en

**Pozměňovací návrh 56**
**Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

**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, 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. | (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 rozvoji schopností a technologické suverenity***, na posílení odolnosti*** Unie. |

Or. en

**Pozměňovací návrh 57**
**Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen**

**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 | (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***. | 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 ***významných ekosystémů v oblasti kybernetické bezpečnosti, výrazných*** schopností ***Unie a spolupráce s podobně smýšlejícími partnery***. |
| | Or. en |

**Pozměňovací návrh 58**
**Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

**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, | (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***, aby se usnadnilo rozbití v současnosti existujících komunikačních uzavřených struktur. Přeshraniční bezpečnostní operační střediska by tak mohla rovněž podpořit*** |

| | |
|---|---|
| indikátory narušení a kontextualizované informace o incidentech, hrozbách a zranitelnostech. Přeshraniční bezpečnostní operační střediska by také měla uzavírat dohody o spolupráci s jinými přeshraničními bezpečnostními operačními středisky. | ***vytvoření modelů výměny dat v celé Unii***. Informace vyměňované mezi účastníky přeshraničního bezpečnostního operačního střediska mohou zahrnovat údaje ze sítí a čidel, zpravodajské informace***, včetně proaktivně získávaných zpravodajských informací,*** o hrozbách, indikátory narušení a kontextualizované informace o incidentech, hrozbách a zranitelnostech. Přeshraniční bezpečnostní operační střediska by také měla uzavírat dohody o spolupráci s jinými přeshraničními bezpečnostními operačními středisky. |
| | Or. en |

**Pozměňovací návrh 59**
**Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen**

**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 dohody o spolupráci s jinými přeshraničními bezpečnostními operačními | (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 ***analyzované*** údaje ze sítí***, čidel, logování a telemetrie***, zpravodajské informace o hrozbách, indikátory narušení a kontextualizované informace o ***taktikách, technikách a postupech,*** incidentech***, vzorcích malware***, hrozbách a zranitelnostech. Přeshraniční bezpečnostní operační střediska by také měla uzavírat dohody o spolupráci s jinými |

| | |
|---|---|
| střediska. | přeshraničními bezpečnostními operačními středisky. |

Or. en

**Pozměňovací návrh 60**
**Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

**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 závislosti na situaci mohou informace, | 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 souladu s již existujícími ustanoveními*** |

| | |
|---|---|
| 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. | ***podle směrnice (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. |

Or. en

**Pozměňovací návrh 61**
**Angelika Niebler, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

**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 vybaveny nejmodernějšími a vysoce bezpečnými nástroji, zařízeními a infrastrukturami ***a vysoce 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. |

Or. en

**Pozměňovací návrh 62**
**Angelika Niebler, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

**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. Sdružování vysoce kvalitních kontrolovaných údajů by mělo rovněž přispět k rozvoji pokročilých technologií umělé inteligence a analýzy dat***. Je však třeba poznamenat, že umělá inteligence je nejúčinnější ve spojení s lidskou analýzou. Vysoce kvalifikovaný personál je proto i nadále nezbytný pro shromažďování vysoce kvalitních dat a proaktivní shromažďování informací o hrozbách***. 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). |

Or. en

**Pozměňovací návrh 63**
**Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen**

**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 | 20) Prostřednictvím shromažďování, sdílení a výměny údajů by měl evropský kybernetický štít posílit ***důležitý ekosystém Unie v oblasti kybernetické bezpečnosti***. Sdružování vysoce kvalitních |

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].

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).

Or. en

**Pozměňovací návrh 64**
**Ville Niinistö**
za skupinu Verts/ALE

**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 ***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 finančních prostředků,*** |

platformami, které jsou odpovědné za sdílení informací v komunitě kybernetické obrany, a to v úzké spolupráci s vysokým představitelem.

***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***.

Or. en

*Odůvodnění*

*V duchu zamezení zdvojování a ochrany práv a svobod musí být spolupráce mezi civilní a obrannou stranou kybernetické bezpečnosti založena na zárukách, které zabrání změně určení civilních finančních prostředků.*

**Pozměňovací návrh 65**
**Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

**Návrh nařízení**
**Bod odůvodnění 24**

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

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

Or. en

**Pozměňovací návrh 66**
**Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

**Návrh nařízení**
**Bod odůvodnění 27**

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

Or. en

**Pozměňovací návrh 67**
**Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

**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 | (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.

nebo rozsáhlých kybernetických bezpečnostních incidentů. Rezerva EU pro kybernetickou bezpečnost by měla zajistit dostupnost a připravenost služeb ***a zároveň posílit odolnost a konkurenceschopnost Unie, včetně účasti evropských poskytovatelů řízených bezpečnostních služeb ve formě malých a středních podniků. 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***. Služby by měly být pokud možno založeny na nejmodernějších technologiích, včetně cloudu a umělé inteligence. 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.

Or. en

**Pozměňovací návrh 68**
**Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen**

**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, ***s počátečním financováním ve výši deseti milionů eur podle tohoto nařízení až do vyhodnocení. Skládala*** by se 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. ***Komise zajistí, aby se podobné iniciativy v rámci NATO neduplikovaly.*** |

Or. en

*Odůvodnění*

*The Commission foresees a "gradual set up" of the Reserve but this is not reflected in the rest of the proposed Regulation. This amendment therefore proposes to reduce the initial budget for the Reserve from 36 million to 10 million euro until the evaluation of this Regulation. This would return 26 million euro to the Digital Europe Program - Special Objective 4 on Advanced Digital Skills (of the 35 million taken from it). Developing a EU Cybersecurity Reserve next to an existing NATO cyber reserve comes with a high risk of duplication and should not be at the expense of investing more in developing and attracting cybersecurity talent in Europe.*

**Pozměňovací návrh 69**
**Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

**Návrh nařízení**
**Bod odůvodnění 35**

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

Or. en

**Pozměňovací návrh 70**
**Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen, Nicola Danti**

**Návrh nařízení**
**Bod odůvodnění 35 a (nový)**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| | ***(35a) S ohledem na další úkoly stanovené v tomto nařízení i v [návrhu horizontálních požadavků na kybernetickou bezpečnost výrobků s digitálními prvky] by agentuře ENISA měly být z rozpočtu Unie poskytnuty nezbytné lidské a finanční zdroje.*** |

Or. en

**Pozměňovací návrh 71**
**Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

**Návrh nařízení**
**Bod odůvodnění 37 a (nový)**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| | ***(37a) Pro poskytování specifických služeb v rámci rezervy pro kybernetickou bezpečnost EU mohou být zapotřebí poskytovatelé služeb reakce na incidenty ze třetích zemí, včetně třetích zemí přidružených k DEP nebo členům NATO či jiným podobně zaměřeným mezinárodním partnerským zemím. V zájmu posílení odolnosti a svrchovanosti Unie a ochrany strategických aktiv, zájmů nebo bezpečnosti Unie může být nezbytné omezit nebo vyloučit účast právních subjektů usazených v zemích, které nejsou přidruženými zeměmi, nebo těmito zeměmi ovládaných.*** |

Or. en

**Pozměňovací návrh 72**
**Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

**Návrh nařízení**
**Bod odůvodnění 38 a (nový)**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| | ***(38a) Vysoce 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 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.***

Or. en

**Pozměňovací návrh 73**
**Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

**Návrh nařízení**
**Bod odůvodnění 38 b (nový)**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| | ***(38b) Pro celounijní koordinovaný přístup k posílení odolnosti kybernetické bezpečnosti Unie má zásadní význam budování kapacit členských států. Jak bylo zdůrazněno ve sdělení Komise ze dne 18. dubna 2023 o Akademii dovedností v oblasti kybernetické bezpečnosti, bezpečnost Unie nelze zaručit bez jejího nejcennějšího aktiva: lidí. Evropský rámec kybernetických dovedností může pomoci lépe porozumět složení pracovní síly Unie, včetně současných a požadovaných kompetencí v rámci zúčastněných subjektů.*** |

Or. en

**Pozměňovací návrh 74**

**Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

**Návrh nařízení**
**Bod odůvodnění 39**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| (39) Cíle tohoto nařízení lze lépe dosáhnout na úrovni Unie než na úrovni členských států. Unie proto může přijmout opatření v souladu se zásadami subsidiarity a proporcionality stanovenými v článku 5 Smlouvy o Evropské unii. Toto nařízení nepřekračuje rámec toho, co je nezbytné pro dosažení tohoto cíle, | (39) Cíle tohoto nařízení***, totiž odbourání komunikačních uzavřených struktur a posílení kapacit Unie v oblasti prevence, odhalování, reakce a obnovy kybernetických hrozeb,***lze lépe dosáhnout na úrovni Unie než na úrovni členských států. Unie proto může přijmout opatření v souladu se zásadami subsidiarity a proporcionality stanovenými v článku 5 Smlouvy o Evropské unii. Toto nařízení nepřekračuje rámec toho, co je nezbytné pro dosažení tohoto cíle, |

Or. en

**Pozměňovací návrh 75**
**Nicola Danti**

**Návrh nařízení**
**Bod odůvodnění 39 a (nový)**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| | ***(39a) S ohledem na další úkoly stanovené v tomto nařízení i v [návrhu horizontálních požadavků na kybernetickou bezpečnost výrobků s digitálními prvky] by agentuře ENISA měly být z rozpočtu Unie poskytnuty nezbytné lidské a finanční zdroje.*** |

Or. en

**Pozměňovací návrh 76**
**Johan Nissinen**

**Návrh nařízení**
**Čl. 1 – odst. 1 – návětí**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| 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: | 1. Tímto nařízením se stanoví opatření k posílení kapacit Unie pro odhalování kybernetických bezpečnostních hrozeb a incidentů, přípravu na ně a reakci na ně, ***přičemž respektuje, že národní bezpečnost, včetně kybernetické oblasti, zůstává výhradní odpovědností každého členského státu, jak se stanoví v čl. 4 odst. 2 SEU, a to*** zejména prostřednictvím těchto kroků: |

Or. en

**Pozměňovací návrh 77**
**Evžen Tošenovský**

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

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| a) ***zavedení celoevropské infrastruktury*** bezpečnostních operačních středisek (***„evropského kybernetického štítu“***) s cílem vybudovat a posílit společné schopnosti odhalování a situačního povědomí; | a) ***posílení týmů pro reakci na počítačové bezpečnostní incidenty (CSIRT) uvedených v článku 10 směrnice (EU) 2022/2555 a sítě CSIRT uvedené v článku 15 směrnice (EU) 2022/2555 a nasazení*** bezpečnostních operačních středisek (***SOC***) s cílem vybudovat a posílit ***vnitrostátní a*** společné schopnosti odhalování a situačního povědomí ***("Evropský kybernetický štít")***; |

Or. en

**Pozměňovací návrh 78**
**Evžen Tošenovský**

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

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| ***c) zřízení evropského mechanismu*** | ***vypouští se*** |

***pro kybernetické bezpečnostní incidenty, který bude přezkoumávat a posuzovat významné nebo rozsáhlé incidenty.***

Or. en

**Pozměňovací návrh 79**
**Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

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

Or. en

**Pozměňovací návrh 80**
**Johan Nissinen**

**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 ***dobrovolné*** 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; |

Or. en

**Pozměňovací návrh 81**
**Johan Nissinen**

**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 ***dobrovolnou spolupráci*** 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; |

Or. en

**Pozměňovací návrh 82**
**Evžen Tošenovský**

**Návrh nařízení**
**Čl. 1 – odst. 2 – písm. c**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| ***c) zvýšit odolnost Unie a přispět k účinné reakci přezkumem a posouzením významných nebo rozsáhlých incidentů, včetně vyvození poučení a případných doporučení.*** | ***vypouští se*** |

Or. en

**Pozměňovací návrh 83**
**Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

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

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|

***ca) koordinovaně rozvíjet a zlepšovat dovednosti a kompetence pracovní síly v odvětví kybernetické bezpečnosti, a to prostřednictvím spolupráce s Akademií kybernetických dovedností, která poskytuje školení a příležitosti s cílem odstranit nedostatek talentů v odvětví kybernetické bezpečnosti.***

Or. en

**Pozměňovací návrh 84**
**Johan Nissinen**

**Návrh nařízení**
**Čl. 1 – odst. 3**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| 3. Tímto nařízením není dotčena prvořadá odpovědnost členských států v oblasti národní bezpečnosti, veřejné bezpečnosti a prevence, vyšetřování, odhalování a stíhání trestných činů. | 3. Tímto nařízením není dotčena prvořadá odpovědnost členských států v oblasti národní bezpečnosti, veřejné bezpečnosti a prevence, vyšetřování, odhalování a stíhání trestných činů ***a vyhnout se zbytečnému zdvojování se stávajícími iniciativami***. |

Or. en

**Pozměňovací návrh 85**
**Evžen Tošenovský**

**Návrh nařízení**
**Čl. 1 – odst. 3**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| 3. Tímto nařízením není dotčena ***prvořadá odpovědnost*** členských států v oblasti národní bezpečnosti, veřejné bezpečnosti a prevence, vyšetřování, odhalování a stíhání trestných činů. | 3. Tímto nařízením není dotčena ***výlučná pravomoc*** členských států v oblasti národní bezpečnosti, veřejné bezpečnosti a prevence, vyšetřování, odhalování a stíhání trestných činů. |

Or. en

**Pozměňovací návrh 86**
**Nicola Danti**

**Návrh nařízení**
**Čl. 1 – odst. 3 a (nový)**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| | ***3a. Komise každoročně při předkládání návrhu rozpočtu na následující rok předloží podrobné posouzení úkolů agentury ENISA podle tohoto nařízení, jakož i [návrhu nařízení o horizontálních požadavcích na kybernetickou bezpečnost výrobků s digitálními prvky] a dalších právních předpisů Unie, a podrobně uvede finanční a lidské zdroje potřebné k plnění těchto úkolů.*** |

Or. en

**Pozměňovací návrh 87**
**Evžen Tošenovský**

**Návrh nařízení**
**Čl. 2 – odst. 1 – bod 1**

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

Or. en

**Pozměňovací návrh 88**
**Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen**

**Návrh nařízení**
**Čl. 2 – odst. 1 – bod 1**

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

Or. en

**Pozměňovací návrh 89**
**Johan Nissinen**

**Návrh nařízení**
**Čl. 2 – odst. 1 – bod 1**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| ***(1)*** „přeshraničním bezpečnostním operačním střediskem“ platforma za účasti více zemí, která v koordinované síťové struktuře sdružuje národní bezpečnostní operační střediska z nejméně tří členských států, jež tvoří hostitelské konsorcium, a která je určena k předcházení kybernetickým hrozbám a incidentům a k | ***1)*** „přeshraničním bezpečnostním operačním střediskem“ platforma za účasti více zemí, která v koordinované síťové struktuře sdružuje národní bezpečnostní operační střediska z nejméně tří členských států, jež tvoří hostitelské konsorcium, a která je určena k předcházení kybernetickým hrozbám a incidentům a k |

| | |
|---|---|
| podpoře vytváření vysoce kvalitních zpravodajských informací, zejména prostřednictvím výměny údajů z různých zdrojů, veřejných i soukromých, jakož i sdílením nejmodernějších nástrojů a společným vývojem schopností detekce, analýzy a prevence a ochrany v kybernetické oblasti v důvěryhodném prostředí; | podpoře vytváření vysoce kvalitních zpravodajských informací, zejména prostřednictvím ***dobrovolné*** výměny údajů z různých zdrojů, veřejných i soukromých, jakož i sdílením nejmodernějších nástrojů a společným vývojem schopností detekce, analýzy a prevence a ochrany v kybernetické oblasti v důvěryhodném prostředí; |

Or. en

**Pozměňovací návrh 90**
**Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

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

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| | ***1a) „Bezpečnostním operačním střediskem“ („SOC“) se rozumí centralizovaná kapacita, která může být interní nebo externí, odpovědná za nepřetržité sledování a zlepšování kybernetické bezpečnosti subjektu s cílem předcházet kybernetickým bezpečnostním hrozbám, odhalovat je, analyzovat a reagovat na ně.*** |

Or. en

**Pozměňovací návrh 91**
**Evžen Tošenovský**

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

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| | ***1a) „Bezpečnostním operačním střediskem“ („SOC“) se rozumí středisko zřízené soukromými a veřejnými subjekty nebo vnitrostátními orgány, které nepřetržitě sleduje a analyzuje*** |

***komunikační sítě a počítačové systémy s cílem odhalit narušení a anomálie v reálném čase.***

Or. en

**Pozměňovací návrh 92**
**Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

**Návrh nařízení**
**Čl. 2 – odst. 1 – bod 1 b (nový)**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| | ***1b) „Národním bezpečnostním operačním střediskem“ centralizovaná kapacita odpovědná za průběžné shromažďování zpravodajských informací o hrozbách a zlepšování postavení subjektů spadajících do vnitrostátní jurisdikce v oblasti kybernetické bezpečnosti prostřednictvím prevence, odhalování a analýzy kybernetických bezpečnostních hrozeb, aby bylo možné na kybernetické bezpečnostní hrozby lépe reagovat. Tato kapacita se případně začlení do již existujících vnitrostátních struktur, jako jsou týmy CSIRT zřízené podle směrnice 2022/2555.*** |

Or. en

**Pozměňovací návrh 93**
**Evžen Tošenovský**

**Návrh nařízení**
**Čl. 2 – odst. 1 – bod 2**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| ***(2) „veřejnoprávním*** subjektem***“ veřejnoprávní subjekt*** ve smyslu čl. ***2 odst. 1 bodu 4*** směrnice ***Evropského parlamentu a Rady 2014/24/EU***[30]; | ***2) „***subjektem ***veřejné správy“ subjekt veřejné správy*** ve smyslu čl. ***6 bodu 35*** směrnice ***(EU) 2022/2555***; |

*[30] 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).*

Or. en

**Pozměňovací návrh 94**
**Evžen Tošenovský**

**Návrh nařízení**
**Čl. 2 – odst. 1 – bod 3**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| ***(3) „hostitelským konsorciem“ konsorcium složené ze zúčastněných států, zastoupených národními bezpečnostními operačními středisky, které souhlasily se zřízením nástrojů a infrastruktury pro přeshraniční bezpečnostní operační střediska a jejich provoz a s poskytnutím příspěvku na pořízení těchto nástrojů a infrastruktury;*** | ***vypouští se*** |

Or. en

**Pozměňovací návrh 95**
**Evžen Tošenovský**

**Návrh nařízení**
**Čl. 2 – odst. 1 – bod 5 a (nový)**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| | ***5a) „řešením incidentu“ řešení incidentu ve smyslu čl. 6 bodu 8 směrnice (EU) 2022/2555;*** |

Or. en

**Pozměňovací návrh 96**

**Evžen Tošenovský**

**Návrh nařízení**
**Čl. 2 – odst. 1 – bod 5 b (nový)**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| | ***5b) „▌ rizikem“ se rozumí riziko ve smyslu čl. 6 bodu 9 směrnice (EU) 2022/2555;*** |

Or. en

**Pozměňovací návrh 97**
**Evžen Tošenovský**

**Návrh nařízení**
**Čl. 2 – odst. 1 – bod 6 a (nový)**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| | ***6a) „významnou kybernetickou hrozbou“ kybernetická hrozba ve smyslu čl. 6 bodu 11 směrnice (EU) 2022/2555;*** |

Or. en

**Pozměňovací návrh 98**
**Evžen Tošenovský**

**Návrh nařízení**
**Čl. 2 – odst. 1 – bod 9**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| ***(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;*** | ***vypouští se*** |

Or. en

**Pozměňovací návrh 99**
**Evžen Tošenovský**

**Návrh nařízení**
**Čl. 2 – odst. 1 – bod 10**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| ***(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;*** | ***vypouští se*** |

Or. en

**Pozměňovací návrh 100**
**Evžen Tošenovský**

**Návrh nařízení**
**Čl. 2 – odst. 1 – bod 11**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| ***(***11) „důvěryhodnými poskytovateli“ poskytovatelé řízených bezpečnostních služeb ve smyslu čl. 6 bodu 40 směrnice (EU) 2022/2555, kteří byli vybráni v souladu s článkem 16 tohoto nařízení. | 11) „důvěryhodnými poskytovateli ***řízených bezpečnostních služeb***“ poskytovatelé řízených bezpečnostních služeb ve smyslu čl. 6 bodu 40 směrnice (EU) 2022/2555, kteří byli vybráni***, aby byli začlenění do rezervy EU pro kybernetickou bezpečnost*** v souladu s článkem 16 tohoto nařízení. |

Or. en

**Pozměňovací návrh 101**
**Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen**

**Návrh nařízení**
**Čl. 3 – odst. 1 – pododstavec 1**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| ***Zřizuje se*** propojená celoevropská infrastruktura bezpečnostních operačních | ***Bude zřízena*** propojená celoevropská infrastruktura bezpečnostních operačních |

| | |
|---|---|
| středisek (dále jen „evropský kybernetický štít“)***, která bude rozvíjet pokročilé schopnosti*** Unie odhalovat, analyzovat a zpracovávat údaje o kybernetických hrozbách a ***incidentech*** v Unii. ***Evropský kybernetický štít se skládá z*** národních bezpečnostních operačních středisek a přeshraničních bezpečnostních operačních středisek. | středisek (dále jen „Evropský kybernetický štít“) ***za účelem rozvoje pokročilých schopností*** Unie odhalovat, analyzovat a zpracovávat údaje o kybernetických hrozbách a ***předcházet incidentům*** v Unii. ***Skládá se ze všech*** národních bezpečnostních operačních středisek ***(dále jen „národní bezpečnostní operační střediska“)*** a přeshraničních bezpečnostních operačních středisek ***(dále jen „přeshraniční bezpečnostní operační střediska“)***. |

Or. en

**Pozměňovací návrh 102**
**Johan Nissinen**

**Návrh nařízení**
**Čl. 3 – odst. 2 – pododstavec 1 – písm. a**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| a) shromažďuje a sdílí údaje o kybernetických hrozbách a incidentech z různých zdrojů ***prostřednictvím*** přeshraničních bezpečnostních operačních středisek; | a) shromažďuje a sdílí údaje o kybernetických hrozbách a incidentech z různých zdrojů ***díky dobrovolnému sdílení informací z*** přeshraničních bezpečnostních operačních středisek; |

Or. en

**Pozměňovací návrh 103**
**Evžen Tošenovský**

**Návrh nařízení**
**Čl. 3 – odst. 2 – pododstavec 1 – písm. a**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| a) shromažďuje a sdílí údaje o kybernetických hrozbách a incidentech z různých zdrojů prostřednictvím přeshraničních bezpečnostních operačních středisek; | a) shromažďuje a sdílí údaje o kybernetických hrozbách a incidentech z různých zdrojů prostřednictvím přeshraničních bezpečnostních operačních středisek***, jak na vnitrostátní, tak na evropské úrovni***; |

Or. en

**Pozměňovací návrh 104**
**Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

**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) ***přispívat*** k lepší ochraně ***kybernetických hrozeb*** a reakci na ***ně, mimo jiné poskytováním konkrétních doporučení subjektům***; |

Or. en

**Pozměňovací návrh 105**
**Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

**Návrh nařízení**
**Čl. 3 – odst. 2 – pododstavec 1 – písm. d**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| d) ***přispívá*** k rychlejšímu odhalování kybernetických hrozeb a ***k situačnímu povědomí*** v celé Unii; | d) ***přispívat*** k rychlejšímu odhalování kybernetických hrozeb a ***informovanosti o situaci*** v celé Unii***, mimo jiné shromažďováním proaktivních zpravodajských informací***; |

Or. en

**Pozměňovací návrh 106**
**Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen**

**Návrh nařízení**
**Čl. 3 – odst. 2 – pododstavec 1 – písm. e**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| e) poskytuje služby a činnosti pro komunitu kybernetické bezpečnosti v Unii, | e) poskytuje služby a činnosti pro komunitu kybernetické bezpečnosti v Unii, |

| | |
|---|---|
| včetně přínosu k vývoji pokročilých nástrojů umělé inteligence a analýzy dat. | včetně přínosu k vývoji pokročilých nástrojů umělé inteligence a analýzy dat. |

Or. en

**Pozměňovací návrh 107**
**Evžen Tošenovský**

**Návrh nařízení**
**Čl. 4 – název**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| ***Národní bezpečnostní operační střediska*** | ***Posílená spolupráce a sdílení informací na vnitrostátní úrovni*** |

Or. en

**Pozměňovací návrh 108**
**Evžen Tošenovský**

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

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| ***Pro účast v evropském kybernetickém*** štítu určí každý členský stát ***alespoň jedno národní*** bezpečnostní ***operační středisko. Národní bezpečnostní operační*** středisko ***musí být veřejnoprávním subjektem***. | ***S cílem přispět k evropskému kybernetickému*** štítu určí každý členský stát ***jeden ze svých týmů pro reakci na počítačové*** bezpečnostní ***incidenty (CSIRT) uvedených v článku 10 směrnice (EU) 2022/2555 jako*** středisko ***pro sdílení a analýzu informací (ISAC)***. |

Or. en

**Pozměňovací návrh 109**
**Evžen Tošenovský**

**Návrh nařízení**
**Čl. 4 – odst. 1 – pododstavec 1 a (nový)**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|

***Soukromé a veřejné organizace nebo vnitrostátní orgány, zejména subjekty působící v kritických nebo vysoce kritických odvětvích, se vybízejí, aby zřídily a provozovaly svá autonomní nebo sdílená bezpečnostní operační střediska.***

Or. en

**Pozměňovací návrh 110**
**Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen**

**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, které shromažďují a analyzují informace o kybernetických bezpečnostních hrozbách a přispívají k přeshraničnímu bezpečnostnímu operačnímu středisku. Je vybaveno nejmodernějšími technologiemi schopnými zjišťovat, agregovat a analyzovat údaje týkající se kybernetických bezpečnostních hrozeb a incidentů. ***Toto středisko nebo vnitrostátní tým CSIRT mohou od důvěryhodných poskytovatelů nebo poskytovatelů řízených bezpečnostních služeb požadovat telemetrii, senzorická nebo protokolovací data, která se týkají odvětví s vysokou kritičností ve smyslu definice v 2022/2555. Tyto údaje mohou být sdíleny pouze na podporu úkolů a povinností vnitrostátního bezpečnostního střediska nebo týmu CSIRT při odhalování kybernetických bezpečnostních incidentů a jejich předcházení.*** |

Or. en

**Pozměňovací návrh 111**
**Evžen Tošenovský**

**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 ***především pro operační střediska zřízená soukromými a veřejnými subjekty nebo vnitrostátními orgány, jinými týmy CSIRT téhož členského státu, koordinátorem pro řízení rozsáhlých kybernetických bezpečnostních incidentů a krizí, jakož i*** pro další veřejné a soukromé organizace na vnitrostátní úrovni ***za účelem shromažďování a analýzy informací*** o kybernetických bezpečnostních hrozbách a incidentech a ***případně sdílení těchto informací s dalšími členy sítě CSIRT***. Je vybaveno nejmodernějšími technologiemi schopnými zjišťovat, agregovat a analyzovat údaje týkající se kybernetických bezpečnostních hrozeb a incidentů. |

Or. en

**Pozměňovací návrh 112**
**Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

**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, ***především jejich bezpečnostní operační střediska,*** 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.

Or. en

**Pozměňovací návrh 113**
**Evžen Tošenovský**

**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.*** | ***vypouští se*** |

Or. en

**Pozměňovací návrh 114**
**Ville Niinistö**
za skupinu Verts/ALE

**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 ***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. |

Or. en

*Odůvodnění*

*Povinná povaha slova „musí“ vyjímá obsah z pojmu „výzva k vyjádření zájmu“ a výběrových řízení. Bezpečnostní operační střediska se samozřejmě mohou účastnit a mohou být vybrána.*

**Pozměňovací návrh 115**
**Evžen Tošenovský**

**Návrh nařízení**
**Čl. 4 – odst. 3**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| ***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,*** | ***vypouští se*** |

***není způsobilé k další podpoře z Unie podle tohoto nařízení.***

Or. en

**Pozměňovací návrh 116**
**Evžen Tošenovský**

**Návrh nařízení**
**Čl. 5 – název**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| ***Přeshraniční bezpečnostní operační střediska*** | ***Společné zadávání veřejných zakázek na nástroje a infrastruktury*** |

Or. en

**Pozměňovací návrh 117**
**Evžen Tošenovský**

**Návrh nařízení**
**Čl. 5 – odst. 1**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| ***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.*** | ***vypouští se*** |

Or. en

**Pozměňovací návrh 118**
**Evžen Tošenovský**

**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 % 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. | 2. Na základě výzvy k vyjádření zájmu ***může*** centrum ECCC ***vybrat týmy CSIRT či střediska ISAC, která se budou*** podílet na společném zadávání zakázek týkajících se nástrojů a infrastruktury s centrem ECCC. Centrum ECCC může ***týmům CSIRT či střediskům ISAC*** 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 ***týmy CSIRT či střediska ISAC***. Před zahájením řízení za účelem pořízení nástrojů a infrastruktur uzavřou centrum ECCC a ***zúčastněné týmy CSIRT či střediska ISAC*** dohodu o hostingu a užívání, která upravuje používání nástrojů a infrastruktur***, včetně jejich používání jinými týmy CSIRT a bezpečnostními operačními středisky v daném členském státě.***. |

Or. en

**Pozměňovací návrh 119**
**Ville Niinistö**
za skupinu Verts/ALE

**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 % nákladů na pořízení nástrojů a infrastruktury a až 50 % nákladů na provoz, přičemž zbývající náklady hradí | 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. | 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. |

Or. en

*Odůvodnění*

*Ačkoli toto nařízení neobsahuje výslovná kritéria, jiné použitelné právní předpisy by mohly snížit jistotu, že žadatel/každý žadatel je úspěšný.*

**Pozměňovací návrh 120**
**Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen**

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

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| | ***2a. Zadávání zakázek soukromým subjektem, který je usazen v podobně smýšlející třetí zemi, a účast tohoto subjektu by měly být povoleny, pokud to není v rozporu s bezpečnostními a obrannými zájmy Unie a členských států stanovenými v rámci společné zahraniční a bezpečnostní politiky podle hlavy V Smlouvy o EU nebo s cíli stanovenými v tomto nařízení. Tyto soukromé subjekty by neměly být kontrolovány nepřidruženou třetí zemí nebo musí být prověřovány ve smyslu nařízení Evropského parlamentu a Rady (EU) 2019/452.*** |

Or. en

**Pozměňovací návrh 121**
**Evžen Tošenovský**

**Návrh nařízení**
**Čl. 5 – odst. 3**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| ***3. Členové hostitelského konsorcia uzavřou písemnou dohodu o konsorciu, která stanoví jejich vnitřní ujednání k provádění dohody o hostingu a užívání.*** | ***vypouští se*** |

Or. en

**Pozměňovací návrh 122**
**Evžen Tošenovský**

**Návrh nařízení**
**Čl. 5 – odst. 4**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| ***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.*** | ***vypouští se*** |

Or. en

**Pozměňovací návrh 123**
**Evžen Tošenovský**

**Návrh nařízení**
**Čl. 6 – název**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| Spolupráce a sdílení informací ***v rámci přeshraničních bezpečnostních operačních středisek a mezi nimi*** | ***Posílená*** spolupráce a sdílení informací ***na úrovni EU*** |

Or. en

**Pozměňovací návrh 124**
**Johan Nissinen**

**Návrh nařízení**
**Čl. 6 – odst. 1 – návětí**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| 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: | 1. Členové hostitelského konsorcia si v rámci přeshraničního bezpečnostního operačního střediska mezi sebou ***mohou vyměňovat*** 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: |

Or. en

**Pozměňovací návrh 125**
**Evžen Tošenovský**

**Návrh nařízení**
**Čl. 6 – odst. 1 – návětí**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| 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 | 1. ***Týmy CSIRT či střediska ISAC a jiné týmy CSIRT*** si v rámci ***sítě CSIRT*** 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: |

informací:

Or. en

**Pozměňovací návrh 126**
**Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen**

**Návrh nařízení**
**Čl. 6 – odst. 1 – písm. a**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| a) ***má za cíl předcházet incidentům, odhalovat je, reagovat na ně, zajišťovat následnou obnovu nebo zmírňovat jejich dopad***; | a) ***zlepšuje výměnu zpravodajských informací o kybernetických hrozbách mezi operačními operačními středisky a průmyslovými středisky ISAC s cílem předcházet incidentům, odhalovat je nebo je zmírňovat***; |

Or. en

**Pozměňovací návrh 127**
**Evžen Tošenovský**

**Návrh nařízení**
**Čl. 6 – odst. 2 – návětí**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| 2. ***Písemná*** dohoda o ***konsorciu podle čl. 5 odst. 3 stanoví***: | 2. Dohoda o ***sdílení operativních a jiných informací mezi týmy CSIRT-ISAC nebo případně jinými týmy CSIRT může stanovit***: |

Or. en

**Pozměňovací návrh 128**
**Johan Nissinen**

**Návrh nařízení**
**Čl. 6 – odst. 2 – písm. a**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|

| | |
|---|---|
| a) závazek ***sdílet významné množství údajů uvedených*** v odstavci 1 a podmínky, za nichž mají být tyto informace vyměňovány; | a) závazek ***dobrovolně sdílet údaje uvedené*** v odstavci 1 a podmínky, za nichž mají být tyto informace vyměňovány; |

Or. en

**Pozměňovací návrh 129**
**Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen**

**Návrh nařízení**
**Čl. 6 – odst. 2 – písm. a**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| a) závazek sdílet ***významné množství údajů uvedených*** v odstavci 1 a podmínky, za nichž mají být tyto informace vyměňovány; | a) závazek sdílet ***údaje uvedené*** v odstavci 1 a podmínky, za nichž mají být tyto informace vyměňovány; |

Or. en

**Pozměňovací návrh 130**
**Evžen Tošenovský**

**Návrh nařízení**
**Čl. 6 – odst. 3**

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

Or. en

**Pozměňovací návrh 131**
**Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen**

**Návrh nařízení**
**Čl. 6 – odst. 3**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| 3. ***S cílem povzbudit výměnu*** informací mezi přeshraničními bezpečnostními operačními středisky zajistí přeshraniční bezpečnostní operační střediska vysokou úroveň ***vzájemné*** interoperability***. Aby*** usnadnila ***interoperabilitu*** mezi přeshraničními bezpečnostními operačními středisky***, může Komise prostřednictvím prováděcích aktů po konzultaci s centrem ECCC stanovit*** podmínky ***této interoperability. Tyto prováděcí akty*** se přijímají přezkumným postupem podle čl. 21 odst***. 2*** tohoto nařízení. | 3. ***V zájmu podpory výměny*** informací mezi přeshraničními bezpečnostními operačními ***operačními*** středisky ***a s průmyslovými středisky ISAC*** zajistí přeshraniční bezpečnostní operační střediska vysokou úroveň interoperability ***mezi sebou navzájem a pokud možno s průmyslovými středisky ISAC. Aby se*** usnadnila ***interoperabilita*** mezi přeshraničními bezpečnostními operačními středisky ***a s průmyslovými ISAC, měly by být normy a protokoly pro sdílení informací harmonizovány s mezinárodními normami a osvědčenými postupy v daném odvětví. ECCC může rovněž požádat Komisi prostřednictvím aktů v přenesené pravomoci, aby navrhla*** podmínky ***pro tuto interoperabilitu v úzké spolupráci s regionálními bezpečnostními operačními středisky a na základě mezinárodních norem a osvědčených postupů v daném odvětví. Tyto akty v přenesené pravomoci*** se přijímají ***v souladu s*** přezkumným postupem podle čl. 21 odst***.2*** tohoto nařízení. |

Or. en

**Pozměňovací návrh 132**
**Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

**Návrh nařízení**
**Čl. 6 – odst. 3**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| 3. S cílem povzbudit výměnu | 3. S cílem povzbudit výměnu |

| | |
|---|---|
| informací mezi přeshraničními bezpečnostními operačními středisky zajistí přeshraniční bezpečnostní operační střediska vysokou úroveň vzájemné interoperability. ***Aby usnadnila*** interoperabilitu mezi přeshraničními bezpečnostními operačními středisky, může Komise prostřednictvím prováděcích aktů po konzultaci s centrem ECCC stanovit podmínky této interoperability. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 21 odst. 2 tohoto nařízení. | informací mezi přeshraničními bezpečnostními operačními středisky zajistí přeshraniční bezpečnostní operační střediska vysokou úroveň vzájemné interoperability. ***Společné zadávání veřejných zakázek na kybernetickou infrastrukturu, služby a nástroje může usnadnit interoperabilitu mezi přeshraničními bezpečnostními operačními středisky. Aby upřesnila podmínky pro*** interoperabilitu mezi přeshraničními bezpečnostními operačními středisky, může Komise prostřednictvím prováděcích aktů po konzultaci s centrem ECCC ***a agenturou ENISA*** stanovit podmínky této interoperability. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 21 odst. 2 tohoto nařízení. |

Or. en

**Pozměňovací návrh 133**
**Evžen Tošenovský**

**Návrh nařízení**
**Čl. 6 – odst. 4**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| ***4. Přeshraniční bezpečnostní operační střediska mezi sebou uzavřou dohody o spolupráci, v nichž stanoví zásady sdílení informací mezi přeshraničními platformami.*** | ***vypouští se*** |

Or. en

**Pozměňovací návrh 134**
**Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

**Návrh nařízení**
**Čl. 6 – odst. 4**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| 4. Přeshraniční bezpečnostní operační střediska mezi sebou uzavřou dohody o spolupráci, v nichž ***stanoví*** zásady sdílení informací mezi přeshraničními platformami. | 4. Přeshraniční bezpečnostní operační střediska mezi sebou uzavřou dohody o spolupráci, v nichž ***upřesní*** zásady sdílení informací mezi přeshraničními platformami***, přičemž zohlední již existující příslušné mechanismy sdílení informací podle směrnice (EU) 2022/2555. V souvislosti s potenciálním nebo probíhajícím rozsáhlým kybernetickým bezpečnostním incidentem musí být mechanismy sdílení informací v souladu s příslušnými ustanoveními směrnice (EU) 2022/2555***. |

Or. en

**Pozměňovací návrh 135**
**Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen**

**Návrh nařízení**
**Čl. 6 – odst. 4**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| 4. Přeshraniční bezpečnostní operační střediska mezi sebou uzavřou dohody o spolupráci, v nichž stanoví zásady sdílení informací mezi přeshraničními platformami. | 4. Přeshraniční bezpečnostní operační střediska mezi sebou ***a s průmyslovými středisky ISAC*** uzavřou dohody o spolupráci, v nichž stanoví zásady sdílení informací ***a interoperability*** mezi přeshraničními platformami. |

Or. en

**Pozměňovací návrh 136**
**Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen**

**Návrh nařízení**
**Čl. 7 – název**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| Spolupráce a sdílení informací se ***subjekty Unie*** | Spolupráce a sdílení informací se ***sítí CSIRT*** |

Or. en

**Pozměňovací návrh 137**
**Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen**

**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 ***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 s ohledem na jejich příslušné úlohy ***a postupy krizového řízení*** v souladu se směrnicí (EU) 2022/2555. |

Or. en

*Odůvodnění*

*Navrhnout zachování postupu NIS2 v případě rozsáhlých incidentů.*

**Pozměňovací návrh 138**
**Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

**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 | 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***, Komisi a agentuře*** |

| | |
|---|---|
| na jejich příslušné úlohy v oblasti řešení krizí v souladu se směrnicí (EU) 2022/2555. | ***ENISA*** s ohledem na jejich příslušné úlohy v oblasti řešení krizí v souladu se směrnicí (EU) 2022/2555. |

Or. en

**Pozměňovací návrh 139**
**Evžen Tošenovský**

**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 ***týmy CSIRT či*** střediska ***ISAC*** získají informace týkající se potenciálního nebo probíhajícího rozsáhlého kybernetického bezpečnostního incidentu, poskytnou neprodleně příslušné informace síti EU-CyCLONe ***a*** síti CSIRT s ohledem na jejich příslušné úlohy v oblasti řešení krizí v souladu se směrnicí (EU) 2022/2555. |

Or. en

**Pozměňovací návrh 140**
**Evžen Tošenovský**

**Návrh nařízení**
**Čl. 7 – odst. 2**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| ***2. Komise může prostřednictvím prováděcích aktů stanovit procesní opatření pro sdílení informací podle odstavce 1. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 21 odst. 2 tohoto nařízení.*** | ***vypouští se*** |

Or. en

**Pozměňovací návrh 141**
**Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen**

**Návrh nařízení**
**Čl. 7 – odst. 2**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| 2. Komise může prostřednictvím prováděcích aktů stanovit procesní opatření pro sdílení informací podle odstavce 1. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 21 odst. 2 tohoto nařízení. | 2. Komise může ***po konzultaci s přeshraničními platformami a sítí CSIRT*** prostřednictvím prováděcích aktů stanovit procesní opatření pro sdílení informací podle odstavce 1. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 21 odst. 2 tohoto nařízení ***a v soualdu se směrnicí (EU) 2022/2555***. |

Or. en

*Odůvodnění*

*Návrh zachovat postup NIS2 pro rozsáhlé incidenty, a proto je třeba nejprve konzultovat síť CSIRT.*

**Pozměňovací návrh 142**
**Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

**Návrh nařízení**
**Čl. 7 – odst. 2**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| 2. Komise může prostřednictvím prováděcích aktů stanovit procesní opatření pro sdílení informací podle odstavce 1. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 21 odst. 2 tohoto nařízení. | 2. Komise může ***po konzultaci agentury ENISA*** prostřednictvím prováděcích aktů stanovit procesní opatření pro sdílení informací podle odstavce 1. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 21 odst. 2 tohoto nařízení. |

Or. en

**Pozměňovací návrh 143**
**Johan Nissinen**

**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 ***důvěrnosti,*** 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. |

Or. en

**Pozměňovací návrh 144**
**Evžen Tošenovský**

**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.*** | ***vypouští se*** |

Or. en

**Pozměňovací návrh 145**
**Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen**

**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 ***a v souladu se směrnicí (EU) 2022/2555 a 2022/2557***. Komise přitom za podpory vysokého představitele zohlední příslušné normy zabezpečení na úrovni obrany, aby usnadnila spolupráci s vojenskými subjekty. |

Or. en

**Pozměňovací návrh 146**
**Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

**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 ***po konzultaci agentury ENISA*** 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. |

Or. en

**Pozměňovací návrh 147**
**Johan Nissinen**

**Návrh nařízení**

**Čl. 9 – odst. 1**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| 1. Zřizuje se mechanismus pro mimořádné události v kybernetické oblasti s cílem zlepšit odolnost Unie vůči zásadním hrozbám v oblasti kybernetické bezpečnosti, připravit se na krátkodobé dopady významných a rozsáhlých kybernetických bezpečnostních incidentů nebo krizí a v duchu solidarity je zmírňovat (dále jen „mechanismus“). | 1. Zřizuje se mechanismus pro mimořádné události v kybernetické oblasti s cílem zlepšit odolnost Unie vůči zásadním hrozbám v oblasti kybernetické bezpečnosti, připravit se na krátkodobé dopady významných a rozsáhlých kybernetických bezpečnostních incidentů nebo krizí a v duchu solidarity je zmírňovat (dále jen „mechanismus“) ***na výslovnou žádost dotčeného členského státu***. |

Or. en

**Pozměňovací návrh 148**
**Evžen Tošenovský**

**Návrh nařízení**
**Čl. 9 – odst. 1**

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

Or. en

**Pozměňovací návrh 149**
**Johan Nissinen**

**Návrh nařízení**
**Čl. 10 – odst. 1 – písm. b**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| b) opatření reakce, která podporují | b) opatření reakce, která podporují |

| | |
|---|---|
| reakci na významné a rozsáhlé kybernetické bezpečnostní incidenty a okamžitou obnovu po nich a která mají poskytovat důvěryhodní poskytovatelé zapojení do rezervy EU pro kybernetickou bezpečnost zřízené podle článku 12; | reakci na významné a rozsáhlé kybernetické bezpečnostní incidenty a okamžitou obnovu po nich a která mají poskytovat důvěryhodní poskytovatelé zapojení do rezervy EU pro kybernetickou bezpečnost zřízené podle článku 12***, na výslovnou žádost dotčeného členského státu***; |

Or. en

**Pozměňovací návrh 150**
**Evžen Tošenovský**

**Návrh nařízení**
**Čl. 10 – odst. 1 – písm. b**

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

Or. en

**Pozměňovací návrh 151**
**Ville Niinistö**
za skupinu Verts/ALE

**Návrh nařízení**
**Čl. 10 – odst.1 a (nový)**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| | ***1a. Po spuštění mechanismu pro mimořádné situace v kybernetické oblasti podá Komise každý rok zprávu o posouzení pozitivního i negativního fungování mechanismu, včetně toho, zda jsou zapotřebí další požadavky na spolupráci nebo odbornou přípravu.*** |

Or. en

**Pozměňovací návrh 152**
**Evžen Tošenovský**

**Návrh nařízení**
**Čl. 11 – odst. 1**

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

Or. en

**Pozměňovací návrh 153**
**Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen**

**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 a vysokým představitelem vypracuje společné rizikové scénáře a metodiky pro koordinované testování ***připravenosti. To bude podkladem pro určení dotčených odvětví nebo pododvětví, z nichž mohou subjekty podléhat koordinovanému testování připravenosti, jak je popsáno v odstavci 1***. |

Or. en

**Pozměňovací návrh 154**
**Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

**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 a subjetky, které mohou podléhat testování připravenosti,*** vypracuje společné rizikové scénáře a metodiky pro koordinované testování. |

Or. en

**Pozměňovací návrh 155**
**Johan Nissinen**

**Návrh nařízení**
**Čl. 12 – odst. 1**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| 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***. | 1. Zřizuje se rezerva EU pro kybernetickou bezpečnost ***s cílem pomoci*** uživatelům uvedeným v odstavci 3 při reakci ***na významné nebo rozsáhlé kybernetické bezpečnostní incidenty*** nebo při poskytování podpory ***při*** reakci na ***tyto incidenty a při okamžitém zotavení z těchto incidentů, a to na výslovnou žádost dotčeného členského státu (dotčených členských států), a aniž je dotčena zvláštní povaha bezpečnostní a obranné politiky některých členských států***. |

Or. en

**Pozměňovací návrh 156**
**Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

**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***, musí posilovat odolnost a svrchovanost Unie a zlepšovat konkurenceschopnost Unie. Se jmény vybraných důvěryhodných poskytovatelů a jejich službami se nakládá jako s důvěrnými***. |

Or. en

**Pozměňovací návrh 157**
**Johan Nissinen**

**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. ***Rezerva EU pro kybernetickou bezpečnost neomezuje potřebu umožnit zemím sledovat a posuzovat své vlastní potřeby.*** |

Or. en

**Pozměňovací návrh 158**

**Evžen Tošenovský**

**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 ***řízených bezpečnostních služeb*** vybraných v souladu s kritérii stanovenými v článku 16. Rezerva zahrnuje předem přislíbené služby. Služby ***je možné na požádání*** provádět ve všech členských státech. |

Or. en

**Pozměňovací návrh 159**
**Evžen Tošenovský**

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

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| b) ***orgány, instituce nebo jiné subjekty Unie***. | b) ***třetí země uvedené v článku 17 tohoto nařízení***. |

Or. en

**Pozměňovací návrh 160**
**Evžen Tošenovský**

**Návrh nařízení**
**Čl. 12 – odst. 4**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| 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 | 4. Uživatelé uvedení v odst. 3 písm. ***a) mohou na základě žádosti využívat*** 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 |

| | |
|---|---|
| incidentech. | okamžité obnově po těchto incidentech. |

Or. en

**Pozměňovací návrh 161**
**Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen**

**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 ***ve spolupráci se skupinou pro spolupráci v oblasti bezpečnosti sítí a informací a*** v souladu s požadavky uživatelů uvedenými v odstavci 3 ***a*** 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. |

Or. en

**Pozměňovací návrh 162**
**Evžen Tošenovský**

**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 | 5. Komise nese celkovou odpovědnost za provádění rezervy EU pro kybernetickou bezpečnost. Komise ***ve spolupráci s agenturou ENISA*** 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 |

| | |
|---|---|
| programy Unie. | tohoto nařízení i s jinými opatřeními a programy Unie. |

Or. en

**Pozměňovací návrh 163**
**Evžen Tošenovský**

**Návrh nařízení**
**Čl. 12 – odst. 6**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| ***6. Komise může provozem a správou rezervy EU pro kybernetickou bezpečnost plně nebo zčásti pověřit agenturu ENISA, a to prostřednictvím dohod o příspěvcích.*** | ***vypouští se*** |

Or. en

**Pozměňovací návrh 164**
**Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

**Návrh nařízení**
**Čl. 12 – odst. 6**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| 6. Komise ***může*** provozem a správou rezervy EU pro kybernetickou bezpečnost plně nebo zčásti ***pověřit*** agenturu ENISA, a to prostřednictvím dohod o příspěvcích. | 6. Komise ***pověří*** provozem a správou rezervy EU pro kybernetickou bezpečnost plně nebo zčásti agenturu ENISA, a to prostřednictvím dohod o příspěvcích. |

Or. en

**Pozměňovací návrh 165**
**Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

**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 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. | 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 potřebných dovedností a kapacity pracovníků v oblasti kybernetické bezpečnosti***. Agentura ENISA po konzultaci s Komisí ***a v partnerství se soukromým sektorem*** 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. |

Or. en

**Pozměňovací návrh 166**
**Evžen Tošenovský**

**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 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. | 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 ***a informuje Radu o potřebách třetích zemí***. |

Or. en

**Pozměňovací návrh 167**
**Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen**

**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*** 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. | 7. S cílem podpořit Komisi při zřizování rezervy EU pro kybernetickou bezpečnost vypracuje agentura ENISA po konzultaci s členskými státy***, Komisí, poskytovateli řízených bezpečnostních služeb a zástupci průmyslu*** 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. |

Or. en

**Pozměňovací návrh 168**
**Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

**Návrh nařízení**
**Čl. 12 – odst. 8**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| 8. Komise může ***prostřednictvím prováděcích aktů specifikovat*** druhy a počet služeb reakce požadovaných pro rezervu EU pro kybernetickou bezpečnost. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 21 odst. 2. | 8. Komise může ***přijmout akt v přenesené pravomoci v souladu s článkem 20a tohoto nařízení, kterým upřesní*** druhy a počet služeb reakce požadovaných pro rezervu EU pro kybernetickou bezpečnost. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 21 odst. 2. |

Or. en

**Pozměňovací návrh 169**
**Evžen Tošenovský**

**Návrh nařízení**
**Čl. 13 – odst. 5 – písm. a**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| a) ***příslušné informace týkající se*** dotčeného subjektu a ***možných dopadů*** incidentu a ***plánovaného*** využití požadované podpory, včetně uvedení odhadovaných potřeb; | a) ***druh*** dotčeného subjektu a ***možné dopady*** incidentu a ***plánované*** využití požadované podpory, včetně uvedení odhadovaných potřeb; |

Or. en

**Pozměňovací návrh 170**
**Evžen Tošenovský**

**Návrh nařízení**
**Čl. 13 – odst. 5 – písm. b**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| b) informace o opatřeních přijatých ke zmírnění následků incidentu, pro který je podpora požadována, jak je uvedeno v odstavci 2; | b) ***obecné*** informace o opatřeních přijatých ke zmírnění následků incidentu, pro který je podpora požadována, jak je uvedeno v odstavci 2; |

Or. en

**Pozměňovací návrh 171**
**Evžen Tošenovský**

**Návrh nařízení**
**Čl. 13 – odst. 5 – písm. c**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| 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.*** | c) informace o dalších formách podpory, které má postižený subjekt k dispozici |

Or. en

**Pozměňovací návrh 172**
**Evžen Tošenovský**

**Návrh nařízení**
**Čl. 13 – odst. 7**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| ***7. Komise může prostřednictvím prováděcích aktů dále upřesnit podrobná opatření pro přidělování podpůrných služeb z rezervy EU pro kybernetickou bezpečnost. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 21 odst. 2.*** | ***vypouští se*** |

Or. en

**Pozměňovací návrh 173**
**Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

**Návrh nařízení**
**Čl. 13 – odst. 7**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| 7. Komise může ***prostřednictvím prováděcích aktů dále upřesnit*** podrobná opatření pro přidělování podpůrných služeb z rezervy EU pro kybernetickou bezpečnost. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 21 odst. 2. | 7. Komise může ***přijmout akty v přenesené pravomoci v souladu s článkem 20a tohoto nařízení, kterými blíže upřesní*** podrobná opatření pro přidělování podpůrných služeb z rezervy EU pro kybernetickou bezpečnost. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 21 odst. 2. |

Or. en

**Pozměňovací návrh 174**
**Evžen Tošenovský**

**Návrh nařízení**
**Čl. 14 – odst. 1**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|

| | |
|---|---|
| 1. Komise za pomoci agentury ENISA ***nebo jak je stanoveno v dohodách o příspěvku podle čl. 12 odst. 6*** posoudí žádosti o podporu z rezervy EU pro kybernetickou bezpečnost a ***odpověď neprodleně*** předá uživatelům uvedeným v čl. 12 odst. 3. | 1. Komise za pomoci agentury ENISA posoudí žádosti o podporu z rezervy EU pro kybernetickou bezpečnost a ***své rozhodnutí*** předá uživatelům uvedeným v čl. 12 odst. 3 ***bez zbytečného odkladu a v každém případě do 24 hodin***. |

Or. en

**Pozměňovací návrh 175**
**Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen**

**Návrh nařízení**
**Čl. 14 – odst. 2 – písm. d**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| d) potenciální přeshraniční povaha incidentu a riziko přelévání do jiných členských států nebo k jiným uživatelům; | d) ***rozsah a*** potenciální přeshraniční povaha incidentu a riziko přelévání do jiných členských států nebo k jiným uživatelům; |

Or. en

**Pozměňovací návrh 176**
**Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

**Návrh nařízení**
**Čl. 14 – odst. 3**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| 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. | 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***. |

Or. en

**Pozměňovací návrh 177**
**Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen**

**Návrh nařízení**
**Čl. 14 – odst. 3**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| 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. | 3. Služby rezervy EU pro kybernetickou bezpečnost se poskytují ***po schválení uživatelem a*** 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. |

Or. en

**Pozměňovací návrh 178**
**Angelika Niebler, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

**Návrh nařízení**
**Čl. 14 – odst. 4**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| 4. Dohody uvedené v odstavci 3 ***mohou vycházet*** ze vzorů, které vypracuje agentura ENISA po konzultaci s členskými státy. | 4. Dohody uvedené v odstavci 3 ***vycházejí*** ze vzorů, které vypracuje agentura ENISA po konzultaci s členskými státy ***a dalšími uživateli rezervy***. |

Or. en

**Pozměňovací návrh 179**
**Evžen Tošenovský**

**Návrh nařízení**
**Čl. 14 – odst. 5**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|

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

Or. en

**Pozměňovací návrh 180**
**Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen**

**Návrh nařízení**
**Čl. 14 – odst. 5**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| 5. Komise a agentura ENISA nenesou žádnou smluvní odpovědnost za škody způsobené třetím osobám službami poskytovanými v rámci provádění 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 nedbalosti při hodnocení žádosti poskytovatele služeb nebo v případech, kdy jsou Komise nebo agentura ENISA uživateli a jsou shledány odpovědnými za škody***. |

Or. en

**Pozměňovací návrh 181**
**Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

**Návrh nařízení**
**Čl. 14 – odst. 5**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| 5. Komise a agentura ENISA nenesou žádnou smluvní odpovědnost za škody způsobené třetím osobám službami poskytovanými v rámci provádění 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, kdy jsou Komise nebo agentura ENISA uživateli rezervy podle čl. 14 odst. 3***. |

Or. en

**Pozměňovací návrh 182**
**Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen**

**Návrh nařízení**
**Čl. 14 – odst. 6**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| 6. Do jednoho měsíce od ukončení podpůrné akce předloží uživatelé Komisi a agentuře ENISA souhrnnou zprávu o poskytnuté službě, dosažených výsledcích a získaných poznatcích. Je-li uživatel ze třetí země podle článku 17, je tato zpráva sdílena s vysokým představitelem. | 6. Do jednoho měsíce od ukončení podpůrné akce předloží uživatelé Komisi a agentuře ENISA souhrnnou zprávu o poskytnuté službě, dosažených výsledcích a získaných poznatcích. Je-li uživatel ze třetí země podle článku 17, je tato zpráva sdílena s vysokým představitelem. ***Zpráva dodržuje unijní nebo vnitrostátní právní předpisy týkající se ochrany citlivých nebo utajovaných informací.*** |

Or. en

**Pozměňovací návrh 183**
**Evžen Tošenovský**

**Návrh nařízení**
**Čl. 14 – odst. 6**

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

Or. en

**Pozměňovací návrh 184**
**Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen**

**Návrh nařízení**
**Čl. 14 – odst. 7**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| 7. Komise podává skupině pro spolupráci v oblasti bezpečnosti sítí a informací pravidelné zprávy o využívání podpory a jejích výsledcích. | 7. Komise 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 nebo vnitrostátním právem týkajícím se ochrany citlivých nebo utajovaných údajů.*** |

Or. en

**Pozměňovací návrh 185**
**Evžen Tošenovský**

**Návrh nařízení**
**Čl. 14 – odst. 7**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| 7. Komise podává skupině pro spolupráci v oblasti bezpečnosti sítí a informací pravidelné zprávy o využívání podpory a jejích výsledcích. | 7. Komise ***nejméně dvakrát ročně*** podává skupině pro spolupráci v oblasti bezpečnosti sítí a informací pravidelné zprávy o využívání podpory a jejích výsledcích. |

Or. en

**Pozměňovací návrh 186**
**Evžen Tošenovský**

**Návrh nařízení**
**Čl. 15 – název**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| Koordinace s mechanismy pro řešení krizí | Koordinace ***mechanismu pro mimořádné události v kybernetické oblasti*** s mechanismy pro řešení krizí |

Or. en

**Pozměňovací návrh 187**
**Evžen Tošenovský**

**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. |

Or. en

**Pozměňovací návrh 188**
**Evžen Tošenovský**

**Návrh nařízení**
**Čl. 16 – název**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| Důvěryhodní poskytovatelé | Důvěryhodní poskytovatelé ***řízených bezpečnostních služeb*** |

Or. en

**Pozměňovací návrh 189**
**Johan Nissinen**

**Návrh nařízení**
**Čl. 16 – odst. 1 – návětí**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|

| | |
|---|---|
| 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: | 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***, aniž je dotčena primární odpovědnost členských států za národní bezpečnost,*** a v souladu s těmito zásadami: |

Or. en

**Pozměňovací návrh 190**
**Evžen Tošenovský**

**Návrh nařízení**
**Čl. 16 – odst. 1 – písm. a**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| 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; | a) zajistit, aby rezerva EU pro kybernetickou bezpečnost zahrnovala služby, které mohou být využívány ve všech členských státech ***a třetích zemích v souladu s článkem 17 tohoto nařízení***, zejména s ohledem na vnitrostátní požadavky na poskytování takových služeb, včetně certifikace nebo akreditace; |

Or. en

**Pozměňovací návrh 191**
**Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

**Návrh nařízení**
**Čl. 16 – odst. 1 – písm. c**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| 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. | 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***, posílení odolnosti a*** |

| | |
|---|---|
| | ***svrchovanosti Unie a zlepšení konkurenceschopnosti Unie***. |

Or. en

**Pozměňovací návrh 192**
**Evžen Tošenovský**

**Návrh nařízení**
**Čl. 16 – odst. 1 – písm. c**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| 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. | c) zajistit, aby rezerva EU pro kybernetickou bezpečnost ***přispívala*** k dosažení cílů stanovených v článku 3 nařízení (EU) 2021/694, včetně podpory rozvoje dovedností v oblasti kybernetické bezpečnosti v EU. |

Or. en

**Pozměňovací návrh 193**
**Angelika Niebler, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

**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 ***aktuálním*** hardwarovým a softwarovým technickým zařízením nezbytným pro podporu požadované služby ***a v příslušných případech splňuje požadavky stanovené v nařízení XX/XXXX (akt o kybernetické odolnosti)***; |

Or. en

**Pozměňovací návrh 194**
**Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu**

**Buşoi, Ioan-Rareş Bogdan**

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

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| | ***fa) poskytovatel prokáže, že jeho rozhodovací a řídící struktury nepodléhají nepatřičnému ovlivňování ze strany vlád států klasifikovaných jako systémové konkurenty Unie;*** |

Or. en

**Pozměňovací návrh 195**
**Evžen Tošenovský**

**Návrh nařízení**
**Čl. 16 – odst. 2 – písm. h**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| h) poskytovatel je schopen poskytnout službu v krátkém časovém rámci v členském státě / členských státech, v němž/nichž může službu poskytovat; | h) poskytovatel je schopen poskytnout službu v krátkém časovém rámci v členském státě / členských státech ***nebo ve třetích zemích***, v němž/nichž může službu poskytovat; |

Or. en

**Pozměňovací návrh 196**
**Evžen Tošenovský**

**Návrh nařízení**
**Čl. 16 – odst. 2 – písm. i**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| i) poskytovatel je schopen poskytnout službu v místním jazyce členského státu / členských států, v němž/nichž může službu poskytovat; | i) poskytovatel je schopen poskytnout službu v místním jazyce členského státu / členských států ***nebo třetích zemí***, v němž/nichž může službu poskytovat***, nebo v jednom z pracovních jazyků orgánů EU***; |

Or. en

**Pozměňovací návrh 197**
**Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

**Návrh nařízení**
**Čl. 16 – odst. 2 – písm. j**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| j) jakmile bude zaveden systém certifikace EU pro řízené bezpečnostní služby podle nařízení (EU) 2019/881, bude poskytovatel certifikován v souladu s tímto systémem. | j) jakmile bude zaveden systém certifikace EU pro řízené bezpečnostní služby podle nařízení (EU) 2019/881, bude poskytovatel certifikován v souladu s tímto systémem ***do dvou let od přijetí tohoto systému***. |

Or. en

**Pozměňovací návrh 198**
**Evžen Tošenovský**

**Návrh nařízení**
**Čl. 16 – odst. 2 – písm. j**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| j) jakmile bude zaveden systém certifikace ***EU*** pro řízené bezpečnostní služby podle nařízení (EU) 2019/881, bude poskytovatel certifikován v souladu s tímto systémem. | 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. |

Or. en

**Pozměňovací návrh 199**
**Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen**

**Návrh nařízení**
**Čl. 16 – odst. 2 – písm. j**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| j) jakmile bude zaveden systém certifikace EU pro ***řízené bezpečnostní*** | j) jakmile bude zaveden systém certifikace EU pro nařízení (EU) 2019/881 |

| | |
|---|---|
| ***služby podle*** nařízení (EU) 2019/881, bude poskytovatel certifikován v souladu s tímto systémem. | ***o řízených bezpečnostních službách***, bude poskytovatel ***do dvou let*** certifikován v souladu s tímto systémem. |

Or. en

*Odůvodnění*

*Komise navrhuje, aby technické požadavky uvedené v tomto nařízení nahradil systém certifikace. Tento pozměňovací návrh poskytuje společnostem, zejména malým a středním podnikům, více času na přechod k tomuto režimu a podporuje rovnější podmínky v celé Unii. Do té doby budou muset dodržovat technické požadavky tohoto nařízení.*

**Pozměňovací návrh 200**
**Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen**

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

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| | ***ja) poskytovatel musí mít možnost oddělit své služby od širší smlouvy, aby uživatel mohl přejít k jinému poskytovateli služeb;*** |

Or. en

**Pozměňovací návrh 201**
**Evžen Tošenovský**

**Návrh nařízení**
**Čl. 17 – odst. 6**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| 6. Komise ***s vysokým představitelem koordinuje činnost týkající se*** obdržených ***žádostí*** a provádění podpory poskytované třetím zemím z rezervy EU pro kybernetickou bezpečnost. | 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***. |

Or. en

**Pozměňovací návrh 202**
**Evžen Tošenovský**

**Návrh nařízení**
**Článek 18**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| ***Článek 18*** | ***vypouští se*** |
| ***Mechanismus přezkumu kybernetických bezpečnostních incidentů*** | |
| ***1. Na žádost Komise, sítě EU-CyCLONe nebo sítě CSIRT agentura ENISA přezkoumá a posoudí hrozby, zranitelná místa a opatření ke zmírnění dopadů v souvislosti s konkrétním významným nebo rozsáhlým kybernetickým bezpečnostním incidentem. Po dokončení přezkumu a posouzení incidentu předá agentura ENISA síti CSIRT, síti EU-CyCLONe a Komisi zprávu o přezkumu incidentu, aby je podpořila při plnění jejich úkolů, zejména s ohledem na úkoly stanovené v článcích 15 a 16 směrnice (EU) 2022/2555. V případě potřeby Komise sdílí zprávu s vysokým představitelem.*** | |
| ***2. Při přípravě zprávy o přezkumu incidentů podle odstavce 1 agentura ENISA spolupracuje se všemi příslušnými zúčastněnými stranami, včetně zástupců členských států, Komise, dalších příslušných orgánů, institucí a jiných subjektů EU, poskytovatelů řízených bezpečnostních služeb a uživatelů služeb kybernetické bezpečnosti. Agentura ENISA v případě potřeby spolupracuje také se subjekty, které byly zasaženy významnými nebo rozsáhlými kybernetickými bezpečnostními incidenty. Na podporu přezkumu může agentura ENISA konzultovat i další typy zúčastněných stran. Konzultovaní zástupci oznámí jakýkoli případný střet zájmů.*** | |
| ***3. Zpráva zahrnuje přezkum a analýzu konkrétního významného nebo rozsáhlého kybernetického bezpečnostního incidentu, včetně hlavních příčin, zranitelností a*** | |

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

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

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

Or. en

**Pozměňovací návrh 203**
**Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

**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***, a získává od nich zpětnou vazbu***. 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. |

Or. en

**Pozměňovací návrh 204**
**Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen**

**Návrh nařízení**
**Čl. 18 – odst. 3**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| 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. | 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.*** |

Or. en

**Pozměňovací návrh 205**
**Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

**Návrh nařízení**
**Čl. 18 – odst. 4**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| 4. Dle potřeby zpráva uvádí doporučení ke zlepšení kybernetické pozice Unie**.** | 4. Dle potřeby zpráva uvádí ***konkrétní*** doporučení***, a to i pro všechny příslušné zúčastněné strany,*** ke zlepšení kybernetické pozice Unie***;*** |

Or. en

**Pozměňovací návrh 206**
**Johan Nissinen**

**Návrh nařízení**
**Čl. 18 – odst. 4**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| 4. Dle potřeby zpráva uvádí doporučení ke zlepšení kybernetické | 4. Dle potřeby zpráva uvádí ***právně nezávazná dobrovolná*** doporučení ke |

| | |
|---|---|
| pozice Unie. | zlepšení kybernetické pozice Unie. |

Or. en

**Pozměňovací návrh 207**
**Evžen Tošenovský**

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

| *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 ***středisek pro sdílení a analýzu informací (ISAC) týmů CSIRT a*** bezpečnostních operačních středisek, které přispívají k situačnímu povědomí v Unii a k posílení zpravodajských kapacit Unie v oblasti kybernetických hrozeb; |

Or. en

**Pozměňovací návrh 208**
**Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

**Návrh nařízení**
**Čl. 19 – odst. 1 – bod 3**
Nařízení (EU) 2021/694
Čl. 14 – odst. 2

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| Program může poskytovat financování kteroukoli z forem stanovených ve finančním nařízení, včetně zejména zadávání veřejných zakázek jako základní formy, jakož i grantů a cen. | Program může poskytovat financování kteroukoli z forem stanovených ve finančním nařízení, včetně zejména zadávání veřejných zakázek jako základní formy, jakož i grantů a cen. ***Agentura ENISA obdrží dodatečné zdroje na plnění svých dodatečných úkolů stanovených v nařízení XX/XXX (akt o kybernetické solidaritě). Toto dodatečné financování neohrozí dosažení cílů programu.*** |

Or. en

**Pozměňovací návrh 209**
**Evžen Tošenovský**

**Návrh nařízení**
**Čl. 19 – odst. 1 – bod 5**
Nařízení (EU) 2021/694
Článek 19

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| Podporu v podobě grantů může v souladu s čl. 195 odst. 1 písm. d) finančního nařízení udělovat ***národním bezpečnostním operačním střediskům*** podle článku 4 nařízení XXXX a ***hostitelskému konsorciu*** podle článku 5 nařízení XXXX přímo centrum ECCC bez výzvy k předkládání návrhů. | Podporu v podobě grantů může v souladu s čl. 195 odst. 1 písm. d) finančního nařízení udělovat ***střediskům pro sdílení a analýzu informací (ISAC) týmů CSIRT*** podle článku 4 nařízení XXXX a podle článku 5 nařízení XXXX přímo centrum ECCC bez výzvy k předkládání návrhů. |

Or. en

**Pozměňovací návrh 210**
**Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

**Návrh nařízení**
**Čl. 20 – název**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| Hodnocení | Hodnocení ***a přezkum*** |

Or. en

**Pozměňovací návrh 211**
**Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

**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 [***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***.<br><br>***Hodnocení posoudí zejména:***<br><br>***a) účast členských států v evropském kybernetickém štítu, včetně počtu národních bezpečnostních operačních středisek a přeshraničních bezpečnostních operačních středisek zřízených v rámci nařízení, a účinnost výměny informací;***<br><br>***b) přínos tohoto nařízení k posílení odolnosti a svrchovanosti Unie, ke zlepšení konkurenceschopnosti příslušných průmyslových odvětví, včetně malých a středních podniků, a k rozvoji dovedností v oblasti kybernetické bezpečnosti v EU;***<br><br>***c) využívání rezervy pro kybernetickou bezpečnost, včetně toho, zda by oblast působnosti rezervy měla být rozšířena na služby připravenosti na incidenty nebo společná cvičení s důvěryhodnými poskytovateli a potenciálními uživateli rezervy pro kybernetickou bezpečnost, aby se v případě potřeby zajistilo účinné fungování rezervy;***<br><br>***d) 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;***<br><br>***e) příspěvek tohoto nařízení k zavádění a vývoji nejmodernějších technologií v Unii;***<br><br>***Komise na základě uvedené zprávy případně předloží Evropskému parlamentu a Radě legislativní návrh na změnu tohoto nařízení.*** |
| | Or. en |

**Pozměňovací návrh 212**

**Evžen Tošenovský**

**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 [čtyř let ode dne použitelnosti tohoto nařízení] předloží Komise Evropskému parlamentu a Radě zprávu o hodnocení a přezkumu tohoto nařízení. ***V případě potřeby se ke zprávě přiloží legislativní návrh.*** |

Or. en

**Pozměňovací návrh 213**
**Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen, Nicola Danti**

**Návrh nařízení**
**Čl. 20 – odst. 1 a (nový)**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| | ***Každý rok při předkládání návrhu rozpočtu na následující rok předloží Komise podrobné posouzení úkolů agentury ENISA podle tohoto nařízení, jakož i [návrhu nařízení o horizontálních požadavcích na kybernetickou bezpečnost produktů s digitálními prvky] a dalších právních předpisů Unie a podrobně uvede finanční a lidské zdroje potřebné k plnění těchto úkolů.*** |

Or. en

**Pozměňovací návrh 214**
**Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

**Návrh nařízení**
**Článek 20 a (nový)**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|

***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. 12 odst. 8 a čl. 13 odst. 7 je svěřena Komisi na dobu pěti let od... [datum vstupu základního legislativního aktu v platnost nebo jakékoli jiné datum stanovené spolunormotvůrci]. Komise vypracuje zprávu o přenesené pravomoci nejpozději devět měsíců před koncem tohoto pětiletého období. Přenesení pravomoci se automaticky prodlužuje o stejně dlouhá období, pokud Evropský parlament nebo 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. 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 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. 12 odst. 8 nebo 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].*** |

Or. en

**Pozměňovací návrh 215**
**Evžen Tošenovský**

**Návrh nařízení**
**Příloha I – odst. 1 – bod 1**
Nařízení (EU) 2021/694
Příloha I – kapitola „Specifický cíl č. 3 – Kybernetická bezpečnost a důvěra“

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| 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. | 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 ***vnitrostátních týmů CSIRT a*** bezpečnostních operačních středisek tvořících evropský kybernetický štít, jakož i dalších nástrojů, které budou zpřístupněny veřejnému i soukromému sektoru v celé Evropě. |

Or. en

**Pozměňovací návrh 216**
**Evžen Tošenovský**

**Návrh nařízení**
**Příloha I – odst. 1 – bod 1**
Nařízení (EU) 2021/694
Příloha I – kapitola „Specifický cíl č. 3 – Kybernetická bezpečnost a důvěra“

| *Znění navržené Komisí* | *Pozměňovací návrh* |
| --- | --- |
| 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 ***kybernetické bezpečnosti*** na úrovni Unie.; | 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.; |

Or. en