EVROPSKÁ UNIE

EVROPSKÝ PARLAMENT **RADA**

Štrasburk 13. prosince 2023
(OR. en)

2022/0085 (COD)
LEX 2289

PE-CONS 57/1/23
REV 1

CYBER 215
TELECOM 267
INST 341
CSC 445
CSCI 163
INF 206
FIN 928
BUDGET 27
DATAPROTECT 236
CODEC 1607

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY, KTERÝM SE STANOVÍ OPATŘENÍ K ZAJIŠTĚNÍ VYSOKÉ SPOLEČNÉ ÚROVNĚ KYBERNETICKÉ BEZPEČNOSTI V ORGÁNECH, INSTITUCÍCH A JINÝCH SUBJEKTECH UNIE

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU, Euratom) 2023/…

ze dne 13. prosince 2023,

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 postoupení návrhu legislativního aktu vnitrostátním parlamentům,

v souladu s řádným legislativním postupem[1],

[1] Postoj Evropského parlamentu ze dne 21. listopadu 2023 (dosud nezveřejněný v Úředním věstníku) a rozhodnutí Rady ze dne 8. prosince 2023.

vzhledem k těmto důvodům:

(1) V digitálním věku tvoří informační a komunikační technologie základ otevřené, efektivní a nezávislé evropské správy. Vyvíjející se technologie a větší složitost a vzájemná propojenost digitálních systémů zesilují kybernetická bezpečnostní rizika, což způsobuje, že subjekty Unie jsou zranitelnější vůči kybernetickým hrozbám a incidentům, a to ohrožuje kontinuitu jejich činností a schopnost zabezpečovat jejich data. Širší využívání služeb cloudu, všudypřítomné používání informačních a komunikačních technologií (IKT), vysoká úroveň digitalizace, práce na dálku a vyvíjející se technologie a propojenost jsou sice základními prvky všech činností subjektů v Unii, zatím však není dostatečně vybudována digitální odolnost.

(2) Prostředí kybernetických hrozeb, jimž jsou vystaveny 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 aktéři hrozeb provádějí své kybernetické útoky, se stále zvyšuje, přičemž jejich kampaně jsou stále sofistikovanější a automatizovanější, zaměřují se na exponované prostory k útoku, které se neustále zvětšují, a rychle využívají zranitelností.

(3) V prostředí IKT subjektů Unie existují vzájemné závislosti a integrované datové toky a jejich uživatelé spolu úzce spolupracují. Tato vzájemná propojenost znamená, že jakékoli narušení, a dokonce i takové narušení, které je původně omezeno na jeden subjekt Unie, může mít širší dominové účinky, jež mohou potenciálně vést k dalekosáhlým a dlouhodobým negativním dopadům na ostatní subjekty Unie. Prostředí IKT některých subjektů Unie je navíc propojeno s prostředím IKT členských států, z čehož vyplývá, že incident týkající se subjektu Unie představuje kybernetické bezpečnostní riziko pro prostředí IKT členských států, a naopak. Sdílení informací týkajících se konkrétních incidentů může usnadnit odhalení podobných kybernetických hrozeb nebo incidentů, jež mají dopad na členské státy.

(4) Subjekty Unie jsou atraktivními cíli, 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 subjektů Unie je tak nezbytné, aby dosáhly vysoké společné úrovně kybernetické bezpečnosti zavedením opatření kybernetické bezpečnosti odpovídajících zjištěným kybernetickým bezpečnostním rizikům, výměnou informací a spoluprací.

(5) Cílem směrnice Evropského parlamentu a Rady (EU) 2022/2555[1] je dále zlepšit kybernetickou odolnost veřejných a soukromých subjektů, příslušných orgánů a subjektů, jakož i Unie jako celku, i jejich schopnosti reagovat na bezpečnostní incidenty. Je proto nezbytné zajistit, aby se zapojily i subjekty Unie tím, že stanoví pravidla, která jsou v souladu se směrnicí (EU) 2022/2555 a odrážejí míru jejích ambicí.

(6) K dosažení vysoké společné úrovně kybernetické bezpečnosti je nezbytné, aby všechny subjekty Unie zavedly vnitřní rámec pro řízení, správu a kontrolu kybernetických bezpečnostních rizik (dále jen „rámec“), který zajistí účinné a obezřetné řízení všech kybernetických bezpečnostních rizik a zohlední požadavky na kontinuitu provozu a krizové řízení. Rámec by měl stanovit politiky v oblasti kybernetické bezpečnosti, včetně cílů a priorit, pro bezpečnost sítí a informačních systémů zahrnující celé neutajované prostředí IKT. Tento rámec by měl být založen na přístupu zohledňujícím všechna rizika, jehož cílem je chránit sítě, informační systémy a fyzické prostředí těchto systémů před takovými událostmi, jako jsou krádež, požár, povodně, selhání telekomunikace nebo výpadek elektrického proudu, nebo jako jsou neoprávněný fyzický přístup k informacím a k zařízením pro zpracování informací subjektu Unie, jejich poškození a zásah do nich, jež by mohly ohrozit dostupnost, pravost, integritu nebo důvěrnost údajů uchovávaných, přenášených, zpracovávaných nebo přístupných prostřednictvím sítí a informačních systémů.

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

(7) Za účelem řízení kybernetických bezpečnostních rizik zjištěných v tomto rámci by měl každý subjekt Unie přijmout vhodná a přiměřená technická, operační a organizační opatření. Tato opatření by se měla zabývat oblastmi a opatřeními k řízení kybernetických bezpečnostních rizik upravenými v tomto nařízení s cílem posílit kybernetickou bezpečnost každého subjektu Unie.

(8) Aktiva a kybernetická bezpečnostní rizika zjištěná v tomto rámci, jakož i závěry vyplývající z pravidelných hodnocení vyspělosti kybernetické bezpečnosti, by měly být zohledněny v plánu kybernetické bezpečnosti vypracovaném každým subjektem Unie. Plán kybernetické bezpečnosti by měl zahrnovat přijatá opatření k řízení kybernetických bezpečnostních rizik.

(9) Vzhledem k tomu, že zajištění kybernetické bezpečnosti je nepřetržitý proces, měla by být vhodnost a účinnost opatření přijatých podle tohoto nařízení pravidelně revidována s ohledem na měnící se kybernetická bezpečnostní rizika, aktiva a vyspělost kybernetické bezpečnosti subjektů Unie. Rámec by měl být pravidelně a nejméně jednou za čtyři roky přezkoumáván, zatímco plán kybernetické bezpečnosti by měl být revidován jednou za dva roky, nebo častěji, je-li to nezbytné na základě hodnocení vyspělosti kybernetické bezpečnosti nebo v souvislosti s jakýmkoli významným přezkumem rámce.

(10) Opatření k řízení kybernetických bezpečnostních rizik zavedená subjekty Unie by měla zahrnovat politiky, jejichž cílem je, tam kde je to možné, zajištění transparentnosti zdrojového kódu, s ohledem na ochranu práv třetích stran či subjektů Unie. Tyto politiky by měly být přiměřené kybernetickému bezpečnostnímu riziku a měly by usnadňovat analýzu kybernetických hrozeb, aniž by přitom zakládaly povinnost zveřejnit kód třetí strany nebo k němu poskytnout právo přístupu nad rámec platných smluvních podmínek.

(11) Nástroje a aplikace v oblasti kybernetické bezpečnosti s otevřeným zdrojovým kódem mohou přispět k vyšší míře otevřenosti. Otevřené standardy usnadňují interoperabilitu mezi bezpečnostními nástroji a přispívají k bezpečnosti zúčastněných stran. Nástroje a aplikace v oblasti kybernetické bezpečnosti s otevřeným zdrojovým kódem mohou umožnit využití širší komunity vývojářů, a umožnit tak diverzifikaci dodavatelů. Otevřený zdrojový kód může zvýšit transparentnost při ověřování nástrojů souvisejících s kybernetickou bezpečností a umožnit odhalování zranitelností komunitou. Subjekty Unie by proto měly mít možnost podporovat používání softwaru s otevřeným zdrojovým kódem a otevřené standardy tím, že budou provádět politiky spojené s využíváním otevřených dat a otevřených zdrojů v rámci přístupu „bezpečnost prostřednictvím transparentnosti“.

(12) Rozdíly mezi subjekty Unie vyžadují pružnost při provádění tohoto nařízení. Opatření k zajištění vysoké společné úrovně kybernetické bezpečnosti stanovená tímto nařízením by neměla obsahovat žádné povinnosti přímo zasahující do plnění úkolů subjektů Unie nebo narušující jejich institucionální autonomii. Tyto subjekty by tudíž měly zavést své vlastní rámce a přijmout svá vlastní opatření k řízení kybernetických bezpečnostních rizik a plány kybernetické bezpečnosti. Při provádění těchto opatření by měly být náležitě zohledněny stávající synergie mezi subjekty Unie s cílem zajistit řádné řízení zdrojů a optimalizaci nákladů. Náležitou pozornost je rovněž třeba věnovat tomu, aby opatření neměla negativní dopad na účinnou výměnu informací a spolupráci mezi subjekty Unie a mezi subjekty Unie a jejich protějšky v členských státech.

(13) Toto nařízení by v zájmu optimalizace využívání zdrojů mělo umožnit, aby dva nebo více subjektů Unie s podobnou strukturou mohly spolupracovat při hodnocení vyspělosti kybernetické bezpečnosti svých příslušných subjektů.

(14) Požadavky na řízení kybernetických bezpečnostních rizik by měly být úměrné kybernetickému bezpečnostnímu riziku, jež dané sítě nebo informační systémy obnáší, aby na subjekty Unie nebyla kladena nepřiměřená finanční a administrativní zátěž, a to s ohledem na nejnovější technický vývoj takových opatření. Cílem každého subjektu Unie by mělo být, aby přiměřenou část svého rozpočtu na IKT vynaložil na zlepšení úrovně své kybernetické bezpečnosti. Z dlouhodobého hlediska by měl být sledován orientační cíl v řádu alespoň 10 %. Při hodnocení vyspělosti kybernetické bezpečnosti by mělo být rovněž zhodnoceno, zda jsou výdaje subjektu Unie na kybernetickou bezpečnost úměrné kybernetickým bezpečnostním rizikům, kterým čelí. Aniž tím jsou dotčena pravidla týkající se ročního rozpočtu Unie podle Smluv, by Komise měla ve svém návrhu prvního ročního rozpočtu, který bude přijímán po vstupu tohoto nařízení v platnost, při posuzování rozpočtových a personálních potřeb subjektů Unie plynoucích z jejich odhadu výdajů zohlednit povinnosti vyplývající z tohoto nařízení.

(15) Vyšší společná úroveň kybernetické bezpečnosti vyžaduje, aby dohled nad kybernetickou bezpečností přešel na nejvyšší úroveň vedení každého subjektu Unie. Za provádění tohoto nařízení, včetně zřízení daného rámce, přijímání opatření k řízení kybernetických bezpečnostních rizik a schvalování plánu kybernetické bezpečnosti, by měla být odpovědná nejvyšší úroveň vedení daného subjektu Unie. Nedílnou součásti rámce a příslušných opatření k řízení kybernetických bezpečnostních rizik ve všech subjektech Unie je řešení kultury kybernetické bezpečnosti, tedy každodenní praxe v oblasti kybernetické bezpečnosti.

(16) Bezpečnost sítí a informačních systémů, které nakládají s utajovanými informacemi EU, je zásadně důležitá. Subjekty Unie, které nakládají s utajovanými informacemi EU, jsou povinny používat komplexní regulační rámce, které byly zavedeny na ochranu těchto informací, včetně zvláštních zásad správy, politik a postupů řízení rizik. Je nezbytné, aby sítě a informační systémy, které nakládají s utajovanými informacemi EU, dodržovaly přísnější bezpečnostní standardy než neutajované sítě a informační systémy. Proto jsou sítě a informační systémy, které nakládají s utajovanými informacemi EU, odolnější vůči kybernetickým hrozbám a incidentům. Potřeba společného rámce se v tomto ohledu sice uznává, ovšem z výše uvedených důvodů by se toto nařízení nemělo uplatňovat na sítě a informační systémy, které nakládají s utajovanými informacemi. Nicméně, pokud o to některý subjekt Unie výslovně požádá, měl by být tým pro reakci na počítačové hrozby v orgánech, institucích a jiných subjektech EU (dále jen „CERT-EU“) schopen poskytnout tomuto subjektu Unie pomoc v souvislosti s incidenty v utajovaných prostředích IKT.

(17) Subjekty Unie by měly posuzovat kybernetická bezpečnostní 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. Opatření kybernetické bezpečnosti by měla být dále upřesněna v pokynech nebo doporučeních CERT-EU. Při stanovení opatření a pokynů by měl být náležitě zohledněn nejnovější technologický vývoj a případně příslušné evropské a mezinárodní standardy, jakož i příslušné právní předpisy a politiky Unie, včetně posouzení kybernetických bezpečnostních rizik a doporučení vydávaných skupinou pro spolupráci zřízenou podle článku 14 směrnice (EU) 2022/2555, jako je koordinované posouzení rizik kybernetické bezpečnosti sítí 5G v EU a souboru opatření EU pro kybernetickou bezpečnost sítí 5G. S ohledem na situaci v oblasti kybernetických hrozeb a důležitost vybudování kybernetické odolnosti subjektů Unie by mohla být navíc vyžadována certifikace příslušných produktů, služeb a procesů IKT, a to v rámci konkrétních evropských systémů certifikace kybernetické bezpečnosti přijatých podle článku 49 nařízení Evropského parlamentu a Rady (EU) 2019/881[1].

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

(18) Generální tajemníci orgánů a institucí Unie se v květnu 2011 rozhodli zřídit přípravný tým CERT-EU, na který bude dohlížet interinstitucionální řídící rada. V červenci 2012 potvrdili generální tajemníci praktická ujednání a dohodli se na tom, že CERT-EU zůstane zachován 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 ustaven pracovní skupinou Komise s interinstitucionálním mandátem. V prosinci 2017 uzavřely orgány a instituce Unie interinstitucionální ujednání o organizaci a fungování CERT-EU[1]. Toto nařízení by mělo poskytnout komplexní soubor pravidel ohledně organizace, fungování a provozu CERT-EU. Ustanovení tohoto nařízení mají přednost před ustanoveními interinstitucionálního ujednání o organizaci a fungování CERT-EU, které bylo uzavřeno v prosinci 2017.

(19) CERT-EU by mělo být přejmenován na Službu kybernetické bezpečnosti pro orgány, instituce a jiné subjekty Unie, avšak měl by si ponechat zkrácený název „CERT-EU“, který je již známý.

---

[1] Ujednání mezi Evropským parlamentem, Evropskou radou, Radou Evropské unie, Evropskou komisí, Soudním dvorem Evropské unie, Evropskou centrální bankou, Evropským účetním dvorem, Evropskou službou pro vnější činnost, Evropským hospodářským a sociálním výborem, Evropským výborem regionů a Evropskou investiční bankou o organizaci a fungování týmu pro reakci na počítačové hrozby pro orgány, instituce a jiné subjekty Unie (CERT-EU) (Úř. věst. C 12, 13.1.2018, s. 1).

(20) Kromě uložení více úkolů CERT-EU a rozšíření její úlohy, toto nařízení zřizuje Interinstitucionální výbor pro kybernetickou bezpečnost (dále jen „výbor IICB“) k dosažení vysoké společné úrovně kybernetické bezpečnosti u subjektů Unie. Výbor IICB by měl hrát výlučnou roli při sledování a podpoře provádění tohoto nařízení ze strany subjektů Unie a při dohledu nad plněním obecných priorit a cílů CERT-EU a poskytovat CERT-EU strategické řízení. Výbor IICB by proto měl zajišťovat zastoupení orgánů Unie a zahrnovat zástupce orgánů, institucí a jiných subjektů Unie prostřednictvím sítě agentur EU (EUAN). Organizace a fungování výboru IICB by se měly dále řídit vnitřním jednacím řádem, který může zahrnovat další upřesnění pravidelných zasedání výboru IICB, včetně každoročních setkání na politické úrovni, na nichž by zástupci nejvyšší úrovně vedení každého člena výboru IICB umožnili tomuto výboru vést strategickou diskusi a poskytli by mu strategické pokyny. Kromě toho by měl mít výbor IICB možnost zřídit výkonný výbor, který mu bude nápomocen při jeho práci, a delegovat na něj některé ze svých úkolů a pravomocí, zejména pokud jde o úkoly, které vyžadují zvláštní odborné znalosti jeho členů, například schválení katalogu služeb a jeho následné aktualizace, ujednání pro smlouvy o poskytování služeb, posuzování dokumentů a zpráv předložených subjekty Unie výboru IICB podle tohoto nařízení, nebo úkoly související s přípravou rozhodnutí o opatřeních k zajištění dodržování povinností vydaných výborem IICB a se sledováním jejich provádění. Výbor IICB by měl stanovit jednací řád výkonného výboru, včetně jeho úkolů a pravomocí.

(21) Cílem výboru IICB je podporovat subjekty Unie při zlepšování stavu jejich kybernetické bezpečnosti prováděním tohoto nařízení. Za účelem podpory subjektů Unie by výbor IICB měl poskytovat poradenství vedoucímu CERT-EU, přijmout víceletou strategii ke zvýšení úrovně kybernetické bezpečnosti v subjektech Unie, stanovit metodiku a jiné aspekty dobrovolných vzájemných hodnocení a usnadnit zřízení neformální skupiny místních referentů pro kybernetickou bezpečnost, podporované Agenturou Evropské unie pro kybernetickou bezpečnost (ENISA), za účelem výměny osvědčených postupů a informací v souvislosti s prováděním tohoto nařízení.

(22) V zájmu dosažení vysoké úrovně kybernetické bezpečnosti ve všech subjektech Unie by měly být zájmy orgánů, institucí a jiných subjektů Unie, které provozují své vlastní prostředí IKT, ve výboru IICB zastupovány třemi zástupci jmenovanými EUAN. Základem ochrany údajů je bezpečnost při zpracovávání osobních údajů, a tudíž i související kybernetická bezpečnost. S ohledem na synergie mezi ochranou údajů a kybernetickou bezpečností by měl být ve výboru IICB zastoupen evropský inspektor ochrany údajů jakožto subjekt Unie podléhající tomuto nařízení s konkrétními odbornými zkušenostmi v oblasti ochrany údajů, zahrnujícími bezpečnost sítí elektronické komunikace. Vzhledem k důležitosti inovací a konkurenceschopnosti v oblasti kybernetické bezpečnosti by mělo být ve výboru IICB zastoupeno Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost. Dále by měly být ve výboru IICB zastoupeny ENISA a Agentura Evropské unie pro Kosmický program, a to vzhledem k úloze ENISA jakožto odborného centra pro kybernetickou bezpečnost a k podpoře, kterou poskytuje, a s ohledem na důležitost kybernetické bezpečnosti kosmické infrastruktury a služeb Unie. S ohledem na roli, která byla přidělena CERT-EU tímto nařízením, by měl předseda výboru IICB zvát vedoucího CERT-EU na všechny schůze výboru IICB, s výjimkou případů, kdy výbor IICB diskutuje o otázkách přímo se týkajících vedoucího CERT-EU.

(23) Výbor IICB by měl sledovat dodržování tohoto nařízení, jakož i provádění pokynů a doporučení a výzev k přijetí opatření. V technických záležitostech by měly výbor IICB podporovat technické poradní skupiny ve složení, jež výbor IICB považuje za vhodné. Tyto technické poradní skupiny by měly dle potřeby úzce spolupracovat se CERT-EU, subjekty Unie a dalšími zúčastněnými stranami.

(24) Pokud výbor IICB zjistí, že některý subjekt Unie toto nařízení nebo pokyny, doporučení či výzvy k přijetí opatření vydané podle tohoto nařízení, účinně neprovedl, měl by mít možnost, aniž by byly dotčeny interní postupy dotčeného subjektu Unie, přistoupit k opatřením k zajištění dodržování povinností. Výbor IICB by měl opatření k zajištění dodržování povinností uplatňovat progresivně, jinými slovy by měl nejprve přijmout nejméně přísné opatření, tedy odůvodněné stanovisko, a pouze pokud jsou nutné stále přísnější opatření, až po to nejpřísnější, tedy doporučení k dočasnému pozastavení datových toků do dotčeného subjektu Unie. Toto doporučení by se mělo uplatnit pouze ve výjimečných případech dlouhodobých, úmyslných, opakovaných či závažných porušování tohoto nařízení dotčeným subjektem Unie.

(25) Odůvodněné stanovisko představuje nejméně přísné opatření k zajištění dodržování povinností, které se zaměřuje na zjištěné nedostatky při provádění tohoto nařízení. Výbor IICB by měl mít možnost vydat v návaznosti na odůvodněné stanovisko pokyny, které subjektu Unie pomohou zajistit soulad jeho rámce, opatření k řízení kybernetických bezpečnostních rizik, plánu kybernetické bezpečnosti a zpráv s tímto nařízením, a následně varování, aby byly zjištěné nedostatky subjektu Unie vyřešeny v rámci určené lhůty. Pokud nedostatky uvedené ve varování nebyly řádně vyřešeny, měl by mít výbor IICB možnost vydat odůvodněné oznámení.

(26) Výbor IICB by měl mít možnost doporučit, aby byl proveden audit subjektu Unie. Subjekt Unie by měl mít možnost za tímto účelem využít svou službu interního auditu. Výbor IICB by rovněž měl mít možnost požádat, aby audit provedl auditní útvar třetí strany, a to i útvar vzájemně dohodnutého poskytovatele služeb ze soukromého sektoru.

(27) Ve výjimečných případech dlouhodobých, úmyslných, opakovaných nebo závažných porušování tohoto nařízení subjektem Unie by měl mít výbor IICB možnost jako krajní opatření doporučit všem členským státům a subjektům Unie dočasné pozastavení datových toků do daného subjektu Unie, které by mělo platit do doby, než tento subjekt Unie příslušné porušování ukončí. Toto doporučení by mělo být sděleno prostřednictvím vhodných a zabezpečených komunikačních kanálů.

(28) Pokud se výbor IICB domnívá, že trvalé porušování tohoto nařízení ze strany subjektu Unie vyplývá přímo z jednání nebo opomenutí jeho zaměstnance, a to i na nejvyšší úrovni vedení, měl by v zájmu zajištění správného provádění tohoto nařízení dotčený subjekt Unie požádat, aby přijal příslušná opatření, přičemž jej může požádat i o to, aby zvážil přijetí opatření disciplinární povahy, v souladu s pravidly a postupy stanovenými ve služebním řádu úředníků Evropské unie a pracovním řádu ostatních zaměstnanců Evropské unie, které jsou uvedeny v nařízení Rady (EHS, Euratom, ESUO) č. 259/68[1] (dále jen „služební řád“), a veškerými dalšími platným pravidly a postupy.

(29) Úkolem CERT-EU by mělo být přispívat k bezpečnosti prostředí IKT ve všech subjektech Unie. Při zvažování, zda na žádost subjektu Unie poskytnout technické poradenství nebo podněty k příslušným politickým záležitostem, by CERT-EU měla zajistit, aby to nebránilo plnění jejích dalších úkolů, které jí byly svěřeny tímto nařízením. CERT-EU by měla jednat jako koordinátor subjektů Unie pro účely koordinovaného zpřístupňování informací o zranitelnostech podle čl. 12 odst. 1 směrnice (EU) 2022/2555.

[1] Nařízení Rady (EHS, Euratom, ESUO) č. 259/68 ze dne 29. února 1968, kterým se stanoví služební řád úředníků a pracovní řád ostatních zaměstnanců Evropských společenství a kterým se zavádějí zvláštní opatření dočasně použitelná na úředníky Komise (Úř. věst. L 56, 4.3.1968, s. 1).

(30) CERT-EU by měla 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 CERT-EU měla vydávat výzvy k přijetí opatření popisující naléhavá bezpečnostní opatření, jimiž jsou subjekty Unie naléhavě vyzvány, aby ve stanovené lhůtě příslušná opatření přijaly. Výbor IICB by měl uložit CERT-EU, aby vydala, stáhla nebo upravila návrh pokynů nebo doporučení nebo výzvy k přijetí opatření.

(31) CERT-EU by rovněž měla plnit úlohu, kterou pro ni stanoví směrnice (EU) 2022/2555 v oblasti spolupráce a výměny informací s týmy pro reakce na počítačové bezpečnostní incidenty (dále jen „týmy CSIRT“) podle článku 15 dané směrnice. V souladu s doporučením Komise (EU) 2017/1584[1] by CERT-EU kromě toho měla spolupracovat a koordinovat reakce s příslušnými zúčastněnými stranami. Aby mohla CERT-EU přispívat k vysoké úrovni kybernetické bezpečnosti v Unii, měla by sdílet informace týkající se konkrétních incidentů s partnery v členských státech. CERT-EU by mělo rovněž spolupracovat s jinými protějšky z veřejného i soukromého sektoru, včetně Organizace Severoatlantické smlouvy, a to po předchozím schválení výborem IICB.

[1] 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).

(32) Při podpoře operační kybernetické bezpečnosti by CERT-EU měla využívat dostupné odborné znalosti ENISA, a to prostřednictvím strukturované spolupráce, jak stanoví nařízení (EU) 2019/881. V případě potřeby by měla být učiněna speciální ujednání mezi oběma subjekty o praktické podobě takové spolupráce a k zabránění zdvojování činností. CERT-EU by měla spolupracovat s ENISA při analýze kybernetických hrozeb a pravidelně s touto agenturou sdílet svou zprávu o prostředí hrozeb.

(33) CERT-EU by měla mít možnost spolupracovat a vyměňovat si informace s příslušnými komunitami v oblasti kybernetické bezpečnosti v Unii a jejích členských státech s cílem podpořit operační spolupráci a umožnit stávajícím sítím realizovat jejich plný potenciál při ochraně Unie.

(34) Jelikož služby a úkoly CERT-EU jsou v zájmu subjektů Unie, měl by každý subjekt Unie s výdaji v oblasti IKT přispívat na tyto služby a úkoly spravedlivým dílem. Těmito příspěvky není dotčena rozpočtová autonomie subjektů Unie.

(35) Mnohé kybernetické útoky jsou součástí širších kampaní, které cílí na skupiny subjektů Unie nebo na zájmové komunity, jichž jsou subjekty Unie součástí. S cílem umožnit aktivní odhalování incidentů, reakci na incidenty nebo opatření ke zmírnění dopadů incidentů a zotavení z incidentů by subjekty Unie měly CERT-EU oznamovat incidenty, kybernetické hrozby, zranitelnosti a významné události a sdílet odpovídající technické údaje, jež umožní odhalovat podobné incidenty, kybernetické hrozby, zranitelnosti a významné události v rámci jiných subjektů Unie, zmírňovat jejich dopady a reagovat na ně. Postupem odpovídajícím postupu podle směrnice (EU) 2022/2555 by subjekty Unie měly mít povinnost podat CERT-EU včasné varování do 24 hodin poté, co se dozví o významném incidentu. Taková výměna informací by měla CERT-EU umožnit šířit tyto informace jiným subjektům Unie, jakož i vhodným protějškům, s cílem pomoci chránit prostředí IKT subjektů Unie a prostředí IKT protějšků subjektů Unie před podobnými incidenty.

(36) Toto nařízení stanoví vícestupňový přístup k hlášení významných incidentů, tak aby bylo dosaženo vhodné rovnováhy mezi rychlým oznamováním, které pomáhá omezit potenciální šíření významných incidentů a umožňuje subjektům Unie žádat o pomoc, na jedné straně, a podrobným oznamováním, které čerpá cenná poučení z jednotlivých incidentů a průběžně zvyšuje kybernetickou odolnost jednotlivých subjektů Unie a přispívá ke zlepšení celkového stavu jejich kybernetické bezpečnosti, na straně druhé. V tomto ohledu by toto nařízení mělo zahrnovat ohlašování incidentů, které by podle počátečního posouzení provedeného dotčeným subjektem Unie mohly subjektu Unie způsobit vážné provozní narušení fungování nebo finanční ztrátu nebo by mohly mít dopad na jiné fyzické či právnické osoby tím, že by způsobily značnou hmotnou či nehmotnou újmu. Toto počáteční posouzení by mělo mimo jiné zohlednit dotčené sítě a informační systémy, zejména jejich význam pro fungování subjektu Unie, závažnost a technické vlastnosti kybernetické hrozby a veškeré související zranitelnosti, které jsou zneužívány, jakož i zkušenosti subjektu Unie s podobnými incidenty. Při určování toho, zda je narušení provozu závažné, by mohly hrát důležitou roli ukazatele, jako je míra dopadu na fungování subjektu Unie, doba trvání incidentu nebo počet dotčených fyzických nebo právnických osob.

(37) Vzhledem k tomu, že infrastruktura, sítě a informační systémy příslušného subjektu Unie a členského státu, v němž se tento subjekt Unie nachází, jsou propojené, je zásadní, aby byl tento členský stát o významném incidentu v rámci tohoto subjektu Unie bez zbytečného odkladu informován. Proto by dotčený subjekt Unie měl informovat všechny příslušné protějšky v členských státech určené nebo zřízené podle článků 8 a 10 směrnice (EU) 2022/2555 o výskytu významného incidentu, který nahlašuje CERT-EU. Pokud se CERT-EU dozví o významném incidentu v členském státě, měla by informovat příslušný protějšek v daném členském státě.

(38) Měl by být zaveden mechanismus pro zajištění účinné výměny informací, koordinace a spolupráce subjektů Unie v případě závažných incidentů, včetně jasného rozdělení úloh a povinností zapojených subjektů Unie. Zástupce Komise v IICB by měl být, podle plánu pro řešení kybernetických krizí, kontaktním místem, který výboru IICB usnadní sdílení relevantních informací v souvislosti se závažnými incidenty s Evropskou sítí styčných organizací pro řešení kybernetických krizí (dále jen „síť EU-CyCLONe“), čímž se přispěje k vytváření společného přehledu o aktuální situaci. Rolí zástupce Komise jako kontaktního místa ve výboru IICB by neměla být dotčena samostatná a odlišná role Komise v síti EU-CyCLONe podle čl. 16 odst. 2 směrnice (EU) 2022/2555.

(39) Na zpracovávání osobních údajů podle tohoto nařízení se použije nařízení Evropského parlamentu a Rady (EU) 2018/1725[1]. K tomuto zpracovávání osobních údajů by mohlo dojít v souvislosti s opatřeními přijatými v rámci řešení kybernetických bezpečnostních rizik, zranitelností a řešení incidentu, při sdílení informací o incidentech, kybernetických hrozbách a zranitelnostech a při koordinaci a spolupráci v rámci reakce na incident. Takováto opatření by mohla vyžadovat zpracování určitých kategorií osobních údajů, jako jsou IP adresy, jednotné adresy zdroje (URLs), doménová jména, e-mailové adresy, postavení subjektů údajů v organizaci, časová razítka, předměty emailů nebo názvy souborů. Veškerá opatření přijatá podle tohoto nařízení by měla být v souladu s rámcem pro ochranu údajů a soukromí a subjekty Unie, CERT-EU a případně výbor IICB by měly přijmout veškeré příslušné technické a organizační opatření, aby byl tento soulad zajištěn odpovědným způsobem.

(40) Toto nařízení stanoví právní základ pro zpracování osobních údajů ze strany subjektů Unie, CERT-EU a případně výboru IICB pro účely plnění jejich úkolů a povinností podle tohoto nařízení v souladu s čl. 5 odst. 1 písm. b) nařízení (EU) 2018/1725. CERT-EU může jednat v postavení zpracovatele nebo správce v závislosti na úkolu, který podle nařízení (EU) 2018/1725 vykonává.

---

[1] 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).

(41) V některých případech může být nutné, aby subjekty Unie a CERT-EU za účelem plnění svých povinností podle tohoto nařízení k zajištění vysoké úrovně kybernetické bezpečnosti, a zejména v souvislosti s řešením zranitelností a incidentů, zpracovávaly zvláštní kategorie osobních údajů uvedené v čl. 10 odst. 1 nařízení (EU) 2018/1725. Toto nařízení stanoví právní základ pro zpracování zvláštních kategorií osobních údajů subjekty Unie a CERT-EU v souladu s čl. 10 odst. 2 písm. g) nařízení (EU) 2018/1725. Zpracování zvláštních kategorií osobních údajů podle tohoto nařízení by mělo být přísně přiměřené sledovanému cíli. Za dodržení podmínek stanovených v čl. 10 odst. 2 písm. g) uvedeného nařízení by subjekty Unie a CERT-EU měly mít možnost zpracovávat tyto údaje pouze v nezbytném rozsahu a v případech výslovně stanovených v tomto nařízení. Při zpracovávání zvláštních kategorií osobních údajů by subjekty Unie a CERT-EU měly respektovat podstatu práva na ochranu údajů a stanovit vhodná a konkrétní opatření na ochranu základních práv a zájmů subjektů údajů.

(42) Podle článku 33 nařízení (EU) 2018/1725 by subjekty Unie a CERT-EU měly s přihlédnutím ke stavu techniky, nákladům na provedení a povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob zavést vhodná technická a organizační opatření k zajištění odpovídající úrovně zabezpečení osobních údajů, což zahrnuje např. poskytování omezených přístupových práv na základě zásady „vědět jen to nejnutnější“, uplatňování zásad auditní stopy, zřízení kontrolního řetězce, uchovávání údajů v kontrolovaném a kontrolovatelném prostředí, standardizované provozní postupy a opatření na ochranu soukromí, jako jsou pseudonymizace nebo šifrování. Tato opatření by neměla být prováděna způsobem, který by měl vliv účel řešení incidentů a integritu důkazů. Pokud subjekt Unie nebo CERT-EU protistraně nebo partnerovi předává pro účely tohoto nařízení osobní údaje související s incidentem, včetně zvláštních kategorií osobních údajů, mělo by být předání těchto údajů v souladu s nařízením (EU) 2018/1725. Pokud jsou zvláštní kategorie osobních údajů předávány třetí straně, měly by subjekty Unie a CERT-EU zajistit, aby tato třetí strana uplatňovala opatření týkající se ochrany osobních údajů na úrovni rovnocenné s nařízením (EU) 2018/1725.

(43) V souladu s nařízením (EU) 2018/1725 by osobní údaje zpracovávané pro účely tohoto nařízení měly být uchovávány pouze po dobu nezbytně nutnou. Plní-li subjekty Unie a případně CERT-EU úlohu správce, měly by stanovit lhůty pro uchovávání údajů, které jsou omezeny na dobu nezbytnou k dosažení stanovených účelů. Zejména v souvislosti s osobními údaji shromažďovanými pro účely řešení incidentů by měly subjekty Unie a CERT-EU rozlišovat mezi osobními údaji, které jsou shromažďovány za účelem odhalování kybernetické hrozby v jejich prostředí IKT, aby se incidentu zabránilo, a osobními údaji, které jsou shromažďovány za účelem zmírnění dopadu incidentu, reakce na něj a zotavení z něj. Pro odhalování kybernetické hrozby je důležité vzít v úvahu dobu, po kterou může aktér hrozby zůstat v systému neodhalen. Pro zmírnění dopadu incidentu, reakci na něj a zotavení z něj je důležité zvážit, zda jsou osobní údaje nezbytné k vysledování a řešení opakujícího se incidentu nebo incidentu podobné povahy, který by s ním mohl souviset.

(44) Nakládání s informacemi ze strany subjektů Unie a CERT-EU by mělo být v souladu s platnými pravidly pro bezpečnost informací. Zahrnutí bezpečnosti lidských zdrojů mezi opatření k řízení kybernetických bezpečnostních rizik by mělo být rovněž provedeno v souladu s platnými pravidly.

(45) Pro účely sdílení informací se používají viditelná označení, jimiž se poukazuje na to, že příjemci informací je mohou sdílet jen omezeně, a to zejména označení podle dohod o mlčenlivosti nebo neformálních dohod o mlčenlivosti, jako je TLP protokol (Trafic light protocol), nebo jiné jasné označení ze strany původce informací TLP protokol je třeba chápat jako prostředek k poskytování informací o jakýchkoli omezeních, pokud jde o další šíření informací. Používá se téměř ve všech týmech CSIRT a v některých střediscích pro analýzu a sdílení informací.

(46) Toto nařízení by mělo být pravidelně vyhodnocováno s ohledem na budoucí jednání o víceletých rozpočtových rámcích, což umožní přijímat další rozhodnutí, pokud jde o fungování a institucionální úlohu CERT-EU, včetně případného ustanovení CERT-EU úřadem Unie.

(47) Výbor IICB by měl za pomoci CERT-EU přezkoumat a vyhodnotit provádění tohoto nařízení a měl 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. Tato zpráva by měla s využitím materiálu poskytnutého výborem IICB vyhodnotit, zda je vhodné zahrnout do oblasti působnosti tohoto nařízení sítě a informační systémy, které nakládají s utajovanými informacemi EU, a to zejména s ohledem na to, že pro bezpečnost informací neexistují pro subjekty Unie společná pravidla.

(48) V souladu se zásadou proporcionality je pro dosažení základního cíle, jímž je vysoká společná úroveň kybernetické bezpečnosti v rámci subjektů Unie, nezbytné a vhodné stanovit pravidla pro kybernetickou bezpečnost subjektů Unie. Toto nařízení nepřekračuje rámec toho, co je pro dosažení sledovaných cílů nezbytné v souladu s čl. 5 odst. 4 Smlouvy o Evropské unii.

(49) Toto nařízení odráží skutečnost, že subjekty Unie se liší velikostí a kapacitou, a to i pokud jde o finanční a lidské zdroje.

(50) Evropský inspektor ochrany údajů byl konzultován v souladu s čl. 42 odst. 1 nařízení (EU) 2018/1725 a dne 17. května 2022 vydal své stanovisko[1],

PŘIJALY TOTO NAŘÍZENÍ:

[1] Úř. věst. C 258, 5.7.2022, s. 10.

Kapitola I
Obecná ustanovení

Článek 1

Předmět

Toto nařízení stanoví opatření, jejichž cílem je dosáhnout vysoké společné úrovně kybernetické bezpečnosti v rámci subjektů Unie, pokud jde o:

a) zřízení vnitřního rámce pro řízení, správu a kontrolu kybernetických bezpečnostních rizik podle článku 6 každým subjektem Unie;

b) řízení kybernetických bezpečnostních rizik, oznamování a sdílení informací;

c) organizaci, fungování a provoz interinstitucionálního výboru pro kybernetickou bezpečnost zřízeného podle článku 10, jakož i organizaci, fungování a provoz služby kybernetické bezpečnosti pro orgány, instituce a jiné subjekty Unie (dále jen „CERT-EU“);

d) monitorování provádění tohoto nařízení.

Článek 2

Oblast působnosti

1. Toto nařízení se vztahuje na subjekty Unie, na interinstitucionální výbor pro kybernetickou bezpečnost zřízený podle článku 10 a na CERT-EU.

2. Tímto nařízením není dotčena institucionální autonomie podle Smluv.

3. S výjimkou čl. 13 odst. 8 se toto nařízení nevztahuje na sítě a informační systémy, které nakládají s utajovanými informacemi EU (EUCI).

Článek 3

Definice

Pro účely tohoto nařízení se rozumí:

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

2) „sítí a informačním systémem“ síť a informační systémy ve smyslu čl. 6 bodu 1 směrnice (EU) 2022/2555;

3) „bezpečností sítí a informačních systémů“ bezpečnost sítí a informačních systémů ve smyslu čl. 6 bodu 2 směrnice (EU) 2022/2555;

4) „kybernetickou bezpečností“ kybernetická bezpečnost ve smyslu čl. 2 bodu 1 nařízení (EU) 2019/881;

5) „nejvyšší úrovní vedení“ vedoucí, vedoucí orgán nebo koordinační orgán a orgán dohledu odpovědný za fungování subjektu Unie na nejvyšší správní úrovni, který má pravomoc přijímat nebo schvalovat rozhodnutí v souladu s opatřeními pro řízení na vysoké úrovni uvedeného subjektu Unie, aniž je dotčena formální odpovědnost jiných úrovní vedení za dodržování pravidel a řízení kybernetických rizik v jejich příslušných oblastech působnosti;

6) „významnou událostí“ významná událost ve smyslu čl. 6 bodu 5 směrnice (EU) 2022/2555;

7) „incidentem“ incident ve smyslu čl. 6 bodu 6 směrnice (EU) 2022/2555;

8) „závažným incidentem“ incident, který způsobí míru narušení, která přesahuje schopnost subjektu Unie a CERT-EU reagovat na tento incident, nebo který má významný dopad na nejméně dva subjekty Unie;

9) „rozsáhlým kybernetickým bezpečnostním incidentem“ rozsáhlý kybernetický bezpečnostní incident ve smyslu čl. 6 bodu 7 směrnice (EU) 2022/2555;

10) „řešením incidentu“ řešení incidentu ve smyslu čl. 6 bodu 8 směrnice (EU) 2022/2555;

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

12) „významnou kybernetickou hrozbou“ významná kybernetická hrozba ve smyslu čl. 6 bodu 11 směrnice (EU) 2022/2555;

(13) „zranitelností“ zranitelnost ve smyslu čl. 6 bodu 15 směrnice (EU) 2022/2555;

14) „kybernetickým bezpečnostním rizikem“ riziko ve smyslu čl. 6 bodu 9 směrnice (EU) 2022/2555;

15) „službou cloud computingu“ služba cloud computingu ve smyslu čl. 6 bodu 30 směrnice (EU) 2022/2555.

Článek 4

Zpracování osobních údajů

1. Zpracování osobních údajů podle tohoto nařízení CERT-EU, Interinstitucionálním výborem pro kybernetickou bezpečnost zřízeným podle článku 10 a subjekty Unie se provádí v souladu s nařízením (EU) 2018/1725.

2. Pokud CERT-EU, interinstitucionální výbor pro kybernetickou bezpečnost zřízený podle článku 10 a subjekty Unie plní úkoly nebo povinnosti podle tohoto nařízení, zpracovávají a vyměňují si osobní údaje pouze v nezbytném rozsahu a výhradně za účelem plnění těchto úkolů nebo povinností.

3. Zpracování zvláštních kategorií osobních údajů uvedených v čl. 10 odst. 1 nařízení (EU) 2018/1725 se považuje za nezbytné z důvodů významného veřejného zájmu podle čl. 10 odst. 2 písm. g) uvedeného nařízení. Takové údaje mohou být zpracovávány pouze v rozsahu nezbytném pro provádění opatření k řízení kybernetických bezpečnostních rizik uvedených v článcích 6 a 8, pro poskytování služeb CERT-EU podle článku 13, pro sdílení informací o konkrétních incidentech podle čl. 17 odst. 3 a čl. 18 odst. 3, pro sdílení informací podle článku 20, pro oznamovací povinnosti podle článku 21, pro koordinaci a spolupráci v rámci reakce na incident podle článku 22 a pro řízení závažných incidentů podle článku 23 tohoto nařízení. Jednají-li subjekty Unie a CERT-EU v postavení správce údajů, uplatňují technická opatření zabraňující zpracování zvláštních kategorií osobních údajů pro jiné účely a stanoví vhodná a konkrétní opatření na ochranu základních práv a zájmů subjektů údajů.

Kapitola II

Opatření k zajištění vysoké společné úrovně kybernetické bezpečnosti

Článek 5

Provádění opatření

1. Do … [osm měsíců ode dne vstupu tohoto nařízení v platnost] vydá interinstitucionální výbor pro kybernetickou bezpečnost zřízený podle článku 10 po konzultaci s Agenturou Evropské unie pro kybernetickou bezpečnost (ENISA) a po obdržení pokynů od CERT-EU pokyny pro subjekty Unie k provedení počátečního přezkumu kybernetické bezpečnosti a zřízení vnitřního rámce pro řízení, správu a kontrolu kybernetických bezpečnostních rizik podle článku 6, pro hodnocení vyspělosti kybernetické bezpečnosti podle článku 7, pro přijetí opatření k řízení kybernetických bezpečnostních rizik podle článku 8 a pro přijetí plánu kybernetické bezpečnosti podle článku 9.

2. Při provádění článků 6 až 9 zohlední subjekty Unie pokyny a doporučení přijaté podle článků 11 a 14.

Článek 6

Rámec pro řízení, správu a kontrolu kybernetických bezpečnostních rizik

1. Do … [15 měsíců ode dne vstupu tohoto nařízení v platnost] poté, co provede počáteční přezkum kybernetické bezpečnosti, jako je audit, zřídí každý subjekt Unie vnitřní rámec pro řízení, správu a kontrolu kybernetických bezpečnostních rizik (dále je „rámec“). Na zřízení rámce dohlíží nejvyšší úroveň vedení subjektu Unie a nese za něj odpovědnost.

2. Rámec zahrnuje celé neutajované prostředí IKT dotčeného subjektu Unie, včetně jakéhokoli prostředí IKT a sítí funkčních technologií v jeho 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 těmto prostředím (dále jen „prostředí IKT“). Rámec je založen na přístupu zohledňujícím všechna rizika.

3. Rámec zajišťuje vysokou úroveň kybernetické bezpečnosti. Rámec stanovuje vnitřní politiky kybernetické bezpečnosti, včetně cílů a priorit, pro bezpečnost sítí a informačních systémů a úlohy a povinnosti zaměstnanců subjektu Unie, jejichž úkolem je zajistit účinné provádění tohoto nařízení. Rámec rovněž zahrnuje mechanismy pro měření účinnosti provádění.

4. Rámec je pravidelně přezkoumáván v kontextu měnících se kybernetických bezpečnostních rizik, nejméně však jednou za čtyři roky. Rámec subjektu Unie může být v případě potřeby a v návaznosti na žádost interinstitucionálního výboru pro kybernetickou bezpečnost zřízeného podle článku 10 aktualizován na základě pokynů CERT-EU týkajících se zjištěných incidentů nebo možných nedostatků v provádění tohoto nařízení.

5. Nejvyšší úroveň vedení každého subjektu Unie odpovídá za provádění tohoto nařízení a dohlíží na to, zda jeho organizace povinnosti související s rámcem plní.

6. V případě potřeby, a aniž je dotčena jeho odpovědnost za provádění tohoto nařízení, může nejvyšší úroveň vedení každého subjektu Unie přenést určité povinnosti podle tohoto nařízení na vyšší vedoucí pracovníky ve smyslu čl. 29 odst. 2 služebního řádu nebo jiné úředníky na rovnocenné úrovni v rámci dotčeného subjektu Unie. Bez ohledu na takové přenesení pravomoci může být nejvyšší úroveň vedení činěna odpovědnou za porušení tohoto nařízení dotčeným subjektem Unie.

7. Každý subjekt Unie má zaveden účinný mechanismus zajišťující, že přiměřená část rozpočtu na IKT bude vynaložena na kybernetickou bezpečnost. Při stanovování tohoto procentního podílu se náležitě zohlední rámec.

8. Každý subjekt Unie jmenuje místního referenta pro kybernetickou bezpečnost nebo osobu vykonávající rovnocennou funkci, kteří působí jako jediné kontaktní místo ve vztahu ke všem aspektům kybernetické bezpečnosti. Místní referent pro kybernetickou bezpečnost usnadňuje provádění tohoto nařízení a o stavu provádění pravidelně přímo informuje nejvyšší úroveň vedení. Aniž je dotčena skutečnost, že místní referent pro kybernetickou bezpečnost je v každém subjektu Unie jediným kontaktním místem, může subjekt Unie přenést některé úkoly místního referenta pro kybernetickou bezpečnost, pokud jde o provádění tohoto nařízení, na CERT-EU, a to na základě smlouvy o poskytování služeb uzavřené mezi tímto subjektem Unie a CERT-EU, nebo tyto úkoly může sdílet několik subjektů Unie. Pokud jsou tyto úkoly přeneseny na CERT-EU, rozhodne interinstitucionální výbor pro kybernetickou bezpečnost zřízený podle článku 10, zda bude tato služba poskytována jako součást základních služeb CERT-EU, a to s přihlédnutím k lidským a finančním zdrojům dotčeného subjektu Unie. Každý subjekt Unie oznámí CERT-EU neprodleně jmenovaného místního referenta pro kybernetickou bezpečnost a veškeré jeho následné změny.

CERT-EU zřídí a vede aktuální seznam jmenovaných místních referentů pro kybernetickou bezpečnost.

9. Vyšší vedoucí pracovníci ve smyslu čl. 29 odst. 2 služebního řádu nebo jiní úředníci na rovnocenné úrovni v rámci dotčeného subjektu Unie, jakož i všichni příslušní pracovníci pověření prováděním opatření a plněním povinností v oblasti řízení kybernetických bezpečnostních rizik stanovených v tomto nařízení pravidelně absolvují zvláštní školení s cílem získat dostatečné znalosti a dovednosti posouzení a vyhodnocení postupů v oblasti kybernetických bezpečnostních rizik a jejich dopadu na provoz subjektu Unie.

Článek 7

Hodnocení vyspělosti kybernetické bezpečnosti

1. Do … [18 měsíců ode dne vstupu tohoto nařízení v platnost] a poté alespoň každé dva roky provede každý subjekt Unie hodnocení vyspělosti kybernetické bezpečnosti zahrnující všechny prvky jeho prostředí IKT.

2. Hodnocení vyspělosti kybernetické bezpečnosti se případně provádí za pomoci specializované třetí strany.

3. Subjekty Unie s podobnými strukturami mohou při provádění hodnocení vyspělosti kybernetické bezpečnosti pro své příslušné subjekty spolupracovat.

4. Na základě žádosti interinstitucionálního výboru pro kybernetickou bezpečnost zřízeného podle článku 10 a s výslovným souhlasem dotčeného subjektu Unie mohou být výsledky hodnocení vyspělosti kybernetické bezpečnosti projednány v tomto výboru nebo v rámci neformální skupiny místních referentů pro kybernetickou bezpečnost, což umožní čerpání ze zkušeností a výměnu osvědčených postupů.

Článek 8

Opatření k řízení kybernetických bezpečnostních rizik

1. Každý subjekt Unie pod dohledem své nejvyšší úrovně vedení bezodkladně a nejpozději do … [20 měsíců ode dne vstupu tohoto nařízení v platnost] přijme odpovídající a přiměřená technická, operační a organizační opatření k řízení kybernetických bezpečnostních rizik zjištěných v rámci a k prevenci dopadů incidentů nebo jejich minimalizaci. S ohledem na nejnovější technologický vývoj a případně na příslušné evropské a mezinárodní normy zajistí tato opatření k řízení rizik takovou úroveň bezpečnosti sítí a informačních systémů v celém prostředí IKT, která je úměrná hrozícím kybernetickým bezpečnostním rizikům. Při posuzování přiměřenosti těchto opatření se náležitě zohlední míra expozice subjektu Unie kybernetickým bezpečnostním rizikům, jeho velikost, pravděpodobnost výskytu incidentů a jejich závažnost, včetně jejich společenského, hospodářského a interinstitucionálního dopadu.

2. Subjekty Unie se při provádění opatření k řízení kybernetických bezpečnostních rizik zaměřují alespoň na tyto oblasti:

a) politiku kybernetické bezpečnosti, včetně opatření potřebných k dosažení cílů a priorit uvedených v čl. 6 odst. 3 tohoto článku;

b) politiku analýzy kybernetických bezpečnostních rizik a politiku bezpečnosti informačních systémů;

c) cíle politiky týkající se využívání služeb cloud computingu;

d) případně audit kybernetické bezpečnosti, který může zahrnovat posouzení kybernetických bezpečnostních rizik, zranitelností a kybernetických hrozeb a pravidelné penetrační testování prováděné důvěryhodným soukromým poskytovatelem;

e) provádění doporučení vyplývajících z auditů kybernetické bezpečnosti uvedených v písmenu d) prostřednictvím aktualizace systému a politiky kybernetické bezpečnosti;

f) organizaci systému kybernetické bezpečnosti, včetně vymezení úloh a odpovědnosti;

g) správu aktiv, včetně seznamu aktiv v oblasti IKT a mapování sítí IKT;

h) bezpečnost lidských zdrojů a kontrolu přístupu;

i) bezpečnost operací;

j) bezpečnost komunikací;

k) akvizici, vývoj a údržbu systému, včetně politiky zveřejňování informací o zranitelností a jejich řešení;

l) případné politiky v oblasti transparentnosti zdrojového kódu;

m) bezpečnost dodavatelského řetězce včetně aspektů souvisejících s bezpečností, které se týkají vztahů mezi každým subjektem Unie a jeho přímými dodavateli nebo poskytovateli služeb;

n) řešení incidentů a spolupráci se CERT-EU, jako je zajištění bezpečnostního monitorování a vedení protokolů bezpečnosti;

o) řízení kontinuity provozu, jako je správa zálohování a obnova provozu po havárii, a krizové řízení a

p) podporu a rozvoj vzdělávání, dovedností, zvyšování povědomí, cvičebních programů a programů odborné přípravy v oblasti kybernetické bezpečnosti.

Pro účely prvního pododstavce písm. m) subjekty Unie zohlední zranitelnosti specifické pro každého přímého dodavatele a poskytovatele služeb a celkovou kvalitu produktů a postupů v oblasti kybernetické bezpečnosti svých dodavatelů a poskytovatelů služeb, včetně jejich postupů bezpečného vývoje.

3. Subjekty Unie přijmou alespoň tato konkrétní opatření pro řízení kybernetických bezpečnostních rizik:

a) technická opatření umožňující a podporující práci z domova;

b) konkrétní kroky pro přechod k zásadám nulové důvěry;

c) používání vícefaktorového ověřování jako normy u sítí a informačních systémů;

d) používání kryptografie a šifrování, a zejména šifrování mezi koncovými body, a bezpečného digitálního podpis

e) případné zavedení zabezpečené hlasové, obrazové a textové komunikace a zabezpečených systémů tísňové komunikace v rámci subjektu Unie;

f) proaktivní opatření pro odhalování a odstraňování malwaru a špionážního softwaru;

g) zabezpečení softwarového dodavatelského řetězce prostřednictvím kritérií pro bezpečný vývoj a hodnocení softwaru;

h) vytvoření a zavedení programů odborné přípravy v oblasti kybernetické bezpečnosti odpovídajících úkolům a předpokládaným schopnostem nejvyšší úrovně vedení a zaměstnanců subjektu Unie pověřených zajištěním účinného provádění tohoto nařízení;

i) pravidelné školení zaměstnanců v oblasti kybernetické bezpečnosti;

j) v příslušných případech účast na analýzách rizik vzájemného propojení mezi subjekty Unie;

k) posílení pravidel pro zadávání veřejných zakázek s cílem usnadnit dosažení vysoké společné úrovně kybernetické bezpečnosti prostřednictvím:

   i) odstranění smluvních překážek, které omezují sdílení informací ohledně incidentů, zranitelností a kybernetických hrozeb obdržených od poskytovatelů služeb IKT se CERT-EU,

   ii) smluvní povinnosti hlásit incidenty, zranitelnosti a kybernetické hrozby a disponovat vhodnými mechanismy reakce na incidenty a jejich monitorování.

Článek 9

Plány kybernetické bezpečnosti

1. Na základě závěrů vyvozených z hodnocení vyspělosti kybernetické bezpečnosti provedeného podle článku 7 a s ohledem na aktiva a kybernetická bezpečnostní rizika zjištěná v rámci a na opatření k řízení kybernetických bezpečnostních rizik přijatá podle článku 8, schválí nejvyšší úroveň vedení subjektu bez zbytečného prodlení a nejpozději do … [24 měsíců ode dne vstupu tohoto nařízení v platnost] Unie plán kybernetické bezpečnosti. Cílem plánu kybernetické bezpečnosti je zvýšit celkovou kybernetickou bezpečnost subjektu Unie, a tím přispět k posílení vysoké společné úrovně kybernetické bezpečnosti uvnitř subjektů Unie. Plán kybernetické bezpečnosti zahrnuje přinejmenším opatření k řízení kybernetických bezpečnostních rizik přijatá podle článku 8. Plán kybernetické bezpečnosti se reviduje každé dva roky, nebo častěji, je-li to nezbytné, na základě hodnocení vyspělosti kybernetické bezpečnosti provedeného podle článku 7 nebo v souvislosti s jakýmkoli významným přezkumem rámce.

2. Plán kybernetické bezpečnosti zahrnuje plán subjektu Unie pro řešení kybernetických krizí v případě závažných incidentů.

3. Subjekt Unie předloží svůj plán kybernetické bezpečnosti interinstitucionálnímu výboru pro kybernetickou bezpečnost zřízenému podle článku 10.

Kapitola III
Interinstitucionální výbor pro kybernetickou bezpečnost

Článek 10

Interinstitucionální výbor pro kybernetickou bezpečnost

1. Zřizuje se interinstitucionální výbor pro kybernetickou bezpečnost (dále jen „výbor IICB“).

2. Výbor IICB je povinen:

   a) sledovat a podporovat provádění tohoto nařízení subjekty Unie;

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

3. Výbor IICB sestává z:

   a) jednoho zástupce jmenovaného každým z těchto subjektů:

      i) Evropský parlament;

      ii) Evropská rada;

iii) Rada Evropské unie;

iv) Komise;

v) Soudní dvůr Evropské unie;

vi) Evropská centrální banka;

vii) Účetní dvůr;

viii) Evropská služba pro vnější činnost;

ix) Evropský hospodářský a sociální výbor;

x) Evropský výbor regionů;

xi) Evropská investiční banka;

xii) Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost;

xiii) ENISA;

xiv) Evropský inspektor ochrany údajů;

xv) Agentura Evropské unie pro kosmický program;

b) tří zástupců jmenovaných sítí agentur EU (EUAN) na návrh jejího poradního výboru pro IKT, aby zastupovali zájmy orgánů, institucí a jiných subjektů Unie, které provozují své vlastní prostředí IKT a které nejsou uvedeny v písmenu a).

Subjekty Unie zastoupené ve výboru IICB usilují o dosažení vyváženého zastoupení žen a mužů mezi jmenovanými zástupci.

4. Členům výboru IICB mohou být nápomocni náhradníci. Další zástupci subjektů Unie uvedených v odstavci 3 nebo jiných subjektů Unie mohou být předsedou pozváni k účasti na zasedáních výboru IICB bez hlasovacích práv.

5. Vedoucí CERT-EU a předsedové skupiny pro spolupráci, sítě týmů CSIRT a sítě EU-CyCLONe zřízených podle článků 14, 15 a 16 směrnice (EU) 2022/2555 nebo jejich náhradníci se mohou zasedání výboru IICB účastnit jako pozorovatelé. Ve výjimečných případech a v souladu se svým jednacím řádem může výbor IICB rozhodnout jinak.

6. Výbor IICB přijímá svůj jednací řád.

7. Výbor IICB v souladu s jednacím řádem určuje z řad svých členů předsedu na období tří let. Náhradník předsedy se na stejnou dobu stává plným členem výboru IICB.

8. Výbor IICB se schází alespoň třikrát za rok z podnětu svého předsedy, na žádost CERT-EU nebo na žádost kteréhokoli ze svých členů.

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

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

11. Funkci sekretariátu výboru IICB zajišťuje Komise a sekretariát je odpovědný předsedovi výboru IICB.

12. Zástupci nominovaní sítí EUAN předávají rozhodnutí výboru IICB členům sítě EUAN. Jakýkoli člen sítě EUAN je oprávněn se obrátit na tyto zástupce nebo předsedu výboru IICB s jakoukoli záležitostí, o níž se domnívají, že by na ni výbor IICB měl být upozorněn.

13. Výbor IICB může zřídit 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.

14. Do … [12 měsíců ode dne vstupu tohoto nařízení v platnost] a poté každoročně předkládá výbor IICB Evropskému parlamentu a Radě zprávu, v níž je podrobně popsán pokrok dosažený při provádění tohoto nařízení, a zejména upřesněn rozsah spolupráce CERT-EU s jeho vnitrostátními protějšky v jednotlivých členských státech. Tato zpráva je podkladem pro dvouletou zprávu o stavu kybernetické bezpečnosti v Unii přijatou podle článku 18 směrnice (EU) 2022/2555.

Článek 11

Úkoly výboru IICB

Při výkonu svých povinností výbor IICB zejména:

a) poskytuje strategické pokyny vedoucímu CERT-EU;

b) účinně sleduje a dohlíží na provádění tohoto nařízení a podporuje subjekty Unie při posilování jejich kybernetické bezpečnosti, a případně v této souvislosti také požaduje od subjektů Unie a CERT-EU zprávy ad hoc;

c) v návaznosti na strategickou diskusi přijímá víceletou strategii pro zvýšení úrovně kybernetické bezpečnosti v subjektech Unie, pravidelně, v každém případě však jednou za pět let, tuto strategii posuzuje a v případě potřeby tuto strategii upravuje;

d) stanovuje metodiku a organizační aspekty pro provádění dobrovolných vzájemných hodnocení subjekty Unie s cílem čerpat ze sdílených zkušeností, posílit vzájemnou důvěru, dosáhnout vysoké společné úrovně kybernetické bezpečnosti a posílit schopnosti subjektů Unie v oblasti kybernetické bezpečnosti, přičemž zajistí, aby tato vzájemná hodnocení prováděli odborníci na kybernetickou bezpečnost jmenovaní jiným subjektem Unie, než je subjekt Unie, který je předmětem přezkumu, a aby tato metodika vycházela z článku 19 směrnice (EU) 2022/2555 a byla případně subjektům Unie přizpůsobena;

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

f) na základě návrhu vedoucího CERT-EU schvaluje katalog služeb CERT-EU a všechny jeho aktualizace;

g) na základě návrhu vedoucího CERT-EU schvaluje roční finanční plán příjmů a výdajů, včetně personálního obsazení, pro činnosti CERT-EU;

h) na základě návrhu vedoucího CERT-EU schvaluje postupy pro uzavírání smluv o poskytování služeb;

i) přezkoumává a schvaluje roční zprávu vypracovanou vedoucím CERT-EU, jež se zabývá činností CERT-EU a řízením jejích finančních prostředků;

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

k) schvaluje ujednání o spolupráci, smlouvy o poskytování služeb nebo smlouvy mezi CERT-EU a dalšími subjekty podle článku 18;

l) přijímá pokyny a doporučení na základě návrhu CERT-EU v souladu s článkem 14 a ukládá CERT-EU, aby vydala, stáhla nebo upravila návrh pokynů nebo doporučení nebo výzvu k přijetí opatření;

m) zřizuje technické poradní skupiny se zvláštními úkoly na podporu činnosti výboru IICB, schvaluje jejich mandát a určuje jejich předsedy;

n) přijímá a posuzuje dokumenty a zprávy předložené subjekty Unie podle tohoto nařízení, jako jsou hodnocení vyspělosti kybernetické bezpečnosti;

o) za účelem výměny osvědčených postupů a informací v souvislosti s prováděním tohoto nařízení usnadňuje zřízení neformální skupiny místních referentů pro kybernetickou bezpečnost subjektů Unie, podporované ENISA;

p) s ohledem na informace o zjištěných kybernetických bezpečnostních rizicích a poznatky poskytnuté CERT-EU sleduje přiměřenost opatření týkajících se propojení mezi prostředími IKT subjektů Unie a poskytuje poradenství ohledně možných zlepšení; no, myslí se tím propojenost na technické úrovni;

q) vypracuje plán řešení kybernetických krizí s cílem podpořit na operativní úrovni koordinované řízení závažných incidentů s dopadem na subjekty Unie a přispět k pravidelné výměně příslušných informací, zejména pokud jde o dopady a závažnost závažných incidentů a možné způsoby jejich zmírnění;

r) koordinuje přijímání plánů jednotlivých subjektů Unie pro řešení kybernetických krizí uvedených v čl. 9 odst. 2;

s) s ohledem na výsledky koordinovaného posouzení rizik kritických dodavatelských řetězců na úrovni Unie uvedených v článku 22 směrnice (EU) 2022/2555 přijímá doporučení v oblasti bezpečnosti dodavatelského řetězce podle čl. 8 odst. 2 prvního pododstavce písm. m) na podporu subjektů Unie při přijímání účinných a přiměřených opatření k řízení kybernetických bezpečnostních rizik.

Článek 12

Dodržování povinností

1. Výbor IICB v souladu s čl. 10 odst. 2 a článkem 11 účinně sleduje provádění tohoto nařízení a přijatých pokynů, doporučení a výzev k přijetí opatření ze strany subjektů Unie. Výbor IICB si může od subjektů Unie vyžádat informace nebo dokumentaci, které jsou pro tento účel nezbytné. Pokud je dotčený subjekt Unie přímo ve výboru IICB zastoupen, nemá pro účely přijetí opatření k zajištění plnění povinností podle tohoto článku hlasovací práva.

2. Pokud výbor IICB zjistí, že některý subjekt Unie toto nařízení nebo pokyny, doporučení či výzvy k přijetí opatření vydané podle tohoto nařízení účinně neprovedl, aniž by byly dotčeny interní postupy dotčeného subjektu Unie, a poté, co subjektu Unie umožní přednést jeho připomínky, může:

   a) předložit dotčenému subjektu Unie odůvodněné stanovisko se zjištěnými nedostatky při uplatňování tohoto nařízení;

   b) poskytnout dotčenému subjektu Unie po konzultaci se CERT-EU pokyny s cílem zajistit, aby jeho rámec, opatření k řízení kybernetických bezpečnostních rizik, plán kybernetické bezpečnosti a podávání zpráv byly ve stanovené lhůtě v souladu s tímto nařízením;

c) vydat varování s cílem řešit zjištěné nedostatky ve stanovené lhůtě, včetně doporučení ke změně opatření přijatých dotčeným subjektem Unie na základě tohoto nařízení;

d) vydat dotčenému subjektu Unie odůvodněné oznámení v případě, že nedostatky uvedené ve varování vydaném podle písmene c) nebyly ve stanovené lhůtě dostatečně vyřešeny;

e) vydat:

   i) doporučení k provedení auditu, nebo

   ii) žádost, aby audit provedl auditní útvar třetí strany;

f) v příslušných případech informovat Účetní dvůr v rámci jeho mandátu o údajném nedodržení povinností;

g) vydat doporučení, aby všechny členské státy a subjekty Unie dočasně pozastavily datové toky do dotčeného subjektu Unie.

Pro účely prvního pododstavce písm. c), je-li to nezbytné s ohledem na kybernetické bezpečnostní riziko, je počet příjemců varování přiměřeně omezen.

Varování a doporučení vydaná podle prvního pododstavce jsou určena nejvyšší úrovni vedení dotčeného subjektu Unie.

3. Pokud výbor IICB přijal opatření podle odst. 2 prvního pododstavce písm. a) až g), dotčený subjekt Unie podrobně informuje o opatřeních a krocích, které k řešení údajných nedostatků zjištěných výborem IICB přijal. Tyto podrobné informace subjekt Unie podá v přiměřené lhůtě dohodnuté s výborem IICB.

4. Pokud se výbor IICB domnívá, že subjekt Unie trvale porušuje toto nařízení a že toto porušování vyplývá přímo z jednání nebo opomenutí úředníka nebo jiného zaměstnance Unie, a to i na nejvyšší úrovni vedení, požádá výbor IICB dotčený subjekt Unie, aby přijal příslušná opatření, přičemž jej může požádat i o to, aby zvážil přijetí opatření disciplinární povahy v souladu s pravidly a postupy stanovenými ve služebním řádu a jakýmikoli dalšími platnými pravidly a postupy. Za tímto účelem výbor IICB předá dotčenému subjektu Unie nezbytné informace.

5. Pokud subjekty Unie oznámí, že nejsou schopny dodržet lhůty stanovené v čl. 6 odst. 1 a čl. 8 odst. 1, může výbor IICB v řádně odůvodněných případech a s ohledem na velikost subjektu Unie povolit prodloužení těchto lhůt.

Kapitola IV
CERT-EU

Článek 13

Poslání a úkoly CERT-EU

1. Posláním CERT-EU je přispívat k bezpečnosti neutajovaného IKT prostředí všech subjektů Unie, a to tak, že jim poskytuje poradenství v oblasti kybernetické bezpečnosti, pomáhá jim předcházet incidentům, odhalovat incidenty, řešit incidenty, zmírňovat incidenty, reagovat na incidenty a zotavovat se z incidentů a působí jako středisko pro výměnu informací v oblasti kybernetické bezpečnosti a pro koordinaci reakcí na incidenty.

2. CERT-EU shromažďuje, spravuje, analyzuje a sdílí se subjekty Unie informace o kybernetických hrozbách, zranitelnostech a incidentech týkajících se infrastruktury IKT pro neutajované informace. Koordinuje reakce na incidenty na interinstitucionální úrovni a na úrovni jednotlivých subjektů Unie, a to i poskytováním specializované operativní pomoci či koordinací jejího poskytování.

3. CERT-EU vykonává pro subjekty Unie tyto úkoly:

   a) podporuje je při provádění tohoto nařízení a přispívá ke koordinaci provádění tohoto nařízení prostřednictvím opatření uvedených v čl. 14 odst. 1 nebo prostřednictvím *ad hoc* zpráv vyžádaných výborem IICB;

b) nabízí standardní služby týmu CSIRT všem subjektům Unie prostřednictvím souboru služeb v oblasti kybernetické bezpečnosti popsaných v jeho katalogu služeb (dále jen „základní služby“);

c) udržuje vzájemnou a partnerskou síť pro podporu služeb popsaných v článcích 17 a 18;

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

e) na základě informací uvedených v odstavci 2 přispívá v úzké spolupráci s ENISA k informovanosti Unie o aktuální kybernetické situaci;

f) koordinuje řízení závažných incidentů;

g) jedná jako specializovaný koordinátor subjektů Unie pro účely koordinovaného zpřístupňování informací o zranitelností podle čl. 12 odst. 1 směrnice (EU) 2022/2555;

h) na žádost subjektu Unie poskytuje proaktivní a nerušivé skenování veřejně přístupných sítí a informačních systémů daného subjektu Unie.

Informace uvedené v prvním pododstavci písm. e) se v případě potřeby sdílejí s výborem IICB, sítí týmů CSIRT a Střediskem Evropské unie pro analýzu zpravodajských informací (EU INTCEN), a to při dodržování patřičných podmínek zachování důvěrnosti.

4. CERT-EU může v souladu s článkem 17 nebo případně 18 spolupracovat s příslušnými komunitami v oblasti kybernetické bezpečnosti v Unii a jejích členských státech, mimo jiné v těchto oblastech:

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

   b) operativní spolupráce týkající se sítě týmů CSIRT, včetně vzájemné pomoci;

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

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

5. CERT-EU se v rámci své působnosti zapojuje do strukturované spolupráce s ENISA v oblasti budování kapacit, operativní spolupráce a dlouhodobých strategických analýz kybernetických hrozeb v souladu s nařízením (EU) 2019/881. CERT-EU může spolupracovat a vyměňovat si informace s Evropským centrem Europolu pro boj proti kyberkriminalitě.

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

a) služby, které podporují kybernetickou bezpečnost prostředí IKT subjektů Unie, jiné než služby uvedené v odstavci 3, na základě smluv o poskytování služeb a s výhradou dostupných zdrojů, zejména širokospektrální monitorování sítě, včetně nepřetržitého monitorování v první linii v případě vysoce rizikových kybernetických hrozeb;

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

c) na požádání proaktivní skenování sítí a informačních systémů dotčeného subjektu Unie s cílem odhalit zranitelnosti s potenciálním významným dopadem;

d) služby, které podporují bezpečnost prostředí IKT jiných organizací než subjektů Unie, které úzce spolupracují se 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.

S ohledem na první pododstavec písm. d) může CERT-EU ve výjimečných případech s předchozím souhlasem výboru IICB uzavřít smlouvy o poskytování služeb s jinými subjekty než se subjekty Unie.

7. CERT-EU organizuje, a může se účastnit cvičení v oblasti kybernetické bezpečnosti nebo doporučovat účast na stávajících cvičeních, a to případně v úzké spolupráci s ENISA, za účelem testování úrovně kybernetické bezpečnosti subjektů Unie.

8. CERT-EU může poskytovat pomoc subjektům Unie v souvislosti s incidenty v sítích a informačních systémech nakládajících s utajovanými informacemi EU, pokud o to dotyčné subjekty Unie výslovně požádají, v souladu s jejich příslušnými postupy. Poskytnutím pomoci CERT-EU podle tohoto odstavce nejsou dotčena platná pravidla týkající se ochrany utajovaných informací.

9. CERT-EU informuje subjekty Unie o svých postupech a procesech pro řešení incidentů.

10. CERT-EU poskytne s vysokou úrovní důvěrnosti a spolehlivosti prostřednictvím vhodných mechanismů spolupráce a oznamování relevantní a anonymizované informace o závažných incidentech a o způsobu, jakým byly řešeny. Tyto informace se zahrnou do zprávy uvedené v čl. 10 odst. 14.

11. CERT-EU ve spolupráci s evropským inspektorem ochrany údajů podpoří dotčené subjekty Unie při řešení incidentů, v jejichž důsledku došlo k porušení ochrany osobních údajů, aniž jsou dotčeny pravomoci a úkoly tohoto inspektora podle nařízení (EU) 2018/1725.

12. CERT-EU může v případě, že jej o to výslovně požádají odborné sekce subjektů Unie, poskytovat technické poradenství nebo informace týkající se příslušné oblasti.

Článek 14

Pokyny, doporučení a výzvy k přijetí opatření

1. CERT-EU podporuje provádění tohoto nařízení vydáváním:

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

b) návrhů pokynů určených všem subjektům Unie nebo jejich části, které předkládá výboru IICB;

c) návrhů doporučení určených jednotlivým subjektům Unie, které předkládá výboru IICB.

Pokud jde o první pododstavec písm. a), dotčený subjekt Unie bez zbytečného odkladu po obdržení výzvy k přijetí opatření informuje CERT-EU o tom, jak byla naléhavá bezpečnostní opatření uplatněna.

2. Pokyny a doporučení mohou obsahovat:

a) společné metodiky a model pro hodnocení vyspělosti kybernetické bezpečnosti subjektů Unie, včetně odpovídajících měřítek nebo klíčových ukazatelů výkonnosti, které slouží jako reference na podporu soustavného zlepšování kybernetické bezpečnosti ve všech subjektech Unie a usnadňují stanovení priorit pro oblasti kybernetické bezpečnosti a opatření s ohledem na stav subjektů z hlediska kybernetické bezpečnosti;

b) postupy pro řízení kybernetických bezpečnostních rizik a opatření k řízení kybernetických bezpečnostních rizik nebo jejich vylepšení;

c) postupy pro hodnocení vyspělosti kybernetické bezpečnosti a postupy pro plány kybernetické bezpečnosti;

d) případně využití společných technologií, architektury, otevřených zdrojů a souvisejících osvědčených postupů s cílem dosáhnout interoperability a společných norem, včetně koordinovaného přístupu k bezpečnosti dodavatelského řetězce;

e) případné informace k usnadnění používání nástrojů kolaborativního zadávání veřejných zakázek pro nákup příslušných služeb a produktů v oblasti kybernetické bezpečnosti od dodavatelů, kteří jsou třetími stranami;

f) ujednání o sdílení informací podle článku 20.

Článek 15

Vedoucí CERT-EU

1. Komise po obdržení souhlasu dvoutřetinové většiny výboru IICB jmenuje vedoucího CERT-EU. Výbor IICB je konzultován ve všech fázích postupu jmenování, zejména při vypracovávání oznámení o volném pracovním místě, posuzování žádostí a jmenování výběrových komisí v souvislosti s tímto pracovním místem. Výběrové řízení, včetně konečného užšího seznamu kandidátů, z nichž má být vedoucí CERT-EU vybrán, zajistí spravedlivé genderové zastoupení ve vztahu k předloženým kandidaturám.

2. Vedoucí CERT-EU je odpovědný za řádné fungování CERT-EU a jedná v rámci svých úkolů pod vedením výboru IICB. Vedoucí CERT-EU pravidelně podává zprávy předsedovi výboru IICB a na požádání předkládá výboru IICB zprávy vypracované ad hoc.

3. Vedoucí CERT-EU je nápomocen příslušné pověřené schvalující osobě při vypracovávání každoroční zprávy o činnosti obsahující finanční a manažerské informace, včetně výsledků kontrol, vypracované v souladu s čl. 74 odst. 9 nařízení Evropského parlamentu a Rady (EU, Euratom) 2018/1046[1], a tuto pověřenou schvalující osobu pravidelně informuje o provádění opatření, u nichž byla pravomoc přenesena na vedoucího CERT-EU.

4. Vedoucí CERT-EU vypracuje každoročně finanční plán správních příjmů a výdajů na své činnosti, návrh ročního pracovního programu, návrh katalogu služeb CERT-EU, navrhované revize katalogu služeb, návrh ujednání pro smlouvy o poskytování služeb a návrh klíčových ukazatelů výkonnosti pro CERT-EU, které v souladu s článkem 11 schvaluje výbor IICB. Při revizi seznamu služeb v katalogu služeb CERT-EU zohlední vedoucí CERT-EU zdroje, které jsou CERT-EU přiděleny.

---

[1] 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, (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).

5. Vedoucí CERT-EU předkládá nejméně jednou ročně výboru IICB a předsedovi výboru IICB zprávy o činnostech a výsledcích CERT-EU během referenčního období, včetně zpráv o plnění rozpočtu, uzavřených smlouvách o poskytování služeb a písemných dohodách, spolupráci s protějšky a partnery a o misích podniknutých jeho zaměstnanci, včetně zpráv podle článku 11. Tyto zprávy obsahují pracovní program na následující období, finanční plánování příjmů a výdajů, včetně personálního obsazení, plánované aktualizace katalogu služeb CERT-EU a posouzení očekávaného dopadu, který tyto aktualizace mohou mít na finanční a lidské zdroje.

Článek 16

Finanční a personální záležitosti

1. CERT-EU se začlení do správní struktury generálního ředitelství Komise, aby mohlo využívat podpůrné struktury Komise v oblasti správy, finančního řízení a účetnictví, přičemž si zachová své postavení samostatného interinstitucionálního poskytovatele služeb pro všechny subjekty Unie. Komise informuje výbor IICB o administrativním umístění CERT-EU a případných změnách tohoto umístění. Komise pravidelně přezkoumává správní ujednání týkající se CERT-EU a v každém případě před zavedením každého víceletého finančního rámce podle článku 312 Smlouvy o fungování EU, aby bylo možné přijmout vhodná opatření. Přezkum zahrne možnost zřízení CERT-EU jako úřadu Unie.

2. Při uplatňování administrativních a finančních postupů jedná vedoucí CERT-EU z pověření Komise a pod dohledem výboru IICB.

3. Úkoly a činnosti CERT-EU, včetně služeb poskytovaných CERT-EU podle čl. 13 odst. 3, 4 a 5 a 7 a čl. 14 odst. 1 subjektům Unie financovaným z okruhu víceletého finančního rámce vyhrazeného evropské veřejné správě jsou financovány prostřednictvím samostatné rozpočtové položky rozpočtu Komise. Místa vyčleněná pro CERT-EU jsou podrobně popsána v poznámce pod čarou k plánu pracovních míst Komise.

4. Subjekty Unie jiné než subjekty Unie uvedené v odstavci 3 tohoto článku každoročně finančně přispívají CERT-EU na úhradu služeb poskytovaných CERT-EU podle uvedeného odstavce. Příspěvky vycházejí z pokynů vydaných výborem IICB a dohodnutých mezi každým subjektem Unie a CERT-EU ve smlouvách o poskytování služeb. Příspěvky představují spravedlivý a přiměřený podíl na celkových nákladech na poskytované služby. Převádějí se na samostatnou rozpočtovou položku uvedenou v odstavci 3 tohoto článku jakožto účelově vázaný příjem stanovený v čl. 21 odst. 3 písm. c) nařízení (EU, Euratom) 2018/1046.

5. Náklady na úkoly stanovené v čl. 13 odst. 6 jsou hrazeny subjekty Unie, které jsou příjemci služeb CERT-EU. Příjmy jsou účelově vázány na rozpočtové položky pokrývající náklady.

Článek 17

Spolupráce CERT-EU s protějšky v členských státech

1. CERT-EU bez zbytečného odkladu spolupracuje s protějšky z členských států, zejména týmy CSIRT určenými nebo zřízenými podle článku 10 směrnice (EU) 2022/2555, nebo případně s příslušnými orgány a jednotnými kontaktními místy určenými nebo zřízenými podle článku 8 uvedené směrnice a vyměňuje si s nimi informace ohledně incidentů, kybernetických hrozeb, zranitelností, významných událostí, možných protiopatření, jakož i o osvědčených postupech, a o veškerých záležitostech, které mají význam pro zlepšení ochrany prostředí IKT subjektů Unie, a to i prostřednictvím sítě týmů CSIRT zřízené podle článku 15 směrnice (EU) 2022/2555. CERT-EU podporuje Komisi v rámci sítě EU-CyCLONe zřízené podle článku 16 o koordinovaném řešení rozsáhlých kybernetických bezpečnostních incidentů a krizí ve směrnici (EU) 2022/2555.

2. Pokud se CERT-EU dozví o významném incidentu, k němuž dojde na území členského státu, neprodleně informuje všechny příslušné protějšky v daném členském státě v souladu s odstavcem 1.

3. Je-li v souladu s právem Unie na ochranu osobních údajů zajištěna ochrana osobních údajů, CERT-EU si s vnitrostátními protějšky v členských státech bez zbytečného odkladu vymění příslušné informace týkající se konkrétních incidentů, které mohou usnadnit odhalování obdobných kybernetických hrozeb nebo incidentů nebo přispět k analýze incidentu, a to bez povolení dotčeného subjektu Unie. CERT-EU vyměňuje informace týkající se konkrétních incidentů, které odhalují totožnost cíle kybernetického bezpečnostního incidentu, pouze pokud nastane některý u z těchto případů:

a) dotčený subjekt Unie udělil svůj souhlas;

b) dotčený subjekt Unie neudělil svůj souhlas, jak je stanoveno v písmenu a), ale zveřejnění totožnosti dotčeného subjektu Unie by zvýšilo pravděpodobnost, že se zabrání incidentům v jiných oblastech nebo se zmírní jejich následky;

c) dotčený subjekt Unie již zveřejnil, že byl obětí incidentu.

Rozhodnutí o výměně informací týkajících se konkrétního incidentu, které odhalují totožnost cíle incidentu podle prvního pododstavce písm. b), schvaluje vedoucí CERT-EU. Před vydáním takového rozhodnutí kontaktuje CERT-EU dotčený subjekt Unie písemně a jasně vysvětlí, jak by zveřejnění jeho totožnosti pomohlo zabránit incidentům v jiných oblastech nebo je zmírnit. Vedoucí CERT-EU poskytne vysvětlení a výslovně požádá subjekt Unie, aby ve stanovené lhůtě uvedl, zda souhlasí. Vedoucí CERT-EU rovněž informuje subjekt Unie o tom, že si s ohledem na poskytnuté vysvětlení vyhrazuje právo informace zveřejnit i bez souhlasu. Dotčený subjekt Unie je informován před zveřejněním informací.

Článek 18

Spolupráce CERT-EU s dalšími protějšky

1. CERT-EU může spolupracovat s protějšky v Unii, jež nejsou uvedeny v článku 17 a na něž se vztahují požadavky Unie na kybernetickou bezpečnost, včetně protějšků zaměřených na konkrétní průmyslová odvětví, v záležitostech týkajících se nástrojů a metod, jako například techniky, taktiky, postupů a osvědčených postupů, jakož i kybernetických hrozeb a zranitelností. Pro účely jakékoliv spolupráce s těmito protějšky požádá CERT-EU výbor IICB o předchozí souhlas pro každý jednotlivý případ. Pokud CERT-EU s těmito protějšky naváže spolupráci, informuje o tom všechny příslušné protějšky členských států uvedené v čl. 17 odst. 1 v členském státě, v němž se protějšek nachází. Ve vhodných a náležitých případech se tato spolupráce a její podmínky, a to i pokud jde o kybernetickou bezpečnost, ochranu údajů a nakládání s informacemi, stanoví ve výslovných ujednáních o zachování důvěrnosti, jako jsou smlouvy nebo správní ujednání. Ujednání o zachování důvěrnosti nevyžadují předchozí souhlas výboru IICB, předseda výboru IICB je však informován. V případě naléhavé a bezprostřední potřeby výměny informací o kybernetické bezpečnosti v zájmu subjektů Unie nebo jiné strany může CERT-EU tímto způsobem postupovat se subjektem, jehož zvláštní způsobilost, kapacita a odborné znalosti jsou důvodně vyžadovány na pomoc v této situaci naléhavé a bezprostřední potřeby, a to i v případě, že CERT-EU s tímto subjektem nemá uzavřenu dohodu o zachování důvěrnosti. V takových případech CERT-EU neprodleně informuje předsedu výboru IICB a výbor IICB informuje prostřednictvím pravidelných zpráv nebo zasedání.

2. CERT-EU může v zájmu shromažďování informací o obecných a konkrétních kybernetických hrozbách, významných událostech, zranitelnostech a možných protiopatřeních spolupracovat s partnery, jako jsou komerční subjekty, včetně subjektů zaměřených na konkrétní průmyslová odvětví, mezinárodní organizace, vnitrostátní subjekty zemí mimo Unii nebo jednotliví odborníci. Pro účely širší spolupráce s těmito partnery požádá CERT-EU výbor IICB o předchozí souhlas pro každý jednotlivý případ.

3. CERT-EU může se souhlasem subjektu Unie dotčeného incidentem a za předpokladu, že s příslušným protějškem nebo partnerem je uzavřeno ujednání nebo smlouva o mlčenlivosti, poskytnout informace týkající se konkrétního incidentu protějškům nebo partnerům uvedeným v odstavcích 1 a 2, a to výhradně za účelem přispění k jeho analýze.

Kapitola V
Povinnosti v oblasti spolupráce a oznamovací povinnosti

Článek 19

Nakládání s informacemi

1. Subjekty Unie a CERT-EU musejí dodržovat povinnost zachování profesního tajemství v souladu s článkem 339 Smlouvy o fungování EU nebo s rovnocennými použitelnými rámci.

2. V souvislosti se žádostmi o přístup veřejnosti k dokumentům v držení CERT-EU se použije nařízení Evropského parlamentu a Rady (ES) č. 1049/2001[1], včetně povinnosti podle uvedeného nařízení konzultovat jiné subjekty Unie nebo případně členskými státy, pokud se žádost týká jejich dokumentů.

3. Nakládání s informacemi ze strany subjektů Unie a CERT-EU musí být v souladu s platnými pravidly o zajištění bezpečnosti informací.

Článek 20

Ujednání o sdílení informací o kybernetické bezpečnosti

1. Subjekty Unie mohou dobrovolně oznamovat CERT-EU incidenty, kybernetické hrozby, významné události a zranitelnosti, které se jich týkají, a poskytovat o nich informace. CERT-EU zajistí, aby v zájmu usnadnění sdílení informací se subjekty Unie byly k dispozici účinné komunikační prostředky s vysokou úrovní sledovatelnosti, důvěrnosti a spolehlivosti. Při zpracování oznámení může CERT-EU upřednostnit zpracování povinných oznámení před dobrovolnými oznámeními. Aniž je dotčen článek 12, při dobrovolném oznámení nemohou být oznamujícímu subjektu Unie uloženy žádné další povinnosti než ty, které by mu byly uloženy, kdyby toto oznámení neučinil.

---

[1] 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).

2. K plnění svého poslání a úkolů svěřených podle článku 13 může CERT-EU požádat subjekty Unie o poskytnutí informací z příslušných soupisů jejich systémů IKT, včetně informací o kybernetických hrozbách, významných událostech, zranitelnostech, indikátorech narušení, varováních při ohrožení kybernetické bezpečnosti a doporučeních týkajících se konfigurace nástrojů kybernetické bezpečnosti určených k odhalování kybernetických incidentů. Dožádaný subjekt Unie bez zbytečného odkladu předá požadované informace a všechny jejich následné aktualizace.

3. CERT-EU si může se subjekty Unie vyměňovat informace týkající se konkrétního incidentu, které odhalují totožnost subjektu Unie, jehož se incident týká, pouze se souhlasem tohoto subjektu. Pokud subjekt Unie odmítne udělit svůj souhlas, poskytne CERT-EU důvody svého rozhodnutí.

4. Subjekty Unie na požádání sdílejí s Evropským parlamentem a Radou informace o dokončení plánů kybernetické bezpečnosti.

5. Výbor IICB nebo případně CERT-EU na požádání sdílí s Evropským parlamentem a Radou pokyny, doporučení a výzvy k přijetí opatření.

6. Povinnosti související se sdílením informací stanovené v tomto článku se nevztahují na:

   a) utajované informace EU;

b) informace, jejichž další šíření bylo vyloučeno viditelným označením, pokud jejich sdílení se CERT-EU nebylo výslovně povoleno..

Článek 21

Oznamovací povinnosti

1. Incident se považuje za závažný, pokud:

a) způsobil nebo může způsobit vážné provozní narušení fungování subjektu Unie nebo finanční ztrátu pro dotčený subjekt Unie;

b) způsobil nebo může způsobit jiným fyzickým nebo právnickým osobám značnou hmotnou nebo nehmotnou újmu.

2. Subjekty Unie předloží CERT-EU:

a) bez zbytečného odkladu a v každém případě do 24 hodin po zjištění významného incidentu, včasné varování, v němž případně uvedou, zda se domnívají, že byl významného incident způsoben nezákonným nebo nepřátelským jednáním nebo že by mohl mít dopad na různé subjekty nebo přeshraniční dopad;

b) bez zbytečného odkladu a v každém případě do 72 hodin po zjištění významného incidentu, oznámení incidentu, v němž případně aktualizují informace uvedené v písmenu a) a předloží počáteční posouzení významného incidentu včetně jeho závažnosti a dopadu a, pokud jsou k dispozici, indikátory narušení;

c) na žádost CERT-EU průběžnou zprávu o příslušném aktuálním vývoji situace;

d) nejpozději do jednoho měsíce od předložení oznámení incidentu podle písmene b) závěrečnou zprávu zahrnující:

   i) podrobný popis incidentu včetně jeho závažnosti a dopadu;

   ii) druh hrozby nebo základní příčinu, která incident pravděpodobně spustila;

   iii) učiněná a probíhající opatření ke zmírnění následků;

   iv) případně přeshraniční dopad incidentu nebo dopad na různé subjekty;

e) v případě, že v době předložení závěrečné zprávy podle písmene d) incident stále trvá, zprávu o pokroku k danému okamžiku a závěrečnou zprávu do jednoho měsíce od vyřešení incidentu.

3. Subjekt Unie bez zbytečného odkladu a v každém případě do 24 hodin od okamžiku, kdy se o významnému incidentu dozvěděl, informuje všechny příslušné protějšky z členských států uvedené v čl. 17 odst. 1 v členském státě, v němž se nachází, o tom, že došlo k významnému incidentu.

4. Subjekty Unie oznámí mimo jiné veškeré informace, které CERT-EU umožní určit jakýkoli dopad na všechny subjekty, dopad na hostitelský členský stát nebo přeshraniční dopad významného incidentu. Aniž je dotčen článek 12, pouhé oznámení nepředstavuje pro subjekt Unie vyšší míru právní odpovědnosti.

5. V příslušných případech subjekty Unie bez zbytečného odkladu sdělí uživatelům dotčených sítí a informačních systémů nebo jiných složek prostředí IKT, kteří jsou potenciálně dotčeni významným incidentem nebo významnou kybernetickou hrozbou a případně potřebují přijmout zmírňující opatření, jakákoli opatření nebo nápravná opatření, která mohou být v reakci na uvedený incident nebo hrozbu přijata. Subjekty Unie případně informují tyto uživatele o samotné významné kybernetické hrozbě.

6. Pokud se významný incident nebo významná kybernetická hrozba dotýká sítě a informačního systému nebo složky prostředí IKT subjektu Unie, která je úmyslně propojena s prostředím IKT jiného subjektu Unie, vydá CERT-EU příslušné bezpečnostní varování.

7. Subjekty Unie na žádost CERT-EU a bez zbytečného odkladu poskytnou CERT-EU digitální informace vytvořené pomocí elektronických zařízení zapojených do příslušných incidentů. CERT-EU může poskytnout další podrobnosti o typech informací, které pro účely situačního přehledu a reakce na incident požaduje.

8. CERT-EU předkládá každé tři měsíce výboru IICB, ENISA, EU INTCEN a síti týmů CSIRT souhrnnou zprávu obsahující anonymizované a agregované údaje o významných incidentech, incidentech, kybernetických hrozbách, významných událostech a zranitelnostech podle článku 20, a významných incidentech oznámených podle odstavce 2 tohoto článku. Souhrnná zpráva je podkladem pro dvouletou zprávu o stavu kybernetické bezpečnosti v Unii přijatou podle článku 18 směrnice (EU) 2022/2555.

9. Výbor IICB do … [šest měsíců ode dne vstupu tohoto nařízení v platnost] vydá pokyny nebo doporučení, v nichž blíže upřesní způsoby, formát a obsah oznamování podle tohoto článku. Při přípravě těchto pokynů nebo doporučení výbor IICB zohlední veškeré prováděcí akty přijaté podle čl. 23 odst. 11 směrnice (EU) 2022/2555, které blíže stanoví druh informací, formát a postup oznámení. CERT-EU šíří vhodné technické údaje s cílem umožnit aktivní odhalování incidentů, reakci na incidenty nebo opatření ke zmírnění dopadů incidentů ze strany subjektů Unie.

10. Oznamovací povinnosti stanovené v tomto článku se nevztahují na:

a) utajované informace EU;

b) informace, jejichž další šíření bylo vyloučeno viditelným označením, pokud jejich sdílení se CERT-EU nebylo výslovně povoleno.

Článek 22

Koordinace a spolupráce v rámci reakce na incidenty

1. CERT-EU, která působí jako středisko pro výměnu informací v oblasti kybernetické bezpečnosti a pro koordinaci reakcí na incidenty, usnadňuje výměnu informací o kybernetických hrozbách, zranitelnostech a významných událostech mezi:

a) subjekty Unie;

b) protějšky uvedenými v článcích 17 a 18.

2. CERT-EU, případně v úzké spolupráci s ENISA, usnadňuje koordinaci reakcí subjektů Unie na incidenty, včetně:

a) přispívání k jednotné vnější komunikaci;

b) vzájemné podpory, jako je sdílení informací relevantních pro subjekty Unie nebo poskytování pomoci, je-li to relevantní, přímo na místě;

c) optimálního využití operativních zdrojů;

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

3. CERT-EU v úzké spolupráci s ENISA podporuje subjekty Unie v oblasti situačního povědomí o kybernetických hrozbách, zranitelnostech a významných událostech, jakož i ve sdílení relevantního vývoje v oblasti kybernetické bezpečnosti.

4. Výbor IICB do … [12 měsíců ode dne vstupu tohoto nařízení v platnost] přijme na základě návrhu CERT-EU pokyny nebo doporučení pro koordinaci reakcí na incidenty a pro spolupráci při významných incidentech. Pokud existuje podezření, že incident má povahu trestného činu, poskytne CERT-EU bez zbytečného odkladu poradenství k tomu, jak oznámit tento incident donucovacím orgánům.

5. Na základě konkrétní žádosti členského státu a se souhlasem dotčených subjektů Unie může CERT-EU vyzvat odborníky ze seznamu uvedeného v čl. 23 odst. 4, aby přispěli k reakci na závažný incident, který má v daném členském státě dopad, nebo na rozsáhlý kybernetický bezpečnostní incident v souladu s čl. 15 odst. 3 písm. g) směrnice (EU) 2022/2555. Zvláštní pravidla pro přístup k technickým odborníkům ze subjektů Unie a jejich využívání schvaluje výbor IICB na základě návrhu CERT-EU.

Článek 23

Řešení závažných incidentů

1. S cílem podpořit koordinované řešení závažných incidentů na operační úrovni, které mají dopad na subjekty Unie, a přispět k pravidelné výměně relevantních informací mezi subjekty Unie a s členskými státy vypracuje výbor IICB v úzké spolupráci se CERT-EU a ENISA plán řešení kybernetické krize na základě činností uvedených v čl. 22 odst. 2. Plán řešení kybernetické krize obsahuje alespoň tyto prvky:

   a) postupy týkající se koordinace a toku informací mezi subjekty Unie za účelem řešení závažných incidentů na operační úrovni;

   b) společné standardní operační postupy (SOP);

   c) společné názvosloví pro závažnost závažných incidentů a spouštěcí body krize;

   d) pravidelná cvičení;

   e) zabezpečené komunikační kanály, jež mají být používány.

2. Na základě plánu řešení kybernetické krize vypracovaného podle odstavce 1 tohoto článku, a aniž je dotčen čl. 16 odst. 2 první pododstavec směrnice (EU) 2022/2555, je zástupce Komise ve výboru IICB kontaktním místem pro sdílení příslušných informací týkajících se závažných incidentů se sítí EU-CyCLONe.

3. CERT-CE koordinuje subjekty Unie při řešení závažných incidentů. Vede seznam dostupných technických odborných znalostí, které by v případě závažných incidentů byly potřebné pro reakci, a pomáhá výboru IICB při koordinaci plánů subjektů Unie pro řešení kybernetických krizí v případě závažných incidentů uvedených v čl. 9 odst. 2.

4. 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.

Kapitola VI
Závěrečná ustanovení

Článek 24

Počáteční přerozdělení rozpočtových prostředků

V zájmu zajištění řádného a stabilního fungování CERT-EU může Komise navrhnout přerozdělení zaměstnanců a finančních zdrojů do rozpočtu Komise pro provoz CERT-EU. Přerozdělení je účinné současně s prvním ročním rozpočtem Unie přijatým po vstupu tohoto nařízení v platnost.

Článek 25

Přezkum

1. Výbor IICB za pomoci CERT-EU podá do … [12 měsíců ode dne vstupu tohoto nařízení v platnost] a poté každoročně Komisi zprávu o provádění tohoto nařízení. Výbor IICB může Komisi doporučit, aby toto nařízení přezkoumala.

2. Komise posoudí provádění tohoto nařízení a podá Evropskému parlamentu a Radě zprávu o provádění tohoto nařízení a o zkušenostech získaných na strategické a operativní úrovni do … [36 měsíců ode dne vstupu tohoto nařízení v platnost] a poté každé dva roky.

Zpráva uvedená v prvním pododstavci tohoto odstavce zahrnuje přezkum možnosti zřízení CERT-EU jako úřadu Unie podle čl. 16 odst. 1.

3. Komise vyhodnotí fungování tohoto nařízení a podá zprávu Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů do … [pět let ode dne vstupu tohoto nařízení v platnost]. Komise rovněž vyhodnotí, zda je vhodné zahrnout do oblasti působnosti tohoto nařízení sítě a informační systémy, které nakládají s utajovanými informacemi EU, a to s přihlédnutím k dalším legislativním aktům Unie, které se na tyto systémy vztahují. V případě potřeby se ke zprávě připojí legislativní návrh.

Článek 26

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.

Ve Štrasburku dne ...

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