Rada
Evropské unie

Brusel 17. prosince 2025
(OR. en)

16960/25

CYBER 389
JAI 1924
DATAPROTECT 345
TELECOM 485
MI 1075
CSC 693
CSCI 284
DELACT 198

PRŮVODNÍ POZNÁMKA

Odesílatel:	Martine DEPREZOVÁ, ředitelka, za generální tajemnici Evropské komise
Datum přijetí:	11. prosince 2025
Příjemce:	Thérèse BLANCHETOVÁ, generální tajemnice Rady Evropské unie
Č. dok. Komise:	C(2025) 8407 final
Předmět:	NAŘÍZENÍ KOMISE V PŘENESENÉ PRAVOMOCI (EU) …/... ze dne 11.12.2025, kterým se doplňuje nařízení Evropského parlamentu a Rady (EU) 2024/2847 stanovením podmínek pro uplatňování důvodů souvisejících s kybernetickou bezpečností, pokud jde o odklad rozesílání oznámení

Delegace naleznou v příloze dokument C(2025) 8407 final.

Příloha: C(2025) 8407 final

EVROPSKÁ
KOMISE

V Bruselu dne 11.12.2025
C(2025) 8407 final

NAŘÍZENÍ KOMISE V PŘENESENÉ PRAVOMOCI (EU) …/...

ze dne 11.12.2025,

kterým se doplňuje nařízení Evropského parlamentu a Rady (EU) 2024/2847 stanovením podmínek pro uplatňování důvodů souvisejících s kybernetickou bezpečností, pokud jde o odklad rozesílání oznámení

(Text s významem pro EHP)

DŮVODOVÁ ZPRÁVA

1. SOUVISLOSTI AKTU V PŘENESENÉ PRAVOMOCI

Nařízení Evropského parlamentu a Rady (EU) 2024/2847 (dále jen „akt o kybernetické odolnosti“) vyžaduje po výrobcích produktů s digitálními prvky, aby prostřednictvím jednotné platformy pro podávání zpráv oznámili jakoukoli aktivně zneužívanou zranitelnost nebo závažný incident, který má dopad na bezpečnost produktu s digitálními prvky. Podle čl. 16 odst. 2 uvedeného nařízení může tým pro reakce na počítačové bezpečnostní incidenty (CSIRT) určený členským státem jako koordinátor, který obdržel oznámení jako první, za výjimečných okolností a na základě opodstatněných důvodů souvisejících s kybernetickou bezpečností odložit rozesílání příslušného oznámení týmům CSIRT jiných členských států, v nichž byl produkt s digitálními prvky zpřístupněn.

Cílem tohoto aktu v přenesené pravomoci je proto doplnit akt o kybernetické odolnosti stanovením podmínek pro uplatňování důvodů souvisejících s kybernetickou bezpečností k odložení rozesílání oznámení. Činí tak určením tří typů důvodů, pro které může tým CSIRT, který obdržel oznámení jako první, rozhodnout, že je další rozesílání ostatním týmům CSIRT nezbytné odložit. Takové rozhodnutí o odložení lze přijmout ve třech případech:

- na základě hodnocení povahy oznámených informací,
- pokud tým CSIRT, kterému má být oznámení zasláno, není schopen zajistit důvěrnost těchto informací,
- pokud bylo narušeno zabezpečení jednotné platformy pro podávání zpráv nebo platforma dočasně nefunguje.

Povinnosti podávat zprávy stanovené v článku 14 nařízení (EU) 2024/2847 se mají použít od 11. září 2026.

2. KONZULTACE PŘED PŘIJETÍM PRÁVNÍHO AKTU

Různé návrhy tohoto aktu byly konzultovány se sítí týmů pro reakce na počítačové bezpečnostní incidenty (síť CSIRT) a s Agenturou Evropské unie pro kybernetickou bezpečnost (ENISA). Dne 26. března 2025 proběhla předběžná diskuse s orientačními otázkami a do 11. dubna 2025 bylo možné předložit písemné příspěvky. První návrh tohoto aktu byl předán síti CSIRT a agentuře ENISA dne 16. května 2025 a diskuse proběhla dne 6. června 2025 s možností předložit písemné příspěvky do 27. června 2025. Druhý návrh aktu byl předán síti CSIRT a agentuře ENISA dne 23. července 2025 a do 1. září 2025 bylo možné předložit písemné příspěvky. Třetí návrh aktu byl předán síti CSIRT a agentuře ENISA dne 25. září 2025 a diskuse proběhla dne 9. října 2025 s možností předložit písemné příspěvky do 27. října 2025.

Návrh aktu byl v období od 16. října 2025 do 13. listopadu 2025 předmětem veřejné konzultace, v jejímž rámci bylo od 31 jednotlivých respondentů obdrženo 34 odpovědí (je zohledněna skutečnost, že tentýž respondent poskytl zpětnou vazbu prostřednictvím čtyř různých podání). Z toho 29,41 % bylo obdrženo od podnikatelských sdružení, 26,47 % od

společností/podniků, 17,65 % od občanů EU, 14,71 % od veřejných orgánů, 5,88 % od nevládních organizací a 5,88 % od akademických/výzkumných institucí[1].

Dne 22. října byl návrh rovněž projednán s expertní skupinou pro kybernetickou bezpečnost produktů s digitálními prvky (E03967), jejíž členy jsou orgány členských států, agentura ENISA, odborníci jmenovaní za svou osobu a organizace v širším slova smyslu (např. společnosti, sdružení, nevládní organizace).

3. PRÁVNÍ STRÁNKA AKTU V PŘENESENÉ PRAVOMOCI

Zmocnění k přijímání aktů v přenesené pravomoci je stanoveno v čl. 14 odst. 9 aktu o kybernetické odolnosti, který vyžaduje, aby Komise do 11. prosince 2025 stanovila podmínky pro uplatňování důvodů souvisejících s kybernetickou bezpečností, pokud jde o odklad rozesílání oznámení.

[1] V uvedených procentních údajích není zohledněna skutečnost, že tentýž respondent poskytl zpětnou vazbu prostřednictvím čtyř různých podání.

NAŘÍZENÍ KOMISE V PŘENESENÉ PRAVOMOCI (EU) …/...

ze dne 11.12.2025,

kterým se doplňuje nařízení Evropského parlamentu a Rady (EU) 2024/2847 stanovením podmínek pro uplatňování důvodů souvisejících s kybernetickou bezpečností, pokud jde o odklad rozesílání oznámení

(Text s významem pro EHP)

EVROPSKÁ KOMISE,

s ohledem na Smlouvu o fungování Evropské unie,

s ohledem na nařízení Evropského parlamentu a Rady (EU) 2024/2847 ze dne 23. října 2024 o horizontálních požadavcích na kybernetickou bezpečnost produktů s digitálními prvky a o změně nařízení (EU) č. 168/2013 a (EU) 2019/1020 a směrnice (EU) 2020/1828 (akt o kybernetické odolnosti)[2], a zejména na čl. 14 odst. 9 uvedeného nařízení,

vzhledem k těmto důvodům:

(1) Za výjimečných okolností, a zejména na žádost výrobce a s ohledem na úroveň citlivosti oznámených informací, a na základě opodstatněných důvodů souvisejících s kybernetickou bezpečností se může tým pro reakce na počítačové bezpečnostní incidenty (CSIRT) určený jako koordinátor, který jako první obdržel oznámení o aktivně zneužívané zranitelnosti nebo závažném incidentu, který má dopad na bezpečnost produktu s digitálními prvky (dále jen „tým CSIRT, který obdržel oznámení jako první“), rozhodnout, že na nezbytně nutnou dobu odloží rozesílání oznámení prostřednictvím jednotné platformy pro podávání zpráv týmům CSIRT určeným jako koordinátoři, na jejichž území byl podle informací výrobce podávajícího oznámení produkt s digitálními prvky zpřístupněn (dále jen „příslušné týmy CSIRT“). Je proto nezbytné stanovit podmínky pro uplatňování těchto důvodů. Pokud takové důvody existují, může tým CSIRT, který obdržel oznámení jako první, na nezbytně nutnou dobu odložit rozesílání oznámení příslušným týmům CSIRT, avšak není povinen tak učinit. Podle čl. 16 odst. 2 nařízení (EU) 2024/2847 platí, že pokud se tým CSIRT, který obdržel oznámení jako první, rozhodne uplatnit tyto důvody, měl by o svém rozhodnutí o odkladu, důvodech k odkladu a o tom, kdy má v úmyslu oznámení dále rozesílat, neprodleně informovat Agenturu Evropské unie pro kybernetickou bezpečnost (ENISA).

(2) V souladu s čl. 16 odst. 2 druhým pododstavcem nařízení (EU) 2024/2847 se podmínky pro uplatňování důvodů souvisejících s kybernetickou bezpečností stanovené v tomto nařízení nevztahují na přístup agentury ENISA k oznámeným informacím. Přístup agentury ENISA k oznámeným informacím může být omezen pouze za zvláště výjimečných okolností: pokud výrobce ve svém oznámení uvede, že je splněna jedna ze tří podmínek uvedených v čl. 16 odst. 2 třetím pododstavci písm. a), b) nebo c) nařízení (EU) 2024/2847, a to pouze ve vztahu k oznámení o zranitelnosti do 72 hodin uvedenému v čl. 14 odst. 2 písm. b) nařízení (EU)

[2] Úř. věst. L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj.

2024/2847. V takových případech jsou agentuře ENISA současně zpřístupněny pouze informace o tom, že výrobce učinil oznámení, obecné informace o produktu s digitálními prvky, informace o obecné povaze zneužívání a informace o tom, že byly uplatněny důvody související s bezpečností.

(3) Přístup k oznámeným informacím umožňuje týmům CSIRT získat přehled o bezpečnostním prostředí na jejich území a zavést zmírňující opatření, čímž se zvýší celková úroveň kybernetické bezpečnosti v Unii. Další omezení rozesílání oznámení s ohledem na povahu oznamovaných informací by proto měla být možná pouze v případech, kdy s ohledem na citlivost oznamovaných informací kybernetická bezpečnostní rizika vyplývající z dalšího rozesílání převažují nad bezpečnostními přínosy pro Unii a tato rizika nelze odpovídajícím způsobem zmírnit zavedením omezení týkajících se zpracování a dalšího sdílení oznámení prostřednictvím vhodných protokolů používaných v rámci sítě CSIRT, jako je TLP protokol (semaforový protokol) nebo PAP protokol („Permissible Actions Protocol“). Tak tomu může být například v případě, kdy výrobce informoval tým CSIRT, který obdržel oznámení jako první, že v dohledné době zajistí zmírňující opatření (např. dočasnou opravu). Může tomu tak být i v případě, kdy se tým CSIRT, který obdržel oznámení jako první, rozhodne sdílet pouze části oznámení, které však postačují k tomu, aby příslušné týmy CSIRT zajistily, že budou schopny zavést odpovídající opatření ke zmírnění rizik. Kromě toho a s cílem podpořit spolupráci v oblasti identifikace a zveřejňování zranitelností mezi výrobci, týmy CSIRT a výzkumnými pracovníky v oblasti bezpečnosti tomu tak může být i v případě, kdy tým CSIRT vystupuje jako důvěryhodný zprostředkovatel v rámci probíhajícího postupu koordinovaného zveřejňování zranitelností, jak je uvedeno v čl. 12 odst. 1 směrnice Evropského parlamentu a Rady (EU) 2022/2555[3]. V takovém případě, pokud se tým CSIRT rozhodne odložit rozesílání oznámení, má tento tým CSIRT v souladu s čl. 16 odst. 6 nařízení (EU) 2024/2847 rozesílání oznámení odložit na nezbytně nutnou dobu, a to až do okamžiku, než získá souhlas stran zapojených do koordinovaného zveřejňování zranitelností se zveřejněním.

(4) Informace obsažené v oznámení pomohou týmům CSIRT plnit jejich úkoly v souvislosti se zmírňováním rizik a řešením incidentů. Ve vzácných případech by však tyto informace mohly postačovat k tomu, aby umožnily dokonce i subjektům s omezenými dovednostmi a zdroji vytvořit bez jakýchkoli hlubších rešerší techniky zneužívání. Pokud by k těmto informacím měly přístup nepřátelské subjekty, mělo by to s ohledem na snadnost zneužívání velký dopad na kybernetickou bezpečnost Unie. Tak by tomu mohlo být například v případě, kdy se nezabezpečená verze softwaru liší od předchozích zabezpečených verzí pouze nepatrně. V takových případech, pokud se tým CSIRT, který obdržel oznámení jako první, domnívá, že kybernetická bezpečnostní rizika vyplývající z dalšího rozesílání nelze odpovídajícím způsobem zmírnit zavedením omezení týkajících se zpracování a dalšího sdílení oznámení, může se tým CSIRT rozhodnout, že rozesílání odloží, dokud nebude k dispozici účinné opatření ke zmírnění rizik, jako je bezpečnostní aktualizace nebo pokyny pro uživatele.

[3] 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).

(5) Pokud příslušný tým CSIRT není schopen náležitě chránit oznámené informace, mohly by mít nepřátelské subjekty přístup k citlivým informacím a k jejich zneužití by mohlo dojít na celém jednotném trhu. Pokud tedy existují vážné obavy ohledně schopnosti příslušného týmu CSIRT zajistit důvěrnost oznamovaných informací, může se tým CSIRT, který obdržel oznámení jako první, rozhodnout, že odloží rozesílání oznámení pouze tomuto příslušnému týmu CSIRT, dokud tyto obavy nebudou vyřešeny. Tak tomu může být v situacích, kdy byl příslušný tým CSIRT zasažen kybernetickým bezpečnostním incidentem, který ovlivnil jeho schopnost provádět svou činnost bezpečně, nebo pokud existují důkazy nebo informace o tom, že byly ve schopnostech týmu CSIRT zjištěny významné nedostatky, jako jsou závažná omezení zdrojů ohrožující jeho schopnost vykonávat své funkce, nebo závislost na zastaralém nebo nezabezpečeném softwaru.

(6) Aby se nepřátelským subjektům zabránilo v přístupu k citlivým informacím, měl by tým CSIRT, který obdržel oznámení jako první, v případě, že byla jednotná platforma pro podávání zpráv stanovená článkem 16 nařízení (EU) 2024/2847 zasažena kybernetickým bezpečnostním incidentem, odložit rozesílání prostřednictvím jednotné platformy pro podávání zpráv, dokud schopnost platformy zajistit důvěrnost oznámených informací nebude obnovena.

(7) V souladu s čl. 16 odst. 2 prvním pododstavcem nařízení (EU) 2024/2847 nemusí tým CSIRT, který obdržel oznámení jako první, zaslat oznámení žádnému jinému příslušnému týmu CSIRT, pokud výrobce uvede, že produkt s digitálními prvky je dodáván na trh pouze toho členského státu týmu CSIRT, který obdržel oznámení jako první.

(8) Komise během přípravy návrhu aktu v přenesené pravomoci konzultovala příslušné zúčastněné strany a požádala je o stanovisko a konzultovala expertní skupinu pro kybernetickou bezpečnost produktů s digitálními prvky.

(9) V souladu s čl. 14 odst. 9 nařízení (EU) 2024/2847 Komise během přípravy návrhu aktu v přenesené pravomoci úzce spolupracovala se sítí CSIRT zřízenou podle článku 15 směrnice (EU) 2022/2555 a s agenturou ENISA,

PŘIJALA TOTO NAŘÍZENÍ:

Článek 1

Předmět

Toto nařízení stanoví podmínky pro uplatňování důvodů souvisejících s kybernetickou bezpečností uvedených v čl. 16 odst. 2 nařízení (EU) 2024/2847, které umožňují týmu CSIRT určenému jako koordinátor, který obdržel oznámení jako první v souladu s čl. 14 odst. 1 a 3 a čl. 15 odst. 1 a 2 uvedeného nařízení, aby odložil zaslání oznámení týmům CSIRT určeným jako koordinátoři, na jejichž území byl podle informací výrobce produkt s digitálními prvky zpřístupněn.

Článek 2

Definice

Pro účely tohoto nařízení se rozumí:

1) „týmem CSIRT, který obdržel oznámení jako první“ tým CSIRT určený jako koordinátor, který obdržel oznámení jako první v souladu s čl. 14 odst. 1 a 3 a čl. 15 odst. 1 a 2 nařízení (EU) 2024/2847;

2) „příslušným týmem CSIRT“ tým CSIRT určený jako koordinátor, na jehož území byl podle informací výrobce zpřístupněn produkt s digitálními prvky.

Článek 3

Podmínky pro uplatňování důvodů souvisejících s kybernetickou bezpečností vyplývajících z povahy oznamovaných informací

Tým CSIRT, který obdržel oznámení jako první, se může rozhodnout, že na nezbytně nutnou dobu odloží rozesílání oznámení nebo jejich částí příslušným týmům CSIRT v případech, kdy s ohledem na citlivost oznámených informací kybernetická bezpečnostní rizika, která rozesílání oznámení představuje, převažují nad jeho bezpečnostními přínosy a tato rizika nelze zmírnit zavedením omezení týkajících se zpracování nebo dalšího sdílení oznámení prostřednictvím vhodných protokolů, jako je TLP protokol (semaforový protokol) nebo PAP protokol („Permissible Actions Protocol“), a v případě, že je splněna alespoň jedna z těchto podmínek:

a) výrobce informoval tým CSIRT, který obdržel oznámení jako první, že se očekává, že do 72 hodin bude k dispozici účinné opatření ke zmírnění rizik, jako je bezpečnostní aktualizace nebo pokyny pro uživatele; pokud účinné opatření ke zmírnění rizika není k dispozici v této lhůtě, tým CSIRT, který obdržel oznámení jako první, toto oznámení zašle příslušným týmům CSIRT;

b) informace obsažené v oznámení jsou s ohledem na povahu oznámené aktivně zneužívané zranitelnosti považovány za dostatečné k vytvoření techniky zneužívání, zejména pokud zranitelnost mohou snadno identifikovat a zneužít subjekty s omezenými dovednostmi a zdroji; jakmile je k dispozici účinné opatření ke zmírnění rizik, jako je bezpečnostní aktualizace nebo pokyny pro uživatele, tým CSIRT, který obdržel oznámení jako první, toto oznámení zašle příslušným týmům CSIRT;

c) tým CSIRT, který obdržel oznámení jako první, je schopen s příslušnými týmy CSIRT sdílet dostatečné informace, aby bylo zajištěno, že příslušné týmy CSIRT mohou zavést odpovídající opatření ke zmírnění rizik; jakmile je k dispozici účinné opatření ke zmírnění rizik, jako je bezpečnostní aktualizace nebo pokyny pro uživatele, tým CSIRT, který obdržel oznámení jako první, zašle příslušným týmům CSIRT úplné oznámení;

d) tým CSIRT, který obdržel oznámení o aktivně zneužívané zranitelnosti jako první, byl o této skutečnosti informován v rámci koordinovaného zveřejňování zranitelností, v souvislosti s nímž tento tým CSIRT vystupuje jako důvěryhodný zprostředkovatel v souladu s čl. 12 odst. 1 směrnice (EU) 2022/2555; v takovém případě a v souladu s čl. 16 odst. 6 nařízení (EU) 2024/2847 tým CSIRT, který obdržel oznámení jako první, toto oznámení zašle příslušným týmům CSIRT, pokud odklad již není nezbytně nutný a pokud získal souhlas stran zapojených do koordinovaného zveřejňování zranitelností se zveřejněním.

Článek 4

Podmínky pro uplatňování důvodů souvisejících s kybernetickou bezpečností, pokud jde o konkrétní tým CSIRT

Tým CSIRT, který obdržel oznámení jako první, se může rozhodnout, že na nezbytně nutnou dobu odloží zaslání oznámení nebo jejich částí konkrétnímu příslušnému týmu CSIRT, a to v případech, kdy:

a) byl příslušný tým CSIRT zasažen kybernetickým bezpečnostním incidentem, což zpochybnilo jeho schopnost zajistit důvěrnost oznámených informací;

b) má dostatečný důvod se domnívat, že schopnosti příslušného týmu CSIRT nejsou dostatečné k zajištění důvěrnosti oznámených informací.

V případech uvedených v prvním pododstavci písm. a) může tým CSIRT, který obdržel oznámení jako první, odložit zaslání oznámení, dokud příslušný tým CSIRT neinformuje síť CSIRT uvedenou v článku 15 směrnice 2022/2555, že byla obnovena jeho schopnost zajistit důvěrnost oznámení.

V případech uvedených v prvním pododstavci písm. b) může tým CSIRT, který obdržel oznámení jako první, odložit zaslání oznámení příslušnému týmu CSIRT, dokud tento tým CSIRT neposkytne důkazy o tom, že zjištěné nedostatky vyřešil.

Článek 5

Podmínky pro uplatňování důvodů souvisejících s kybernetickou bezpečností, pokud jde o jednotnou platformu pro podávání zpráv

Tým CSIRT, který obdržel oznámení jako první, se může rozhodnout odložit jeho rozesílání prostřednictvím jednotné platformy pro podávání zpráv zřízené článkem 16 nařízení (EU) 2024/2847, pokud agentura ENISA v souladu s čl. 16 odst. 4 uvedeného nařízení informovala síť CSIRT o tom, že jednotná platforma pro podávání zpráv byla zasažena kybernetickým bezpečnostním incidentem, což zpochybnilo její schopnost zajistit důvěrnost oznámených informací. V takových případech může tým CSIRT, který obdržel oznámení jako první, odložit jeho rozesílání prostřednictvím jednotné platformy pro podávání zpráv, dokud agentura ENISA neinformuje síť CSIRT o tom, že byla obnovena schopnost platformy zajistit důvěrnost oznámení.

Článek 6

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 Bruselu dne 11.12.2025

Za Komisi
předsedkyně
Ursula VON DER LEYEN