**Evropský parlament**
2019-2024

*Výbor pro průmysl, výzkum a energetiku*

**2023/0108(COD)**

21.9.2023

# POZMĚŇOVACÍ NÁVRHY 17 - 52

**Návrh zprávy**
**Josianne Cutajar**
(PE752.802v01-00)

Návrh nařízení Evropského parlamentu a Rady, kterým se mění nařízení (EU) 2019/881, pokud jde o řízené bezpečnostní služby

Návrh nařízení
(COM(2023)0208 – C9-0137/2023 – 2023/0108(COD))

**Pozměňovací návrh 17**
**Evžen Tošenovský**

**Návrh nařízení**
**Bod odůvodnění 2**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| (2) Řízené bezpečnostní služby, které spočívají v provádění činností souvisejících s řízením kybernetických bezpečnostních rizik zákazníků nebo v poskytování pomoci s těmito činnostmi, mají stále větší význam při prevenci a zmírňování kybernetických bezpečnostních incidentů. Poskytovatelé těchto služeb jsou proto považováni za základní nebo důležité subjekty náležející k vysoce kritickému odvětví podle ***směrnice Evropského parlamentu a Rady*** (EU) 2022/***2555***[8] . Podle 86. bodu odůvodnění uvedené směrnice mají poskytovatelé řízených bezpečnostních služeb zvlášť důležitou úlohu v pomoci subjektům v jejich úsilí o předcházení incidentům, při jejich odhalování, reakci na ně nebo zotavení se z nich v oblastech jako reakce na incidenty, penetrační testování, bezpečnostní audity a konzultační činnost. Poskytovatelé řízených bezpečnostních služeb se však také sami stávají terčem kybernetických útoků a představují zvláštní riziko vzhledem k úzkému začlenění do činností svých zákazníků. Základní a důležité subjekty ve smyslu směrnice (EU) 2022/2555 by proto měly při výběru poskytovatele řízených bezpečnostních služeb postupovat s větší péčí. | (2) Řízené bezpečnostní služby, které ***poskytují poskytovatelé řízených bezpečnostních služeb podle čl. 6 bodu 40 směrnice Evropského parlamentu a Rady (EU) 2022/2555. Tyto služby*** spočívají v provádění činností souvisejících s řízením kybernetických bezpečnostních rizik zákazníků nebo v poskytování pomoci s těmito činnostmi, mají stále větší význam při prevenci a zmírňování kybernetických bezpečnostních incidentů. Poskytovatelé těchto ***řízených bezpečnostních*** služeb jsou proto považováni za základní nebo důležité subjekty náležející k vysoce kritickému odvětví podle ***bodu 10 přílohy I směrnice*** (EU) 2022/***2555***. Podle 86. bodu odůvodnění uvedené směrnice mají poskytovatelé řízených bezpečnostních služeb zvlášť důležitou úlohu v pomoci subjektům v jejich úsilí o předcházení incidentům, při jejich odhalování, reakci na ně nebo zotavení se z nich v oblastech jako reakce na incidenty, penetrační testování, bezpečnostní audity a konzultační činnost. Poskytovatelé řízených bezpečnostních služeb se však také sami stávají terčem kybernetických útoků a představují zvláštní riziko vzhledem k úzkému začlenění do činností svých zákazníků. Základní a důležité subjekty ve smyslu směrnice (EU) 2022/2555 by proto měly při výběru poskytovatele řízených bezpečnostních služeb postupovat s větší péčí. |
| [8] 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 | [8] 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).

směrnice (EU) 2016/1148 (směrnice NIS 2) (Úř. věst. L 333, 27.12.2022, s. 80).

Or. en

**Pozměňovací návrh 18**
**Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

**Návrh nařízení**
**Bod odůvodnění 2**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| (2) Řízené bezpečnostní služby, které spočívají v provádění činností souvisejících s řízením kybernetických bezpečnostních rizik zákazníků nebo v poskytování pomoci s těmito činnostmi, mají stále větší význam při prevenci a zmírňování kybernetických bezpečnostních incidentů. Poskytovatelé těchto služeb jsou proto považováni za základní nebo důležité subjekty náležející k vysoce kritickému odvětví podle směrnice Evropského parlamentu a Rady (EU) 2022/2555[8] . Podle 86. bodu odůvodnění uvedené směrnice mají poskytovatelé řízených bezpečnostních služeb zvlášť důležitou úlohu v pomoci subjektům v jejich úsilí o předcházení incidentům, při jejich odhalování, reakci na ně nebo zotavení se z nich v oblastech jako reakce na incidenty, penetrační testování, bezpečnostní audity a konzultační činnost. Poskytovatelé řízených bezpečnostních služeb se však také sami stávají terčem kybernetických útoků a představují zvláštní riziko vzhledem k úzkému začlenění do činností svých zákazníků. Základní a důležité subjekty ve smyslu směrnice (EU) 2022/2555 by proto měly při výběru poskytovatele řízených bezpečnostních služeb postupovat s větší péčí. | (2) Řízené bezpečnostní služby, které spočívají v provádění činností souvisejících s řízením kybernetických bezpečnostních rizik zákazníků nebo v poskytování pomoci s těmito činnostmi, ***včetně předcházení incidentům, jejich odhalování, reakce na ně nebo obnova po nich,*** mají stále větší význam při prevenci a zmírňování kybernetických bezpečnostních incidentů. Poskytovatelé těchto služeb jsou proto považováni za základní nebo důležité subjekty náležející k vysoce kritickému odvětví podle směrnice Evropského parlamentu a Rady (EU) 2022/2555[8] . Podle 86. bodu odůvodnění uvedené směrnice mají poskytovatelé řízených bezpečnostních služeb zvlášť důležitou úlohu v pomoci subjektům v jejich úsilí o předcházení incidentům, při jejich odhalování, reakci na ně nebo zotavení se z nich v oblastech jako reakce na incidenty, penetrační testování, bezpečnostní audity a konzultační činnost. Poskytovatelé řízených bezpečnostních služeb se však také sami stávají terčem kybernetických útoků a představují zvláštní riziko vzhledem k úzkému začlenění do činností svých zákazníků. Základní a důležité subjekty ve smyslu směrnice (EU) 2022/2555 by proto měly při výběru poskytovatele řízených bezpečnostních služeb postupovat s větší péčí. |

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

[8] 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 19**
**Evžen Tošenovský**

**Návrh nařízení**
**Bod odůvodnění 3**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| (3) Poskytovatelé řízených bezpečnostních služeb rovněž hrají důležitou úlohu v rezervě EU pro kybernetickou bezpečnost, jejíž postupné vytváření je podpořeno nařízením (EU) .../… [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]. Rezerva EU pro kybernetickou bezpečnost se použije na podporu reakce a okamžitých opatření obnovy v případě významných a rozsáhlých kybernetických bezpečnostních incidentů. Nařízení (EU).../... [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] stanoví postup výběru poskytovatelů tvořících rezervu EU pro kybernetickou bezpečnost, který by měl mimo jiné přihlížet k tomu, zda dotčený poskytovatel získal evropskou nebo vnitrostátní certifikaci kybernetické bezpečnosti. ***Příslušné služby poskytované „důvěryhodnými poskytovateli“ podle*** | (3) Poskytovatelé řízených bezpečnostních služeb rovněž hrají důležitou úlohu v rezervě EU pro kybernetickou bezpečnost, jejíž postupné vytváření je podpořeno nařízením (EU) .../… [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]. Rezerva EU pro kybernetickou bezpečnost se použije na podporu reakce a okamžitých opatření obnovy v případě významných a rozsáhlých kybernetických bezpečnostních incidentů. Nařízení (EU).../... [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] stanoví postup výběru poskytovatelů ***řízených bezpečnostních služeb*** tvořících rezervu EU pro kybernetickou bezpečnost, který by měl mimo jiné přihlížet k tomu, zda dotčený poskytovatel získal evropskou nebo vnitrostátní certifikaci kybernetické bezpečnosti. ***Kromě toho, jakmile bude*** |

| | |
|---|---|
| ***nařízení (EU).../... [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] odpovídají „řízeným bezpečnostním službám“ v souladu s tímto nařízením***. | ***zaveden evropský systém certifikace kybernetické bezpečnosti pro řízené bezpečnostní služby, který by rovněž nahradil všechny příslušné vnitrostátní systémy certifikace kybernetické bezpečnosti, měla by se*** pro ***začlenění důvěryhodných poskytovatelů řízených bezpečnostních služeb do rezervy EU pro kybernetickou bezpečnost vyžadovat povinná certifikace podle tohoto systému certifikace***. |

Or. en

**Pozměňovací návrh 20**
**Johan Nissinen**

**Návrh nařízení**
**Bod odůvodnění 4**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| (4) Certifikace řízených bezpečnostních služeb je důležitá nejen pro proces výběru rezervy EU pro kybernetickou bezpečnost, ale je také zásadním ukazatelem kvality pro soukromé a veřejné subjekty, které mají v úmyslu tyto služby nakupovat. S ohledem na kritičnost řízených bezpečnostních služeb a citlivost údajů, které zpracovávají, by certifikace mohla potenciálním zákazníkům poskytnout důležitá vodítka a záruky ohledně důvěryhodnosti těchto služeb. Evropské systémy certifikace řízených bezpečnostních služeb pomáhají zabránit roztříštění jednotného trhu. Cílem tohoto nařízení je proto zlepšit fungování vnitřního trhu. | (4) Certifikace řízených bezpečnostních služeb je důležitá nejen pro proces výběru rezervy EU pro kybernetickou bezpečnost, ale je také zásadním ukazatelem kvality pro soukromé a veřejné subjekty, které mají v úmyslu tyto služby nakupovat. S ohledem na kritičnost řízených bezpečnostních služeb a citlivost údajů, které zpracovávají, by certifikace mohla potenciálním zákazníkům poskytnout důležitá vodítka a záruky ohledně důvěryhodnosti těchto služeb. Evropské systémy certifikace řízených bezpečnostních služeb pomáhají zabránit roztříštění jednotného trhu. Cílem tohoto nařízení je proto zlepšit fungování vnitřního trhu. ***Tyto četné účely nařízení by zároveň měly nalézt rovnováhu s možnou regulační zátěží a náklady spojenými s certifikací, neboť splnění požadavků na certifikaci bude vyžadovat dodatečné náklady a administrativní úsilí, což by mohlo představovat problém pro menší poskytovatele.*** |

Or. en

**Pozměňovací návrh 21**
**Ville Niinistö**
za skupinu Verts/ALE

**Návrh nařízení**
**Bod odůvodnění 4 a (nový)**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| | ***(4a) Vzhledem k tomu, že trh a vzdělávací systémy nabízejí různé vzdělávací zdroje i formální odbornou přípravu, je třeba zdůraznit, že znalosti jsou získávány také neformálně a dovednosti lze prokázat diplomy a certifikací, nikoli však výlučně. Zejména v rychle se vyvíjejícím prostředí hrozeb by členské státy a příjemci řízených bezpečnostních služeb měli zohlednit vysoce kvalifikované výzkumné pracovníky v oblasti zranitelnosti. Kromě toho by subjekty a fyzické osoby, které provádějí výzkum týkající se zranitelných míst, mohly v některých členských státech být vystaveny trestní a občanskoprávní odpovědnosti, proto jsou členské státy vybízeny, aby vydaly pokyny pro výzkum bezpečnosti informací, a výjimky z občanskoprávní odpovědnosti za tuto činnost.*** |

Or. en

*Odůvodnění*

*Schopnosti pracovníků v oblasti bezpečnosti se částečně liší v důsledku různých nestandardizovaných profesních drah, přístupu k formálnímu vzdělávání a ke zdrojům, které mají být certifikovány. Proto musíme podporovat zaměstnávání kvalifikovaných osob a zajistit rámec přívětivý pro činnosti, které vedou ke zlepšení kybernetické bezpečnosti.*

**Pozměňovací návrh 22**
**Josianne Cutajar**

**Návrh nařízení**
**Bod odůvodnění 4 a (nový)**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| | ***(4a) Systém certifikace Unie pro řízené bezpečnostní služby by měl zajistit dostupnost zabezpečených a vysoce kvalitních služeb, které zaručují bezpečnou digitální transformaci a přispívají k dosažení cílů stanovených v politickém programu Cesta k digitální dekádě[8a], zejména pokud jde o cíl, aby 75 % společností v EU začalo používat cloud/UI/data velkého objemu, aby více než 90 % malých a středních podniků dosáhlo alespoň základní úrovně digitální intenzity a aby klíčové veřejné služby byly nabízeny on-line.*** |
| | ***[8a] Rozhodnutí Evropského parlamentu a Rady (EU) 2022/2481 ze dne 14. prosince 2022, kterým se zavádí politický program Digitální dekáda 2030*** |

Or. en

**Pozměňovací návrh 23**
**Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

**Návrh nařízení**
**Bod odůvodnění 4 a (nový)**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| | ***(4a) Evropské systémy certifikace pro řízené bezpečnostní služby by měly usnadnit využívání těchto služeb, zejména menším subjektům, včetně místních a regionálních orgánů nebo malých a středních podniků, které často nemají finanční a lidské kapacity k tomu, aby tyto služby provozovaly samy, ale jsou zranitelné vůči kybernetickým útokům s potenciálně významnými důsledky.*** |

Or. en

**Pozměňovací návrh 24**
**Josianne Cutajar**

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

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| (5) Kromě zavádění produktů, služeb nebo procesů IKT poskytují řízené bezpečnostní služby často další prvky služeb, které se opírají o kompetence, odborné znalosti a zkušenosti jejich zaměstnanců. Velmi vysoká úroveň těchto kompetencí, odborných znalostí a zkušeností, jakož i vhodné vnitřní postupy by měly být součástí bezpečnostních cílů, aby byla zajištěna velmi vysoká kvalita poskytovaných řízených bezpečnostních služeb. Aby se zajistilo, že se na všechny prvky řízených bezpečnostních služeb bude vztahovat systém certifikace, je proto nutné změnit nařízení (EU) 2019/881. V souladu s čl. 42 odst. 1 nařízení Evropského parlamentu a Rady (EU) 2018/1725 byl konzultován evropský inspektor ochrany údajů, který vydal stanovisko dne [DD/MM/RRRR]**,** | (5) Kromě zavádění produktů, služeb nebo procesů IKT poskytují řízené bezpečnostní služby často další prvky služeb, které se opírají o kompetence, odborné znalosti a zkušenosti jejich zaměstnanců. Velmi vysoká úroveň těchto kompetencí, odborných znalostí a zkušeností, jakož i vhodné vnitřní postupy by měly být součástí bezpečnostních cílů, aby byla zajištěna velmi vysoká kvalita poskytovaných řízených bezpečnostních služeb. Aby se zajistilo, že se na všechny prvky řízených bezpečnostních služeb bude vztahovat systém certifikace, je proto nutné změnit nařízení (EU) 2019/881. ***Systém certifikace zřízený podle tohoto nařízení by měl rovněž zohlednit výsledky a doporučení hodnocení a přezkumu podle článku 67 uvedeného v tomto nařízení.*** V souladu s čl. 42 odst. 1 nařízení Evropského parlamentu a Rady (EU) 2018/1725 byl konzultován evropský inspektor ochrany údajů, který vydal stanovisko dne [DD/MM/RRRR] |

Or. en

**Pozměňovací návrh 25**
**Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

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

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| (5) Kromě zavádění produktů, služeb nebo procesů IKT poskytují řízené bezpečnostní služby často další prvky služeb, které se opírají o kompetence, odborné znalosti a zkušenosti jejich zaměstnanců. Velmi vysoká úroveň těchto kompetencí, odborných znalostí a zkušeností, jakož i vhodné vnitřní postupy by měly být součástí bezpečnostních cílů, aby byla zajištěna velmi vysoká kvalita poskytovaných řízených bezpečnostních služeb. Aby se zajistilo, že se na všechny prvky řízených bezpečnostních služeb bude vztahovat systém certifikace, je proto nutné změnit nařízení (EU) 2019/881. V souladu s čl. 42 odst. 1 nařízení Evropského parlamentu a Rady (EU) 2018/1725 byl konzultován evropský inspektor ochrany údajů, který vydal stanovisko dne [DD/MM/RRRR], | (5) Kromě zavádění produktů, služeb nebo procesů IKT poskytují řízené bezpečnostní služby často další prvky služeb, které se opírají o kompetence, odborné znalosti a zkušenosti jejich zaměstnanců. Velmi vysoká úroveň těchto kompetencí, odborných znalostí a zkušeností, jakož i vhodné vnitřní postupy by měly být součástí bezpečnostních cílů, aby byla zajištěna velmi vysoká kvalita ***a spolehlivost*** poskytovaných řízených bezpečnostních služeb. Aby se zajistilo, že se na všechny prvky řízených bezpečnostních služeb bude vztahovat systém certifikace, je proto nutné změnit nařízení (EU) 2019/881. V souladu s čl. 42 odst. 1 nařízení Evropského parlamentu a Rady (EU) 2018/1725 byl konzultován evropský inspektor ochrany údajů, který vydal stanovisko dne [DD/MM/RRRR], |

Or. en

**Pozměňovací návrh 26**
**Evžen Tošenovský**

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

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| (5) Kromě zavádění produktů, služeb nebo procesů IKT poskytují řízené bezpečnostní služby často další prvky služeb, které se opírají o kompetence, odborné znalosti a zkušenosti jejich zaměstnanců. Velmi vysoká úroveň těchto kompetencí, odborných znalostí a zkušeností, jakož i vhodné vnitřní postupy by měly být součástí bezpečnostních cílů, aby byla zajištěna velmi vysoká kvalita poskytovaných řízených bezpečnostních služeb. Aby se zajistilo, že se na všechny prvky řízených bezpečnostních služeb bude | (5) Kromě zavádění produktů, služeb nebo procesů IKT poskytují řízené bezpečnostní služby často další prvky služeb, které se opírají o kompetence, odborné znalosti a zkušenosti jejich zaměstnanců. Velmi vysoká úroveň těchto kompetencí, odborných znalostí a zkušeností, jakož i vhodné vnitřní postupy by měly být součástí bezpečnostních cílů, aby byla zajištěna velmi vysoká kvalita poskytovaných řízených bezpečnostních služeb. Aby se zajistilo, že se na všechny prvky řízených bezpečnostních služeb bude |

| | |
|---|---|
| vztahovat systém certifikace, je proto nutné změnit nařízení (EU) 2019/881. V souladu s čl. 42 odst. 1 nařízení Evropského parlamentu a Rady (EU) 2018/1725 byl konzultován evropský inspektor ochrany údajů, který vydal stanovisko dne [DD/MM/RRRR], | vztahovat ***specializovaný*** systém certifikace, je proto nutné změnit nařízení (EU) 2019/881. V souladu s čl. 42 odst. 1 nařízení Evropského parlamentu a Rady (EU) 2018/1725 byl konzultován evropský inspektor ochrany údajů, který vydal stanovisko dne [DD/MM/RRRR], |

Or. en

**Pozměňovací návrh 27**
**Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

**Návrh nařízení**
**Bod odůvodnění 5 a (nový)**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| | ***(5a) Vzhledem k tomu, že evropské systémy kybernetické bezpečnosti by měly osvědčovat, že řízené bezpečnostní služby jsou poskytovány vysoce kvalifikovanými pracovníky, kteří jsou schopni tyto služby poskytovat spolehlivě a zajišťovat nejvyšší standardy kybernetické bezpečnosti, je nezbytné, aby těchto vysoce kvalifikovaných pracovníků byl v Unii dostatečný počet. Unie se však potýká s nedostatkem talentů v podobě nedostatku kvalifikovaných odborníků, a 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.***

Or. en

**Pozměňovací návrh 28**
**Johan Nissinen**

**Návrh nařízení**
**Bod odůvodnění 5 a (nový)**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| | ***(5a) Vzhledem k tomu, že systémy certifikace přidají již tak komplexnímu regulačnímu prostředí na složitosti, zabránit možnému překrývání nebo rozporům se stávajícími předpisy a normami v oblasti kybernetické bezpečnosti má zásadní význam. Dále zdůrazňuje nutnost při provádění nařízení pečlivě zvažovat a dbát na proporcionalitu, aby se omezily negativní dopady na svobodu trhu a inovace.*** |

Or. en

**Pozměňovací návrh 29**
**Josianne Cutajar**

**Návrh nařízení**
**Bod odůvodnění 5 a (nový)**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| | ***(5a) Měly by být zváženy odpovídající finanční prostředky a zdroje, které by doprovázely další úkoly, které se agentuře ENISA tímto aktem svěřují.*** |

Or. en

**Pozměňovací návrh 30**
**Evžen Tošenovský**

**Návrh nařízení**
**Čl. 1 – odst. 1 – bod 2 – písm. a – návětí**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| a) body 9, 10 a 11 se nahrazují tímto: | a) body ***7,*** 9, 10 a 11 se nahrazují tímto: |

Or. en

**Pozměňovací návrh 31**
**Evžen Tošenovský**

**Návrh nařízení**
**Čl. 1 – odst. 1 – bod 2 – písm. a**
Nařízení (EU) 2019/881
Čl. 2 – bod 7

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| | ***7) „řešením incidentu“ řešení incidentu ve smyslu čl. 6 bodu 8 směrnice (EU) 2022/2555;*** |

Or. en

**Pozměňovací návrh 32**
**Evžen Tošenovský**

**Návrh nařízení**
**Čl. 1 – odst. 1 – bod 2 – písm. b – návětí**

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| b) ***vkládá*** se ***nový bod***, ***který zní***: | b) ***doplňují*** se ***nové body***, ***které znějí***: |

Or. en

**Pozměňovací návrh 33**
**Evžen Tošenovský**

**Návrh nařízení**
**Čl. 1 – odst. 1 – bod 2 – písm. b**
Nařízení (EU) 2019/881
Čl. 2 – bod 7a

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| | ***7a) „rizikem“ riziko ve smyslu čl. 6 bodu 9 směrnice (EU) 2022/2555.*** |

Or. en

**Pozměňovací návrh 34**
**Evžen Tošenovský**

**Návrh nařízení**
**Čl. 1 – odst. 1 – bod 2 – písm. b**
Nařízení (EU) 2019/881
Čl. 2 – bod 14a

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| 14a) „řízenou bezpečnostní službou“ ***služba spočívající v provádění činností souvisejících s řízením kybernetických bezpečnostních rizik nebo v poskytování pomoci při takových činnostech, včetně reakce na incidenty, penetračního testování, bezpečnostních auditů a konzultační činnosti***; | 14a) „řízenou bezpečnostní službou“ ***řízená bezpečnostní služba ve smyslu čl. 6 bodu 40 směrnice (EU) 2022/2555***; |

Or. en

**Pozměňovací návrh 35**
**Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

**Návrh nařízení**
**Čl. 1 – odst. 1 – bod 2 – písm. b**
Nařízení (EU) 2019/881
Čl. 2 – bod 14a

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| 14a) „řízenou bezpečnostní službou“ služba spočívající v provádění činností souvisejících s řízením kybernetických bezpečnostních rizik nebo v poskytování pomoci při takových činnostech, včetně ***reakce na incidenty***, ***penetračního testování***, ***bezpečnostních auditů a konzultační činnosti***; | 14a) „řízenou bezpečnostní službou“ ***řízená*** služba spočívající v provádění činností souvisejících s řízením kybernetických bezpečnostních rizik nebo v poskytování pomoci při takových činnostech, včetně ***prevence incidentů***, ***jejich odhalování***, ***reakce na incidenty nebo obnovy po nich***; |

Or. en

**Pozměňovací návrh 36**
**Evžen Tošenovský**

**Návrh nařízení**
**Čl. 1 – odst. 1 – bod 2 – písm. b**
Nařízení (EU) 2019/881
Čl. 2 – bod 14aa

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| | ***14aa) „poskytovatelem řízených bezpečnostních služeb“ poskytovatel řízených bezpečnostních služeb ve smyslu čl. 6 bodu 40 směrnice (EU) 2022/2555;*** |

Or. en

**Pozměňovací návrh 37**
**Ville Niinistö**
za skupinu Verts/ALE

**Návrh nařízení**
**Čl. 1 – odst. 1 – bod 6**
Nařízení (EU) 2019/881
Čl. 47 – odst. 2

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| 2. Průběžný pracovní program Unie obsahuje zejména seznam produktů, služeb a procesů IKT či jejich kategorií a řízených | 2. Průběžný pracovní program Unie obsahuje zejména seznam produktů, služeb a procesů IKT či jejich kategorií a řízených |

| | |
|---|---|
| bezpečnostních služeb, pro něž by mohlo být prospěšné zahrnutí do oblasti působnosti některého z evropských systémů kybernetické bezpečnosti. | bezpečnostních služeb, pro něž by mohlo být prospěšné zahrnutí do oblasti působnosti některého z evropských systémů kybernetické bezpečnosti. ***Musí být zahrnuta podpůrná opatření k posouzení potřeb kvalifikovaných zaměstnanců, typů dovedností a stávajících způsobů odborné přípravy spolu s opatřeními k překlenutí veškerých zjištěných nedostatků.*** |

Or. en

*Odůvodnění*

*Zavádění produktů, služeb a procesů IKT nebo jejich kategorií a řízených bezpečnostních služeb musí být doprovázeno posouzením dovedností a opatřeními k překlenutí nedostatků.*

**Pozměňovací návrh 38**
**Bart Groothuis, Alin Mituța, Ivars Ijabs, Andrus Ansip, Morten Løkkegaard**

**Návrh nařízení**
**Čl. 1 – odst. 1 – bod 6**
Nařízení (EU) 2019/881
Čl. 47 – odst. 3 – písm. a

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| a) dostupnost a rozvoj vnitrostátních systémů certifikace kybernetické bezpečnosti vztahujících se na konkrétní kategorii produktů, služeb nebo procesů IKT nebo řízených bezpečnostních služeb, zejména pokud jde o riziko roztříštěnosti; | a) dostupnost a rozvoj vnitrostátních systémů certifikace kybernetické bezpečnosti ***a mezinárodních a průmyslových norem*** vztahujících se na konkrétní kategorii produktů, služeb nebo procesů IKT nebo řízených bezpečnostních služeb, zejména pokud jde o riziko roztříštěnosti; |

Or. en

*Odůvodnění*

*Průběžný pracovní program Unie by měl posuzovat nejen vývoj vnitrostátních systémů, ale také průmyslové a mezinárodní normy.*

**Pozměňovací návrh 39**
**Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

**Návrh nařízení**
**Čl. 1 – odst. 1 – bod 7**
Nařízení (EU) 2019/881
Čl. 49 – odst. 7

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| ***7) v článku 49 se odstavec 7 nahrazuje tímto:*** | ***vypouští se*** |
| ***7. Na základě návrhu systému vypracovaného agenturou ENISA může Komise přijmout prováděcí akty, kterými stanoví evropský systém certifikace kybernetické bezpečnosti pro produkty, služby a procesy IKT a řízené bezpečnostní služby, který splňuje požadavky stanovené v článcích 51, 52 a 54. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 66 odst. 2.;*** | |

Or. en

**Pozměňovací návrh 40**
**Bart Groothuis, Alin Mituța, Ivars Ijabs, Andrus Ansip, Morten Løkkegaard, Nicola Danti**

**Návrh nařízení**
**Čl. 1 – odst. 1 – bod 7**
Nařízení (EU) 2019/881
Čl. 49 – odst. 7

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| 7. Na základě návrhu systému vypracovaného agenturou ENISA může Komise přijmout prováděcí akty, kterými stanoví evropský systém certifikace kybernetické bezpečnosti pro produkty, služby a procesy IKT a řízené bezpečnostní služby, který splňuje požadavky stanovené v článcích 51, 52 a 54. ***Tyto prováděcí akty*** | 7. Na základě návrhu systému vypracovaného agenturou ENISA může Komise přijmout ***specializované*** prováděcí akty, kterými stanoví evropský systém certifikace kybernetické bezpečnosti pro produkty, služby a procesy IKT a řízené bezpečnostní služby, který splňuje požadavky stanovené v článcích 51, 52 a |

| | |
|---|---|
| ***se přijímají přezkumným postupem podle čl. 66 odst. 2.;*** | 54. |
| | ***(Tento pozměňovací návrh se vztahuje na celý text.*** *Jeho přijetí si vyžádá odpovídající změny v celém textu.)* |

Or. en

*Odůvodnění*

*Since the adoption of the Cyber Security Act, no certification schemes have been adopted, nor has the Union Rolling Work Programme (URWP), which reflects wider stakeholder involvement, been formalized. Instead, some proposals, such as the EUCS, have introduced wide-ranging requirements that are not risk-based, hinder innovation and competitiveness, are highly political and therefore outside of ENISA's mandate in the CSA, and have not been properly consulted with relevant stakeholders or tested through impact assessments. It is therefore suggested that the adoption of a scheme is done through delegated act, and preceded by a impact assessment involving SCCG and ECCG consultations to improve the transparency of schemes and the effectiveness of the certification framework in general.*

**Pozměňovací návrh 41**
**Bart Groothuis, Alin Mituța, Ivars Ijabs, Andrus Ansip, Morten Løkkegaard, Nicola Danti**

**Návrh nařízení**
**Čl. 1 – odst. 1 – bod 7**
Nařízení (EU) 2019/881
Čl. 49 – odst. 7a (nový)

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| | ***7a. Před přijetím těchto aktů v přenesené pravomoci Komise ve spolupráci s agenturou ENISA provede a zveřejní posouzení dopadů navrhovaného evropského systému certifikace kybernetické bezpečnosti. Při přípravě posouzení dopadů bude Komise vést veřejné konzultace a konzultace s Evropskou skupinou pro certifikaci kybernetické bezpečnosti (ECCG) a Skupinou zúčastněných stran pro certifikaci kybernetické bezpečnosti (SCCG).*** |

Or. en

*Odůvodnění*

*Since the adoption of the Cyber Security Act, no certification schemes have been adopted, nor has the Union Rolling Work Programme (URWP), which reflects wider stakeholder involvement, been formalized. Instead, some proposals, such as the EUCS, have introduced wide-ranging requirements that are not risk-based, hinder innovation and competitiveness, are highly political and therefore outside of ENISA's mandate in the CSA, and have not been properly consulted with relevant stakeholders or tested through impact assessments. It is therefore suggested that the adoption of a scheme is done through delegated act, and preceded by a impact assessment involving SCCG and ECCG consultations to improve the transparency of schemes and the effectiveness of the certification framework in general.*

**Pozměňovací návrh 42**
**Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

**Návrh nařízení**
**Čl. 1 – odst. 1 – bod 7 a (nový)**
Nařízení (EU) 2019/881
Čl. 49 – odst. 7a (nový)

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| | ***7a) vkládá se nový odstavec, který zní:*** |
| | ***„7a. Na základě návrhu systému vypracovaného agenturou ENISA může Komise přijmout akty v přenesené pravomoci, kterými stanoví evropský systém certifikace kybernetické bezpečnosti pro řízené bezpečnostní služby, splňující požadavky stanovené v článcích 51, 52 a 54. Tyto akty v přenesené pravomoci se přijímají postupem podle čl. 66a.“*** |

Or. en

**Pozměňovací návrh 43**
**Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

**Návrh nařízení**
**Čl. 1 – odst. 1 – bod 9**
Nařízení (EU) 2019/881
Čl. 51a – odst. 1 – písm. b

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| b) zajistit, aby měl poskytovatel zavedeny vhodné vnitřní postupy k zajištění toho, aby řízené bezpečnostní služby byly vždy poskytovány na velmi vysoké úrovni kvality; | b) zajistit, aby měl poskytovatel zavedeny vhodné vnitřní postupy k zajištění toho, aby řízené bezpečnostní služby byly vždy poskytovány na velmi vysoké úrovni kvality ***a spolehlivosti***; |

Or. en

**Pozměňovací návrh 44**
**Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

**Návrh nařízení**
**Čl. 1 – odst. 1 – bod 9**
Nařízení (EU) 2019/881
Čl. 51a – odst. 1 – písm. g

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| g) zajistit, aby produkty, služby a procesy IKT [a hardware] zaváděné v rámci poskytování řízených bezpečnostních služeb byly bezpečné na úrovni standardního nastavení a výchozího návrhu, aby neobsahovaly žádné známé zranitelnosti a aby zahrnovaly nejnovější bezpečnostní aktualizace;; | g) zajistit, aby produkty, služby a procesy IKT [a hardware] zaváděné v rámci poskytování řízených bezpečnostních služeb byly bezpečné na úrovni standardního nastavení a výchozího návrhu, ***byly vybaveny aktualizovaným softwarem a hardwarem,*** aby neobsahovaly žádné známé zranitelnosti a aby zahrnovaly nejnovější bezpečnostní aktualizace;; |

Or. en

**Pozměňovací návrh 45**
**Evžen Tošenovský**

**Návrh nařízení**
**Čl. 1 – odst. 1 – bod 9**
Nařízení (EU) 2019/881
Čl. 51a – odst. 1 – písm. g

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| g) zajistit, aby produkty, služby a procesy IKT ***[a hardware]*** zaváděné v rámci poskytování řízených bezpečnostních služeb byly bezpečné na úrovni standardního nastavení a výchozího návrhu, aby neobsahovaly žádné známé zranitelnosti a aby zahrnovaly nejnovější bezpečnostní aktualizace;; | g) zajistit, aby produkty, služby a procesy IKT zaváděné v rámci poskytování řízených bezpečnostních služeb byly bezpečné na úrovni standardního nastavení a výchozího návrhu, aby neobsahovaly žádné známé zranitelnosti a aby zahrnovaly nejnovější bezpečnostní aktualizace;; |

Or. en

**Pozměňovací návrh 46**
**Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

**Návrh nařízení**
**Čl. 1 – odst. 1 – bod 13 – písm. b – písm. ii – písm. aa**
Nařízení (EU) 2019/881
Čl. 56 – odst. 3 – třetí pododstavec – písm. a

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| a) zohlední dopad opatření na výrobce nebo poskytovatele daných produktů, služeb či procesů IKT nebo řízených bezpečnostních služeb a na uživatele z hlediska nákladů na tato opatření a společenských nebo hospodářských přínosů plynoucích z očekávaného zvýšení úrovně bezpečnosti pro dotyčné produkty, služby a procesy IKT nebo řízené bezpečnostní služby;; | a) zohlední dopad opatření na výrobce nebo poskytovatele daných produktů, služeb či procesů IKT nebo řízených bezpečnostních služeb***, včetně malých a středních podniků,*** a na uživatele z hlediska nákladů na tato opatření a společenských nebo hospodářských přínosů plynoucích z očekávaného zvýšení úrovně bezpečnosti pro dotyčné produkty, služby a procesy IKT nebo řízené bezpečnostní služby;; ***Komise by měla zajistit, aby malé a střední podniky měly při provádění opatření přístup k odpovídající finanční podpoře z již existujících programů Unie***; |

Or. en

**Pozměňovací návrh 47**
**Bart Groothuis, Alin Mituța, Ivars Ijabs, Andrus Ansip, Morten Løkkegaard, Nicola**

**Danti**

**Návrh nařízení**
**Čl. 1 – odst. 1 – bod 14**
Nařízení (EU) 2019/881
Čl. 57 – odst. 1

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| 1. Aniž je dotčen odstavec 3 tohoto článku, vnitrostátní systémy certifikace kybernetické bezpečnosti a související postupy pro produkty, služby a procesy IKT a řízené bezpečnostní služby zahrnuté do evropského systému certifikace kybernetické bezpečnosti pozbývají účinnosti ode dne stanoveného v ***prováděcím*** aktu ***přijatém podle čl. 49 odst. 7***. Vnitrostátní systémy certifikace kybernetické bezpečnosti a související postupy pro produkty, služby a procesy IKT a řízené bezpečnostní služby, na něž se evropský systém certifikace kybernetické bezpečnosti nevztahuje, zůstávají v platnosti. | 1. Aniž je dotčen odstavec 3 tohoto článku, vnitrostátní systémy certifikace kybernetické bezpečnosti a související postupy pro produkty, služby a procesy IKT a řízené bezpečnostní služby zahrnuté do evropského systému certifikace kybernetické bezpečnosti pozbývají účinnosti ode dne stanoveného v aktu ***v přenesené pravomoci***. Vnitrostátní systémy certifikace kybernetické bezpečnosti a související postupy pro produkty, služby a procesy IKT a řízené bezpečnostní služby, na něž se evropský systém certifikace kybernetické bezpečnosti nevztahuje, zůstávají v platnosti.<br>*(Tento pozměňovací návrh se vztahuje na celý text. Jeho přijetí si vyžádá odpovídající změny v celém textu.)* |

Or. en

*Odůvodnění*

*Tento pozměňovací návrh odráží pozměňovací návrh k článku 49.*

**Pozměňovací návrh 48**
**Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan**

**Návrh nařízení**
**Čl. 1 – odst. 1 – bod 16 a (nový)**
Nařízení (EU) 2019/881
Článek 66a (nový)

| *Znění navržené Komisí* | *Pozměňovací návrh* |
| --- | --- |
| | ***16a) vkládá se nový článek, který zní:*** |
| | ***Článek 66a (nový)*** |
| | ***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. 49 odst. 7a je svěřena Komisi na dobu pěti let ode dne ... [datum vstupu v platnost základního právního aktu 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 článku 49 odst. 7a 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 článku 49 odst. 7a 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 49**
**Evžen Tošenovský**

**Návrh nařízení**
**Čl. 1 – odst. 1 – bod 17 – návětí**
Nařízení (EU)2019/881
Článek 67

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| 17) v článku 67 se odstavce 2 a 3 nahrazují tímto: | 17) v článku 67 se odstavce 1, 2, 3 a 4 nahrazují tímto: |

Or. en

**Pozměňovací návrh 50**
**Evžen Tošenovský**

**Návrh nařízení**
**Čl. 1 – odst. 1 – bod 17**
Nařízení (EU) 2019/881
Čl. 67 – odst. 1

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| | ***1. Do 28. června 2024 a poté každé čtyři roky Komise vyhodnotí dopad, efektivitu a účinnost agentury ENISA a jejích pracovních postupů, jakož i případnou potřebu změnit mandát agentury ENISA a finanční důsledky této změny. Hodnocení zohledňuje zpětnou*** |

***vazbu, kterou agentura ENISA v reakci na svou činnost zaznamenala. Pokud se Komise domnívá, že pokračující fungování agentury ENISA již není s ohledem na cíle, mandát a úkoly, které jí byly uděleny, odůvodněné, může navrhnout, aby byla ustanovení tohoto nařízení týkající se agentury ENISA změněna.***

Or. en

**Pozměňovací návrh 51**
**Evžen Tošenovský**

**Návrh nařízení**
**Čl. 1 – odst. 1 – bod 17**
Nařízení (EU) 2019/881
Čl. 67 – odst. 2

| *Znění navržené Komisí* | *Pozměňovací návrh* |
|---|---|
| 2. Hodnocení rovněž posoudí dopad, efektivnost a účinnost ustanovení hlavy III tohoto nařízení s ohledem na cíle zajištění odpovídající úrovně kybernetické bezpečnosti produktů, služeb a procesů IKT a řízených bezpečnostních služeb v Unii a zlepšení fungování vnitřního trhu. | 2. Hodnocení rovněž posoudí dopad, efektivnost a účinnost ustanovení hlavy III tohoto nařízení s ohledem na cíle zajištění odpovídající úrovně kybernetické bezpečnosti produktů, služeb a procesů IKT a řízených bezpečnostních služeb v Unii a zlepšení fungování vnitřního trhu***, včetně posouzení postupu a harmonogramů směřujících k přípravě a přijetí prvního evropského systému certifikace kybernetické bezpečnosti a také, jak může tento postup být vylepšen a urychlen pro následující systémy certifikace***. |

Or. en

**Pozměňovací návrh 52**
**Evžen Tošenovský**

**Návrh nařízení**
**Čl. 1 – odst. 1 – bod 17**

Nařízení (EU) 2019/881
Čl. 67 – odst. 4

| *Znění navržené Komisí* | *Pozměňovací návrh* |
| --- | --- |
| | ***4. Do 28. června 2024 a poté každé čtyři roky předá Komise zprávu o hodnocení společně se svými závěry Evropskému parlamentu, Radě a správní radě. Zjištění této zprávy se zveřejní. V případě potřeby se ke zprávě přiloží legislativní návrh.*** |

Or. en