Rada
Evropské unie

Brusel 22. března 2022
(OR. en)

7474/22

Interinstitucionální spis:
2022/0085(COD)

CYBER 93
TELECOM 116
JAI 383
INST 89
INF 32
CSC 119
CSCI 39
DATAPROTECT 81
FIN 353
BUDGET 2
CODEC 349
IA 30

NÁVRH

Odesílatel:	Martine DEPREZOVÁ, ředitelka, za generální tajemnici Evropské komise
Datum přijetí:	22. března 2022
Příjemce:	Jeppe TRANHOLM-MIKKELSEN, generální tajemník Rady Evropské unie
Č. dok. Komise:	COM(2022) 122 final
Předmět:	Návrh NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY, kterým se stanoví opatření k zajištění vysoké společné úrovně kybernetické bezpečnosti v orgánech, institucích a jiných subjektech Unie

Delegace naleznou v příloze dokument COM(2022) 122 final.

Příloha: COM(2022) 122 final

EVROPSKÁ
KOMISE

V Bruselu dne 22.3.2022
COM(2022) 122 final

2022/0085 (COD)

Návrh

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY,

kterým se stanoví opatření k zajištění vysoké společné úrovně kybernetické bezpečnosti v orgánech, institucích a jiných subjektech Unie

{SWD(2022) 67 final} - {SWD(2022) 68 final}

DŮVODOVÁ ZPRÁVA

1. SOUVISLOSTI NÁVRHU

• Odůvodnění a cíle návrhu

Tento návrh stanoví rámec pro zajištění společných pravidel a opatření k zajištění kybernetické bezpečnosti v orgánech, institucích a jiných subjektech Unie. Jeho cílem je další zvýšení odolnosti všech subjektů a jejich schopnosti reagovat na incidenty. Je v souladu s prioritami Evropské komise připravit Evropu na digitální věk a vybudovat hospodářství připravené na budoucnost, které bude pracovat pro lidi. Zajištění bezpečné a odolné veřejné správy je navíc základem digitální transformace celé společnosti.

Tento návrh navazuje na strategii bezpečnostní Unie EU (COM(2020) 605 final) a na strategii kybernetické bezpečnosti EU pro digitální dekádu (JOIN(2020) 18 final).

Návrh modernizuje stávající právní rámec CERT-EU a zohledňuje změny a nárůst digitalizace orgánů, institucí a jiných subjektů v posledních letech, jakož i vyvíjející se prostředí kybernetických bezpečnostních hrozeb. Oba vývojové trendy od vypuknutí krize COVID-19 dále zesílily, přičemž počet incidentů dále narůstá a útoky přicházející z celé řady zdrojů jsou stále sofistikovanější.

Návrh přejmenovává CERT-EU z „týmu pro reakci na počítačové hrozby“ na „centrum pro kybernetickou bezpečnost“ orgánů, institucí a jiných subjektů Unie v souladu s vývojem v členských státech a ve světovém měřítku, kdy se mnohé týmy CERT přejmenovávají na centra pro kybernetickou bezpečnost, avšak ponechává zkrácený název „CERT-EU“, který je již známý.

• Soulad s platnými předpisy v této oblasti politiky

Tento návrh je zaměřen na zvýšení kybernetické odolnosti orgánů, institucí a jiných subjektů Unie proti kybernetickým hrozbám, přičemž je sladěn se stávajícími právními předpisy:

- směrnicí (EU) 2016/1148 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii. Je také sladěn s návrhem směrnice (EU) XXXX/XXXX o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o zrušení směrnice (EU) 2016/1148 (návrh směrnice NIS 2),
- nařízením (EU) 2019/881 o agentuře ENISA (Agentuře Evropské unie pro kybernetickou bezpečnost) a o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií (akt o kybernetické bezpečnosti),
- návrhem nařízení (EU) XXXX/XXXX o bezpečnosti informací v orgánech, institucích a jiných subjektech Unie.
- doporučením Komise (EU) ze dne 23. června 2021 o vybudování společné kybernetické jednotky,
- doporučením Komise (EU) 2017/1584 ze dne 13. září 2017 o koordinované reakci na rozsáhlé kybernetické bezpečnostní incidenty a krize.

Příloha doporučení Komise (EU) 2017/1584 ze dne 13. září 2017 o koordinované reakci na rozsáhlé kybernetické bezpečnostní incidenty a krize stanoví plán koordinované reakce na rozsáhlé přeshraniční kybernetické bezpečnostní incidenty a krize.

Rada Evropské unie ve svém usnesení ze dne 9. března 2021 zdůraznila, že kybernetická bezpečnost má zásadní význam pro fungování veřejné správy na vnitrostátní úrovni i na úrovni EU, jakož i pro celou společnost a hospodářství, a zdůraznila důležitost robustního a

jednotného bezpečnostního rámce k ochraně všech zaměstnanců, dat, komunikačních sítí a informačních systémů v EU a rozhodovacích procesů. Toho lze dosáhnout zejména prostřednictvím větší odolnosti a lepší bezpečnostní kultury orgánů, institucí a jiných subjektů Unie. Je třeba zpřístupnit dostatečné zdroje a kapacity, a to i v souvislosti s posílením mandátu centra CERT-EU.

2. PRÁVNÍ ZÁKLAD, SUBSIDIARITA A PROPORCIONALITA

• Právní základ

Právním základem pro toto nařízení je článek 298 Smlouvy o fungování Evropské unie (dále jen „Smlouva o fungování EU“), který stanoví, že při plnění svých úkolů se orgány, instituce a jiné subjekty Unie opírají o otevřenou, efektivní a nezávislou evropskou správu. V souladu se služebním řádem a pracovním řádem přijatými na základě článku 336 přijmou Evropský parlament a Rada řádným legislativním postupem formou nařízení za tímto účelem ustanovení.

Informační technologie poskytly orgánům, institucím a jiným subjektům Unie nové možnosti, jak pracovat a komunikovat s občany a zlepšovat celkovou činnost. Ruku v ruce s pokračujícím rozvojem technologií se vyvíjí i prostředí kybernetických hrozeb. Orgány, instituce a jiné subjekty Unie se staly vysoce atraktivními cíli sofistikovaných kybernetických útoků. Zdá se, že zavádění systémů a požadavků na zajištění kybernetické bezpečnosti přispívá k efektivitě a nezávislosti evropské správy, takže orgány, instituce a jiné subjekty Unie mohou při plnění svých úkolů v digitálním světě fungovat efektivněji.

Dalšími překážkami pro otevřenou, efektivní a nezávislou evropskou správu jsou navíc stávající rozdíly mezi postoji a přístupy orgánů, institucí a jiných subjektů Unie v oblasti kybernetické bezpečnosti, jak je uvedeno níže v oddíle 3. Bez společného přístupu by se postoje orgánů, institucí a jiných subjektů Unie ke kybernetické bezpečnosti i nadále vyvíjely v různých směrech. Tento právní základ je proto vhodný vzhledem k tomu, že cílem nařízení je vytvořit společný právní rámec pro kybernetickou bezpečnost v rámci orgánů, institucí a jiných subjektů Unie.

• Subsidiarita

Nařízení, kterým se stanoví opatření k zajištění vysoké společné úrovně kybernetické bezpečnosti pro všechny orgány, instituce a jiné subjekty Unie, spadá do výlučné pravomoci Unie.

• Proporcionalita

Pravidla navrhovaná v tomto nařízení nepřekračují rámec toho, co je nezbytné pro uspokojivé dosažení specifických cílů. Předpokládaná opatření přispějí k dosažení vysoké společné úrovně kybernetické bezpečnosti, aniž by přesahovala rámec toho, co je nezbytné pro dosažení tohoto cíle vzhledem ke stále větším rizikům, kterým čelí.

• Volba nástroje

Volba nařízení, které je přímo použitelné, se považuje za vhodný právní nástroj pro vymezení a zefektivnění povinností uložených orgánům, institucím a jiným subjektům Unie. Aby byla umožněna cílená zlepšení, je nejvhodnějším právním nástrojem nařízení.

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

- **Hodnocení *ex ante***

Centrum CERT-EU provedlo posouzení hlavních kybernetických hrozeb, jimž jsou orgány, instituce a jiné subjekty Unie v současnosti vystaveny nebo je pravděpodobné, že jim budou vystaveny v dohledné budoucnosti.

V analýze byly použity tři kategorie pozorování:

- pokusy narušit IT infrastrukturu orgánů, institucí a jiných subjektů Unie (pokud jsou úspěšné, je s nimi zacházeno jako s incidenty, v ostatních případech jsou přesto zaznamenány jako zjištěné pokusy),
- hrozby zjištěné v blízkosti orgánů, institucí a jiných subjektů Unie (např. v odvětvích s nimi souvisejících, v komunitách jejich zúčastněných stran nebo v Evropě),
- hlavní trendy pozorované ve světovém měřítku.

Analýza dále posoudila, jak významné probíhající změny ovlivňují způsoby, jimiž orgány a instituce Unie spravují a využívají svou infrastrukturu a služby v oblasti informačních technologií. Tyto změny zahrnují:

- zvýšení podílu práce na dálku,
- migraci systémů do cloudu,
- zvýšené zadávání služeb informačních technologií externím subjektům.

V období od roku 2019 do roku 2021 se prudce zvýšil počet významných incidentů[1] postihujících orgány, instituce a subjekty Unie, jejichž původci byli aktéři pokročilé trvalé hrozby (APT). V první polovině roku 2021 došlo ke stejnému počtu významných incidentů jako za celý rok 2020. To se rovněž odrazilo v počtu bitových kopií pro forenzní analýzu (snímků obsahu dotčených systémů nebo zařízení), které analyzovalo centrum CERT-EU v roce 2020; tento počet se ve srovnání s rokem 2019 ztrojnásobil, přičemž počet významných incidentů se od roku 2018 zvýšil více než desetinásobně.

V roce 2020 řídící rada CERT-EU stanovila pro CERT-EU nový strategický cíl zajistit pro všechny orgány, instituce a jiné subjekty komplexní úroveň kybernetické obrany s vhodnou šířkou a hloubkou a s neustálým přizpůsobováním se aktuálním nebo potenciálním hrozbám, včetně útoků zaměřených na mobilní zařízení, prostředí cloudu a zařízení internetu věcí.

Jako doplněk k analýze hrozeb týmem CERT-EU provedla Komise hodnocení kybernetické bezpečnosti fungující ve dvaceti orgánech, institucích a jiných subjektech Unie. To poskytlo představu o zavedených postupech v oblasti kybernetické bezpečnosti a schopnostech řízení kybernetické bezpečnosti v porovnání s externími referenčními hodnotami některých technických bezpečnostních kontrol.

Toto hodnocení vycházelo z dotazníků, na něž tyto orgány, instituce a jiné subjekty odpověděly, z veřejně dostupných údajů a údajů poskytnutých přímo samotnými orgány, institucemi a jinými subjekty Unie. To poskytuje dostatečnou představu o současné situaci, aby bylo možné dospět k níže uvedeným závěrům:

[1] „Významným incidentem“ se rozumí jakýkoli incident, pokud nemá omezený dopad a není pravděpodobné, že je již dobře znám z hlediska metody nebo technologie.

- Vyspělost kybernetického zabezpečení, velikost infrastruktury informačních technologií a úroveň schopností se u hodnocených orgánů, institucí a jiných subjektů Unie podstatně liší.
- Zatímco mnohé orgány, instituce a jiné subjekty Unie mají zpravidla vyspělé schopnosti odhalování a reakce, jejich schopnosti v oblasti správy kybernetické bezpečnosti vykazují různé úrovně integrovaného řízení rizik.
- Zatímco rámce pro kybernetickou bezpečnost (strategický, politický a předpisový) hodnocených orgánů, institucí a jiných subjektů Unie jsou v klíčových oblastech kybernetické bezpečnosti, uvedených v příloze I tohoto nařízení, celkově dobře zavedeny, v některých orgánech, institucích a jiných subjektech Unie chybí vyspělé řízení kontinuity provozu, kontrola dodržování předpisů, audit a neustálé zlepšování.
- Bylo shledáno, že technická opatření považovaná za osvědčené postupy jsou hodnocenými orgány, institucemi a jinými subjekty Unie uplatňována nerovnoměrně.

Souhrnně lze říci, že z analýzy dvaceti orgánů, institucí a jiných subjektů Unie vyplývá, že jejich správa, kybernetická hygiena, celková schopnost a vyspělost se značně liší. Požadavek, aby všechny orgány, instituce a jiné subjekty Unie prováděly určitá základní opatření k zajištění kybernetické bezpečnosti, proto pomůže tuto rozdílnou vyspělost řešit a dostat všechny orgány, instituce a jiné subjekty Unie na vysokou společnou úroveň kybernetické bezpečnosti.

Žádný právní předpis Unie se dosud nezaměřil na kybernetickou bezpečnost orgánů, institucí a jiných subjektů Unie a komplexně se nezabýval prostředím kybernetických bezpečnostních hrozeb a nově vznikajícími riziky v oblasti informačních technologií vyplývajícími z digitalizace.

- **Konzultace se zúčastněnými stranami**

Komise provedla konzultace se zúčastněnými stranami ve všech orgánech, institucích a jiných subjektech Unie, jakož i se zástupci členských států v Radě a zúčastněnými stranami v Evropském parlamentu. Dne 25. června 2021 se zástupci členských států a příslušné zúčastněné strany z orgánů, institucí a jiných subjektů Unie zúčastnili pracovního setkání zorganizovaného Komisí, kde diskutovali o obsahu budoucího návrhu nařízení.

- **Posouzení dopadů**

Tento návrh bude mít dopad na orgány, instituce a jiné subjekty Unie. Zvláštní posouzení dopadů tak není nutné, neboť se nebude vztahovat na členské státy.

- **Základní práva**

Evropská unie je odhodlána zajistit přísné normy ochrany základních práv. Veškeré sdílení informací mezi subjekty vyplývající z tohoto nařízení by se provádělo v atmosféře důvěry, při plném dodržování práva na ochranu osobních údajů stanoveného v článku 8 Listiny základních práv Evropské unie a v příslušných právních předpisech pro ochranu údajů, a zejména v nařízení Evropského parlamentu a Rady (EU) 2018/1725.

4. ROZPOČTOVÉ DŮSLEDKY

Z tržních referenčních hodnot a studií[2] vyplývá, že přímé výdaje na kybernetickou bezpečnost se obvykle pohybují mezi 4 a 7 % celkových výdajů organizací na informační technologie. Analýza rizik provedená týmem CERT-EU na podporu tohoto legislativního návrhu však naznačuje, že mezinárodní subjekty a politické organizace jsou vystaveny zvýšeným rizikům, a proto by se jako přiměřenější cíl jevila úroveň výdajů na kybernetickou bezpečnost ve výši 10 % výdajů na informační technologie. Přesné náklady takového úsilí není možné určit kvůli nedostatku podrobných informací o výdajích orgánů, institucí a jiných subjektů Unie na informační technologie a příslušném podílu výdajů na kybernetickou bezpečnost.

Ačkoli je proto pravděpodobné, že mnohé orgány, instituce a jiné subjekty Unie vynakládají na kybernetickou bezpečnost méně, než by měly, toto nařízení samo o sobě zvýšení těchto běžných výdajů nezpůsobí. I bez nařízení by každý subjekt musel odpovídající úroveň kybernetické bezpečnosti zajistit. Nařízení pokračuje v předchozí spolupráci v řídícím výboru týmu CERT-EU a formalizuje úroveň výměny informací, která již dnes částečně existuje. Jak je podrobně uvedeno v legislativním finančním výkazu, centrum CERT-EU bude potřebovat dodatečné zdroje, aby mohlo plnit svou rozšířenou úlohu, a tyto zdroje by měly být přerozděleny z orgánů, institucí a jiných subjektů Unie, které služeb týmu CERT-EU využívají.

5. OSTATNÍ PRVKY

- **Provádění, monitorování, hodnocení a podávání zpráv**

Interinstitucionální výbor pro kybernetickou bezpečnost (IICB) by měl za pomoci týmu CERT-EU přezkoumat fungování tohoto nařízení, provést hodnocení a předložit Komisi zprávu se svými zjištěními. Komise by měla zajistit podávání pravidelných zpráv Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů.

Centrum CERT-EU může vypracovávat návrhy pokynů nebo doporučení, které se výbor IICB může rozhodnout přijmout. Pokyny jsou poradenský materiál určený všem orgánům, institucím a jiným subjektům Unie nebo jejich podmnožině, zatímco doporučení je určeno jednotlivým orgánům, institucím a jiným subjektům Unie. Výzva k přijetí opatření je poradenský materiál centra CERT-EU, který popisuje naléhavá bezpečnostní opatření, a orgány, instituce a jiné subjekty Unie se naléhavě vyzývají, aby ve stanovené lhůtě tato opatření přijaly.

- **Podrobné vysvětlení konkrétních ustanovení návrhu**

Obecná ustanovení

Nařízení stanoví opatření s cílem zajistit vysokou společnou úroveň kybernetické bezpečnosti a vztahuje se na orgány, instituce a jiné subjekty Unie s cílem umožnit jim plnění jejich příslušných úkolů otevřeným, efektivním a nezávislým způsobem. (články 1–3, 23–25).

Opatření k zajištění vysoké společné úrovně kybernetické bezpečnosti

[2] Zdroj: Gartner, „Identifying the Real Information Security Budget“ (Určení skutečného rozpočtu na bezpečnost informací) (2016). To je třeba přičíst k nepřímým výdajům na bezpečnost informačních technologií, např. na zabezpečení sítě, jako jsou firewally, antivirový software a povinnosti vlastníka systému, jako je posuzování rizik a provádění bezpečnostních kontrol. Materiál z roku 2020 uvádí výdaje na kybernetickou bezpečnost ve finančních institucích ve výši 10–11 % výdajů v oblasti informačních technologií, zdroj: DI_2020-FS-ISAC-Cybersecurity.pdf (deloitte.com).

Orgány, instituce a jiné subjekty Unie jsou povinny zavést interní rámec pro řízení, správu a kontrolu kybernetických bezpečnostních rizik, který zajistí účinné a obezřetné řízení všech bezpečnostních rizik. Orgány, instituce a jiné subjekty Unie kromě toho musí přijmout základní soubor opatření k zajištění kybernetické bezpečnosti pro řešení rizik zjištěných podle tohoto rámce, provádět pravidelná hodnocení vyspělosti kybernetické bezpečnosti a přijmout plán kybernetické bezpečnosti. (články 4–8)

Interinstitucionální výbor pro kybernetickou bezpečnost

Zřizuje se Interinstitucionální výbor pro kybernetickou bezpečnost, který je odpovědný za sledování provádění tohoto nařízení orgány, institucemi a jinými subjekty Unie, jakož i za dohled nad plněním obecných priorit a cílů centrem CERT-EU a poskytování strategického řízení centru CERT-EU. (články 9–11)

Centrum CERT-EU

Centrum CERT-EU přispívá k bezpečnosti prostředí informačních technologií ve všech orgánech, institucích a jiných subjektech Unie, a to tak, že jim poskytuje poradenství, pomáhá jim předcházet incidentům, odhalovat incidenty, zmírňovat incidenty a reagovat na incidenty a působí jako středisko pro výměnu informací v oblasti kybernetické bezpečnosti a pro koordinaci reakcí na incidenty. (články 12-17)

Povinnosti v oblasti spolupráce a oznamovací povinnosti

Nařízení zajišťuje spolupráci a výměnu informací mezi centrem CERT-EU a orgány, institucemi a jinými subjekty Unie s cílem rozvíjet vzájemnou důvěru. Za tímto účelem může centrum CERT-EU požádat orgány, instituce a jiné subjekty Unie, aby mu poskytly příslušné informace, a centrum CERT-EU si může s orgány, institucemi a jinými subjekty Unie vyměňovat informace o incidentech s cílem usnadnit odhalování podobných kybernetických hrozeb nebo incidentů, a to bez souhlasu dotčeného zúčastněného subjektu. Informace týkající se konkrétních incidentů, které odhalují totožnost cíle kybernetického bezpečnostního incidentu, si může centrum CERT-EU vyměňovat pouze se souhlasem dotčeného zúčastněného subjektu.

Všechny orgány, instituce a jiné subjekty Unie musí centru CERT-EU oznamovat zejména významné kybernetické hrozby, významná zranitelná místa a významné incidenty, a to bez zbytečného odkladu, v každém případě do 24 hodin poté, co se o nich dozvěděly. (články 18-22)

2022/0085 (COD)

Návrh

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY,

kterým se stanoví opatření k zajištění vysoké společné úrovně kybernetické bezpečnosti v orgánech, institucích a jiných subjektech Unie

EVROPSKÝ PARLAMENT A RADA EVROPSKÉ UNIE,

s ohledem na Smlouvu o fungování Evropské unie, a zejména na článek 298 této smlouvy,

s ohledem na Smlouvu o založení Evropského společenství pro atomovou energii, a zejména na článek 106a této smlouvy,

s ohledem na návrh Evropské komise,

po předložení návrhu legislativního aktu vnitrostátním parlamentům,

v souladu s řádným legislativním postupem,

vzhledem k těmto důvodům:

(1) V digitálním věku tvoří informační a komunikační technologie základ otevřené, efektivní a nezávislé unijní správy. Vyvíjející se technologie a větší složitost a vzájemná propojenost digitálních systémů zesilují kybernetická bezpečnostní rizika, což činí unijní správu zranitelnější vůči kybernetickým hrozbám a incidentům, které v konečném důsledku ohrožují kontinuitu činností správy a schopnost zabezpečovat její data. Širší využívání služeb cloudu, všudypřítomné používání informačních technologií, vysoká úroveň digitalizace, práce na dálku a vyvíjející se technologie a propojenost jsou nyní základními prvky všech činností správních subjektů v Unii, zatím však není dostatečně vybudována digitální odolnost.

(2) Prostředí kybernetických hrozeb, v němž působí orgány, instituce a jiné subjekty Unie, se neustále vyvíjí. Taktika, metody a postupy používané aktéry hrozeb se neustále vyvíjejí, avšak hlavní motivy takových útoků se nijak výrazně nemění, a to od krádeže cenných neveřejných informací přes získání finančních prostředků a manipulaci s veřejným míněním až po narušení digitální infrastruktury. Tempo, jímž provádějí své kybernetické útoky, se stále zvyšuje, přičemž jejich kampaně jsou stále sofistikovanější a automatizovanější, zaměřují se na exponované prostory k útoku, které se stále rozšiřují, a rychle využívají zranitelná místa.

(3) V prostředí informačních technologií orgánů, institucí a jiných subjektů Unie existují vzájemné závislosti a integrované toky dat a jejich uživatelé spolu úzce spolupracují. Tato vzájemná propojenost znamená, že jakékoli narušení, a dokonce i takové narušení, které je původně omezeno na jeden orgán, instituci nebo jiný subjekt Unie, může mít širší dominové účinky, jež mohou potenciálně vést k dalekosáhlým negativním dopadům na ostatní. Prostředí informačních technologií některých orgánů, institucí nebo jiných subjektů je navíc propojeno s informačním prostředím členských států, z čehož vyplývá, že incident v rámci jednoho subjektu Unie představuje riziko pro kybernetickou bezpečnost prostředí informačních technologií členských států, a naopak.

(4) Orgány, instituce a jiné subjekty Unie jsou atraktivní cíle, které musejí čelit vysoce kvalifikovaným a dobře finančně zajištěným aktérům hrozeb, jakož i jiným hrozbám. Přitom úroveň a vyspělost kybernetické odolnosti a schopnost odhalovat nepřátelské činnosti v kyberprostoru a reagovat na ně se u zmíněných subjektů značně liší. Pro fungování evropské správy je tak nezbytné, aby orgány, instituce a jiné subjekty Unie dosáhly vysoké společné úrovně kybernetické bezpečnosti prostřednictvím základní úrovně kybernetické bezpečnosti (soubor minimálních pravidel k zajištění kybernetické bezpečnosti, s nimiž musí být sítě a informační systémy v souladu, aby se minimalizovala kybernetická bezpečnostní rizika), výměny informací a spolupráce.

(5) Cílem směrnice [návrhu směrnice NIS 2] o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii je dále zlepšit odolnost veřejných a soukromých subjektů, příslušných vnitrostátních orgánů a subjektů, jakož i Unie jako celku v oblasti kybernetické bezpečnosti i jejich schopnosti reagovat na bezpečnostní incidenty. Je proto nezbytné, aby se zapojily i orgány, instituce a jiné subjekty Unie tím, že zajistí pravidla, která jsou v souladu se směrnicí [návrhem směrnice NIS 2] a odrážejí míru jejích ambicí.

(6) K dosažení vysoké společné úrovně kybernetické bezpečnosti je nezbytné, aby všechny orgány, instituce a jiné subjekty Unie zavedly interní rámec pro řízení, správu a kontrolu kybernetických bezpečnostních rizik, který zajistí účinné a obezřetné řízení všech kybernetických bezpečnostních rizik a zohlední řízení kontinuity činností a krizové řízení.

(7) Rozdíly mezi orgány, institucemi a jinými subjekty Unii vyžadují pružnost při provádění, protože univerzální řešení nebude vyhovovat všem. Opatření k zajištění vysoké společné úrovně kybernetické bezpečnosti by neměla obsahovat žádné povinnosti přímo zasahující do plnění úkolů orgánů, institucí nebo jiných subjektů Unie nebo narušující jejich institucionální autonomii. Tyto orgány, instituce a jiné subjekty by tak měly zavést své vlastní rámce pro řízení, správu a kontrolu kybernetických bezpečnostních rizik a přijmout své vlastní základní soubory opatření k zajištění kybernetické bezpečnosti a plány kybernetické bezpečnosti.

(8) Požadavky na řízení kybernetických bezpečnostních rizik by měly být úměrné rizikům, jež daná síť nebo informační systém obnáší, aby na orgány, instituce nebo jiné subjekty Unie nebyla uvalena nepřiměřená finanční a administrativní zátěž, a to s ohledem na nejnovější technický vývoj takových opatření. Cílem každého orgánu, instituce a jiného subjektu Unie by mělo být, aby přiměřenou část svého rozpočtu na informační technologie vynaložily na zlepšení úrovně své kybernetické bezpečnosti; z dlouhodobého hlediska by měl být sledován cíl v řádu 10 %.

(9) Vyšší společná úroveň kybernetické bezpečnosti vyžaduje, aby dohled nad kybernetickou bezpečností přešel na nejvyšší úroveň vedení každého orgánu, instituce nebo jiného subjektu Unie, které by mělo schválit základní soubor opatření k zajištění kybernetické bezpečnosti, který by měl řešit rizika zjištěná v rámci, jenž má být každým orgánem, institucí nebo jiným subjektem zaveden. Nedílnou součásti základního souboru opatření k zajištění kybernetické bezpečnosti ve všech orgánech, institucích a jiných subjektech Unie je řešení kultury kybernetické bezpečnosti, tedy každodenní praxe v oblasti kybernetické bezpečnosti.

(10) Orgány, instituce a jiné subjekty Unie by měly posuzovat rizika související se vztahy s dodavateli a poskytovateli služeb, včetně poskytovatelů služeb ukládání a zpracování dat nebo řízených bezpečnostních služeb, a přijímat vhodná opatření k řešení těchto rizik. Tato opatření by měla být součástí základního souboru opatření k zajištění

kybernetické bezpečnosti a měla by být dále upřesněna v pokynech nebo doporučeních centra CERT-EU. Při stanovení opatření a pokynů by měly být náležitě zohledněny příslušné právní předpisy a politiky EU, včetně posouzení rizik a doporučení vydávaných skupinou pro spolupráci v oblasti bezpečnosti sítí a informací (skupinou NIS), jako je koordinované posouzení rizik v EU a souboru opatření EU pro kybernetickou bezpečnost sítí 5G. Mohla by být rovněž vyžadována certifikace příslušných produktů, služeb a procesů IKT, a to v rámci konkrétních evropských systémů certifikace kybernetické bezpečnosti přijatých podle článku 49 nařízení (EU) 2019/881.

(11) Generální tajemníci orgánů a institucí Unie se v květnu 2011 rozhodli zřídit přípravný tým pro vytvoření týmu pro reakci na počítačové hrozby pro orgány, instituce a jiné subjekty Unie (centrum CERT-EU), na který bude dohlížet interinstitucionální řídící rada. V červenci 2012 potvrdili generální tajemníci praktická ujednání a dohodli se na tom, že centrum CERT-EU zůstane zachováno jako trvalý subjekt, který bude nadále napomáhat zvyšování celkové úrovně bezpečnosti v oblasti informačních technologií v rámci orgánů, institucí a jiných subjektů Unie jakožto příklad viditelné interinstitucionální spolupráce v oblasti kybernetické bezpečnosti. V září 2012 byl CERT-EU založen jako pracovní skupina Evropské komise s interinstitucionálním mandátem. V prosinci 2017 uzavřely orgány a instituce Unie interinstitucionální ujednání o organizaci a provozu CERT-EU[3]. Toto ujednání by se mělo dále vyvíjet s cílem podpořit provádění tohoto nařízení.

(12) CERT-EU by měl být přejmenován z „týmu pro reakci na počítačové hrozby“ na „centrum pro kybernetickou bezpečnost“ orgánů, institucí a jiných subjektů Unie v souladu s vývojem v členských státech a ve světovém měřítku, kdy se mnohé týmy CERT přejmenovávají na centra pro kybernetickou bezpečnost, avšak měl by si ponechat zkrácený název „CERT-EU“, který je již známý.

(13) Mnohé kybernetické útoky jsou součástí širších kampaní, které cílí na skupiny orgánů, institucí a jiných subjektů Unie nebo na zájmové komunity, jež orgány, instituce a jiné subjekty Unie zahrnují. S cílem umožnit aktivní odhalování incidentů, reakci na incidenty nebo opatření ke zmírnění dopadů incidentů by orgány, instituce a jiné subjekty Unie měly centru CERT-EU oznamovat významné kybernetické hrozby, významná zranitelná místa a významné incidenty a sdílet vhodné technické podrobnosti, jež umožňují odhalovat podobné kybernetické hrozby v rámci jiných orgánů, institucí a jiných subjektů Unie, zmírňovat dopady takových hrozeb a na tyto hrozby reagovat. Podle stejného přístupu, jaký se předpokládá ve směrnici [návrhu směrnice NIS 2], by subjekty, které se dozvědí o významném incidentu, měly mít povinnost předložit centru CERT-EU počáteční oznámení do 24 hodin. Taková výměna informací by měla centru CERT-EU umožnit šířit tyto informace do jiných orgánů, institucí nebo jiných subjektů Unie, jakož i vhodným protějškům, s cílem pomoci chránit prostředí informačních technologií Unie a prostředí informačních prostředí protějšků Unie před podobnými incidenty, hrozbami a zranitelnými místy.

(14) Kromě uložení více úkolů centru CERT-EU a rozšíření jeho úlohy by měl být zřízen Interinstitucionální výbor pro kybernetickou bezpečnost (IICB), který by měl usnadňovat dosažení vysoké společné úrovně kybernetické bezpečnosti u orgánů, institucí a jiných subjektů Unie tak, že bude sledovat provádění tohoto nařízení ze strany orgánů, institucí a jiných subjektů Unie, dohlížet na plnění obecných priorit a

[3] Úř. věst. C 12, 13.1.2018, s. 1.

cílů centrem CERT-EU a poskytovat centru CERT-EU strategické řízení. Výbor IICB by měl zajišťovat zastoupení orgánů a zahrnovat zástupce jiných subjektů a institucí prostřednictvím sítě agentur Unie.

(15) Centrum CERT-EU by mělo podporovat provádění opatření pro zajištění vysoké společné úrovně kybernetické bezpečnosti vypracováním návrhů pokynů a doporučení předkládaných výboru IICB nebo vydáváním výzev k přijetí opatření. Tyto pokyny a doporučení by měl schvalovat výbor IICB. V případě potřeby by centrum CERT-EU mělo vydávat výzvy k přijetí opatření popisující naléhavá bezpečnostní opatření, přičemž orgány, instituce a jiné subjekty Unie se naléhavě vyzývají, aby ve stanovené lhůtě tato opatření přijaly.

(16) Výbor IICB by měl sledovat dodržování tohoto nařízení, jakož i následná opatření přijímaná v návaznosti na pokyny a doporučení a na výzvy k přijetí opatření vydávané centrem CERT-EU. V technických záležitostech by měly výbor IICB podporovat technické poradní skupiny ve složení, jež výbor IICB považuje za vhodné, které by měly dle potřeby úzce spolupracovat s centrem CERT-EU, orgány, institucemi nebo jinými subjekty Unie a dalšími zúčastněnými stranami. V případě potřeby by měl výbor IICB vydávat nezávazná varování a doporučovat audity.

(17) Úkolem centra CERT-EU by mělo být přispívat k bezpečnosti prostředí informačních technologií ve všech orgánech, institucích a jiných subjektech Unie. Centrum CERT-EU by mělo jednat jako jakýsi specializovaný koordinátor orgánů, institucí a jiných subjektů Unie pro účely koordinovaného zpřístupňování informací o zranitelných místech v evropském registru zranitelných míst podle článku 6 směrnice [návrhu směrnice NIS 2].

(18) V roce 2020 řídící rada CERT-EU stanovila pro CERT-EU nový strategický cíl zajistit pro všechny orgány, instituce a jiné subjekty Unie komplexní úroveň kybernetické obrany s vhodnou šířkou a hloubkou a s neustálým přizpůsobováním se aktuálním nebo potenciálním hrozbám, včetně útoků zaměřených na mobilní zařízení, prostředí cloudu a zařízení internetu věcí. Tento strategický cíl zahrnuje také široké spektrum bezpečnostních operačních středisek, jež monitorují sítě, a nepřetržité monitorování vysoce rizikových hrozeb. U větších orgánů, institucí a jiných subjektů Unie by centrum CERT-EU mělo podporovat jejich týmy pro bezpečnost informačních technologií, včetně nepřetržitého monitorování v první linii. Menším a některým středně velkým orgánům, institucím a jiným subjektům by centrum CERT-EU mělo poskytovat veškeré služby.

(19) Centrum CERT-EU by rovněž mělo plnit úlohu, kterou pro ně stanoví směrnice [návrh směrnice NIS 2] v oblasti spolupráce a výměny informací se sítí týmů pro reakce na počítačové bezpečnostní incidenty (týmů CSIRT). V souladu s doporučením Komise (EU) 2017/1584[4] by centrum CERT-EU kromě toho mělo spolupracovat a koordinovat reakce s příslušnými zúčastněnými stranami. Aby mohlo centrum CERT-EU přispívat k vysoké úrovni kybernetické bezpečnosti v Unii, mělo by sdílet informace týkající se konkrétních incidentů s vnitrostátními partnery. Centrum CERT-EU by mělo rovněž spolupracovat s jinými protějšky z veřejného i soukromého sektoru, včetně NATO, a to po předchozím schválení výborem IICB.

[4] Doporučení Komise (EU) 2017/1584 ze dne 13. září 2017 o koordinované reakci na rozsáhlé kybernetické bezpečnostní incidenty a krize (Úř. věst. L 239, 19.9.2017, s. 36).

(20) Při podpoře operační kybernetické bezpečnosti by centrum CERT-EU mělo využívat dostupné odborné znalosti Agentury Evropské unie pro kybernetickou bezpečnost, a to prostřednictvím strukturované spolupráce, jak stanoví nařízení Evropského parlamentu a Rady (EU) 2019/881[5]. V případě potřeby by měla být učiněna speciální ujednání mezi oběma subjekty o praktické podobě takové spolupráce a mělo by se zabránit zdvojování činností. Centrum CERT-EU by mělo spolupracovat s Agenturou Evropské unie pro kybernetickou bezpečnost při analýze hrozeb a pravidelně s touto agenturou sdílet svou zprávu o prostředí hrozeb.

(21) Při podpoře Společné kybernetické jednotky vybudované v souladu s doporučením Komise ze dne 23. června 2021[6] by centrum CERT-EU mělo spolupracovat a vyměňovat si informace se zúčastněnými stranami s cílem podpořit operační spolupráci a umožnit stávajícím sítím realizovat jejich plný potenciál při ochraně Evropské unie.

(22) Veškeré osobní údaje zpracovávané v rámci tohoto nařízení by se měly zpracovávat v souladu s právními předpisy o ochraně údajů včetně nařízení Evropského parlamentu a Rady (EU) 2018/1725[7].

(23) Nakládání s informacemi ze strany centra CERT-EU a orgánů, institucí a jiných subjektů Unie by mělo být v souladu s pravidly stanovenými v nařízení [navrhovaném nařízení o zajištění bezpečnosti informací]. S cílem zajistit koordinaci ohledně bezpečnostních záležitostí by veškeré kontakty s centrem CERT-EU iniciované nebo vyžádané vnitrostátními bezpečnostními a zpravodajskými službami měly být bez zbytečného prodlení sděleny Bezpečnostnímu ředitelství Komise a předsedovi výboru IICB.

(24) Jelikož služby a úkoly centra CERT-EU jsou v zájmu všech orgánů, institucí a jiných subjektů Unie, měl by každý orgán, instituce a jiný subjekt Unie s výdaji v oblasti informačních technologií přispívat na tyto služby a úkoly spravedlivým dílem. Těmito příspěvky není dotčena rozpočtová autonomie orgánů, institucí a jiných subjektů Unie.

(25) IICB by za pomoci týmu CERT-EU měla přezkoumat a vyhodnotit provádění tohoto nařízení a měla by o svých zjištěních informovat Komisi. Na základě těchto informací by Komise měla podávat zprávy Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů,

---

[5] 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).

[6] Doporučení Komise C/2021/4520 ze dne 23. června 2021 o vybudování společné kybernetické jednotky.

[7] Nařízení Evropského parlamentu a Rady (EU) 2018/1725 ze dne 23. října 2018 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány, institucemi a jinými subjekty Unie a o volném pohybu těchto údajů a o zrušení nařízení (ES) č. 45/2001 a rozhodnutí č. 1247/2002/ES (Úř. věst. L 295, 21.11.2018, s. 39).

PŘIJALY TOTO NAŘÍZENÍ:

Kapitola I
OBECNÁ USTANOVENÍ

Článek 1
Předmět

Toto nařízení stanoví:

a) orgánům, institucím a jiným subjektům Unie povinnosti s cílem zavést interní rámec pro řízení, správu a kontrolu kybernetických bezpečnostních rizik;

b) orgánům, institucím a jiným subjektům Unie povinnosti v oblasti řízení kybernetických bezpečnostních rizik a oznamovací povinnosti;

c) pravidla týkající se organizace a provozu Centra pro kybernetickou bezpečnost orgánů, institucí a jiných subjektů Unie (CERT-EU) a organizace a provozu Interinstitucionálního výboru pro kybernetickou bezpečnost (IICB).

Článek 2
Oblast působnosti

Toto nařízení se vztahuje na řízení, správu a kontrolu kybernetických bezpečnostních rizik všemi orgány, institucemi a jinými subjekty Unie a na organizaci a provoz centra CERT-EU a Interinstitucionálního výboru pro kybernetickou bezpečnost.

Článek 3
Definice

Pro účely tohoto nařízení se rozumí:

1) „orgány, institucemi a jinými subjekty Unie“ orgány, instituce a jiné subjekty zřízené Smlouvou o Evropské unii, Smlouvou o fungování Evropské unie nebo Smlouvou o založení Evropského společenství pro atomovou energii nebo na základě uvedených smluv;

2) „sítí a informačním systémem“ síť a informační systém ve smyslu čl. 4 odst. 1 směrnice [návrh směrnice NIS 2];

3) „bezpečností sítí a informačních systémů“ bezpečnost sítí a informačních systémů ve smyslu čl. 4 odst. 2 směrnice [návrh směrnice NIS 2];

4) „kybernetickou bezpečností“ kybernetická bezpečnost ve smyslu čl. 4 odst. 3 směrnice [návrh směrnice NIS 2];

5) „nejvyšší úrovní vedení“ vedoucí, vedení nebo koordinační orgán a orgán dohledu na nejvyšší správní úrovni, odpovídající za vysokou úroveň správních opatření v každém orgánu, instituci nebo jiném subjektu Unie;

6) „incidentem“ incident ve smyslu čl. 4 odst. 5 směrnice [návrh směrnice NIS 2];

7) „významným incidentem“ jakýkoli incident, pokud nemá omezený dopad a není pravděpodobné, že je již dobře znám z hlediska metody nebo technologie;

8) „významným útokem“ každý incident vyžadující více zdrojů, než jaké jsou k dispozici v dotčeném orgánu, instituci nebo jiném subjektu Unie a v centru CERT-EU;

9) „řešením incidentu“ řešení incidentu ve smyslu čl. 4 odst. 6 směrnice [návrh směrnice NIS 2];

10) „kybernetickou hrozbou“ kybernetická hrozba ve smyslu čl. 2 odst. 8 nařízení (EU) 2019/881;

11) „významnou kybernetickou hrozbou“ kybernetická hrozba s úmyslem, příležitostí a schopností způsobit významný incident;

12) „zranitelností“ zranitelnost ve smyslu čl. 4 odst. 8 směrnice [návrh směrnice NIS 2];

13) „významnou zranitelností“ zranitelnost, která v případě zneužití pravděpodobně povede k významnému incidentu;

14) „kybernetickým bezpečnostním rizikem“ jakákoli přiměřeně rozpoznatelná okolnost nebo událost, která by mohla mít negativní dopad na bezpečnost sítí a informačních systémů;

15) „společnou kybernetickou jednotkou“ virtuální a fyzická platforma pro spolupráci různých komunit v oblasti kybernetické bezpečnosti v Unii, se zaměřením na operativní a technickou koordinaci v boji proti významným přeshraničním kybernetickým hrozbám a incidentům ve smyslu doporučení Komise ze dne 23. června 2021;

16) „základním souborem opatření k zajištění kybernetické bezpečnosti“ soubor minimálních pravidel v oblasti kybernetické bezpečnosti, která musí splňovat sítě a informační systémy a jejich provozovatelé i uživatelé, aby se minimalizovala kybernetická bezpečnostní rizika.

Kapitola II
OPATŘENÍ K ZAJIŠTĚNÍ VYSOKÉ SPOLEČNÉ ÚROVNĚ KYBERNETICKÉ BEZPEČNOSTI

Článek 4
Řízení, správa a kontrola rizik

1. Každý orgán, instituce a jiný subjekt Unie zřídí svůj vlastní interní rámec pro řízení, správu a kontrolu kybernetických bezpečnostních rizik (dále jen „rámec“) na podporu poslání subjektu a výkonu jeho institucionální autonomie. Na tuto práci dohlíží nejvyšší úroveň vedení subjektu, aby bylo zajištěno účinné a obezřetné řízení všech kybernetických bezpečnostních rizik. Rámec bude zaveden nejpozději do … [15 měsíců od vstupu tohoto nařízení v platnost].

2. Rámec zahrnuje celé prostředí informačních technologií dotčeného orgánu, instituce nebo jiného subjektu Unie, včetně jakéhokoli prostředí informačních technologií v jejich prostorách, externě zajišťovaných aktiv a služeb v prostředí cloud computingu nebo hostovaných třetími stranami, mobilních zařízení, podnikových sítí, obchodních sítí nepřipojených k internetu a jakýchkoli zařízení připojených k prostředí informačních technologií. Rámec zohledňuje řízení kontinuity činnosti v době krize a bere v úvahu bezpečnost dodavatelského řetězce, jakož i řízení lidských rizik, jež by mohla ovlivnit kybernetickou bezpečnost dotčeného orgánu, instituce nebo jiného subjektu Unie.

3. Nejvyšší úroveň vedení každého orgánu, instituce nebo agentury Unie zajišťuje dohled nad tím, jak jejich organizace plní povinnosti týkající se řízení, správy a kontroly kybernetických bezpečnostních rizik, aniž jsou dotčeny formální odpovědnosti jiných úrovní řízení za dodržování předpisů a řízení rizik v jejich příslušných oblastech odpovědnosti.

4. Každý orgán, instituce a jiný subjekt Unie má zaveden účinný mechanismus zajišťující, že přiměřená část rozpočtu na informační technologie bude vynaložena na kybernetickou bezpečnost.

5. Každý orgán, instituce nebo jiný subjekt Unie jmenuje místního referenta pro kybernetickou bezpečnost nebo osobu vykonávající rovnocennou funkci, která působí jako jediné kontaktní místo pro všechny aspekty kybernetické bezpečnosti.

Článek 5

Základní soubor opatření k zajištění kybernetické bezpečnosti

1. Nejvyšší úroveň vedení každého orgánu, instituce nebo jiného subjektu Unie schválí základní soubor opatření k zajištění vlastní kybernetické bezpečnosti subjektu pro řešení rizik zjištěných v rámci uvedeném v čl. 4 odst. 1. Činí tak na podporu svého poslání a výkonu své institucionální autonomie. Základní soubor opatření k zajištění kybernetické bezpečnosti musí být zaveden nejpozději do … [18 měsíců od vstupu tohoto nařízení v platnost] a řeší oblasti uvedené v příloze I a opatření uvedená v příloze II.

2. Vrcholné vedení každého orgánu, instituce a jiného subjektu Unie pravidelně absolvuje zvláštní školení, aby získalo dostatečné znalosti a dovednosti umožňující posuzovat a vyhodnocovat kybernetická bezpečnostní rizika a řídicí postupy a jejich dopad na provoz organizace.

Článek 6

Hodnocení vyspělosti

Každý orgán, instituce a jiný subjekt Unie provádí alespoň každé tři roky hodnocení vyspělosti kybernetické bezpečnosti, které zahrnuje všechny prvky jejich prostředí informačních technologií popsané v článku 4, přičemž zohlední příslušné pokyny a doporučení přijaté v souladu s článkem 13.

Článek 7

Plány kybernetické bezpečnosti

1. Na základě závěrů vyvozených z hodnocení vyspělosti a s ohledem na aktiva a rizika zjištěná podle článku 4 nejvyšší úroveň vedení každého orgánu, instituce nebo jiného subjektu EU po zavedení rámce pro řízení, správu a kontrolu rizik a základního souboru opatření k zajištění kybernetické bezpečnosti bez zbytečného prodlení schválí plán kybernetické bezpečnosti. Cílem plánu je zvýšit celkovou kybernetickou bezpečnost dotčeného subjektu, a tím přispět k dosažení nebo posílení vysoké společné úrovně kybernetické bezpečnosti ve všech orgánech, institucích a jiných subjektech Unie. Na podporu poslání subjektu na základě jeho institucionální autonomie zahrnuje plán přinejmenším oblasti uvedené v příloze I, opatření uvedená v příloze II, jakož i opatření týkající se připravenosti na incidenty, reakce na incidenty a zotavení z incidentů, jako je monitorování a vedení protokolů

bezpečnosti. Plán se nejméně každé tři roky reviduje, a to na základě hodnocení vyspělosti provedených podle článku 6.

2. Plán kybernetické bezpečnosti obsahuje úkoly zaměstnanců a odpovědnost za jeho provádění.

3. Plán kybernetické bezpečnosti zohledňuje příslušné pokyny a doporučení vydané centrem CERT-EU.

Článek 8
Provádění

1. Po dokončení hodnocení vyspělosti orgány, instituce a jiné subjekty Unie předloží tato hodnocení Interinstitucionálnímu výboru pro kybernetickou bezpečnost. Po dokončení bezpečnostních plánů oznámí orgány, instituce a jiné subjekty Unie jejich dokončení Interinstitucionálnímu výboru pro kybernetickou bezpečnost. Na žádost výboru informují o konkrétních aspektech této kapitoly.

2. Pokyny a doporučení vydané v souladu s článkem 13 podporují provádění ustanovení stanovených v této kapitole.

Kapitola III
INTERINSTITUCIONÁLNÍ VÝBOR PRO KYBERNETICKOU BEZPEČNOST

Článek 9
Interinstitucionální výbor pro kybernetickou bezpečnost

1. Zřizuje se Interinstitucionální výbor pro kybernetickou bezpečnost (IICB).

2. Výbor IICB je povinen:

   a) sledovat provádění tohoto nařízení orgány, institucemi a jinými subjekty Unie;

   b) dohlížet na plnění obecných priorit a cílů centrem CERT-EU a poskytovat centru CERT-EU strategické řízení.

3. Výbor IICB sestává ze tří zástupců nominovaných sítí agentur Unie (EUAN) na návrh jejího poradního výboru pro IKT, aby zastupovali zájmy orgánů a jiných subjektů, které provozují své vlastní prostředí informačních technologií, a po jednom zástupci vyslaném každým z těchto subjektů:

   a) Evropský parlament;

   b) Rada Evropské unie;

   c) Evropská komise;

   d) Soudní dvůr Evropské unie;

   e) Evropská centrální banka;

   f) Evropský účetní dvůr;

   g) Evropská služba pro vnější činnost;

   h) Evropský hospodářský a sociální výbor;

   i) Evropský výbor regionů;

   j) Evropská investiční banka;

k) Agentura Evropské unie pro kybernetickou bezpečnost.

Členům může být nápomocen náhradník. Další zástupci výše uvedených organizací nebo jiných orgánů, institucí a jiných subjektů Unie mohou být předsedou pozváni k účasti na zasedáních výboru IICB bez hlasovacích práv.

4. Výbor IICB přijímá svůj jednací řád.

5. Výbor IICB v souladu s jednacím řádem určuje z řad svých členů předsedu na období čtyř let. Jeho náhradník se na stejnou dobu trvání stává plným členem výboru IICB.

6. Výbor IICB se schází z podnětu svého předsedy, na žádost centra CERT-EU nebo na žádost kteréhokoli ze svých členů.

7. Každý člen výboru IICB má jeden hlas. Rozhodnutí výboru IICB se přijímají prostou většinou, není-li v tomto nařízení stanoveno jinak. Předseda nehlasuje kromě případů rovnosti hlasů, kdy může odevzdat rozhodující hlas.

8. Výbor IICB může jednat zjednodušeným písemným postupem zahájeným v souladu s jednacím řádem výboru IICB. Na základě tohoto postupu se příslušné rozhodnutí ve lhůtě stanovené předsedou považuje za schválené, s výjimkou případů, kdy některý z členů vznese námitku.

9. Zasedání výboru IICB se účastní vedoucí centra CERT-EU nebo jeho náhradník, pokud výbor IICB nerozhodne jinak.

10. Funkci sekretariátu výboru IICB zajišťuje Komise.

11. Zástupci nominovaní sítí EUAN na návrh poradního výboru pro IKT předávají rozhodnutí výboru IICB agenturám a společným podnikům Unie. Jakákoli instituce či jiný subjekt Unie jsou oprávněny se obrátit na zástupce nebo předsedu výboru IICB s jakoukoli záležitostí, o níž se domnívají, že by na ni výbor IICB měl být upozorněn.

12. Výbor IICB může jednat zjednodušeným písemným postupem zahájeným předsedou, na jehož základě se příslušné rozhodnutí ve lhůtě stanovené předsedou považuje za schválené, s výjimkou případů, kdy některý z členů vznese námitku.

13. Výbor IICB může nominovat výkonný výbor, aby mu pomáhal v jeho práci, a přenést na něj některé své úkoly a pravomoci. Výbor IICB stanoví jednací řád výkonného výboru, včetně jeho úkolů a pravomocí a funkčního období jeho členů.

Článek 10
Úkoly výboru IICB

Při výkonu svých povinností výbor IICB zejména:

a) přezkoumává všechny zprávy požadované centrem CERT-EU, které se týkají stavu provádění tohoto nařízení ze strany orgánů, institucí a jiných subjektů Unie;

b) na základě návrhu vedoucího centra CERT-EU schvaluje roční pracovní program centra CERT-EU a sleduje jeho provádění;

c) na základě návrhu vedoucího centra CERT-EU schvaluje katalog služeb centra CERT-EU;

d) na základě návrhu předloženého vedoucím centra CERT-EU schvaluje roční finanční plán příjmů a výdajů, včetně personálního obsazení, pro činnosti centra CERT-EU;

e) na základě návrhu vedoucího centra CERT-EU schvaluje postupy pro uzavírání dohod o úrovni služeb;

f) zkoumá a schvaluje výroční zprávu o činnosti centra CERT-EU a správě finančních prostředků centra CERT-EU vypracovanou vedoucím centra CERT-EU;

g) schvaluje a sleduje klíčové ukazatele výkonnosti pro centrum CERT-EU stanovené na základě návrhu vedoucího centra CERT-EU;

h) schvaluje ujednání o spolupráci, ujednání o úrovni služeb nebo smlouvy mezi centrem CERT-EU a dalšími subjekty podle článku 17;

i) zřizuje tolik technických poradních skupin, kolik je nezbytné, aby napomáhaly práci výboru IICB, schvaluje jejich mandát a určuje jejich příslušné předsedy.

Článek 11
Dodržování povinností

Výbor IICB sleduje provádění tohoto nařízení a přijatých pokynů, doporučení a výzev k přijetí opatření ze strany orgánů, institucí a jiných subjektů Unie Pokud výbor IICB zjistí, že orgány, instituce nebo jiné subjekty Unie toto nařízení nebo pokyny, doporučení a výzvy k přijetí opatření vydané podle tohoto nařízení účinně neuplatňují nebo neprovádějí, může, aniž by byly dotčeny interní postupy příslušného orgánu, instituce nebo jiného subjektu Unie:

a) vydat varování; je-li to nezbytné vzhledem k závažnému kybernetickému bezpečnostnímu riziku, okruh osob, jimž je varování určeno, se vhodně omezí;

b) doporučit, aby příslušná auditorská služba provedla audit.

Kapitola IV
Centrum CERT-EU

Článek 12
Poslání a úkoly centra CERT-EU

1. Posláním CERT-EU, autonomního interinstitucionálního centra kybernetické bezpečnosti pro všechny orgány, instituce a agentury Unie, je přispívat k bezpečnosti neutajovaného IT prostředí všech orgánů, institucí a jiných subjektů Unie, a to tak, že jim poskytuje poradenství v oblasti kybernetické bezpečnosti, pomáhá jim předcházet incidentům, odhalovat incidenty, zmírňovat incidenty a reagovat na incidenty a působí jako středisko pro výměnu informací v oblasti kybernetické bezpečnosti a pro koordinaci reakcí na incidenty.

2. Centrum CERT-EU vykonává pro orgány, instituce a jiné subjekty Unie tyto úkoly:

   a) podporuje je při provádění tohoto nařízení a přispívá ke koordinaci uplatňování tohoto nařízení prostřednictvím opatření uvedených v čl. 13 odst. 1 nebo prostřednictvím *ad hoc* zpráv vyžádaných IICB;

   b) podporuje je pomocí souboru služeb v oblasti kybernetické bezpečnosti popsaných v jeho katalogu služeb (dále jen „základní služby“);

   c) udržuje síť kolegů a partnerů pro podporu služeb popsaných v článcích 16 a 17;

   d) upozorňuje výbor IICB na jakýkoli problém týkající se provádění tohoto nařízení a provádění pokynů, doporučení a výzev k přijetí opatření;

e) nahlašuje kybernetické hrozby, jimž čelí orgány, instituce a jiné subjekty Unie, a přispívá k informovanosti EU o aktuální kybernetické situaci.

3. Centrum CERT-EU přispívá k činnosti Společné kybernetické jednotky, vybudované v souladu s doporučením Komise ze dne 23. června 2021, mimo jiné v těchto oblastech:

a) připravenost, koordinace při řešení incidentů, výměna informací a reakce na krize na technické úrovni v případech souvisejících s orgány, institucemi a jinými subjekty Unie;

b) operativní spolupráce týkající se sítě týmů pro reakce na počítačové bezpečnostní incidenty (týmů CSIRT), včetně vzájemné pomoci, a týkající se širší komunity v oblasti kybernetické bezpečnosti;

c) zpravodajské informace o kybernetických hrozbách, včetně informovanosti o aktuální situaci;

d) ohledně jakéhokoli tématu vyžadujícího technické odborné znalosti centra CERT-EU v oblasti kybernetické bezpečnosti.

4. Centrum CERT-EU se zapojuje do strukturované spolupráce s Agenturou Evropské unie pro kybernetickou bezpečnost v oblasti budování kapacit, operativní spolupráce a dlouhodobých strategických analýz kybernetických hrozeb v souladu s nařízením Evropského parlamentu a Rady (EU) 2019/881.

5. Centrum CERT-EU může poskytovat tyto služby, které nejsou popsány v jeho katalogu služeb (dále jen „zpoplatněné služby“):

a) služby, které podporují kybernetickou bezpečnost prostředí informačních technologií orgánů, institucí nebo jiných subjektů Unie, jiné než služby uvedené v odstavci 2, na základě dohod o úrovni služeb, a to s výhradou dostupných zdrojů;

b) služby, které podporují operace nebo projekty orgánů, institucí a dalších subjektů Unie v oblasti kybernetické bezpečnosti, jiné než služby na ochranu jejich prostředí informačních technologií, na základě písemných dohod a po předchozím schválení výborem IICB;

c) služby, které podporují bezpečnost prostředí informačních technologií jiných organizací než orgánů, institucí a jiných subjektů Unie, které úzce spolupracují s orgány, institucemi nebo jinými subjekty Unie například tak, že jim byly uloženy úkoly nebo povinnosti podle práva Unie, a to na základě písemných dohod a po předchozím schválení výborem IICB.

6. Centrum CERT-EU může v úzké spolupráci s Agenturou Evropské unie pro kybernetickou bezpečnost, je-li to použitelné, organizovat cvičení v oblasti kybernetické bezpečnosti za účelem testování úrovně kybernetické bezpečnosti orgánů, institucí a jiných subjektů Unie.

7. Centrum CERT-EU může poskytovat pomoc orgánům, institucím a jiným subjektům Unie v souvislosti s incidenty v utajovaných prostředích informačních technologií, pokud o to dotyčný zúčastněný subjekt výslovně požádá.

Článek 13

Pokyny, doporučení a výzvy k přijetí opatření

1. Centrum CERT-EU podporuje provádění tohoto nařízení vydáváním:

a) výzev k přijetí opatření popisujících naléhavá bezpečnostní opatření, jejichž přijetí ve stanovené lhůtě je vyžadováno od orgánů, institucí a jiných subjektů Unie;

b) návrhů pokynů určených všem orgánům, institucím a jiným subjektům Unie nebo jejich podmnožinám, které předkládá výboru IICB;

c) návrhů doporučení určených jednotlivým orgánům, institucím nebo jiným subjektům Unie, které předkládá výboru IICB.

2. Pokyny a doporučení mohou obsahovat:

a) postupy pro řízení kybernetických bezpečnostních rizik a vypracování základního souboru opatření k zajištění kybernetické bezpečnosti nebo jejich vylepšení;

b) postupy pro hodnocení vyspělosti a vypracování plánů v oblasti kybernetické bezpečnosti a

c) případně využití společných technologií, architektury a souvisejících osvědčených postupů s cílem dosáhnout interoperability a společných norem ve smyslu čl. 4 odst. 10 směrnice [návrh směrnice NIS 2].

3. Výbor IICB může přijímat pokyny nebo doporučení na návrh centra CERT-EU.

4. Výbor IICB může uložit centru CERT-EU, aby návrh pokynů nebo doporučení nebo výzvu k přijetí opatření vydalo, stáhlo nebo upravilo.

Článek 14
Vedoucí centra CERT-EU

Vedoucí centra CERT-EU předkládá výboru IICB a předsedovi výboru IICB pravidelné zprávy o výsledcích činnosti centra CERT-EU, finančním plánu, příjmech, plnění rozpočtu, uzavřených dohodách o úrovni služeb a písemných dohodách, spolupráci s protějšky a partnery a o misích podniknutých jeho zaměstnanci, včetně zpráv podle čl. 10 odst. 1.

Článek 15
Finanční a personální záležitosti

1. Komise po obdržení jednomyslného schválení výborem IICB jmenuje vedoucího centra CERT-EU. Výbor IICB je konzultován ve všech fázích postupu předcházejícího jmenování vedoucího centra CERT-EU, a to zejména při vypracovávání oznámení o volném pracovním místě, posuzování žádostí a jmenování výběrových komisí v souvislosti s tímto pracovním místem.

2. Při uplatňování administrativních a finančních postupů jedná vedoucí centra CERT-EU z pověření Komise.

3. Úkoly a činnosti centra CERT-EU, včetně služeb poskytovaných centrem CERT-EU podle čl. 12 odst. 2, 3, 4 a 6 a uvedené v čl. 13 odst. 1 orgánům, institucím a jiným subjektům Unie financovaným z okruhu víceletého finančního rámce vyhrazeného evropské veřejné správě jsou financovány prostřednictvím samostatné rozpočtové položky rozpočtu Komise. Místa vyčleněná pro centrum CERT-EU jsou podrobně popsána v poznámce pod čarou k plánu pracovních míst Komise.

4. Orgány, instituce a jiné subjekty Unie jiné než orgány, instituce a jiné subjekty Unie uvedené v odstavci 3 každoročně finančně přispívají centru CERT-EU na úhradu

služeb poskytovaných centrem CERT-EU podle uvedeného odstavce 3. Příslušné příspěvky vycházejí z pokynů vydaných výborem IICB a dohodnutých mezi každým subjektem a centrem CERT-EU v dohodách o úrovni služeb. Příspěvky představují spravedlivý a přiměřený podíl na celkových nákladech na poskytované služby. Převádějí se na samostatnou rozpočtovou položku uvedenou v odstavci 3 jakožto účelově vázaný příjem stanovený v čl. 21 odst. 3 písm. c) nařízení Evropského parlamentu a Rady (EU, Euratom) 2018/1046[8].

5. Náklady na úkoly stanovené v čl. 12 odst. 5 jsou hrazeny orgány, institucemi a jinými subjekty Unie, které jsou příjemci služeb centra CERT-EU. Příjmy jsou účelově vázány na rozpočtové položky podporující náklady.

Článek 16

Spolupráce centra CERT-EU s protějšky v členských státech

1. Centrum CERT-EU spolupracuje s vnitrostátními protějšky v členských státech, včetně týmů CERT, národních center pro kybernetickou bezpečnost, týmů CSIRT a jednotných kontaktních míst uvedených v článku 8 směrnice [návrh směrnice NIS 2] a vyměňuje si s nimi informace ohledně hrozeb, zranitelných míst a incidentů v oblasti kybernetické bezpečnosti, ohledně možných protiopatření a ohledně veškerých záležitostí, které mají význam pro zlepšení ochrany prostředí informačních technologií v orgánech, institucích nebo jiných subjektech Unie, a to i prostřednictvím sítě týmů CSIRT uvedené v článku 13 směrnice [návrhu směrnice NIS 2].

2. Centrum CERT-EU si s vnitrostátními protějšky v členských státech může vyměňovat informace týkající se konkrétních incidentů za účelem usnadnění odhalování obdobných kybernetických hrozeb, a to bez souhlasu dotčeného zúčastněného subjektu. Informace týkající se konkrétních incidentů, které odhalují totožnost cíle kybernetického bezpečnostního incidentu, si může centrum CERT-EU vyměňovat pouze se souhlasem dotčeného zúčastněného subjektu.

Článek 17

Spolupráce centra CERT-EU s protějšky v nečlenských státech

1. Centrum CERT-EU může spolupracovat s protějšky v nečlenských státech, včetně protějšků zaměřených na konkrétní průmyslová odvětví, ohledně nástrojů a metod, jako například techniky, taktiky, postupů a osvědčených postupů, jakož i ohledně kybernetických hrozeb a zranitelných míst. Pro účely veškeré spolupráce s těmito protějšky, včetně spolupráce na základě rámců, v nichž protějšky ze zemí mimo EU spolupracují s vnitrostátními protějšky členských států, požádá centrum CERT-EU výbor IICB o předchozí souhlas.

2. Centrum CERT-EU může v zájmu shromažďování informací o obecných a konkrétních hrozbách, zranitelných místech a možných protiopatřeních spolupracovat s dalšími partnery, jako jsou komerční subjekty, mezinárodní organizace, vnitrostátní subjekty zemí mimo Evropskou unii nebo jednotliví

[8] Nařízení Evropského parlamentu a Rady (EU, Euratom) 2018/1046 ze dne 18. července 2018, kterým se stanoví finanční pravidla pro souhrnný rozpočet Unie, mění nařízení (EU) č. 1296/2013, (EU) č. 1301/2013, (EU) č. 1303/2013, (EU) č. 1304/2013, (EU) č. 1309/2013, (EU) č. 1316/2013, (EU) č. 223/2014 a (EU) č. 283/2014 a rozhodnutí č. 541/2014/EU a zrušuje nařízení (EU, Euratom) č. 966/2012 (Úř. věst. L 193, 30.7.2018, s. 1).

odborníci. Pro účely širší spolupráce s těmito partnery požádá centrum CERT-EU výbor IICB o předchozí souhlas.

3. Centrum CERT-EU může se souhlasem zúčastněného subjektu dotčeného incidentem poskytnout informace týkající se tohoto incidentu partnerům, kteří mohou přispět k jeho analýze.

Kapitola V
POVINNOSTI V OBLASTI SPOLUPRÁCE A OZNAMOVACÍ POVINNOSTI

Článek 18
Nakládání s informacemi

1. Centrum CERT-EU a orgány, instituce nebo jiné subjekty Unie musejí dodržovat povinnost zachování profesního tajemství v souladu s článkem 339 Smlouvy o fungování Evropské unie nebo s rovnocennými použitelnými rámci.

2. V souvislosti se žádostmi o přístup veřejnosti k dokumentům v držení centra CERT-EU se použijí ustanovení nařízení Evropského parlamentu a Rady (ES) č. 1049/2001[9], včetně povinnosti podle uvedeného nařízení konzultovat s jinými orgány, institucemi nebo jinými subjekty, pokud se žádost týká jejich dokumentů.

3. Zpracování osobních údajů prováděné podle tohoto nařízení se řídí nařízením Evropského parlamentu a Rady (EU) 2018/1725.

4. Nakládání s informacemi ze strany centra CERT-EU a orgánů, institucí a jiných subjektů Unie musí být v souladu s pravidly stanovenými v nařízení [navrhovaném nařízení o zajištění bezpečnosti informací].

5. Ředitelství pro bezpečnost Komise a předseda výboru IICB jsou neprodleně informováni o jakýchkoli kontaktech s centrem CERT-EU, které iniciují nebo o jejichž navázání usilují vnitrostátní bezpečnostní a zpravodajské služby.

Článek 19
Sdílení povinností

1. Aby se centru CERT-EU umožnilo koordinovat řízení zranitelnosti a reakce na incidenty, může požádat orgány, instituce a jiné subjekty Unie o poskytnutí informací ze soupisů jejich příslušných systémů informačních technologií, které mají význam pro podporu ze strany centra CERT-EU. Dožádaný orgán, instituce nebo jiný subjekt bez zbytečného odkladu předá požadované informace a všechny jejich následné aktualizace.

2. Orgány, instituce a jiné subjekty Unie na žádost centra CERT-EU a bez zbytečného odkladu digitální informace vytvořené použitím elektronických zařízení, která se podílela na jejich příslušných incidentech. Centrum CERT-EU může dále upřesnit, které typy těchto digitálních informací požaduje pro situační přehled a reakci na incidenty.

3. Centrum CERT-EU si může vyměňovat informace týkající se konkrétního incidentu, které odhalují totožnost orgánu, instituce nebo jiného subjektu Unie, jichž se incident

[9] Nařízení Evropského parlamentu a Rady (ES) č. 1049/2001 ze dne 30. května 2001 o přístupu veřejnosti k dokumentům Evropského parlamentu, Rady a Komise (Úř. věst. L 145, 31.5.2001, s. 43).

týká, pouze se souhlasem tohoto subjektu. Informace týkající se konkrétních incidentů, které odhalují totožnost cíle kybernetického bezpečnostního incidentu, si může centrum CERT-EU vyměňovat pouze se souhlasem zúčastněného subjektu dotčeného tímto incidentem.

4. Povinnosti související se sdílením informací se nevztahují na utajované informace EU a na informace, které orgán, instituce nebo jiný subjekt Unie obdržely od bezpečnostní a zpravodajské služby nebo donucovacího orgánu členského státu za výslovné podmínky, že nebudou sdíleny s orgánem CERT-EU.

Článek 20

Oznamovací povinnosti

1. Všechny orgány, instituce a jiné subjekty Unie předloží centru CERT-EU první oznámení o významných kybernetických hrozbách, významných zranitelných místech a významných incidentech, a to bez zbytečného odkladu, v každém případě do 24 hodin poté, co se o nich dozvěděly.

   V řádně odůvodněných případech a po dohodě s centrem CERT-EU se dotčený orgán, instituce nebo jiný subjekt Unie může odchýlit od lhůty stanovené v předchozím odstavci.

2. Orgány, instituce a jiné subjekty Unie dále bez zbytečného prodlení oznámí orgánu CERT-EU vhodné technické podrobnosti o kybernetických hrozbách, zranitelných místech a incidentech, které umožňují odhalování incidentů, reakci na incidenty nebo opatření ke zmírnění dopadů incidentů. Oznámení obsahují tyto prvky, jsou-li dostupné:

   a) příslušné indikátory narušení;

   b) příslušné detekční mechanismy;

   c) potenciální dopad;

   d) příslušná opatření ke zmírnění dopadů.

3. Orgán CERT-EU předkládá agentuře ENISA měsíční souhrnnou zprávu obsahující anonymizované a agregované údaje o významných kybernetických hrozbách, významných zranitelných místech a významných incidentech oznámených v souladu s odstavcem 1.

4. Výbor IICB může vydávat pokyny nebo doporučení týkající se způsobů oznamování a obsahu oznámení. Centrum CERT-EU šíří vhodné technické podrobnosti s cílem umožnit aktivní odhalování incidentů, reakci na incidenty nebo opatření ke zmírnění dopadů incidentů ze strany orgánů, institucí nebo jiných subjektů Unie.

5. Oznamovací povinnosti se nevztahují na utajované informace EU a na informace, které orgán, instituce nebo jiný subjekt Unie obdržely od bezpečnostní a zpravodajské služby nebo donucovacího orgánu členského státu za výslovné podmínky, že nebudou sdíleny s orgánem CERT-EU.

Článek 21

Koordinace reakcí na incidenty a spolupráce ohledně významných incidentů

1. Centrum CERT-EU, které působí jako středisko pro výměnu informací v oblasti kybernetické bezpečnosti a pro koordinaci reakcí na incidenty, usnadňuje výměnu informací o kybernetických hrozbách, zranitelných místech a incidentech mezi:

a) orgány, institucemi a jinými subjekty Unie;

b) protějšky uvedenými v článcích 16 a 17.

2. Centrum CERT-EU usnadňuje koordinaci reakcí orgánů, institucí a jiných subjektů Unie na incidenty, včetně:

a) přispívání k jednotné vnější komunikaci;

b) vzájemné pomoci;

c) optimálního využití operativních zdrojů;

d) koordinace s dalšími mechanismy reakce na krizové situace na úrovni Unie.

3. Centrum CERT-EU podporuje orgány, instituce a jiné subjekty Unie v oblasti situačního povědomí o kybernetických hrozbách, zranitelných místech a incidentech.

4. Výbor IICB vydává pokyny pro koordinaci reakcí na incidenty a pro spolupráci při významných incidentech. Pokud existuje podezření, že incident má povahu trestného činu, centrum CERT-EU poskytne poradenství k tomu, jak oznámit tento incident donucovacím orgánům.

Článek 22
Významné útoky

1. Centrum CERT-CE koordinuje reakce orgánů, institucí a jiných subjektů Unie na významné útoky. Vede seznam technických odborných znalostí, které by v případě takových útoků byly potřebné, aby bylo možné na incident reagovat.

2. Orgány, instituce a jiné subjekty Unie přispívají k seznamu technických odborných znalostí tím, že poskytují každoročně aktualizovaný seznam odborníků, kteří jsou k dispozici v rámci jejich příslušných organizací, s podrobným uvedením jejich konkrétních technických dovedností.

3. Se souhlasem dotčených orgánů, institucí nebo jiných subjektů Unie se centrum CERT-EU může rovněž obrátit na odborníky ze seznamu uvedeného v odstavci 2, aby přispěli k reakci na významný útok v některém členském státě, a to v souladu s operačními postupy Společné kybernetické jednotky.

Kapitola VI
ZÁVĚREČNÁ USTANOVENÍ

Článek 23
Počáteční přerozdělení rozpočtových prostředků

Komise navrhne přerozdělení zaměstnanců a finančních zdrojů od příslušných orgánů, institucí a jiných subjektů Unie do rozpočtu Komise. Přerozdělení je účinné současně s prvním rozpočtem přijatým po vstupu tohoto nařízení v platnost.

Článek 24
Přezkum

1. Výbor IICB za pomoci týmu CERT-EU pravidelně podává Komisi zprávy o provádění tohoto nařízení. Výbor IICB může také Komisi doporučit, aby navrhla změny tohoto nařízení.

2. Komise podá Evropskému parlamentu a Radě zprávu o provádění tohoto nařízení nejpozději 48 měsíců po vstupu tohoto nařízení v platnost a poté každé tři roky.

3. Komise vyhodnotí fungování tohoto nařízení a podá zprávu Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů nejdříve pět let ode dne jeho vstupu v platnost.

Článek 25
Vstup v platnost

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

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

LEGISLATIVNÍ FINANČNÍ VÝKAZ

1. RÁMEC NÁVRHU/PODNĚTU

1.1. Název návrhu/podnětu

1.2. Příslušné oblasti politik

1.3. Povaha návrhu/podnětu

1.4. Cíle

1.4.1. Obecné cíle

1.4.2. Specifické cíle

1.4.3. Očekávané výsledky a dopady

1.4.4. Ukazatele výkonnosti

1.5. Odůvodnění návrhu/podnětu

1.5.1. Potřeby, které mají být uspokojeny v krátkodobém nebo dlouhodobém horizontu, včetně podrobného harmonogramu pro zahajovací fázi provádění podnětu.

1.5.2. Přidaná hodnota ze zapojení Unie (může být důsledkem různých faktorů, např. přínosů z koordinace, právní jistoty, vyšší účinnosti nebo doplňkovosti). Pro účely tohoto bodu se „přidanou hodnotou ze zapojení Unie“ rozumí hodnota plynoucí ze zásahu Unie, jež doplňuje hodnotu, která by jinak vznikla činností samotných členských států.

1.5.3. Závěry vyvozené z podobných zkušeností v minulosti

1.5.4. Slučitelnost s víceletým finančním rámcem a možné synergie s dalšími vhodnými nástroji

1.5.5. Posouzení různých dostupných možností financování, včetně prostoru pro přerozdělení prostředků

1.6. Doba trvání a finanční dopad návrhu/podnětu

1.7. Předpokládaný způsob řízení

2. SPRÁVNÍ OPATŘENÍ

2.1. Pravidla pro sledování a podávání zpráv

2.2. Systémy řízení a kontroly

2.2.1. Odůvodnění navrhovaných způsobů řízení, mechanismů provádění financování, způsobů plateb a kontrolní strategie

2.2.2. Informace o zjištěných rizicích a systémech vnitřní kontroly zřízených k jejich zmírnění

2.2.3. Odhad a odůvodnění nákladové efektivnosti kontrol (poměr „náklady na kontroly ÷ hodnota souvisejících spravovaných finančních prostředků“) a posouzení očekávané míry rizika výskytu chyb (při platbě a při uzávěrce)

2.3. Opatření k zamezení podvodů a nesrovnalostí

3. ODHADOVANÝ FINANČNÍ DOPAD NÁVRHU/PODNĚTU

3.1. Okruhy víceletého finančního rámce a dotčené výdajové rozpočtové položky

3.2. Odhadovaný finanční dopad návrhu na prostředky

3.2.1. Odhadovaný souhrnný dopad na operační prostředky

3.2.2. Odhadovaný výstup financovaný z operačních prostředků

3.2.3. Odhadovaný souhrnný dopad na správní prostředky

3.2.4. Slučitelnost se stávajícím víceletým finančním rámcem

3.2.5. Příspěvky třetích stran

3.3. Odhadovaný dopad na příjmy

LEGISLATIVNÍ FINANČNÍ VÝKAZ

1. RÁMEC NÁVRHU/PODNĚTU

1.1. Název návrhu/podnětu

Návrh nařízení Evropského parlamentu a Rady, kterým se stanoví opatření k zajištění vysoké společné úrovně kybernetické bezpečnosti v orgánech, institucích a jiných subjektech Unie

1.2. Příslušné oblasti politik

Evropská veřejná správa

Návrh se týká opatření, jež zajistí vysokou společnou úroveň kybernetické bezpečnosti v orgánech, institucích a jiných subjektech Unie

1.3. Návrh/podnět se týká:

☑nové akce

☐ nové akce následující po pilotním projektu / přípravné akci[10]

☐ prodloužení stávající akce

☑ sloučení jedné či více akcí v jinou/novou akci nebo přesměrování jedné či více akcí na jinou/novou akci

1.4. Cíle

1.4.1. Obecné cíle

– Stanovit rámec, který zajistí vysokou společnou úroveň kybernetické bezpečnosti v orgánech, institucích a jiných subjektech Unie

– Poskytnout nový právní základ pro centrum CERT-EU s cílem posílit jeho mandát a financování

1.4.2. Specifické cíle

(1) Stanovit orgánům, institucím a jiným subjektům Unie povinnosti s cílem zavést interní rámec pro řízení, správu a kontrolu kybernetických bezpečnostních rizik

(2) Stanovit orgánům, institucím a jiným subjektům Unie povinnosti s cílem podávat zprávy o řízení rizik, správě a kontrole kybernetické bezpečnosti a o kybernetických bezpečnostních incidentech

(3) Stanovit pravidla týkající se organizace a provozu Centra pro kybernetickou bezpečnost orgánů, institucí a jiných subjektů Unie (CERT-EU) a organizace a provozu Interinstitucionálního výboru pro kybernetickou bezpečnost (IICB)

(4) Přispívat k činnosti Společné kybernetické jednotky

1.4.3. Očekávané výsledky a dopady

Upřesněte účinky, které by návrh/podnět měl mít na příjemce / cílové skupiny.

[10] Uvedené v čl. 58 odst. 2 písm. a) nebo b) finančního nařízení.

– Interní rámec pro řízení, správu a kontrolu kybernetických bezpečnostních rizik, základní soubory opatření k zajištění kybernetické bezpečnosti, pravidelná hodnocení vyspělosti a plány kybernetické bezpečnosti v orgánech, institucích a jiných subjektech Unie – Zvyšování odolnosti orgánů, institucí a jiných subjektů Unie v oblasti kybernetické bezpečnosti a jejich schopnosti reagovat na incidenty – Modernizace centra CERT-EU – Přispívání k činnosti Společné kybernetické jednotky

1.4.4. Ukazatele výkonnosti

Upřesněte ukazatele pro sledování pokroku a dosažených výsledků.

– V orgánech, institucích a jiných subjektech Unie jsou rámce a základní soubory opatření zavedeny, pravidelná hodnocení vyspělosti a plány kybernetické bezpečnosti se provádějí – Lepší řešení incidentů – Lepší povědomí o kybernetických bezpečnostních rizicích na úrovni vrcholného vedení orgánů, institucí a jiných subjektů Unie – Vyrovnání výdajů na bezpečnost IKT vyjádřených jako procento celkových výdajů na IKT – Silné vedení výboru IICB a centra CERT-EU – Intenzivnější sdílení informací mezi orgány, institucemi a jinými subjekty Unie a s příslušnými subjekty a zúčastněnými stranami v EU – Intenzivnější spolupráce v oblasti kybernetické bezpečnosti s příslušnými subjekty a zúčastněnými stranami v EU prostřednictvím centra CERT-EU a agentury ENISA

1.5. Odůvodnění návrhu/podnětu

1.5.1. Potřeby, které mají být uspokojeny v krátkodobém nebo dlouhodobém horizontu, včetně podrobného harmonogramu pro zahajovací fázi provádění podnětu.

Cílem návrhu je zvýšit úroveň kybernetické odolnosti orgánů, institucí a jiných subjektů Unie, snížit rozdíly v odolnosti všech těchto subjektů a zlepšit úroveň společné informovanosti o situaci a kolektivní schopnosti připravit se a reagovat. Návrh je plně v souladu s dalšími souvisejícími iniciativami, a zejména s návrhem směrnice o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o zrušení směrnice (EU) 2016/1148 [návrhem směrnice NIS 2]. Návrh tvoří nezbytnou část strategie bezpečnostní unie EU a strategie kybernetické bezpečnosti EU pro digitální dekádu. Evropská komise plánuje předložit toto nařízení v říjnu 2021, přijetí nařízení Evropským parlamentem a Radou se předpokládá v roce 2022 a ustanovení budou použitelná od data vstupu nařízení v platnost. Předpokládá se, že finanční dopady a dopady na lidské zdroje popsané v tomto legislativním finančním výkazu započnou v roce 2023. Přípravné období začalo již v roce 2021, avšak přípravné činnosti v letech 2021 a 2022 jsou mimo finanční dopad návrhu.

1.5.2. Přidaná hodnota ze zapojení Unie (může být důsledkem různých faktorů, např. přínosů z koordinace, právní jistoty, vyšší účinnosti nebo doplňkovosti). Pro účely tohoto bodu se „přidanou hodnotou ze zapojení Unie“ rozumí hodnota plynoucí ze zásahu Unie, jež doplňuje hodnotu, která by jinak vznikla činností samotných členských států.

Důvody pro akci na evropské úrovni (*ex ante*)

V období od roku 2019 do roku 2021 prudce vzrostl počet významných incidentů postihujících orgány, instituce a jiné subjekty Unie, jejichž původci byli aktéři pokročilé trvalé hrozby. V první polovině roku 2021 došlo ke stejnému počtu významných incidentů jako za celý rok 2020. To se také odrazilo v počtu bitových kopií pro forenzní analýzu (snímků obsahu dotčených systémů nebo zařízení), které analyzovalo centrum CERT-EU v roce 2020; tento počet se ve srovnání s rokem 2019 ztrojnásobil, přičemž počet významných incidentů se od roku 2018 zvýšil více než desetinásobně.

Úroveň vyspělosti kybernetické bezpečnosti se u různých subjektů podstatně liší[11]. Toto nařízení zajišťuje, že všechny orgány, instituce a jiné subjekty Unie budou provádět základní soubor bezpečnostních opatření a vzájemně spolupracovat s cílem zajistit otevřené a efektivní fungování unijní správy.

Systémy, které mají být chráněny, spadají do autonomní správy orgánů, institucí a jiných subjektů Unie a jsou jimi provozovány; členské státy by navrhovaná opatření nemohly vytvořit.

1.5.3. Závěry vyvozené z podobných zkušeností v minulosti

Směrnice o bezpečnosti sítí a informací byla prvním horizontálním nástrojem vnitřního trhu, jehož cílem je zlepšit odolnost sítí a systémů v Unii vůči kybernetickým bezpečnostním rizikům. Od svého vstupu v platnost v roce 2016 velkou měrou přispěla ke zvýšení společné úrovně kybernetické bezpečnosti v členských státech. Návrh směrnice NIS 2 usiluje o další zlepšení těchto opatření.

Cílem tohoto nařízení je poskytnout podobná opatření pro orgány, instituce a jiné subjekty Unie.

1.5.4. Slučitelnost s víceletým finančním rámcem a možné synergie s dalšími vhodnými nástroji

Návrh je v souladu s víceletým finančním rámcem a tvoří nezbytnou součást strategie bezpečnostní unie EU, jakož i strategie kybernetické bezpečnosti EU pro digitální dekádu.

Návrh předpokládá uplatňování opatření k zajištění vysoké společné úrovně kybernetické bezpečnosti ve vztahu k orgánům, institucím a jiným subjektům Unie. Návrh je v souladu s návrhem směrnice o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o zrušení směrnice (EU) 2016/1148 [návrhem směrnice NIS 2].

[11] Odkaz: [Zvláštní zpráva EÚD o kybernetické bezpečnosti v orgánech, institucích a jiných subjektech Unie].

1.5.5. Posouzení různých dostupných možností financování, včetně prostoru pro přerozdělení prostředků

Správa těchto úkolů ze strany centra CERT-EU vyžaduje specifické profily a další pracovní zátěž, kterou nelze absorbovat bez zvýšení lidských a finančních zdrojů.

1.6. Doba trvání a finanční dopad návrhu/podnětu

☐ **Časově omezená doba trvání**

– ☐ s platností od [DD.MM.]RRRR do [DD.MM.]RRRR,

– ☐ finanční dopad od RRRR do RRRR u prostředků na závazky a od RRRR do RRRR u prostředků na platby.

☑ **Časově neomezená doba trvání**

– Finanční dopad by měl začít prvním rozpočtem přijatým po vstupu nařízení v platnost. V prvním roce, který je považován za rok přechodný, by došlo k přerozdělení zdrojů od orgánů a hlavních institucí Unie ke Komisi; k tomuto a dalšímu přerozdělení nebo přidělení zdrojů dojde v rámci ročních rozpočtů. Pokud bude nařízení přijato v roce 2022, bude rozpočtový rok 2023 přechodným obdobím a v roce 2024 začne nařízení fungovat v plném rozsahu.

1.7. Předpokládaný způsob řízení[12]

☑ **Přímé řízení** Komisí a každým orgánem, institucí a jiným subjektem Unie

– ☑ prostřednictvím jejích útvarů, včetně jejích zaměstnanců v delegacích Unie,

– ☐ prostřednictvím výkonných agentur.

☐ **Sdílené řízení** s členskými státy

☐ **Nepřímé řízení**, při kterém jsou úkoly souvisejícími s plněním rozpočtu pověřeny:

– ☐ třetí země nebo subjekty určené těmito zeměmi,

– ☐ mezinárodní organizace a jejich agentury (upřesněte),

– ☐ EIB a Evropský investiční fond,

– ☐ subjekty uvedené v článcích 70 a 71 finančního nařízení,

– ☐ veřejnoprávní subjekty,

– ☐ soukromoprávní subjekty pověřené výkonem veřejné služby v rozsahu, v jakém poskytují dostatečné finanční záruky,

– ☐ soukromoprávní subjekty členského státu pověřené uskutečňováním partnerství veřejného a soukromého sektoru a poskytující dostatečné finanční záruky,

– ☐ osoby pověřené prováděním specifických akcí v rámci společné zahraniční a bezpečnostní politiky podle hlavy V Smlouvy o EU a určené v příslušném základním právním aktu.

– *Pokud vyberete více způsobů řízení, upřesněte je v části „Poznámky“.*

Poznámky

Při používání správních a finančních postupů jedná centrum CERT-EU pod dohledem Komise. Dodatečné zdroje vyplývající z návrhu nařízení:

[12] Vysvětlení způsobů řízení spolu s odkazem na finanční nařízení jsou k dispozici na stránkách BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx

Provádění článku 12 a 13 návrhu nařízení vede k rozšíření katalogu služeb o další základní služby. Při plném provozu budou nutné následující dodatečné zdroje (do konce VFR na konci roku 2027): 21 FTE a 14,05 milionu EUR.

Rozdělení dodatečných zdrojů v rámci rozpočtu na jednotlivé úkoly je následující:

(a) na plnění úkolů pro orgány, instituce a jiné subjekty Unie uvedené v čl. 12 odst. 2 písm. a), b), c) a e): 13,75 FTE a 11,275 milionu EUR;

(b) na plnění úkolů uvedených v čl. 12 odst. 3 (přispívání k činnosti Společné kybernetické jednotky): 2 FTE a 381 000 EUR;

(c) na plnění úkolů uvedených v čl. 12 odst. 4 (strukturovaná spolupráce s agenturou ENISA): 0,25 FTE a 236 000 EUR;

(d) na provádění úkolů uvedených v čl. 12 odst. 6 (cvičení v oblasti kybernetické bezpečnosti): 0,25 FTE a 79 000 EUR;

(e) na plnění úkolů uvedených v čl. 12 odst. 2 písm. d) a článku 13 (analýza a podávání zpráv o provádění nařízení, vypracovávání pokynů, doporučení a výzev k přijetí opatření): 3,75 FTE a 2,079 milionu EUR;

(f) na plnění úkolů podpory sekretariátu Interinstitucionálního výboru pro kybernetickou bezpečnost (IICB): 1 FTE.

Přehled současných zdrojů a přechod na plné fungování:

V září 2021 byl CERT-EU provozován s těmito zdroji:

– stálá a dočasná pracovní místa: 14 FTE,

– smluvní zaměstnanci financovaní na základě dohod o úrovni služeb: 24 FTE,

– celkem 38 FTE.

Rozpočet CERT-EU v roce 2020 činil: 250 000 EUR v rámci rozpočtu Komise, 3,5 milionu EUR prostřednictvím účelově vázaných příjmů vyplývajících z dohod o úrovni služeb. Celkem: 3,75 milionu EUR. To představovalo celý rozpočet CERT-EU zahrnující odbornou přípravu, hardware, software, mise, podporu, smluvní zaměstnance a konference.

Jakmile nařízení vstoupí v platnost, předpokládá se, že budoucí zdroje CERT-EU budou tyto:

– stálá pracovní místa: 34 FTE,

– smluvní zaměstnanci: 15 FTE,

– celkem 49 FTE, tj. čistý nárůst o 11 FTE.

Změna poměru mezi počtem stálých pracovních míst a smluvních zaměstnanců řeší objektivní překážku při najímání a udržení zkušených odborníků v oblasti kybernetické bezpečnosti vzhledem k jejich nedostatku na trhu práce.

Kromě toho bude požadován smluvní zaměstnanec na plný pracovní úvazek (1 FTE) v rámci Generálního ředitelství pro informatiku Komise na podporu IICB (Interinstitucionálního výboru pro kybernetickou bezpečnost).

Celkově tak bude požadováno 21 FTE navíc na provádění nařízení (20 FTE pro CERT-EU a 1 FTE pro Generální ředitelství pro informatiku Komise). To budce kompenzováno souběžným snížením o devět smluvních zaměstnanců na plný pracovní úvazek v centru CERT-EU, kteří byli dříve financováni prostřednictvím účelově vázaných příjmů pocházejících z dohod o úrovni služeb.

Rozpočet centra CERT-EU na jiné než lidské zdroje v roce 2024 po přechodném období bude zahrnovat úkoly uvedené výše pod písmenem a) až e) a předpokládá se, že bude financován takto:

– 8,921 milionu EUR ročně od orgánů Unie financovaných v rámci okruhu 7 rozpočtu Unie,

– 2,459 milionu EUR od orgánů, institucí a jiných subjektů Unie financovaných v rámci okruhů 1 až 6 rozpočtu Unie,

– 2,670 milionu EUR od samofinancovaných orgánů, institucí a jiných subjektů Unie,

– celkový rozpočet centra CERT-EU: 14,05 milionu EUR.

Úkoly uvedené v čl. 12 odst. 5 nejsou uvedeny v katalogu jeho služeb, jedná se o zpoplatněné služby. Jsou to pomocné služby, představují poměrně nízké částky, jsou většinou dočasné a náklady na tyto služby budou získány zpět od příjemců služeb prostřednictvím dohod o úrovni služeb nebo písemných dohod.

Pokud jde o příspěvky na zaměstnance centra CERT-EU: orgány a hlavní instituce Unie budou přispívat spravedlivým dílem, který je úměrný příslušnému podílu stálých zaměstnanců třídy AD v dané organizaci. Je třeba posoudit, zda ECB a EIB mohou rovněž přispívat spravedlivým dílem prostřednictvím vysílání stálých zaměstnanců.

2. SPRÁVNÍ OPATŘENÍ

2.1. Pravidla pro sledování a podávání zpráv

Upřesněte četnost a podmínky.

Komise bude s pomocí výboru IICB a centra CERT-EU pravidelně přezkoumávat fungování tohoto nařízení a podá zprávu Evropskému parlamentu Radě a Komisi poprvé nejpozději 48 měsíců od vstupu nařízení v platnost a poté každé tři roky.

Zdroje údajů použité pro přezkumy budou většinou pocházet z výboru IICB a centra CERT-EU. Kromě toho mohou být v případě potřeby použity konkrétní nástroje pro shromažďování údajů, např. průzkumy v orgánech, institucích a jiných subjektech Unie, agentuře ENISA nebo síti týmů CSIRT.

2.2. Systémy řízení a kontroly

2.2.1. Odůvodnění navrhovaných způsobů řízení, mechanismů provádění financování, způsobů plateb a kontrolní strategie

Opatření vyplývající z nařízení budou v rámci každého orgánu, instituce nebo jiného subjektu Unie řízena v souladu s jejich příslušnými platnými pravidly a předpisy.

Administrativní a finanční řízení činností centra CERT-EU je začleněno do správy Komise a řídí se jejími platnými řídicími a prováděcími mechanismy, způsoby plateb a kontrolami.

Interní auditor Komise vykonává ve vztahu k centru CERT-EU stejné pravomoci jako ve vztahu k útvarům Komise.

2.2.2. Informace o zjištěných rizicích a systémech vnitřní kontroly zřízených k jejich zmírnění

Riziko je velmi nízké, neboť centrum CERT-EU je již správně připojeno jako pracovní skupina Komise ke generálnímu řediteli pro informatiku a výbor IICB je modelován podle stávající řídící rady CERT-EU. Ekosystém finančního řízení a vnitřní kontroly je tak již zaveden.

2.2.3. Odhad a odůvodnění nákladové efektivnosti kontrol (poměr „náklady na kontroly ÷ hodnota souvisejících spravovaných finančních prostředků“) a posouzení očekávané míry rizika výskytu chyb (při platbě a při uzávěrce)

Postupy pro zadávání veřejných zakázek, finanční řízení a kontrolu jsou již zavedeny a dobře vyzkoušeny. Nákladová efektivnost kontrol a míra rizika výskytu chyb odpovídá nákladové efektivnosti a míře rizika výskytu chyb orgánů, institucí a jiných subjektů Unie a v případě činností centra CERT-EU odpovídá nákladové efektivnosti a míře rizika výskytu chyb Komise.

2.3. Opatření k zamezení podvodů a nesrovnalostí

Upřesněte stávající či předpokládaná preventivní a ochranná opatření, např. opatření uvedená ve strategii pro boj proti podvodům.

Na činnosti CERT-EU se vztahují systémy finančního řízení a vnitřní kontroly Komise.

V zájmu boje proti podvodům, korupci a jiným protiprávním činnostem se na agenturu bez omezení vztahuje nařízení Evropského parlamentu a Rady (EU,

Euratom) č. 883/2013 ze dne 11. září 2013 o vyšetřování prováděném Evropským úřadem pro boj proti podvodům (OLAF).

3. ODHADOVANÝ FINANČNÍ DOPAD NÁVRHU/PODNĚTU

3.1. Okruhy víceletého finančního rámce a dotčené výdajové rozpočtové položky

- Stávající rozpočtové položky

V pořadí okruhů víceletého finančního rámce a rozpočtových položek.

Okruh víceletého finančního rámce	Rozpočtová položka	Druh výdaje	Příspěvek			
	Číslo	RP/NRP[13]	zemí ESVO[14]	kandidátských zemí[15]	třetích zemí	ve smyslu čl. 21 odst. 2 písm. b) finančního nařízení
1 až 6	Rozpočtové položky, které se týkají příspěvků Unie decentralizovaným agenturám a institucím	Rozdíl	NE	NE	NE	NE
7	Rozpočtové položky, které se týkají odměňování zaměstnanců, výdajů na informační technologie a další správní náklady v různých oddílech rozpočtu EU	NRP	NE	NE	NE	NE

- Nové rozpočtové položky, jejichž vytvoření se požaduje

V pořadí okruhů víceletého finančního rámce a rozpočtových položek.

Okruh víceletého finančního rámce	Rozpočtová položka	Druh výdaje	Příspěvek			
	Číslo	RP/NRP	zemí ESVO	kandidátských zemí	třetích zemí	ve smyslu čl. 21 odst. 2 písm. b) finančního nařízení
	Žádné		ANO/NE	ANO/NE	ANO/NE	ANO/NE

[13] RP = rozlišené prostředky / NRP = nerozlišené prostředky.
[14] ESVO: Evropské sdružení volného obchodu.
[15] Kandidátské země a případně potenciální kandidáti ze západního Balkánu.

3.2. Odhadovaný finanční dopad návrhu na prostředky

3.2.1. Odhadovaný souhrnný dopad na operační prostředky

– ☐ Návrh/podnět nevyžaduje využití operačních prostředků.

– ☑ Návrh/podnět vyžaduje využití operačních prostředků, jak je vysvětleno dále:

v milionech EUR (zaokrouhleno na tři desetinná místa)

Okruh víceletého finančního rámce	1 až 6	Okruhy, které se týkají příspěvků decentralizovaným agenturám a institucím

GŘ: několik			Rok **2023**	Rok **2024**	Rok **2025**	Rok **2026**	Rok **2027**	**CELKEM**
○ Operační prostředky								
Rozpočtové položky, které se týkají příspěvků Unie decentralizovaným agenturám (xx 10 xx xx)[16]	Závazky	(1a)	2,459	2,459	2,459	2,459	2,459	12,293
	Platby	(2a)	2,459	2,459	2,459	2,459	2,459	12,293
Prostředky správní povahy financované z rámce na zvláštní programy[17]								
Rozpočtová položka		(3)						
CELKEM prostředky na GŘ: několik	Závazky	=1a+1b +3	2,459	2,459	2,459	2,459	2,459	12,293
	Platby	=2a+2b +3	2,459	2,459	2,459	2,459	2,459	12,293

[16] Podle oficiální rozpočtové nomenklatury.

[17] Technická a/nebo administrativní pomoc a výdaje na podporu provádění programů a/nebo akcí EU (bývalé položky „BA“), nepřímý výzkum, přímý výzkum.

○ Operační prostředky CELKEM	Závazky	(4)	2,459	2,459	2,459	2,459	2,459	12,293
	Platby	(5)	2,459	2,459	2,459	2,459	2,459	12,293
○ Prostředky správní povahy financované z rámce na zvláštní programy CELKEM		(6)						
Prostředky z OKRUHŮ 1 až 6 víceletého finančního rámce víceletého finančního rámce **CELKEM**	Závazky	=4+6	2,459	2,459	2,459	2,459	2,459	12,293
	Platby	=5+6	2,459	2,459	2,459	2,459	2,459	12,293

Pokud je návrhem/podnětem dotčen více než jeden operační okruh, zopakuje se výše uvedený oddíl:

○ Operační prostředky CELKEM (všechny operační okruhy)	Závazky	(4)	2,459	2,459	2,459	2,459	2,459	12,293
	Platby	(5)	2,459	2,459	2,459	2,459	2,459	12,293
Prostředky správní povahy financované z rámce na zvláštní programy (všechny operační okruhy) CELKEM		(6)						
Prostředky z OKRUHŮ 1 až 6 víceletého finančního rámce víceletého finančního rámce **CELKEM** (referenční částka)	Závazky	=4+6	2,459	2,459	2,459	2,459	2,459	12,293
	Platby	=5+6	2,459	2,459	2,459	2,459	2,459	12,293

Okruh víceletého finančního rámce	7	Správní výdaje

Tento oddíl se vyplní pomocí „rozpočtových údajů správní povahy“, jež se nejprve uvedou v příloze legislativního finančního výkazu (příloha V interních pravidel), která se pro účely konzultace mezi útvary vloží do aplikace DECIDE.

v milionech EUR (zaokrouhleno na tři desetinná místa)

		Rok **2023**	Rok **2024**	Rok **2025**	Rok **2026**	**Rok 2027**	**CELKEM**
GŘ: DIGIT (CERT-EU)							
○ Lidské zdroje		1,184	2,126	2,754	3,225	3,225	12,514
○ Ostatní správní výdaje		7,938	8,921	8,921	8,921	8,921	43,622
GŘ DIGIT (CERT-EU) CELKEM	Prostředky	9,122	11,047	11,675	12,146	12,146	56,136

CELKEM prostředky z OKRUHU 7 víceletého finančního rámce **CELKEM**	(Závazky celkem = platby celkem)	9,122	11,047	11,675	12,146	12,146	**56,136**

v milionech EUR (zaokrouhleno na tři desetinná místa)

		Rok 2023	Rok 2024	Rok 2025	Rok 2026	Rok 2027	**CELKEM**
Prostředky z OKRUHŮ 1 až 7 víceletého finančního rámce víceletého finančního rámce (*) **CELKEM**	Závazky	11,581	13,506	14,134	14,605	14,605	68,429
	Platby	11,581	13,506	14,134	14,605	14,605	68,429

(*) Příspěvky od samofinancovaných orgánů, institucí a jiných subjektů Unie se odhadují ve výši 2,670 milionu EUR ročně (za pět let celkem 13,350 milionu EUR). Tyto příspěvky budou představovat účelově vázané příjmy centra CERT-EU. Ve výše uvedených tabulkách je uveden pouze odhadovaný celkový dopad na rozpočet Unie a tyto příspěvky v nich nejsou uvedeny.

3.2.2. Odhadovaný výstup financovaný z operačních prostředků

Prostředky na závazky v milionech EUR (zaokrouhleno na tři desetinná místa)

Uveďte cíle a výstupy ⇩			Rok **N**		Rok **N+1**		Rok **N+2**		Rok **N+3**		Vložit počet let podle trvání finančního dopadu (viz bod 1.6)						**CELKEM**	
	VÝSTUPY																	
	Druh[18]	Průměrné náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Celkový počet	Náklady celkem
SPECIFICKÝ CÍL č. 1[19] …																		
– Výstup																		
– Výstup																		
– Výstup																		
Mezisoučet za specifický cíl č. 1																		
SPECIFICKÝ CÍL č. 2 …																		
– Výstup																		
Mezisoučet za specifický cíl č. 2																		
CELKEM																		

[18] Výstupy se rozumí produkty a služby, které mají být dodány (např. počet financovaných studentských výměn, počet vybudovaných kilometrů silnic atd.).

[19] Popsaný v bodě 1.4.2. „Specifické cíle…".

3.2.3. Odhadovaný souhrnný dopad na správní prostředky

– ☐ Návrh/podnět nevyžaduje využití prostředků správní povahy.

– ☑ Návrh/podnět vyžaduje využití prostředků správní povahy, jak je vysvětleno dále:

v milionech EUR (zaokrouhleno na tři desetinná místa)

	Rok 2023	Rok 2024	Rok 2025	Rok 2026	Rok 2027	**CELKEM**
OKRUH 7 víceletého finančního rámce CELKEM						
Lidské zdroje						
Stálí zaměstnanci (třídy AD)	1,099	2,041	2,669	3,14	3,14	12,089
Smluvní zaměstnanci	0,085	0,085	0,085	0,085	0,085	0,425
Ostatní správní výdaje	7,938	8,921	8,921	8,921	8,921	43,622
Mezisoučet za OKRUH 7 víceletého finančního rámce CELKEM	9,122	11,047	11,675	12,146	12,146	56,136

Mimo OKRUH 7[20] víceletého finančního rámce						
Lidské zdroje						
Ostatní výdaje správní povahy						
Mezisoučet mimo OKRUH 7 víceletého finančního rámce CELKEM						

CELKEM	9,122	11,047	11,675	12,146	12,146	56,136

Potřebné prostředky na oblast lidských zdrojů a na ostatní výdaje správní povahy budou pokryty z prostředků GŘ, které jsou již vyčleněny na řízení akce a/nebo byly vnitřně přerozděleny v rámci GŘ a případně doplněny z dodatečného přídělu, který lze řídícímu GŘ poskytnout v rámci ročního přidělování a s ohledem na rozpočtová omezení.

[20] Technická a/nebo administrativní pomoc a výdaje na podporu provádění programů a/nebo akcí EU (bývalé položky „BA“), nepřímý výzkum, přímý výzkum.

3.2.3.1. Odhadované potřeby v oblasti lidských zdrojů

– ☐ Návrh/podnět nevyžaduje využití lidských zdrojů.

– ☑ Návrh/podnět vyžaduje využití lidských zdrojů, jak je vysvětleno dále:

Odhad vyjádřete v přepočtu na plné pracovní úvazky

		Rok 2023	Rok 2024	Rok 2025	Rok 2026	Rok 2027		
O Pracovní místa podle plánu pracovních míst (místa úředníků a dočasných zaměstnanců)								
20 01 02 01 (v ústředí a v zastoupeních Komise)		7	13	17	20	20		
20 01 02 03 (při delegacích)								
01 01 01 01 (v nepřímém výzkumu)								
01 01 01 11 (v přímém výzkumu)								
Jiné rozpočtové položky (upřesněte)								
O Externí zaměstnanci (v přepočtu na plné pracovní úvazky: FTE)[21]								
20 02 01 (SZ, VNO, ZAP z celkového rámce)		1	1	1	1	1		
20 02 03 (SZ, MZ, VNO, ZAP a MOD při delegacích)								
XX 01 xx **yy zz** [22]	– v ústředí							
	– při delegacích							
01 01 01 02 (SZ, VNO, ZAP v nepřímém výzkumu)								
01 01 01 12 (SZ, VNO, ZAP v přímém výzkumu)								
Jiné rozpočtové položky (upřesněte)								
CELKEM		**8**	**14**	**18**	**21**	**21**		

XX je oblast politiky nebo dotčená hlava rozpočtu.

Potřeby v oblasti lidských zdrojů budou pokryty ze zdrojů GŘ, které jsou již vyčleněny na řízení akce a/nebo byly vnitřně přeobsazeny v rámci GŘ, a případně doplněny z dodatečného přídělu, který lze řídícímu GŘ poskytnout v rámci ročního přidělování a s ohledem na rozpočtová omezení.

Popis úkolů:

Úředníci a dočasní zaměstnanci	Úředníci budou plnit úkoly a činnosti centra CERT-EU podle nařízení, zejména kapitol IV a V.
Externí zaměstnanci	Smluvní zaměstnanec bude nápomocen při plnění funkcí sekretariátu Interinstitucionálního výboru pro kybernetickou bezpečnost.

[21] SZ = smluvní zaměstnanec; MZ = místní zaměstnanec; VNO = vyslaný národní odborník; ZAP = zaměstnanec agentury práce; MOD = mladý odborník při delegaci.

[22] Dílčí strop na externí zaměstnance financované z operačních prostředků (bývalé položky „BA“).

3.2.4. Slučitelnost se stávajícím víceletým finančním rámcem

Návrh/podnět:

– ☑ může být v plném rozsahu financován přerozdělením prostředků v rámci příslušného okruhu víceletého finančního rámce (VFR).

Upřesněte, jaká úprava se požaduje, příslušné rozpočtové položky a odpovídající částky. V případě zásadní úpravy přiložte excelovou tabulku.

– ☐ vyžaduje použití nepřiděleného rozpětí v rámci příslušného okruhu VFR a/nebo použití zvláštních nástrojů definovaných v nařízení o VFR.

Upřesněte, co se požaduje, příslušné okruhy a rozpočtové položky, odpovídající částky a navrhované nástroje, které mají být použity.

– ☐ vyžaduje revizi VFR.

Upřesněte, co se požaduje, příslušné okruhy a rozpočtové položky a odpovídající částky.

3.2.5. Příspěvky třetích stran

Návrh/podnět:

– ☑ nepočítá se spolufinancováním od třetích stran[23]

– ☐ počítá se spolufinancováním od třetích stran podle následujícího odhadu:

prostředky v milionech EUR (zaokrouhleno na tři desetinná místa)

	Rok **N**[24]	Rok **N+1**	Rok **N+2**	Rok **N+3**	Vložit počet let podle trvání finančního dopadu (viz bod 1.6)			Celkem
Upřesněte spolufinancující subjekt								
Spolufinancované prostředky CELKEM								

[23] Účelově vázané příjmy pocházející z příležitostného poskytování služeb organizací, které nejsou zúčastněnými subjekty, stanovené v čl. 12 odst. 5 písm. c) nebyly odhadnuty, protože by měly být marginální.

[24] Rokem N se rozumí rok, kdy se návrh/podnět začíná provádět. Výraz „N“ nahraďte předpokládaným prvním rokem provádění (například 2021). Totéž proveďte u let následujících.

3.3. Odhadovaný dopad na příjmy

– ☑ Návrh/podnět nemá žádný finanční dopad na příjmy.

– ☐ Návrh/podnět má tento finanční dopad:

  – ☐ na vlastní zdroje

  – ☐ na jiné příjmy

  – uveďte, zda je příjem účelově vázán na výdajové položky ☐

v milionech EUR (zaokrouhleno na tři desetinná místa)

Příjmová rozpočtová položka:	Prostředky dostupné v běžném rozpočtovém roce	Dopad návrhu/podnětu[25]						
		Rok **N**	Rok **N+1**	Rok **N+2**	Rok **N+3**	Vložit počet let podle trvání finančního dopadu (viz bod 1.6)		
Článek …….								

U účelově vázaných příjmů upřesněte dotčené výdajové rozpočtové položky.

Jiné poznámky (např. způsob/vzorec výpočtu dopadu na příjmy nebo jiné údaje).

[25] Pokud jde o tradiční vlastní zdroje (cla, dávky z cukru), je třeba uvést čisté částky, tj. hrubé částky po odečtení 20 % nákladů na výběr.