EVROPSKÁ
KOMISE

Ve Štrasburku dne 18.4.2023
COM(2023) 208 final

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)

DŮVODOVÁ ZPRÁVA

1. SOUVISLOSTI NÁVRHU

• Odůvodnění a cíle návrhu

Tato důvodová zpráva doprovází návrh nařízení Evropského parlamentu a Rady, kterým se mění nařízení (EU) 2019/881[1], pokud jde o řízené bezpečnostní služby.

Účelem navrhované cílené změny je umožnit prostřednictvím prováděcích aktů Komise přijímat evropské systémy certifikace kybernetické bezpečnosti vedle produktů, služeb a procesů informačních a komunikačních technologií (IKT), na něž se akt o kybernetické bezpečnosti již vztahuje, také pro „řízené bezpečnostní služby“. Řízené bezpečnostní služby hrají stále důležitější úlohu při prevenci kybernetických bezpečnostních incidentů a zmírňování jejich dopadů.

Rada ve svých závěrech ze dne 23. května 2022[2] o rozvoji kybernetické pozice Evropské unie vyzvala Unii a její členské státy, aby zintenzivnily úsilí o zvýšení celkové úrovně kybernetické bezpečnosti, například usnadněním vzniku důvěryhodných poskytovatelů služeb kybernetické bezpečnosti, a zdůraznila, že podpora rozvoje těchto poskytovatelů by měla být prioritou průmyslové politiky Unie v oblasti kybernetické bezpečnosti. Vyzvala rovněž Komisi, aby navrhla možnosti, jak podpořit vznik důvěryhodného odvětví služeb kybernetické bezpečnosti. Certifikace řízených bezpečnostních služeb je účinným prostředkem budování důvěry v kvalitu těchto služeb, což napomáhá vzniku důvěryhodného evropského odvětví služeb kybernetické bezpečnosti.

Ve společném sdělení „Politika kybernetické obrany EU“, které Komise a vysoký představitel přijali dne 10. listopadu 2022[3], bylo oznámeno, že Komise prozkoumá vývoj systémů certifikace v oblasti kybernetické bezpečnosti pro odvětví kybernetické bezpečnosti a soukromé společnosti na úrovni EU. Poskytovatelé řízených bezpečnostních služeb budou rovněž hrát důležitou úlohu v rezervě pro kybernetickou bezpečnost na úrovni EU, jejíž postupné vytváření je podpořeno aktem o kybernetické solidaritě navrženým souběžně s tímto nařízením. Rezerva pro kybernetickou bezpečnost na úrovni EU má být použita na podporu reakce a okamžitých opatření obnovy v případě významných a rozsáhlých kybernetických bezpečnostních incidentů. Příslušné služby kybernetické bezpečnosti poskytované „důvěryhodnými poskytovateli“ podle aktu o kybernetické solidaritě odpovídají „řízeným bezpečnostním službám“ v tomto návrhu.

Některé členské státy již začaly přijímat systémy certifikace pro řízené bezpečnostní služby. V důsledku nejednotnosti systémů certifikace kybernetické bezpečnosti v Unii proto roste riziko roztříštění vnitřního trhu s řízenými bezpečnostními službami. Tento návrh umožňuje vytvoření evropských systémů certifikace kybernetické bezpečnosti pro tyto služby s cílem takové roztříštěnosti zabránit.

• Soulad s platnými předpisy v této oblasti politiky

Tento návrh je v souladu s aktem o kybernetické bezpečnosti, jejž mění. Vychází z ustanovení uvedeného nařízení a upravuje je tak, aby zahrnovala i řízené bezpečnostní služby.

---

[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] 9364/22.

[3] JOIN(2022) 49 final.

Navrhované změny se omezují na to, co je nezbytně nutné, a nemění charakteristiky ani fungování aktu o kybernetické bezpečnosti.

Tento návrh je rovněž v souladu se směrnicí 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)[4]. Poskytovatelé řízených bezpečnostních služeb jsou považováni za základní nebo důležité subjekty náležející k vysoce kritickému odvětví podle směrnice (EU) 2022/2555. V 86. bodě odůvodnění zmíněné směrnice se uvádí, že poskytovatelé řízených bezpečnostních služeb mají 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.

Cílem tohoto návrhu je zlepšit kvalitu řízených bezpečnostních služeb a zvýšit jejich porovnatelnost. Umožňuje tak základním a důležitým subjektům postupovat při výběru poskytovatele řízených bezpečnostních služeb s větší péčí, jak vyžaduje směrnice (EU) 2022/2555. Navíc definice „spravovaných bezpečnostních služeb“ v tomto návrhu je odvozena od definice „poskytovatelů řízených bezpečnostních služeb“ ve směrnici (EU) 2022/2555 a je jí velmi podobná. Z těchto důvodů návrh do značné míry doplňuje směrnici NIS 2.

V neposlední řadě tento návrh doplňuje navrhovaný akt o kybernetické solidaritě. Navrhovaný akt o kybernetické solidaritě stanoví postup pro výběr poskytovatelů, kteří vytvoří rezervu pro kybernetickou bezpečnost na úrovni EU, jenž by měl mimo jiné zohlednit, zda tito poskytovatelé získali evropskou nebo vnitrostátní certifikaci kybernetické bezpečnosti. Budoucí systémy certifikace pro řízené bezpečnostní služby tak budou hrát při provádění aktu o kybernetické solidaritě významnou úlohu.

- **Soulad s ostatními politikami Unie**

Tímto návrhem není dotčen soulad aktu o kybernetické bezpečnosti s nařízením (EU) 2016/679 (obecným nařízením o ochraně osobních údajů, „GDPR“)[5] a jeho ustanoveními o zavedení mechanismů pro vydávání osvědčení a pečetí a známek dokládajících ochranu údajů za účelem prokázání souladu operací zpracování prováděných správci a zpracovateli s uvedeným nařízením. Aktem o kybernetické bezpečnosti není dotčena certifikace operací zpracování údajů podle GDPR, včetně případů, kdy jsou tyto operace nedílnou součástí produktů a služeb.

Tento návrh rovněž nemá vliv na slučitelnost aktu o kybernetické bezpečnosti s nařízením (ES) č. 765/2008 o požadavcích na akreditaci a dozor nad trhem[6], zejména pokud jde o rámec pro vnitrostátní akreditační orgány a subjekty posuzování shody a vnitrostátní orgány dozoru nad certifikací.

[4] Úř. věst. L 333, 27.12.2022, s. 810.
[5] Úř. věst. L 119, 4.5.2016, s. 1.
[6] Úř. věst. L 218, 13.8.2008, s. 30.

2. PRÁVNÍ ZÁKLAD, SUBSIDIARITA A PROPORCIONALITA

• Právní základ

Tento návrh mění akt o kybernetické bezpečnosti, který vychází z článku 114 Smlouvy o fungování Evropské unie (SFEU). Stejně jako v případě aktu o kybernetické bezpečnosti je cílem tohoto návrhu zabránit roztříštěnosti vnitřního trhu, konkrétně umožněním přijetí evropských systémů certifikace kybernetické bezpečnosti pro řízené bezpečnostní služby. Členské státy již začaly přijímat vnitrostátní systémy certifikace pro řízené bezpečnostní služby. Existuje tedy konkrétní riziko roztříštění vnitřního trhu s těmito službami, které má tento návrh řešit. Článek 114 SFEU je proto relevantním právním základem této iniciativy.

• Subsidiarita (v případě nevýlučné pravomoci)

Cíle umožnit přijímání evropských systémů certifikace kybernetické bezpečnosti pro řízené bezpečnostní služby a zabránit roztříštění vnitřního trhu nelze dosáhnout na vnitrostátní úrovni, ale pouze na úrovni Unie. Řízené bezpečnostní služby, které jsou předmětem navrhované změny, navíc nabízejí poskytovatelé, kteří působí v celé Unii, stejně jako jejich největší potenciální zákazníci. Přijetí opatření na úrovni Unie je proto jednak nezbytné, jednak účinnější než přijetí opatření na vnitrostátní úrovni.

• Proporcionalita

Návrh je cílenou změnou aktu o kybernetické bezpečnosti. Omezuje se na to, co je nezbytně nutné k dosažení jeho cíle, tj. umožnit přijímání evropských systémů certifikace kybernetické bezpečnosti vedle produktů, služeb a procesů IKT také pro řízené bezpečnostní služby. Navrhované změny upravují zejména oblast působnosti evropského rámce pro certifikaci kybernetické bezpečnosti tak, aby zahrnoval i „řízené bezpečnostní služby“, zavádějí definici těchto služeb v souladu se směrnicí NIS 2 a mění bezpečnostní cíle evropské certifikace kybernetické bezpečnosti s cílem přizpůsobit ji „řízeným bezpečnostním službám“. Ostatní změny jsou technické povahy a jejich cílem je zajistit, aby se příslušné články vztahovaly i na „řízené bezpečnostní služby“. Navrhovaná iniciativa je tedy přiměřená svému cíli.

• Volba nástroje

Jelikož návrh mění nařízení (EU) 2019/881, je vhodným právním nástrojem nařízení.

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

• Hodnocení *ex post* / kontroly účelnosti platných právních předpisů

Nevztahuje se na tento návrh.

• Konzultace se zúčastněnými stranami

Proběhly cílené konzultace s členskými státy a agenturou ENISA. V rámci těchto konzultací členské státy prezentovaly své současné aktivity a stanoviska, pokud jde o certifikaci řízených bezpečnostních služeb. ENISA prezentovala svá stanoviska a zjištění z diskusí s členskými státy a zúčastněnými stranami. Připomínky a informace obdržené od členských států a agentury ENISA jsou v tomto návrhu zohledněny.

• Sběr a využití výsledků odborných konzultací

Nevztahuje se na tento návrh.

- **Posouzení dopadů**

Bylo požádáno o výjimku z povinnosti provést posouzení dopadů, neboť návrh představuje pouze minimální a cílenou změnu aktu o kybernetické bezpečnosti. Tato změna by zmocnila Komisi, aby prostřednictvím prováděcích aktů přijímala kromě systémů certifikace produktů, služeb a procesů IKT, na které se akt již vztahuje, i systémy certifikace pro „řízené bezpečnostní služby“. Změna by však měla účinek až poté, co budou tyto systémy certifikace přijaty v pozdější fázi. Změna by navíc nezměnila dobrovolnou povahu systémů certifikace.

- **Účelnost právních předpisů a zjednodušení**

Nevztahuje se na tento návrh.

- **Základní práva**

Návrh nemá žádné předvídatelné důsledky pro ochranu základních práv.

4. ROZPOČTOVÉ DŮSLEDKY

Žádné.

5. OSTATNÍ PRVKY

- **Plány provádění a způsoby monitorování, hodnocení a podávání zpráv**

Ustanovení, která mají být návrhem pozměněna, budou vyhodnocena v rámci pravidelného hodnocení aktu o kybernetické bezpečnosti, které provede Komise v souladu s jeho článkem 67. Hodnocení posoudí mimo jiné dopad, efektivnost a účinnost ustanovení týkajících se rámce pro certifikaci kybernetické bezpečnosti s ohledem na cíle zajištění odpovídající úrovně kybernetické bezpečnosti produktů, služeb a procesů IKT v Unii a zlepšení fungování vnitřního trhu. Součástí návrhu je i změna zajišťující, aby se toto hodnocení vztahovalo i na řízené bezpečnostní služby. Komise rovněž zašle zprávu o hodnocení a svých závěrech Evropskému parlamentu, Radě a správní radě agentury ENISA a zjištění zprávy zveřejní.

- **Podrobné vysvětlení konkrétních ustanovení návrhu**

Návrh obsahuje dva články. Článek 1 obsahuje změny nařízení (EU) 2019/881 a článek 2 se týká vstupu v platnost. Článek 1 obsahuje cílené změny za účelem úpravy oblasti působnosti evropského rámce pro certifikaci kybernetické bezpečnosti v aktu o kybernetické bezpečnosti tak, aby zahrnovala i „řízené bezpečnostní služby“ (články 1 a 46 aktu o kybernetické bezpečnosti). Zavádí definici těchto služeb, která je velmi úzce sladěna s definicí „poskytovatelů řízených bezpečnostních služeb“ podle směrnice NIS 2 (článek 2 aktu o kybernetické bezpečnosti). Doplňuje rovněž nový článek 51a o bezpečnostních cílech evropské certifikace kybernetické bezpečnosti přizpůsobených „řízeným bezpečnostním službám“. V neposlední řadě návrh obsahuje řadu technických změn, které mají zajistit, aby se příslušné články vztahovaly i na „řízené bezpečnostní služby“.

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,

s ohledem na návrh Evropské komise,

po postoupení návrhu legislativního aktu vnitrostátním parlamentům,

s ohledem na stanovisko Evropského hospodářského a sociálního výboru,

s ohledem na stanovisko Výboru regionů,

v souladu s řádným legislativním postupem,

vzhledem k těmto důvodům:

(1) Nařízení Evropského parlamentu a Rady (EU) 2019/881[7] stanoví rámec pro zavedení evropského systému certifikace kybernetické bezpečnosti, jehož účelem je zajistit odpovídající úroveň kybernetické bezpečnosti produktů, služeb a procesů IKT v Unii a zabránit roztříštění vnitřního trhu, pokud jde o systémy certifikace kybernetické bezpečnosti v Unii.

(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.

---

[7] 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).

[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).

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 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.

(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],

PŘIJALY TOTO NAŘÍZENÍ:

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 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;“

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.

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;

d) vývoj v oblasti kybernetických hrozeb;

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

7) v článku 49 se odstavec 7 nahrazuje tímto:

„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.“;

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 výchozího návrhu, 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 malých a středních podniků;“;

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 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.

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);“;

17) v článku 67 se odstavce 2 a 3 nahrazují tímto:

„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.

3. Hodnocení posoudí, 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.“.

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.

Ve Štrasburku dne

Za Evropský parlament *předseda/předsedkyně*	*Za Radu* *předseda/předsedkyně*