POZMĚŇOVACÍ NÁVRHY 001-001
které předložil Výbor pro průmysl, výzkum a energetiku

Zpráva
Josianne Cutajar **A9-0307/2023**
Řízené bezpečnostní služby

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

Pozměňovací návrh 1

POZMĚŇOVACÍ NÁVRHY EVROPSKÉHO PARLAMENTU*

k návrhu Komise

2023/0108(COD)

Návrh

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY,

kterým se mění nařízení (EU) 2019/881, pokud jde o řízené bezpečnostní služby

(Text s významem pro EHP)

EVROPSKÝ PARLAMENT A RADA EVROPSKÉ UNIE,

s ohledem na Smlouvu o fungování Evropské unie, a zejména na článek 114 této smlouvy,

---

* Pozměňovací návrhy: nový text či text nahrazující původní znění je označen tučně a kurzivou, vypuštění textu je označeno symbolem ▌.

s ohledem na návrh Evropské komise,

po postoupení návrhu legislativního aktu vnitrostátním parlamentům,

s ohledem na stanovisko Evropského hospodářského a sociálního výboru[1],

s ohledem na stanovisko Výboru regionů,

v souladu s řádným legislativním postupem[2],

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

[2] ***Postoj Evropského parlamentu ze dne … (dosud nezveřejněný v Úředním věstníku) a rozhodnutí Rady ze dne ….***

vzhledem k těmto důvodům:

(1) Nařízení Evropského parlamentu a Rady (EU) 2019/881[1] stanoví rámec pro zavedení evropského systému certifikace kybernetické bezpečnosti, jehož účelem je zajistit odpovídající úroveň kybernetické bezpečnosti produktů ***informačních a komunikačních technologií (IKT)***, služeb a procesů IKT v Unii a zabránit roztříštění vnitřního trhu, pokud jde o systémy certifikace kybernetické bezpečnosti v Unii.

(1a) S cílem zajistit odolnost Unie vůči kybernetickým útokům a předcházet případným zranitelnostem na trhu Unie má toto nařízení doplnit horizontální regulační rámec, kterým se stanoví komplexní požadavky na kybernetickou bezpečnost pro všechny produkty s digitálními prvky v souladu s nařízením Evropského parlamentu a Rady (EU) …/…[2] (2022/0272(COD)), a to stanovením základních požadavků na řízené služby kybernetické bezpečnosti, jejich uplatňování a důvěryhodnost.

(2) Řízené bezpečnostní služby, které spočívají v provádění činností souvisejících s řízením kybernetických bezpečnostních rizik zákazníků***, včetně odhalování incidentů, reakce na ně nebo obnovy po incidentech,*** nebo v poskytování pomoci s těmito činnostmi, mají stále větší význam při prevenci a zmírňování kybernetických bezpečnostních incidentů. ***Činnosti poskytovatelů řízených bezpečnostních služeb zahrnují služby týkající se prevence, identifikace, ochrany, odhalování, analýzy, zamezení šíření, reakce a obnovy, mimo jiné poskytování zpravodajských informací o kybernetických hrozbách, monitorování hrozeb v reálném čase prostřednictvím proaktivních technik, včetně bezpečnosti již od fáze návrhu, posuzování rizik, rozšířeného odhalování, nápravy a reakce.*** Poskytovatelé těchto služeb jsou proto považováni za základní nebo důležité subjekty náležející k vysoce kritickému

---

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

2 Nařízení Evropského parlamentu a Rady (EU) …/… ze dne … (Úř. věst. L, …, ELI: …).

odvětví podle směrnice Evropského parlamentu a Rady (EU) 2022/2555[1]. 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.

(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 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.

(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

[1] 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).

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.

(4a) Evropské systémy certifikace řízených bezpečnostních služeb by měly vést k rozšíření těchto služeb a k posílení konkurence v této oblasti, přičemž by měly zohledňovat specifické potřeby poskytovatelů i příjemců. Tyto systémy by proto měly zajistit rovnováhu mezi svým cílem a potenciální regulační, správní a finanční zátěží, s níž by se poskytovatelé, zejména mikropodniky nebo malé a střední podniky, mohli setkat. Kromě toho by tyto systémy měly podporovat využívání certifikovaných řízených bezpečnostních služeb tím, že přispějí k jejich dostupnosti, zejména pro menší subjekty, jako jsou mikropodniky a malé a střední podniky, jakož i místní a regionální orgány, které mají omezené kapacity a zdroje, ale které jsou náchylnější k narušení kybernetické bezpečnosti, což má finanční, právní, reputační a provozní důsledky.

(4b) 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 Digitální dekáda, zejména pokud jde o cíl, aby 75 % podniků v Unii začalo používat cloud/UI/data velkého objemu, aby více než 90 % mikropodniků a malých a středních podniků dosáhlo alespoň základní úrovně digitální intenzity a aby klíčové veřejné služby byly nabízeny on-line.

(4c) V současném rychle se vyvíjejícím digitálním a technologickém prostředí se nabídka vzdělávacích zdrojů a formálních školení liší a znalosti lze získávat různými způsoby, a to jak formálními, například prostřednictvím univerzit nebo kurzů, tak neformálními, například prostřednictvím profesní přípravy na pracovišti nebo dlouhodobé pracovní praxe v příslušném oboru.

(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 ***specializovaný*** systém certifikace, je proto nutné změnit nařízení (EU) 2019/881***. Vývoj systémů certifikace zavedených podle tohoto nařízení by měl zohlednit výsledky a doporučení hodnocení a přezkumu podle tohoto nařízení***.

(5a) S cílem usnadnit růst spolehlivého trhu Unie a zároveň vytvořit partnerství s podobně smýšlejícími třetími zeměmi, a to i s ohledem na ustanovení nařízení Evropského parlamentu a Rady (EU) …/…[1] (2023/0109(COD)), pokud jde o přístup k rezervě EU pro kybernetickou bezpečnost, by měl být proces certifikace zavedený v rámci stanoveném tímto nařízením zefektivněn, aby se zajistilo mezinárodní uznávání a sladění s mezinárodními normami.

(5b) Poskytovatelé řízených bezpečnostních služeb a členské státy by měli spolupracovat a přispívat ke shromažďování údajů o situaci a vývoji na trhu práce v oblasti kybernetické bezpečnosti za účelem zajištění rozvoje důvěryhodného trhu Unie s těmito službami.

(5c) Celounijní koordinovaný přístup ke zvyšování odolnosti kritické infrastruktury je založen na budování kapacit členských států. 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. V zájmu usnadnění vzniku vysoce kvalitních a nezbytných řízených bezpečnostních služeb a získání lepšího přehledu o struktuře pracovníků Unie v oblasti kybernetické bezpečnosti by proto měla být posílena spolupráce mezi členskými státy, Komisí, agenturou ENISA a zúčastněnými stranami, včetně soukromého sektoru a akademické obce, a to prostřednictvím rozvoje partnerství veřejného a soukromého sektoru, podpory výzkumných a inovačních iniciativ, rozvoje a vzájemného uznávání společných norem a certifikace dovedností v oblasti kybernetické bezpečnosti, mimo jiné prostřednictvím evropského rámce dovedností v oblasti kybernetické bezpečnosti. To by mělo rovněž usnadňovat mobilitu odborníků na kybernetickou bezpečnost v

[1] Nařízení Evropského parlamentu a Rady (EU) …/… (Úř. věst. L, …, ELI: …).

rámci Unie a začlenění znalostí a odborné přípravy v oblasti kybernetické bezpečnosti do vzdělávacích programů a zároveň mladým lidem, včetně osob žijících ve znevýhodněných regionech, jako jsou ostrovy, řídce osídlené, venkovské a odlehlé oblasti, zajišťovat přístup k učňovské přípravě a stážím. Cílem těchto opatření by mělo rovněž být přilákat do této oblasti více žen a dívek a přispět k řešení nedostatku žen v přírodních vědách, technologiích, inženýrství a matematice. Soukromý sektor by se měl rovněž zaměřovat na poskytování profesní přípravy na pracovišti zaměřené na dovednosti, které jsou nejvíce žádané, se zapojením veřejné správy a začínajících podniků, jakož i mikropodniků a malých a středních podniků.

(5d) ***Pro účely plnění dalších úkolů svěřených agentuře ENISA, které vyplývají ze změn nařízení (EU) 2019/881 zavedených tímto nařízením, by mělo být zajištěno odpovídající financování a zdroje.***

(5e) ***Za účelem doplnění některých jiných než podstatných prvků tohoto nařízení by měla být na Komisi přenesena pravomoc přijímat akty v souladu s článkem 290 Smlouvy o fungování Evropské unie s cílem stanovit evropský systém certifikace kybernetické bezpečnosti pro produkty, služby a procesy IKT a řízené bezpečnostní služby. Je obzvláště důležité, aby Komise v rámci přípravné činnosti vedla odpovídající konzultace, a to i na odborné úrovni, a aby tyto konzultace probíhaly v souladu se zásadami stanovenými v interinstitucionální dohodě ze dne 13. dubna 2016 o zdokonalení tvorby právních předpisů[1]. Za účelem zajištění rovné účasti na přípravě aktů v přenesené pravomoci obdrží Evropský parlament a Rada veškeré dokumenty ve stejnou dobu jako odborníci členských států a jejich odborníci mají pravidelný přístup na zasedání odborných skupin Komise, které se zabývají přípravou aktů v přenesené pravomoci.***

(5e) ***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][2],***

PŘIJALY TOTO NAŘÍZENÍ:

---

1 Úř. věst. L 123, 12.5.2016, s. 1

2 ***Úř. věst. C …/…***

Článek 1

Změny nařízení (EU) 2019/881

Nařízení (EU) 2019/881 se mění takto:

(1) v čl. 1 odst. 1 prvním pododstavci se písmeno b) nahrazuje tímto:

„b) rámec pro zavedení evropských systémů certifikace kybernetické bezpečnosti s cílem zajistit odpovídající úroveň kybernetické bezpečnosti produktů, služeb a procesů IKT a řízených bezpečnostních služeb v Unii a zabránit roztříštění vnitřního trhu, pokud jde o systémy certifikace kybernetické bezpečnosti v Unii.“;

2) článek 2 se mění takto:

a) body 9***)***, 10***)*** a 11***)*** se nahrazují tímto:

„9) „evropským systémem certifikace kybernetické bezpečnosti“ komplexní soubor pravidel, technických požadavků, norem a postupů, které jsou stanoveny na úrovni Unie a vztahují se na certifikaci nebo posuzování shody určitých produktů, služeb a procesů IKT nebo řízených bezpečnostních služeb;

10) „vnitrostátním systémem certifikace kybernetické bezpečnosti“ komplexní soubor pravidel, technických požadavků, norem a postupů, které vyvinuly a přijaly vnitrostátní veřejné orgány a které se vztahují na certifikaci nebo na posuzování shody produktů, služeb a procesů IKT a řízených bezpečnostních služeb spadajících do oblasti působnosti příslušného systému;

11) „evropským certifikátem kybernetické bezpečnosti“ dokument vydaný příslušným orgánem osvědčující, že byl posouzen soulad daného produktu, služby nebo procesu IKT nebo řízené bezpečnostní služby se zvláštními bezpečnostními požadavky stanovenými v evropském systému certifikace kybernetické bezpečnosti;“;

b) vkládá se nový bod, který zní:

„14a) „řízenou bezpečnostní službou“ služba ***poskytovaná třetí straně***

spočívající v provádění činností souvisejících s řízením kybernetických bezpečnostních rizik nebo v poskytování pomoci ***či poradenství*** při takových činnostech, včetně ***řešení incidentů***, penetračního testování, bezpečnostních auditů a konzultační činnosti;“***;***

c) body 20***)***, 21***)*** a 22***)*** se nahrazují tímto:

„20) „technickými specifikacemi“ dokument, který stanoví technické požadavky, jež má produkt, služba nebo proces IKT nebo řízená bezpečnostní služba splňovat, nebo postup posuzování shody produktu, služby nebo procesu IKT nebo řízené bezpečnostní služby;

21) „úrovní záruky“ míra jistoty, že produkt, služba nebo proces IKT nebo řízená bezpečnostní služba splňuje bezpečnostní požadavky určitého evropského systému certifikace kybernetické bezpečnosti, přičemž tento údaj uvádí, na jakou úroveň byly produkt, služba nebo proces IKT nebo řízená bezpečnostní služba vyhodnoceny, avšak jako takový neměří bezpečnost dotyčného produktu, služby nebo procesu IKT nebo řízené bezpečnostní služby;

22) „vlastním posuzováním shody“ úkon prováděný výrobcem nebo poskytovatelem produktů, služeb nebo procesů IKT nebo řízených bezpečnostních služeb, jímž se vyhodnocuje, zda tyto produkty, služby nebo procesy IKT nebo řízené bezpečnostní služby splňují požadavky určitého evropského systému certifikace kybernetické bezpečnosti.“;

(3) v článku 4 se odstavec 6 nahrazuje tímto:

„6. Agentura ENISA prosazuje využívání evropské certifikace kybernetické bezpečnosti, aby se zabránilo roztříštění vnitřního trhu. S cílem zvýšit transparentnost kybernetické bezpečnosti produktů, služeb a procesů IKT a řízených bezpečnostních služeb, a posílit tak důvěru v digitální vnitřní trh a jeho konkurenceschopnost, přispívá agentura ENISA k zavedení a správě evropského rámce pro certifikaci kybernetické bezpečnosti v souladu s hlavou III tohoto nařízení.“;

(4) článek 8 se mění takto:

a) odstavec 1 se nahrazuje tímto:

„1. Agentura ENISA podporuje a prosazuje tvorbu a provádění politiky Unie v oblasti certifikace kybernetické bezpečnosti produktů, služeb a procesů IKT a řízených bezpečnostních služeb, jak je stanoveno v hlavě III tohoto nařízení, tím, že:

a) průběžně monitoruje vývoj v souvisejících oblastech normalizace a doporučuje vhodné technické specifikace k využití při tvorbě evropských systémů certifikace kybernetické bezpečnosti podle čl. 54 odst. 1 písm. c) v případech, kdy normy nejsou k dispozici;

b) připravuje návrhy evropských systémů certifikace kybernetické bezpečnosti (dále jen „návrhy systémů“) pro produkty, služby a procesy IKT a řízené bezpečnostní služby v souladu s článkem 49;

c) vyhodnocuje přijaté evropské systémy certifikace kybernetické bezpečnosti v souladu s čl. 49 odst. 8;

d) účastní se vzájemných hodnocení podle čl. 59 odst. 4;

e) je nápomocna Komisi při zajišťování služeb sekretariátu pro Evropskou skupinu pro certifikaci kybernetické bezpečnosti podle čl. 62 odst. 5.“;

b) odstavec 3 se nahrazuje tímto:

„3. Agentura ENISA ve spolupráci s vnitrostátními orgány certifikace kybernetické bezpečnosti a s odvětvovými subjekty oficiálním, strukturovaným a transparentním způsobem sestavuje a zveřejňuje pokyny a vypracovává osvědčené postupy týkající se požadavků na kybernetickou bezpečnost produktů, služeb a procesů IKT a řízených bezpečnostních služeb.“;

c) odstavec 5 se nahrazuje tímto:

„5. Agentura ENISA je nápomocna při tvorbě a zavádění evropských a mezinárodních norem pro řízení rizik a pro bezpečnost produktů, služeb a procesů IKT a řízených bezpečnostních služeb.“;

(5) v článku 46 se odstavce 1 a 2 nahrazují tímto:

„1. Za účelem vytvoření jednotného digitálního trhu s produkty, službami a

procesy IKT a řízenými bezpečnostními službami se zřizuje evropský rámec pro certifikaci kybernetické bezpečnosti s cílem zlepšit podmínky pro fungování vnitřního trhu tím, že se zvýší úroveň kybernetické bezpečnosti v Unii a umožní se harmonizovaný přístup k evropským systémům certifikace kybernetické bezpečnosti na úrovni Unie.

2. Evropský rámec pro certifikaci kybernetické bezpečnosti stanoví mechanismus pro vytváření evropských systémů certifikace kybernetické bezpečnosti. Ten doloží, že produkty, služby a procesy IKT hodnocené v souladu s takovými systémy splňují stanovené bezpečnostní požadavky, pokud jde o ochranu dostupnosti, pravosti, integrity nebo důvěrnosti uchovávaných, předávaných či zpracovávaných údajů nebo funkcí či služeb nabízených nebo přístupných prostřednictvím těchto produktů, služeb a procesů během celého jejich životního cyklu. Kromě toho doloží, že řízené bezpečnostní služby, které byly hodnoceny v souladu s těmito systémy, splňují stanovené bezpečnostní požadavky, pokud jde o ochranu dostupnosti, pravosti, integrity a důvěrnosti údajů, které jsou v souvislosti s poskytováním těchto služeb předmětem přístupu, zpracování, ukládání či předávání, a že tyto služby jsou trvale poskytovány s nezbytnými kompetencemi, odborností a zkušenostmi zaměstnanci s velmi vysokou úrovní příslušných technických znalostí a profesní bezúhonností.“;

6) v článku 47 se odstavce 2 a 3 nahrazují tímto:

„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. ***V této souvislosti může Komise zahrnout hloubkové posouzení stávajících způsobů odborné přípravy k překlenutí zjištěného nedostatku kvalifikovaných pracovníků a seznam návrhů na řešení potřeb kvalifikovaných pracovníků a jednotlivých druhů dovedností.***

3. Zařazení konkrétního produktu, služby či procesu IKT či jejich kategorií nebo řízených bezpečnostních služeb do průběžného pracovního programu Unie musí být podloženo jedním či více z následujících důvodů:

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;

b) příslušné právní předpisy či politika Unie nebo členského státu;

c) tržní poptávka;

ca) technologický vývoj a dostupnost a rozvoj mezinárodních systémů certifikace kybernetické bezpečnosti a mezinárodních a odvětvových norem.

d) vývoj v oblasti kybernetických hrozeb;

e) žádost o vypracování konkrétního návrhu systému ze strany Evropské skupiny pro certifikaci kybernetické bezpečnosti.“;

7) ***článek*** 49 se ***mění takto***:

a) odstavec 7 ***se*** nahrazuje tímto:

„*7.* ***Komise je*** na základě návrhu systému vypracovaného agenturou ENISA ***zmocněna přijímat*** akty ***v přenesené pravomoci v souladu s článkem 65a***, kterými ***doplní toto nařízení stanovením evropského systému*** certifikace kybernetické bezpečnosti pro produkty, služby a procesy IKT a řízené bezpečnostní služby, který splňuje požadavky stanovené v článcích 51, 52 a 54.“;

b) vkládá se nový odstavec, který zní:

„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 vede Komise veřejné konzultace a konzultace se Skupinou zúčastněných stran pro certifikaci kybernetické bezpečnosti a Evropskou skupinou pro certifikaci kybernetické bezpečnosti.

8) článek 51 se mění takto:

a) název se nahrazuje tímto:

„Bezpečnostní cíle evropských systémů certifikace kybernetické bezpečnosti pro produkty, služby a procesy IKT“;

b) úvodní věta se nahrazuje tímto:

„Evropský systém certifikace kybernetické bezpečnosti pro produkty, služby nebo procesy IKT je navržen tak, aby v příslušných případech bylo dosaženo alespoň těchto bezpečnostních cílů:“;

9) vkládá se nový článek, který zní:

„Článek 51a

Bezpečnostní cíle evropských systémů certifikace kybernetické bezpečnosti pro řízené bezpečnostní služby

Evropský systém certifikace kybernetické bezpečnosti pro řízené bezpečnostní služby je navržen tak, aby v příslušných případech bylo dosaženo alespoň těchto bezpečnostních cílů:

a) zajistit, aby řízené bezpečnostní služby byly poskytovány s nezbytnými kompetencemi, odborností a zkušenostmi, což zahrnuje, že zaměstnanci odpovědní za poskytování těchto služeb mají velmi vysokou úroveň technických znalostí a kompetencí v dané oblasti, dostatečné a odpovídající zkušenosti a nejvyšší úroveň profesní bezúhonnosti;

b) zajistit, aby měl poskytovatel zavedeny vhodné vnitřní postupy k zajištění toho, aby řízené bezpečnostní služby byly vždy poskytovány na velmi vysoké úrovni kvality;

c) chránit údaje, jež jsou v souvislosti s poskytováním řízených bezpečnostních služeb předmětem přístupu, ukládání či předávání nebo jiného zpracování, proti náhodnému nebo neoprávněnému přístupu, ukládání, sdělení, zničení, jinému zpracování, ztrátě, změně či nedostupnosti;

d) zajistit včasné obnovení dostupnosti údajů, služeb a funkcí a přístupu k nim v případě fyzických nebo technických incidentů;

e) zajistit, aby oprávněné osoby, programy nebo stroje měly přístup pouze k údajům, službám nebo funkcím, jichž se týkají jejich přístupová práva;

f) zaznamenat a umožnit posouzení, které údaje, služby nebo funkce byly předmětem přístupu, použití nebo jiného zpracování, kdy k tomu došlo a kdo tak učinil;

g) zajistit, aby produkty, služby a procesy IKT [a hardware] zaváděné v rámci poskytování řízených bezpečnostních služeb byly bezpečné na úrovni standardního nastavení a ***již od fáze*** návrhu***, byly vybaveny aktualizovaným softwarem a hardwarem***, aby neobsahovaly žádné známé zranitelnosti a aby zahrnovaly nejnovější bezpečnostní aktualizace;“;

10) článek 52 se mění takto:

a) odstavec 1 se nahrazuje tímto:

„1. Evropský systém certifikace kybernetické bezpečnosti může u produktů, služeb a procesů IKT a řízených bezpečnostních služeb určit jednu nebo více těchto úrovní záruky: „základní“, „významná“ nebo „vysoká“. Úroveň záruky je přiměřená úrovni rizika, jež je spojeno se zamýšleným využitím produktu, služby nebo procesu IKT nebo řízené bezpečnostní služby, z hlediska pravděpodobnosti a dopadu případného incidentu.“;

b) odstavec 3 se nahrazuje tímto:

„3. Evropský systém certifikace kybernetické bezpečnosti stanoví bezpečnostní požadavky, které odpovídají každé úrovni záruky, včetně odpovídajících bezpečnostních funkcí a odpovídající míry přísnosti a podrobnosti hodnocení, kterým má produkt, služba nebo proces IKT nebo řízená bezpečnostní služba projít.“;

c) odstavce 5, 6 a 7 se nahrazují tímto:

„5. Evropský certifikát kybernetické bezpečnosti nebo EU prohlášení o shodě, které odkazují na úroveň záruky „základní“, poskytují záruku, že produkty, služby a procesy IKT a řízené bezpečnostní služby, pro něž jsou tento certifikát nebo toto EU prohlášení o shodě vydány, splňují odpovídající bezpečnostní požadavky včetně bezpečnostních funkcí a že byly vyhodnoceny na úrovni, jejímž cílem je minimalizovat známá základní rizika incidentů a kybernetických útoků. Prováděné hodnotící činnosti zahrnují alespoň přezkum technické dokumentace. Pokud takový

přezkum není vhodný, provedou se náhradní hodnotící činnosti s rovnocenným účinkem.

6. Evropský certifikát kybernetické bezpečnosti, který odkazuje na úroveň záruky „významná“, poskytuje záruku, že produkty, služby a procesy IKT a řízené bezpečnostní služby, pro něž je tento certifikát vydán, splňují odpovídající bezpečnostní požadavky včetně bezpečnostních funkcí a že byly vyhodnoceny na úrovni, jejímž cílem je minimalizovat známá kybernetická rizika a rizika incidentů a kybernetických útoků prováděných subjekty s omezenými dovednostmi a zdroji. Prováděné hodnotící činnosti zahrnují alespoň: přezkum s cílem prokázat absenci veřejně známých zranitelností a testování s cílem prokázat, že produkty, služby a procesy IKT nebo řízené bezpečnostní služby správně uplatňují nezbytné bezpečnostní funkce. Pokud některá z těchto hodnotících činností není vhodná, provedou se náhradní hodnotící činnosti s rovnocenným účinkem.

7. Evropský certifikát kybernetické bezpečnosti, který odkazuje na úroveň záruky „vysoká“, poskytuje záruku, že produkty, služby a procesy IKT a řízené bezpečnostní služby, pro něž je tento certifikát vydán, splňují odpovídající bezpečnostní požadavky včetně bezpečnostních funkcí a že byly vyhodnoceny na úrovni, jejímž cílem je minimalizovat rizika sofistikovaných kybernetických útoků prováděných subjekty s významnými dovednostmi a zdroji. Prováděné hodnotící činnosti zahrnují alespoň: přezkum s cílem prokázat absenci veřejně známých zranitelností; testování s cílem prokázat, že produkty, služby, procesy IKT nebo řízené bezpečnostní služby IKT správně uplatňují nezbytné bezpečnostní funkce odpovídající aktuálnímu stavu techniky, a posouzení jejich odolnosti vůči zručným útočníkům prostřednictvím penetračního testování. Pokud některá z těchto hodnotících činností není vhodná, provedou se náhradní hodnotící činnosti s rovnocenným účinkem.“;

11) v článku 53 se odstavce 1, 2 a 3 nahrazují tímto:

„1. Evropský systém certifikace kybernetické bezpečnosti může umožnit vlastní posuzování shody pod výhradní odpovědností výrobce nebo poskytovatele

produktů, služeb či procesů IKT nebo řízených bezpečnostních služeb. Vlastní posuzování shody je přípustné pouze u produktů, služeb a procesů IKT a řízených bezpečnostních služeb, které vykazují nízké riziko odpovídající úrovni záruky „základní“.

2. Výrobce nebo poskytovatel produktů, služeb či procesů IKT nebo řízených bezpečnostních služeb může vydat EU prohlášení o shodě uvádějící, že bylo prokázáno plnění požadavků stanovených v příslušném systému. Vydáním tohoto prohlášení výrobce produktů IKT nebo poskytovatel služeb či procesů IKT nebo řízených bezpečnostních služeb přebírá odpovědnost za soulad produktu, služby nebo procesu IKT nebo řízené bezpečnostní služby s požadavky stanovenými v daném systému.

3. Výrobce nebo poskytovatel produktů, služeb či procesů IKT nebo řízených bezpečnostních služeb zpřístupní EU prohlášení o shodě, technickou dokumentaci a veškeré ostatní příslušné informace související se shodou produktů, služeb a procesů IKT nebo řízených bezpečnostních služeb se systémem vnitrostátnímu orgánu certifikace kybernetické bezpečnosti uvedenému v článku 58 po dobu stanovenou v odpovídajícím evropském systému certifikace kybernetické bezpečnosti. Jedno vyhotovení EU prohlášení o shodě se předkládá vnitrostátnímu orgánu certifikace kybernetické bezpečnosti a jedno vyhotovení agentuře ENISA.“;

12) v článku 54 se odstavec 1 mění takto:

a) písmeno a) se nahrazuje tímto:

„a) předmět a oblast působnosti systému certifikace včetně druhu nebo kategorií zahrnutých produktů, služeb a procesů IKT a řízených bezpečnostních služeb;“;

b) písmeno j) se nahrazuje tímto:

„j) pravidla pro monitorování souladu produktů, služeb a procesů IKT a řízených bezpečnostních služeb s požadavky evropských certifikátů kybernetické bezpečnosti nebo EU prohlášení o shodě, včetně mechanismů prokázání pokračujícího plnění specifikovaných požadavků kybernetické bezpečnosti;“;

c) písmeno l) se nahrazuje tímto:

„l) pravidla upravující důsledky pro produkty, služby a procesy IKT a řízené bezpečnostní služby, jež jsou certifikovány nebo pro něž bylo vydáno EU prohlášení o shodě, avšak nesplňují požadavky systému;“;

d) písmeno o) se nahrazuje tímto:

„o) identifikaci vnitrostátních nebo mezinárodních systémů certifikace kybernetické bezpečnosti zahrnující stejné druhy nebo kategorie produktů, služeb a procesů IKT a řízených bezpečnostních služeb, bezpečnostní požadavky a hodnotící kritéria a metody a úrovně záruky;“;

e) písmeno q) se nahrazuje tímto:

„q) dobu dostupnosti EU prohlášení o shodě, technické dokumentace a veškerých dalších relevantních informací, které má výrobce nebo poskytovatele produktů, služeb či procesů IKT nebo řízených bezpečnostních služeb zpřístupnit;“;

13) článek 56 se mění takto:

a) odstavec 1 se nahrazuje tímto:

„1. U produktů, služeb a procesů IKT a řízených bezpečnostních služeb, které byly certifikovány v rámci evropského systému certifikace kybernetické bezpečnosti přijatého podle článku 49, se předpokládá, že splňují požadavky daného systému.“;

b) odstavec 3 se mění takto:

i) první pododstavec se nahrazuje tímto:

„Komise pravidelně hodnotí účinnost a využití přijatých evropských systémů certifikace kybernetické bezpečnosti, přičemž rovněž posuzuje, zda by se určitý evropský systém certifikace kybernetické bezpečnosti měl na základě příslušných právních předpisů Unie stát povinným v zájmu zajištění patřičné úrovně kybernetické bezpečnosti produktů, služeb a procesů IKT a řízených bezpečnostních služeb v Unii a v zájmu zlepšení fungování vnitřního trhu. První takové hodnocení proběhne do 31. prosince 2023 a následná hodnocení se poté uskuteční alespoň každé

dva roky. Na základě výsledku těchto hodnocení Komise z produktů, služeb a procesů IKT a řízených bezpečnostních služeb, na něž se již vztahuje stávající systém certifikace, určí ty, na něž by se měl vztahovat povinný systém certifikace.“;

ii) třetí pododstavec se mění takto:

aa) písmeno a) se nahrazuje tímto:

„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;“;

bb) písmeno d) se nahrazuje tímto:

„d) zohlední prováděcí lhůty, přechodná opatření nebo přechodná období, zejména se zřetelem na možný dopad daného opatření na výrobce nebo poskytovatele produktů, služeb či procesů IKT nebo řízených bezpečnostních služeb, včetně ***zvláštních zájmů a potřeb mikropodniků a*** malých a středních podniků;“;

iii) doplňuje se nový pododstavec, který zní:

„Pokud jde o třetí pododstavec písm. d) tohoto článku, Komise zajistí vhodnou finanční podporu v regulačním rámci stávajících programů Unie, zejména s cílem snížit finanční zátěž mikropodniků a malých a středních podniků, včetně začínajících podniků působících v oblasti řízených bezpečnostních služeb.“;

c) odstavce 7 a 8 se nahrazují tímto:

„7. Fyzická nebo právnická osoba, která předkládá produkty, služby nebo procesy IKT nebo řízené bezpečnostní služby k certifikaci, zpřístupní vnitrostátnímu orgánu certifikace kybernetické bezpečnosti podle článku

58, pokud je tento orgán subjektem vydávajícím evropský certifikát kybernetické bezpečnosti, nebo subjektu posuzování shody uvedenému v článku 60 veškeré informace nezbytné pro provedení certifikace.

8. Držitel evropského certifikátu kybernetické bezpečnosti informuje orgán či subjekt uvedený v odstavci 7 o veškerých později zjištěných zranitelnostech nebo nesrovnalostech týkajících se bezpečnosti certifikovaného produktu, služby nebo procesu IKT nebo řízených bezpečnostních služeb, které by mohly mít dopad na jejich soulad s požadavky souvisejícími s certifikací. Tento orgán či subjekt neprodleně tyto informace postoupí příslušnému vnitrostátnímu orgánu certifikace kybernetické bezpečnosti.“;

14) v článku 57 se odstavce 1 a 2 nahrazují tímto:

„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*** 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.

2. Členské státy nezavedou nové vnitrostátní systémy certifikace kybernetické bezpečnosti pro produkty, služby a procesy IKT a řízené bezpečnostní služby, které jsou již zahrnuty do platného evropského systému certifikace kybernetické bezpečnosti.“;

15) článek 58 se mění takto:

a) odstavec 7 se mění takto:

i) písmena a) a b) se nahrazují tímto:

„a) dohlížejí na pravidla zahrnutá v evropských systémech certifikace kybernetické bezpečnosti podle čl. 54 odst. 1 písm. j) pro monitorování souladu produktů, procesů, služeb a procesů IKT a řízených bezpečnostních služeb s požadavky evropských certifikátů

kybernetické bezpečnosti, jež byly vydány na území jejich států, a dodržování těchto pravidel vymáhají, přičemž spolupracují s dalšími příslušnými orgány dohledu nad trhem;

b) sledují dodržování povinností výrobců a poskytovatelů produktů, služeb a procesů IKT nebo řízených bezpečnostních služeb, kteří jsou usazeni na území jejich států a kteří provádějí vlastní posuzování shody, zejména pak povinností těchto výrobců a poskytovatelů stanovených v čl. 53 odst. 2 a 3 a v odpovídajícím evropském systému certifikace kybernetické bezpečnosti, a dodržování těchto povinností vymáhají;“;

ii) písmeno h) se nahrazuje tímto:

„h) spolupracují s dalšími vnitrostátními orgány certifikace kybernetické bezpečnosti nebo jinými veřejnými orgány, mimo jiné prostřednictvím sdílení informací o možných případech nesouladu produktů, služeb a procesů IKT a řízených bezpečnostních služeb s požadavky tohoto nařízení nebo s požadavky konkrétních evropských systémů certifikace kybernetické bezpečnosti; a“;

b) odstavec 9 se nahrazuje tímto:

„9. Vnitrostátní orgány certifikace kybernetické bezpečnosti spolupracují mezi sebou a s Komisí, a zejména si vyměňují informace, zkušenosti a osvědčené postupy týkající se certifikace kybernetické bezpečnosti a technických otázek v oblasti kybernetické bezpečnosti, produktů, služeb a procesů IKT a řízených bezpečnostních služeb.“;

16) v čl. 59 odst. 3 se písmena b) a c) nahrazují tímto:

„b) postupy dohledu nad pravidly pro monitorování souladu produktů, služeb a procesů IKT a řízených bezpečnostních služeb s evropskými certifikáty kybernetické bezpečnosti a vymáhání těchto pravidel, v souladu čl. 58 odst. 7 písm. a);

c) postupy pro sledování a vymáhání povinností výrobců nebo poskytovatelů produktů, služeb a procesů IKT nebo řízených bezpečnostních služeb podle čl. 58 odst. 7 písm. b);“;

16a) vkládá se nový článek, který zní:

„Článek 65a

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 uvedené v čl. 49 odst. 7 je svěřena Komisi na dobu pěti let od … [datum vstupu tohoto pozměněného nařízení v platnost]. Komise vypracuje zprávu o přenesené pravomoci nejpozději devět měsíců před koncem tohoto pětiletého období. Přenesení pravomoci se automaticky prodlužuje o stejně dlouhá období, pokud Evropský parlament ani Rada nevysloví proti tomuto prodloužení námitku nejpozději tři měsíce před koncem každého z těchto období.

3. Evropský parlament nebo Rada mohou přenesení pravomoci podle čl. 49 odst. 7 kdykoli zrušit. Rozhodnutím o zrušení se ukončuje přenesení pravomoci v něm určené. Rozhodnutí nabývá účinku prvním dnem po zveřejnění v Úředním věstníku Evropské unie nebo k pozdějšímu dni, který je v něm upřesněn. Nedotýká se platnosti žádných již platných aktů v přenesené pravomoci.

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

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

6. Akt v přenesené pravomoci přijatý podle čl. 49 odst. 7 vstoupí v platnost pouze tehdy, pokud proti němu Evropský parlament ani Rada nevysloví námitky ve lhůtě dvou měsíců ode dne, kdy jim byl tento akt oznámen, nebo pokud Evropský parlament i Rada před uplynutím této lhůty informují Komisi o tom, že námitky nevysloví. Z podnětu Evropského parlamentu nebo Rady se tato lhůta prodlouží o [dva měsíce].“;

17) ***článek*** 67 se ***nahrazuje*** tímto:

„Článek 67

Vyhodnocení a přezkum

1. ***Do 28. června 2024 a poté každé tři roky Komise provede posouzení dopadu, účinnosti a účelnosti agentury ENISA a jejích pracovních postupů, jakož i případné potřeby 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.***

2. ***Hodnocení rovněž posoudí dopad, účinnost a účelnost 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.***

3. ***V rámci hodnocení se rovněž posuzuje:***

   a) ***účinnost a účelnost postupů vedoucích ke konzultacím, přípravě a přijetí evropských systémů certifikace kybernetické bezpečnosti, jakož i způsoby, jak tyto postupy zlepšit a urychlit;***

   b) ***zda jsou základní požadavky na kybernetickou bezpečnost pro přístup na vnitřní trh nezbytné k tomu, aby se zabránilo produktům, službám a procesům IKT a řízeným bezpečnostním službám, které nesplňují základní požadavky na kybernetickou bezpečnost, vstupovat na trh Unie.***

4. ***Komise předá zprávu o hodnocení společně se svými závěry Evropskému parlamentu, Radě a správní radě do 28. června 2024 a poté každé tři roky. Zjištění této zprávy se zveřejní.***“.

Článek 2

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

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

V … dne ...

Za Evropský parlament	*Za Radu*
předsedkyně	*předseda* nebo *předsedkyně*