Rada
Európskej únie

V Bruseli 22. marca 2022
(OR. en)

7474/22

Medziinštitucionálny spis:
2022/0085(COD)

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

NÁVRH

Od:	Martine DEPREZOVÁ, riaditeľka, v zastúpení generálnej tajomníčky Európskej komisie
Dátum doručenia:	22. marca 2022
Komu:	Jeppe TRANHOLM-MIKKELSEN, generálny tajomník Rady Európskej únie
Č. dok. Kom.:	COM(2022) 122 final
Predmet:	Návrh NARIADENIA EURÓPSKEHO PARLAMENTU A RADY, ktorým sa stanovujú opatrenia na zaistenie vysokej spoločnej úrovne kybernetickej bezpečnosti v inštitúciách, orgánoch, úradoch a agentúrach Únie

Delegáciám v prílohe zasielame dokument COM(2022) 122 final.

Príloha: COM(2022) 122 final

EURÓPSKA
KOMISIA

V Bruseli 22. 3. 2022
COM(2022) 122 final

2022/0085 (COD)

Návrh

NARIADENIE EURÓPSKEHO PARLAMENTU A RADY,

ktorým sa stanovujú opatrenia na zaistenie vysokej spoločnej úrovne kybernetickej bezpečnosti v inštitúciách, orgánoch, úradoch a agentúrach Únie

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

DÔVODOVÁ SPRÁVA

1. KONTEXT NÁVRHU

• Dôvody a ciele návrhu

Týmto návrhom sa stanovuje rámec na zaistenie spoločných pravidiel a opatrení inštitúcií, orgánov a agentúr Únie v oblasti kybernetickej bezpečnosti. Jeho cieľom je ďalej zlepšovať odolnosť a kapacity všetkých subjektov na reakcie na incidenty. Je v súlade s prioritami Komisie pripraviť Európu na digitálny vek a vybudovať hospodárstvo pripravené na budúcnosť, ktoré pracuje v prospech ľudí. Zaistenie bezpečnej a odolnej verejnej správy je navyše základným prvkom digitálnej transformácie spoločnosti ako celku.

Tento návrh vychádza zo Stratégie EÚ pre bezpečnostnú úniu [COM(2020) 605 final] a zo stratégie kybernetickej bezpečnosti EÚ v digitálnej dekáde [JOIN(2020) 18 final].

V návrhu sa modernizuje existujúci právny rámec CERT-EU a berie sa do úvahy zmenená a zvýšená digitalizácia v inštitúciách, orgánoch a agentúrach v posledných rokoch, ako aj vyvíjajúca sa panoráma kybernetickobezpečnostných hrozieb. Vývoj sa v oboch prípadoch ešte zintenzívnil po začatí krízy spôsobenej pandémiou COVID-19, zatiaľ čo počet incidentov naďalej stúpa a dochádza k čoraz sofistikovanejším útokom zo širokej škály zdrojov.

V návrhu sa CERT-EU premenúva z „tímu reakcie na núdzové počítačové situácie“ na „centrum kybernetickej bezpečnosti“ pre inštitúcie, orgány a agentúry Únie v súlade s vývojom v členských štátoch aj na celom svete, kde sa mnohé tímy CERT premenúvajú na centrá kybernetickej bezpečnosti, no ponecháva sa im skratka „CERT-EU“ z dôvodu rozpoznania názvu.

• Súlad s existujúcimi ustanoveniami v tejto oblasti politiky

Cieľom tohto návrhu je zvýšiť odolnosť inštitúcií, orgánov a agentúr Únie v oblasti kybernetickej bezpečnosti proti kybernetickým hrozbám a zároveň zabezpečiť súlad s existujúcimi právnymi predpismi, ktorými sú:

- smernica (EÚ) 2016/1148 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii. Takisto je v súlade s návrhom smernice (EÚ) XXXX/XXXX o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii a o zrušení smernice (EÚ) 2016/1148 [návrh smernice NIS 2],
- nariadenie (EÚ) 2019/881 o Agentúre Európskej únie pre kybernetickú bezpečnosť a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií (akt o kybernetickej bezpečnosti),
- návrh nariadenia (EÚ) XXXX/XXXX o informačnej bezpečnosti v inštitúciách, orgánoch, úradoch a agentúrach Únie,
- odporúčanie Komisie z 23. júna 2021 o zriadení spoločnej kybernetickej jednotky,
- odporúčanie Komisie (EÚ) 2017/1584 z 13. septembra 2017 o koordinovanej reakcii na kybernetické incidenty a krízy veľkého rozsahu.

V prílohe k odporúčaniu Komisie (EÚ) 2017/1584 z 13. septembra 2017 o koordinovanej reakcii na kybernetické incidenty a krízy veľkého rozsahu sa uvádza koncepcia koordinovanej reakcie na cezhraničné kybernetické incidenty a krízy veľkého rozsahu.

Rada Európskej únie vo svojom uznesení z 9. marca 2021 zdôraznila, že kybernetická bezpečnosť má zásadný význam pre fungovanie verejnej správy na vnútroštátnej úrovni aj na

úrovni EÚ, ako aj pre spoločnosť a hospodárstvo ako celok, a poukázala na význam robustného a konzistentného bezpečnostného rámca na ochranu všetkých zamestnancov EÚ a jej údajov, komunikačných sietí a informačných systémov a rozhodovacích procesov. To sa má dosiahnuť najmä posilnením odolnosti a zlepšením bezpečnostnej kultúry inštitúcií, orgánov a agentúr Únie. Majú sa sprístupniť dostatočné zdroje a spôsobilosti, a to aj v kontexte posilnenia mandátu CERT-EU.

2. PRÁVNY ZÁKLAD, SUBSIDIARITA A PROPORCIONALITA

- **Právny základ**

Právnym základom tohto nariadenia je článok 298 Zmluvy o fungovaní Európskej únie (ďalej len „ZFEÚ“), v ktorom sa stanovuje, že pri vykonávaní svojich poslaní sú inštitúcie, orgány, úrady a agentúry Únie podporované otvorenou, efektívnou a nezávislou európskou administratívou. Európsky parlament a Rada v súlade s riadnym legislatívnym postupom prijmú na tento účel prostredníctvom nariadení ustanovenia dodržiavajúc služobný poriadok a podmienky zamestnávania prijaté na základe článku 336.

Informačné technológie priniesli nové spôsoby, akými inštitúcie, orgány a agentúry Únie pracujú, komunikujú s občanmi a celkovo zlepšujú činnosti. Ako sa technológie ďalej vyvíjajú, panoráma kybernetických hrozieb sa vyvíja spolu s nimi. Inštitúcie, orgány a agentúry Únie sa stali veľmi atraktívnymi cieľmi sofistikovaných kybernetických útokov. Zdá sa, že vytváraním systémov a požiadaviek na zaistenie kybernetickej bezpečnosti sa prispieva k efektívnosti a nezávislosti európskej správy, aby mohli inštitúcie, orgány, úrady a agentúry Únie pracovať pri plnení svojho poslania v digitálnom svete efektívnejším spôsobom.

Súčasné rozdiely v stave kybernetickej bezpečnosti a prístupe ku kybernetickej bezpečnosti jednotlivých inštitúcií, orgánov a agentúr Únie, ako sa vysvetľuje v oddiele 3, navyše predstavujú ďalšie prekážky otvorenej, efektívnej a nezávislej európskej správy. Bez spoločného prístupu by sa stav kybernetickej bezpečnosti v rámci jednotlivých inštitúcií, orgánov a agentúr Únie naďalej vyvíjal rôznymi smermi. Tento právny základ je preto primeraný vzhľadom na to, že cieľom nariadenia je vytvoriť spoločný právny rámec kybernetickej bezpečnosti v inštitúciách, orgánoch, úradoch a agentúrach Únie.

- **Subsidiarita**

Nariadenie, ktorým sa stanovujú opatrenia na zaistenie vysokej spoločnej úrovne kybernetickej bezpečnosti v inštitúciách, orgánoch, úradoch a agentúrach Únie, patrí do výlučnej právomoci Únie.

- **Proporcionalita**

Pravidlá navrhnuté v tomto nariadení neprekračujú rámec nevyhnutný na uspokojivé plnenie špecifických cieľov. Plánovanými opatreniami sa prispeje k dosiahnutiu vysokej spoločnej úrovne kybernetickej bezpečnosti bez presiahnutia rámca nevyhnutného na dosiahnutie cieľa so zreteľom na čoraz vyššie riziká, ktorým čelia.

- **Výber nástroja**

Zvolené nariadenie, ktoré je priamo uplatniteľné, sa považuje za vhodný právny nástroj na vymedzenie a zefektívnenie povinností uložených inštitúciám, orgánom a agentúram Únie. Aby sa umožnili cielené zlepšenia, najvhodnejším právnym nástrojom je nariadenie.

3. VÝSLEDKY HODNOTENÍ *EX ANTE*, KONZULTÁCIÍ SO ZAINTERESOVANÝMI STRANAMI A POSÚDENÍ VPLYVU

- **Hodnotenia *ex ante***

CERT-EU vykonalo posúdenie hlavných kybernetických hrozieb, ktorým sú v súčasnosti vystavené inštitúcie, orgány a agentúry Únie alebo ktorým pravdepodobne budú vystavené v blízkej budúcnosti.

V rámci analýzy sa použili tri kategórie pozorovaní:

- pokusy o narušenie infraštruktúry IT inštitúcií, orgánov a agentúr Únie (ak sú úspešné, považujú sa za incidenty, v ostatných prípadoch sa stále zaznamenajú ako odhalené pokusy),
- hrozby odhalené v blízkosti inštitúcií, orgánov a agentúr Únie (napr. v súvisiacich sektoroch, komunitách ich zainteresovaných strán alebo v Európe),
- významné trendy hrozieb pozorované na celosvetovej úrovni.

V analýze sa okrem toho vzalo do úvahy, ako významné prebiehajúce zmeny ovplyvňujú spôsoby, akými inštitúcie Únie spravujú a používajú svoju infraštruktúru a služby IT. K týmto zmenám patria:

- intenzívnejšia telepráca,
- migrácia systémov na cloud,
- rozsiahlejšie externé zabezpečovanie služieb IT.

V rokoch 2019 až 2021 sa výrazne zvýšil počet významných incidentov[1] ovplyvňujúcich inštitúcie, orgány a agentúry Únie, ktorých pôvodcami boli aktéri označovaní ako pokročilé pretrvávajúce hrozby (advanced persistent threat, APT). V prvej polovici roka 2021 došlo k rovnakému počtu významných incidentov ako počas celého roka 2020. To sa prejavuje aj v počte forenzných obrázkov (momentkových snímok obsahu dotknutých systémov alebo zariadení), ktoré CERT-EU analyzovalo v roku 2020, ktorý sa v porovnaní s rokom 2019 strojnásobil, zatiaľ čo počet významných incidentov od roku 2018 vzrástol viac než desaťnásobne.

Riadiaca rada CERT-EU v roku 2020 stanovila pre CERT-EU nový strategický cieľ zaručiť komplexnú úroveň kybernetickej obrany s primeraným rozsahom a intenzitou pre všetky inštitúcie, orgány a agentúry a nepretržité prispôsobovanie sa aktuálnym alebo nadchádzajúcim hrozbám vrátane útokov na mobilné zariadenia, cloudové prostredia a zariadenia internetu vecí.

Komisia na doplnenie analýzy hrozieb CERT-EU vykonala hodnotenie fungovania 20 inštitúcií, orgánov a agentúr Únie v oblasti kybernetickej bezpečnosti. V rámci neho sa získali informácie o zavedených postupoch a schopnostiach riadenia v oblasti kybernetickej bezpečnosti s vonkajším referenčným porovnávaním niektorých technických bezpečnostných kontrol.

Toto hodnotenie vychádzalo z dotazníkov, ktoré vyplnili inštitúcie, orgány a agentúry, z verejne dostupných údajov a údajov poskytnutých priamo inštitúciami, orgánmi

[1] „Významný incident“ je každý incident, pokiaľ nemá obmedzený vplyv a nie je už pravdepodobne dobre známy z hľadiska metódy alebo technológie.

a agentúrami Únie. Poskytuje dostatočné informácie o aktuálnej situácii na vyvodenie záveru, že:

- vyspelosť v oblasti kybernetickej bezpečnosti, veľkosť infraštruktúry IT a úrovne schopností sa v hodnotených inštitúciách, orgánoch a agentúrach Únie podstatne líšia,
- zatiaľ čo v mnohých inštitúciách, orgánoch a agentúrach Únie vo všeobecnosti existujú vyspelé schopnosti odhaľovania a reakcie, úrovne integrovaného riadenia rizík v rámci ich schopností správy v oblasti kybernetickej bezpečnosti sa líšia,
- zatiaľ čo rámce kybernetickej bezpečnosti (stratégia, politika a základné pravidlá) hodnotených inštitúcií, orgánov a agentúr Únie v kľúčových oblastiach kybernetickej bezpečnosti uvedených v prílohe I k tomuto nariadeniu vo všeobecnosti dobre fungujú, niektorým inštitúciám, orgánom a agentúram Únie chýba vyspelé riadenie v oblasti kontinuity činností, dodržiavanie súladu, audit a neustále zlepšovanie,
- hodnotené inštitúcie, orgány a agentúry Únie neuplatňujú technické opatrenia považované za najlepšie postupy rovnomerne.

Možno zhrnúť, že z analýzy 20 inštitúcií, orgánov a agentúr Únie vyplýva, že ich správa, kybernetická hygiena, celkové schopnosti a vyspelosť sa líšia a pohybujú sa v širokom rozpätí. Požiadavka, aby všetky inštitúcie, orgány a agentúry Únie vykonali základné kybernetickobezpečnostné opatrenia, je teda kľúčová v záujme riešenia tejto nerovnakej vyspelosti a dosiahnutia vysokej spoločnej kybernetickej bezpečnosti všetkých inštitúcií, orgánov a agentúr Únie.

Žiadne právne predpisy Únie sa dosiaľ na kybernetickú bezpečnosť inštitúcií, orgánov a agentúr Únie nezameriavali ani sa v nich komplexne neriešila panoráma kybernetickobezpečnostných hrozieb a nové riziká v oblasti IT vyvolané digitalizáciou.

- **Konzultácie so zainteresovanými stranami**

Komisia uskutočnila konzultácie so zainteresovanými stranami v rámci inštitúcií, orgánov a agentúr Únie, ako aj so zástupcami členských štátov v Rade a so zainteresovanými stranami v Európskom parlamente. Zástupcovia členských štátov a relevantné zainteresované strany z inštitúcií, orgánov a agentúr Únie sa 25. júna 2021 zúčastnili na seminári organizovanom Komisiou s cieľom viesť dialóg o obsahu budúceho návrhu nariadenia.

- **Posúdenie vplyvu**

Tento návrh bude mať vplyv na inštitúcie, orgány a agentúry Únie. V dôsledku toho osobitné posúdenie vplyvu nie je potrebné, keďže sa nebude uplatňovať na členské štáty.

- **Základné práva**

Európska únia je odhodlaná zabezpečovať vysoké normy ochrany základných práv. Výmena všetkých informácií na základe tohto nariadenia by sa uskutočňovala v dôveryhodnom prostredí pri úplnom rešpektovaní práva na ochranu osobných údajov, ako sa stanovuje v článku 8 Charty základných práv Európskej únie, a dodržiavaní príslušných právnych predpisov o ochrane údajov, najmä nariadenia Európskeho parlamentu a Rady (EÚ) 2018/1725.

4. VPLYV NA ROZPOČET

Z trhových referenčných hodnôt a zo štúdií[2] vyplýva, že priame výdavky na kybernetickú bezpečnosť sa zvyčajne pohybujú v rozmedzí 4 % až 7 % súhrnných výdavkov organizácií v oblasti IT. Z analýzy hrozieb, ktorú vykonalo CERT-EU ako podklad tohto legislatívneho návrhu, však vyplýva, že medzinárodné orgány a politické organizácie čelia zvýšeným rizikám, a preto by sa zdala primeranejším cieľom v prípade výdavkov na kybernetickú bezpečnosť úroveň 10 % výdavkov v oblasti IT. Presné náklady na tieto snahy nemožno určiť vzhľadom na neexistenciu podrobných informácií o výdavkoch inštitúcií, orgánov a agentúr EÚ v oblasti IT a o relevantnom podiele výdavkov na kybernetickú bezpečnosť.

Zatiaľ čo je teda pravdepodobné, že mnohé inštitúcie, orgány a agentúry Únie majú menšie výdavky na kybernetickú bezpečnosť, než by mali mať, toto nariadenie samo osebe nepovedie k zvýšeniu týchto bežných výdavkov. Aj bez nariadenia by všetky subjekty museli zaistiť primeranú úroveň kybernetickej bezpečnosti. V rámci nariadenia sa pokračuje v predchádzajúcej spolupráci v riadiacej rade CERT-EU a formalizuje sa úroveň výmeny informácií, ktorá čiastočne existuje už dnes. Ako sa podrobne uvádza v legislatívnom finančnom výkaze, CERT-EU si bude vyžadovať dodatočné zdroje s cieľom plniť svoju rozšírenú úlohu, pričom tieto zdroje by sa mali prerozdeliť z inštitúcií, orgánov a agentúr Únie, ktoré využívajú služby CERT-EU.

5. ĎALŠIE PRVKY

- **Spôsob vykonávania, monitorovania, hodnotenia a podávania správ**

Medziinštitucionálna rada pre kybernetickú bezpečnosť (IICB) s pomocou CERT-EU by mali preskúmať fungovanie tohto nariadenia, vykonať hodnotenia a predložiť Komisii správu so svojimi zisteniami. Komisia by mala zabezpečiť pravidelné predkladanie správ Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov.

CERT-EU môže vypracovať návrh usmerňovacieho dokumentu alebo odporúčania, ktoré sa IICB môže rozhodnúť prijať. Usmerňovací dokument je usmernenie, ktorého adresátmi sú všetky inštitúcie, orgány a agentúry Únie alebo len časť z nich, zatiaľ čo odporúčanie je adresované jednotlivým inštitúciám, orgánom a agentúram Únie. Výzva na činnosť je usmernenie CERT-EU, v ktorom sa opisujú naliehavé bezpečnostné opatrenia a v ktorom sa inštitúcie, orgány a agentúry Únie naliehavo vyzývajú, aby prijali tieto opatrenia v stanovenom časovom rámci.

- **Podrobné vysvetlenie konkrétnych ustanovení návrhu**

Všeobecné ustanovenia

V nariadení sa stanovujú opatrenia v záujme zaistenia vysokej spoločnej úrovne kybernetickej bezpečnosti, ktorá sa uplatňuje na inštitúcie, orgány a agentúry Únie s cieľom umožniť im plniť ich poslanie otvoreným, efektívnym a nezávislým spôsobom. (články 1 – 3, 23 – 25)

Opatrenia na zaistenie vysokej spoločnej úrovne kybernetickej bezpečnosti

[2] Zdroj: Gartner, *Identifying the Real Information Security Budget* (Identifikácia skutočného rozpočtu na informačnú bezpečnosť) (2016). Ide o výdavky nad rámec nepriamych výdavkov na bezpečnosť v oblasti IT, napríklad výdavkov na bezpečnosť sietí, ako sú výdavky na firewally, antivírusy a povinnosti vlastníka systému, ako je posudzovanie rizík a vykonávanie bezpečnostných kontrol. V práci z roku 2020 sa uvádzajú výdavky na kybernetickú bezpečnosť vo finančných inštitúciách na úrovni 10 – 11 % výdavkov v oblasti IT, zdroj: DI_2020-FS-ISAC-Cybersecurity.pdf (deloitte.com).

Inštitúcie, orgány a agentúry Únie sú povinné vytvoriť vnútorný rámec riadenia, správy a kontroly kybernetickobezpečnostných rizík, ktorým sa zaistí účinné a obozretné riadenie všetkých kybernetickobezpečnostných rizík. Inštitúcie, orgány a agentúry navyše prijmú základné kybernetickobezpečnostné pravidlá v záujme riešenia rizík identifikovaných v danom rámci, vykonávania pravidelného posudzovania vyspelosti v oblasti kybernetickej bezpečnosti a prijatia plánu kybernetickej bezpečnosti. (články 4 – 8)

Medziinštitucionálna rada pre kybernetickú bezpečnosť

Zriaďuje sa Medziinštitucionálna rada pre kybernetickú bezpečnosť, ktorá zodpovedá za monitorovanie vykonávania tohto nariadenia inštitúciami, orgánmi a agentúrami Únie, ako aj za dohľad nad vykonávaním všeobecných priorít a cieľov zo strany CERT-EU a za strategické riadenie CERT-EU. (články 9 – 11)

CERT-EU

CERT-EU prispieva k bezpečnosti prostredia IT všetkých inštitúcií, orgánov a agentúr Únie tým, že im poskytuje poradenstvo, pomáha im predchádzať incidentom, odhaľovať ich, zmierňovať a reagovať na ne a vystupuje ako centrum na výmenu informácií a koordináciu reakcie na incidenty v oblasti kybernetickej bezpečnosti. (články 12 – 17)

Spolupráca a oznamovacie povinnosti

Nariadením sa zabezpečuje spolupráca a výmena informácií medzi CERT-EU a inštitúciami, orgánmi a agentúrami Únie v záujme rozvíjania dôvery a istoty. CERT-EU môže na tento účel požiadať inštitúcie, orgány a agentúry Únie, aby mu poskytli relevantné informácie, pričom CERT-EU si môže vymieňať informácie o konkrétnom incidente s inštitúciami, orgánmi a agentúrami Únie s cieľom uľahčiť odhaľovanie podobných kybernetických hrozieb alebo incidentov bez súhlasu dotknutej zložky. CERT-EU môže informácie o konkrétnom incidente, v rámci ktorých sa uvádza identita cieľa kybernetickobezpečnostného incidentu, poskytovať iba so súhlasom dotknutej zložky.

Všetky inštitúcie, orgány a agentúry Únie predovšetkým oznamujú CERT-EU významné kybernetické hrozby, významné zraniteľnosti a významné incidenty bez zbytočného odkladu a v každom prípade najneskôr 24 hodín po tom, ako sa o nich dozvedia. (články 18 – 22)

2022/0085 (COD)

Návrh

NARIADENIE EURÓPSKEHO PARLAMENTU A RADY,

ktorým sa stanovujú opatrenia na zaistenie vysokej spoločnej úrovne kybernetickej bezpečnosti v inštitúciách, orgánoch, úradoch a agentúrach Únie

EURÓPSKY PARLAMENT A RADA EURÓPSKEJ ÚNIE,

so zreteľom na Zmluvu o fungovaní Európskej únie, a najmä na jej článok 298,

so zreteľom na Zmluvu o založení Európskeho spoločenstva pre atómovú energiu, a najmä na jej článok 106a,

so zreteľom na návrh Európskej komisie,

po postúpení návrhu legislatívneho aktu národným parlamentom,

konajúc v súlade s riadnym legislatívnym postupom,

keďže:

(1) V digitálnom veku sú informačné a komunikačné technológie základom otvorenej, efektívnej a nezávislej správy Únie. Vyvíjajúce sa technológie, rastúca zložitosť a vzájomná prepojenosť digitálnych systémov zväčšujú kybernetickobezpečnostné riziká, v dôsledku čoho je správa Únie zraniteľnejšia voči kybernetickým hrozbám a incidentom, čo napokon predstavuje hrozbu pre kontinuitu činností správy a jej schopnosť zabezpečiť svoje údaje. Zatiaľ čo intenzívnejšie používanie cloudových služieb, všadeprítomné používanie IT, vysoká miera digitalizácie, práca na diaľku a vyvíjajúce sa technológie a pripojiteľnosť sú v súčasnosti hlavnými prvkami všetkých činností subjektov v rámci administratívy Únie, digitálna odolnosť zatiaľ nie je dostatočne vybudovaná.

(2) Panoráma kybernetických hrozieb, ktorej čelia inštitúcie, orgány a agentúry Únie, sa neustále vyvíja. Taktiky, techniky a postupy, ktoré aktéri hrozby využívajú, sa neustále vyvíjajú, zatiaľ čo hlavné motívy týchto útokov sa menia len málo, a to od krádeže cenných neverejných informácií až po zarábanie peňazí, manipuláciu verejnej mienky alebo narušanie digitálnej infraštruktúry. Tempo, akým vykonávajú svoje kybernetické útoky, sa zrýchľuje, zatiaľ čo ich operácie sú čoraz sofistikovanejšie a automatizovanejšie, pričom sa zameriavajú na nechránené plochy útoku, stále sa rozširujú a rýchlo využívajú zraniteľnosti.

(3) Prostredia IT inštitúcií, orgánov a agentúr Únie sú vzájomne previazané, majú integrované toky údajov a ich používatelia úzko spolupracujú. Toto vzájomné prepojenie znamená, že akékoľvek narušenie dokonca aj v prípade, že sa spočiatku obmedzuje na jednu inštitúciu, jeden orgán alebo jednu agentúru Únie, môže mať širšie kaskádovité účinky, čo môže viesť k ďalekosiahlym a dlhotrvajúcim negatívnym vplyvom na ostatné. Prostredia IT niektorých inštitúcií, orgánov a agentúr sú navyše prepojené s prostrediami IT členských štátov, čo spôsobuje, že incident v rámci jedného subjektu Únie predstavuje riziko pre kybernetickú bezpečnosť prostredí IT členských štátov a naopak.

(4) Inštitúcie, orgány a agentúry Únie sú atraktívne ciele, ktoré čelia aktérom hrozby s vysokou úrovňou zručností a s dostatočnými zdrojmi, ako aj iným hrozbám. Úroveň a vyspelosť kybernetickej odolnosti a schopnosť odhaľovať škodlivé kybernetické činnosti a reagovať na ne sa v týchto subjektoch zároveň výrazne líši. Z hľadiska fungovania európskej správy je preto potrebné, aby inštitúcie, orgány a agentúry Únie dosiahli vysokú spoločnú úroveň kybernetickej bezpečnosti prostredníctvom základných kybernetickobezpečnostných pravidiel (s ktorými musia byť zosúladené siete a informačné systémy a ktoré musia dodržiavať ich prevádzkovatelia a používatelia v záujme minimalizácie kybernetickobezpečnostných rizík), ako aj prostredníctvom výmeny informácií a spolupráce.

(5) Cieľom smernice [návrh smernice NIS 2] o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii je ďalšie zlepšenie odolnosti v oblasti kybernetickej bezpečnosti a kapacít verejných a súkromných subjektov, vnútroštátnych príslušných orgánov a subjektov, ako aj Únie ako celku, na reakcie na incidenty. Je preto potrebné, aby sa pripojili aj inštitúcie, orgány a agentúry Únie a zabezpečili pravidlá, ktoré budú v súlade so smernicou [návrh smernice NIS 2] a budú odrážať jej úroveň ambícií.

(6) Dosiahnutie vysokej spoločnej úrovne kybernetickej bezpečnosti si vyžaduje, aby si všetky inštitúcie, orgány a agentúry Únie vytvorili vnútorný rámec riadenia, správy a kontroly kybernetickobezpečnostných rizík, ktorým sa zabezpečí účinné a obozretné riadenie všetkých kybernetickobezpečnostných rizík a v ktorom sa zohľadní krízové riadenie kontinuity činností.

(7) Rozdiely medzi inštitúciami, orgánmi a agentúrami Únie si vyžadujú flexibilitu pri vykonávaní, keďže jedno riešenie nebude vyhovovať všetkým. Opatrenia na zaistenie vysokej spoločnej úrovne kybernetickej bezpečnosti by nemali zahŕňať žiadne povinnosti, ktorými by sa priamo zasahovalo do plnenia poslania inštitúcií, orgánov a agentúr Únie alebo by sa narúšala ich inštitucionálna autonómia. Tieto inštitúcie, orgány a agentúry by si teda mali vytvoriť vlastné rámce riadenia, správy a kontroly kybernetickobezpečnostných rizík a prijať vlastné základné kybernetickobezpečnostné pravidlá a plány.

(8) S cieľom vyhnúť sa neprimeranému finančnému a administratívnemu zaťaženiu inštitúcií, orgánov a agentúr Únie by požiadavky na riadenie kybernetickobezpečnostných rizík mali byť primerané riziku, ktoré predstavuje daná sieť a daný informačný systém, pričom by sa mal zohľadniť najnovší vývoj v oblasti takýchto opatrení. Cieľom všetkých inštitúcií, orgánov a agentúr Únie by malo byť pridelenie primeraného percentuálneho podielu ich rozpočtu v oblasti IT na zlepšenie úrovne kybernetickej bezpečnosti. V dlhodobejšom horizonte by sa mali vyvinúť snahy o dosiahnutie cieľa rádovo na úrovni 10 %.

(9) Vysoká spoločná úroveň kybernetickej bezpečnosti si vyžaduje, aby nad kybernetickou bezpečnosťou vykonával dohľad manažment najvyššej úrovne jednotlivých inštitúcií, orgánov a agentúr Únie, ktorý by mal schváliť základné kybernetickobezpečnostné pravidlá, prostredníctvom ktorých by sa mali riešiť riziká identifikované na základe rámca zavedeného jednotlivými inštitúciami, orgánmi a agentúrami. Neoddeliteľnou súčasťou základných kybernetickobezpečnostných pravidiel vo všetkých inštitúciách, orgánoch a agentúrach Únie je riešenie kultúry v oblasti kybernetickej bezpečnosti, t. j. každodennej praxe v oblasti kybernetickej bezpečnosti.

(10) Inštitúcie, orgány a agentúry Únie by mali posudzovať riziká súvisiace so vzťahmi s dodávateľmi a poskytovateľmi služieb vrátane poskytovateľov služieb dátového úložiska a spracúvania údajov alebo riadených bezpečnostných služieb a prijať primerané opatrenia na ich riešenie. Tieto opatrenia by mali byť súčasťou základných kybernetickobezpečnostných pravidiel a mali by sa ďalej vymedziť v usmerňovacích dokumentoch alebo odporúčaniach, ktoré vydá CERT-EU. Pri vymedzení opatrení a usmernení by sa mali náležite zohľadniť relevantné právne predpisy a politiky EÚ vrátane posúdení rizík a odporúčaní vydaných skupinou pre spoluprácu v oblasti NIS, ako je koordinované posúdenie rizík na úrovni EÚ a súbor nástrojov EÚ pre kybernetickú bezpečnosť 5G. Okrem toho by sa mohla vyžadovať certifikácia príslušných produktov, služieb a postupov IKT v rámci špecifických systémov certifikácie kybernetickej bezpečnosti EÚ prijatých podľa článku 49 nariadenia (EÚ) 2019/881.

(11) Generálni tajomníci inštitúcií a orgánov Únie sa v máji 2011 rozhodli vytvoriť v predbežnom zoskupení tím reakcie na núdzové počítačové situácie v inštitúciách, orgánoch a agentúrach Únie (CERT-EU) pod dohľadom medziinštitucionálnej riadiacej rady. Generálni tajomníci v júli 2012 potvrdili praktické dojednania a dohodli sa na zachovaní CERT-EU ako stáleho subjektu s cieľom pomôcť zlepšiť celkovú úroveň bezpečnosti informačných technológií inštitúcií, orgánov a agentúr Únie ako príklad viditeľnej medziinštitucionálnej spolupráce v oblasti kybernetickej bezpečnosti. V septembri 2012 sa CERT-EU zriadilo ako pracovná skupina Európskej komisie s medziinštitucionálnym mandátom. Inštitúcie a orgány Únie v decembri 2017 uzavreli medziinštitucionálnu dohodu o organizácii a fungovaní tímu CERT-EU[3]. Táto dohoda by sa mala naďalej vyvíjať na účely podpory vykonávania tohto nariadenia.

(12) Malo by dôjsť k premenovaniu CERT-EU z „tímu reakcie na núdzové počítačové situácie“ na „centrum kybernetickej bezpečnosti“ pre inštitúcie, orgány a agentúry Únie v súlade s vývojom v členských štátoch aj na celom svete, kde sa mnohé tímy CERT premenúvajú na centrá kybernetickej bezpečnosti, no mala by sa mu ponechať skratka „CERT-EU“ z dôvodu rozpoznania názvu.

(13) Mnohé kybernetické útoky sú súčasťou rozsiahlejších kampaní, ktoré sa zameriavajú na skupiny inštitúcií, orgánov a agentúr Únie alebo na významné komunity, ktoré zahŕňajú inštitúcie, orgány a agentúry Únie. S cieľom umožniť proaktívne odhaľovanie, reakciu na incidenty alebo prijímanie zmierňujúcich opatrení by inštitúcie, orgány a agentúry Únie mali CERT-EU oznamovať významné kybernetické hrozby, významné zraniteľnosti a významné incidenty a poskytovať mu primerané technické podrobnosti, ktoré umožnia odhaľovanie alebo zmierňovanie podobných kybernetických hrozieb, zraniteľností a incidentov v iných inštitúciách, orgánoch a agentúrach Únie, ako aj reakciu na ne. Pri uplatnení rovnakého prístupu, ako sa stanovuje v smernici [návrh smernice NIS 2], ak sa subjekty dozvedia o významnom incidente, malo by sa od nich vyžadovať, aby CERT-EU do 24 hodín predložili prvotné oznámenie. Takouto výmenou informácií by sa centru CERT-EU malo umožniť poskytnúť informácie ostatným inštitúciám, orgánom a agentúram Únie, ako aj príslušným náprotivkom s cieľom pomôcť chrániť prostredia IT Únie a prostredia IT náprotivkov Únie pred podobnými incidentmi, hrozbami a zraniteľnosťami.

(14) Okrem toho, že by sa malo centru CERT-EU zveriť viac povinností a mala by sa rozšíriť jeho úloha, by sa mala zriadiť Medziinštitucionálna rada pre kybernetickú

[3] Ú. v. EÚ C 12, 13.1.2018, s. 1 – 11.

bezpečnosť (IICB), ktorá by mala uľahčovať dosiahnutie vysokej spoločnej úrovne kybernetickej bezpečnosti inštitúcií, orgánov a agentúr Únie tým, že bude monitorovať vykonávanie tohto nariadenia inštitúciami, orgánmi a agentúrami Únie, dohliadať na vykonávanie všeobecných priorít a cieľov centrom CERT-EU a strategicky riadiť CERT-EU. IICB by mala zabezpečiť zastúpenie inštitúcií a zapojiť zástupcov agentúr a orgánov prostredníctvom siete agentúr Únie.

(15) CERT-EU by malo podporovať vykonávanie opatrení na zaistenie vysokej spoločnej úrovne kybernetickej bezpečnosti prostredníctvom návrhov usmerňovacích dokumentov a odporúčaní pre IICB alebo vydávaním výziev na činnosť. Takéto usmerňovacie dokumenty a odporúčania by mala schvaľovať IICB. V prípade potreby by CERT-EU malo vydávať výzvy na činnosť, v ktorých sa opisujú naliehavé bezpečnostné opatrenia a v ktorých sa inštitúcie, orgány a agentúry Únie naliehavo vyzývajú, aby prijali tieto opatrenia v stanovenom časovom rámci.

(16) IICB by mala monitorovať dodržiavanie tohto nariadenia, ako aj opatrenia prijaté v nadväznosti na usmerňovacie dokumenty a odporúčania a výzvy na činnosť vydané CERT-EU. V technických záležitostiach by IICB mala mať podporu technických poradných skupín v zložení podľa uváženia IICB, ktoré by mali podľa potreby úzko spolupracovať s CERT-EU, inštitúciami, orgánmi a agentúrami Únie, ako aj s inými zainteresovanými stranami. V prípade potreby by IICB mala vydávať nezáväzné varovania a odporúčať audity.

(17) Poslaním CERT-EU by malo byť prispievať k bezpečnosti prostredia IT všetkých inštitúcií, orgánov a agentúr Únie. CERT-EU by malo konať ako poverený koordinátor pre inštitúcie, orgány a agentúry Únie na účely koordinovaného zverejňovania informácií o zraniteľnosti v európskom registri zraniteľností uvedenom v článku 6 smernice [návrh smernice NIS 2].

(18) Riadiaca rada CERT-EU v roku 2020 stanovila pre CERT-EU nový strategický cieľ zaručiť komplexnú úroveň kybernetickej obrany s primeraným rozsahom a intenzitou pre všetky inštitúcie, orgány a agentúry Únie a nepretržité prispôsobovanie sa aktuálnym alebo nadchádzajúcim hrozbám vrátane útokov na mobilné zariadenia, cloudové prostredia a zariadenia internetu vecí. Súčasťou tohto strategického cieľa sú aj širokospektrálne centrá bezpečnostných operácií, ktoré monitorujú siete, a nepretržité monitorovanie hrozieb s vysokou závažnosťou. V prípade väčších inštitúcií, orgánov a agentúr Únie by CERT-EU malo poskytovať podporu ich tímom pre bezpečnosť IT vrátane bežného nepretržitého monitorovania. V prípade menších inštitúcií, orgánov a agentúr Únie a niektorých inštitúcií, orgánov a agentúr Únie strednej veľkosti by malo CERT-EU poskytovať všetky služby.

(19) CERT-EU by malo plniť aj úlohu stanovenú v smernici [návrh smernice NIS 2], pokiaľ ide o spoluprácu a výmenu informácií so sieťou jednotiek pre riešenie počítačových bezpečnostných incidentov (CSIRT). V súlade s odporúčaním Komisie (EÚ) 2017/1584[4] by malo CERT-EU navyše spolupracovať a koordinovať reakciu s relevantnými zainteresovanými stranami. S cieľom prispieť k vysokej úrovni kybernetickej bezpečnosti v celej Únii by malo CERT-EU poskytovať informácie o konkrétnych incidentoch vnútroštátnym náprotivkom. CERT-EU by malo spolupracovať aj s inými verejnými, ako aj súkromnými náprotivkami vrátane NATO po predchádzajúcom súhlase IICB.

[4] Odporúčanie Komisie (EÚ) 2017/1584 z 13. septembra 2017 o koordinovanej reakcii na kybernetické incidenty a krízy veľkého rozsahu (Ú. v. EÚ L 239, 19.9.2017, s. 36).

(20) CERT-EU by mal na podporu operačnej kybernetickej bezpečnosti využiť dostupné odborné znalosti Agentúry Európskej únie pre kybernetickú bezpečnosť prostredníctvom štruktúrovanej spolupráce, ktorá sa stanovuje v nariadení Európskeho parlamentu a Rady (EÚ) 2019/881[5]. Podľa potreby by sa mali medzi oboma subjektmi uzavrieť účelové dohody o fungovaní tejto spolupráce v praxi a zabránení zdvojovaniu činností. CERT-EU by malo spolupracovať s Agentúrou Európskej únie pre kybernetickú bezpečnosť na analýze hrozieb a pravidelne agentúre poskytovať svoju správu o panoráme hrozieb.

(21) V rámci podpory spoločnej kybernetickej jednotky zriadenej v súlade s odporúčaním Komisie z 23. júna 2021[6] by CERT-EU malo spolupracovať a vymieňať si informácie so zainteresovanými stranami s cieľom podporiť operačnú spoluprácu a umožniť existujúcim sieťam dosiahnuť ich plný potenciál, pokiaľ ide o ochranu Únie.

(22) Všetky osobné údaje spracúvané podľa tohto nariadenia by sa mali spracúvať v súlade s právnymi predpismi o ochrane údajov vrátane nariadenia Európskeho parlamentu a Rady (EÚ) 2018/1725[7].

(23) Zaobchádzanie s informáciami zo strany CERT-EU a inštitúcií, orgánov a agentúr Únie by malo byť v súlade s pravidlami stanovenými v nariadení [navrhované nariadenie o informačnej bezpečnosti]. Ak dôjde k nadviazaniu kontaktu alebo k snahe o nadviazanie kontaktu s CERT-EU zo strany vnútroštátnych bezpečnostných a spravodajských služieb, v záujme zaistenia koordinácie bezpečnostných záležitostí by sa to malo bez zbytočného odkladu oznámiť riaditeľstvu Komisie pre bezpečnosť a predsedovi IICB.

(24) Keďže služby a úlohy CERT-EU sú v záujme všetkých inštitúcií, orgánov a agentúr Únie, všetky inštitúcie, orgány a agentúry Únie s výdavkami v oblasti IT by mali na tieto služby a úlohy prispieť spravodlivým podielom. Tieto príspevky nemajú vplyv na rozpočtovú autonómiu inštitúcií, orgánov a agentúr Únie.

(25) IICB s pomocou CERT-EU by mali preskúmať a hodnotiť vykonávanie tohto nariadenia a oznámiť Komisii svoje zistenia. Na základe tohto vstupu by Komisia mala predkladať správy Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov,

---

[5] Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/881 zo 17. apríla 2019 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013 (akt o kybernetickej bezpečnosti) (Ú. v. EÚ L 151, 7.6.2019, s. 15).

[6] Odporúčanie Komisie C(2021) 4520 z 23. júna 2021 o zriadení spoločnej kybernetickej jednotky.

[7] Nariadenie Európskeho parlamentu a Rady (EÚ) 2018/1725 z 23. októbra 2018 o ochrane fyzických osôb pri spracúvaní osobných údajov inštitúciami, orgánmi, úradmi a agentúrami Únie a o voľnom pohybe takýchto údajov, ktorým sa zrušuje nariadenie (ES) č. 45/2001 a rozhodnutie č. 1247/2002/ES (Ú. v. EÚ L 295, 21.11.2018, s. 39).

PRIJALI TOTO NARIADENIE:

Kapitola I
VŠEOBECNÉ USTANOVENIA

Článok 1
Predmet úpravy

V tomto nariadení sa stanovujú:

a) povinnosti inštitúcií, orgánov a agentúr Únie, pokiaľ ide o vytvorenie vnútorného rámca riadenia, správy a kontroly kybernetickobezpečnostných rizík;

b) povinnosti inštitúcií, orgánov a agentúr Únie, pokiaľ ide o riadenie kybernetickobezpečnostných rizík, ako aj ich oznamovacie povinnosti;

c) pravidlá organizácie a činnosti Centra kybernetickej bezpečnosti pre inštitúcie, orgány a agentúry Únie (CERT-EU), ako aj organizácie a činnosti Medziinštitucionálnej rady pre kybernetickú bezpečnosť.

Článok 2
Rozsah pôsobnosti

Toto nariadenie sa uplatňuje na riadenie, správu a kontrolu kybernetickobezpečnostných rizík všetkých inštitúcií, orgánov a agentúr Únie, ako aj na organizáciu a činnosť CERT-EU a Medziinštitucionálnej rady pre kybernetickú bezpečnosť.

Článok 3
Vymedzenie pojmov

Na účely tohto nariadenia sa uplatňuje toto vymedzenie pojmov:

1. „inštitúcie, orgány a agentúry Únie“ sú inštitúcie, orgány a agentúry Únie zriadené Zmluvou o Európskej únii, Zmluvou o fungovaní Európskej únie alebo Zmluvou o založení Európskeho spoločenstva pre atómovú energiu alebo na ich základe;

2. „sieť a informačný systém“ je sieť a informačný systém v zmysle článku 4 bodu 1 smernice [návrh smernice NIS 2];

3. „bezpečnosť sietí a informačných systémov“ je bezpečnosť sietí a informačných systémov v zmysle článku 4 bodu 2 smernice [návrh smernice NIS 2];

4. „kybernetická bezpečnosť“ je kybernetická bezpečnosť v zmysle článku 4 bodu 3 smernice [návrh smernice NIS 2];

5. „manažment najvyššej úrovne“ je manažér, manažment alebo orgán koordinácie a dohľadu na najvyššej správnej úrovni, pričom sa zohľadní mechanizmus vrcholovej správy a riadenia v jednotlivých inštitúciách, orgánoch alebo agentúrach Únie;

6. „incident“ je incident v zmysle článku 4 bodu 5 smernice [návrh smernice NIS 2];

7. „významný incident“ je každý incident, pokiaľ nemá obmedzený vplyv a nie je už pravdepodobne dobre známy z hľadiska metódy alebo technológie;

8. „významný útok“ je akýkoľvek incident, ktorý si vyžaduje viac zdrojov, ako je k dispozícii v dotknutej inštitúcii, orgáne alebo agentúre Únie a v CERT-EU;

9. „riešenie incidentov“ je riešenie incidentov v zmysle článku 4 bodu 6 smernice [návrh smernice NIS 2];

10. „kybernetická hrozba“ je kybernetická hrozba v zmysle článku 2 bodu 8 nariadenia (EÚ) 2019/881;

11. „významná kybernetická hrozba“ je kybernetická hrozba so zámerom, s príležitosťou a so schopnosťou spôsobiť významný incident;

12. „zraniteľnosť“ je zraniteľnosť v zmysle článku 4 bodu 8 smernice [návrh smernice NIS 2];

13. „významná zraniteľnosť“ je zraniteľnosť, ktorá pravdepodobne povedie k významnému incidentu, ak sa využije;

14. „kybernetickobezpečnostné riziko“ je každá primerane rozpoznateľná okolnosť alebo udalosť, ktorá môže mať nepriaznivý vplyv na bezpečnosť sietí a informačných systémov;

15. „spoločná kybernetická jednotka“ je virtuálna a fyzická platforma na spoluprácu rôznych komunít v oblasti kybernetickej bezpečnosti v Únii so zameraním na operačnú a technickú koordináciu v boji proti významným cezhraničným kybernetickým hrozbám a incidentom v zmysle odporúčania Komisie z 23. júna 2021;

16. „základné kybernetickobezpečnostné pravidlá“ sú súbor minimálnych pravidiel v oblasti kybernetickej bezpečnosti, s ktorými musia byť zosúladené siete a informačné systémy a ktoré musia dodržiavať ich prevádzkovatelia a používatelia v záujme minimalizácie kybernetickobezpečnostných rizík.

Kapitola II
OPATRENIA NA ZAISTENIE VYSOKEJ SPOLOČNEJ ÚROVNE KYBERNETICKEJ BEZPEČNOSTI

Článok 4
Riadenie, správa a kontrola rizík

1. Každá inštitúcia, orgán a agentúra Únie si zriadi vlastný vnútorný rámec riadenia, správy a kontroly kybernetickobezpečnostných rizík (ďalej len „rámec“) na podporu poslania subjektu a vykonávanie jeho inštitucionálnej autonómie. Nad touto prácou má dohľad najvyšší manažment subjektu s cieľom zabezpečiť účinné a obozretné riadenie všetkých kybernetickobezpečnostných rizík. Rámec sa zavedie najneskôr do … [15 mesiacov od nadobudnutia účinnosti tohto nariadenia].

2. Rámec sa vzťahuje na celé prostredie IT dotknutej inštitúcie, orgánu alebo agentúry vrátane prostredia IT v jej priestoroch, externe zabezpečovaných aktív a služieb v prostrediach cloud computingu alebo služieb s hostingom tretích strán, mobilných zariadení, korporátnych sietí, sietí podnikov, ktoré nie sú pripojené k internetu, a akýchkoľvek zariadení pripojených k prostrediu IT. V rámci sa zohľadní krízové riadenie kontinuity činností, pričom sa vezme do úvahy bezpečnosť dodávateľského reťazca, ako aj riadenie rizík vyvolaných človekom, ktoré by mohli mať vplyv na kybernetickú bezpečnosť dotknutých inštitúcií, orgánov alebo agentúr Únie.

3. Najvyšší manažment každej inštitúcie, orgánu a agentúry Únie zabezpečuje dohľad nad tým, ako ich organizácia dodržiava povinnosti týkajúce sa riadenia, správy a kontroly kybernetickobezpečnostných rizík, a to bez toho, aby boli dotknuté

formálne povinnosti iných úrovní manažment, pokiaľ ide o súlad a riadenie rizík v ich príslušných oblastiach zodpovednosti.

4. Jednotlivé inštitúcie, orgány a agentúry Únie majú zavedené účinné mechanizmy s cieľom zabezpečiť, aby sa na kybernetickú bezpečnosť vynakladal primeraný percentuálny podiel z rozpočtu na IT.

5. Jednotlivé inštitúcie, orgány a agentúry Únie vymenujú miestneho úradníka pre kybernetickú bezpečnosť alebo osobu v rovnocennej funkcii, ktorá koná ako ich jednotné kontaktné miesto v súvislosti so všetkými aspektmi kybernetickej bezpečnosti.

Článok 5

Základné kybernetickobezpečnostné pravidlá

1. Najvyšší manažment jednotlivých inštitúcií, orgánov a agentúr Únie schvaľuje vlastné základné kybernetickobezpečnostné pravidlá subjektu v záujme riešenia rizík identifikovaných v rámci uvedenom v článku 4 ods. 1. Koná tak na podporu svojho poslania a vykonávania svojej inštitucionálnej autonómie. Základné kybernetickobezpečnostné pravidlá sa zavedú najneskôr do … [18 mesiacov od nadobudnutia účinnosti tohto nariadenia] a budú sa nimi riešiť oblasti uvedené v prílohe I a opatrenia uvedené v prílohe II.

2. Vrcholový manažment jednotlivých inštitúcií, orgánov a agentúr Únie sa pravidelne zúčastňuje na osobitnej odbornej príprave s cieľom získať dostatočné vedomosti a zručnosti na pochopenie a posúdenie kybernetickobezpečnostného rizika a postupov riadenia, ako aj ich vplyvu na činnosti organizácie.

Článok 6

Posúdenia vyspelosti

Všetky inštitúcie, orgány a agentúry Únie aspoň každé tri roky vykonajú posúdenie vyspelosti v oblasti kybernetickej bezpečnosti, pričom doň začlenia všetky prvky svojho prostredia IT, ako sa opisuje v článku 4, a zohľadnia relevantné usmerňovacie dokumenty a odporúčania prijaté v súlade s článkom 13.

Článok 7

Plány kybernetickej bezpečnosti

1. V nadväznosti na závery vyvodené z posúdenia vyspelosti a vzhľadom na aktíva a riziká identifikované podľa článku 4 manažment najvyššej úrovne jednotlivých inštitúcií, orgánov a agentúr Únie bez zbytočného odkladu po vytvorení rámca riadenia, správy a kontroly rizík a stanovení základných kybernetickobezpečnostných pravidiel schváli plán kybernetickej bezpečnosti. Cieľom plánu je zvýšiť celkovú kybernetickú bezpečnosť dotknutého subjektu, takže sa ním prispieva k dosiahnutiu alebo zlepšeniu vysokej spoločnej úrovne kybernetickej bezpečnosti všetkých inštitúcií, orgánov a agentúr Únie. Na podporu poslania subjektu na základe jeho inštitucionálnej autonómie sa do plánu zahrnú aspoň oblasti uvedené v prílohe I, opatrenia uvedené v prílohe II, ako aj opatrenia súvisiace s pripravenosťou a reakciou na incidenty a obnovou po incidentoch, ako je monitorovanie bezpečnosti a vedenie záznamov. Plán sa reviduje aspoň každé tri roky v nadväznosti na posúdenia vyspelosti vykonané podľa článku 6.

2. Plán kybernetickej bezpečnosti zahŕňa úlohy a povinnosti zamestnancov pri jeho vykonávaní.

3. V pláne kybernetickej bezpečnosti sa zohľadnia všetky uplatniteľné usmerňovacie dokumenty a odporúčania, ktoré vydalo CERT-EU.

Článok 8
Vykonávanie

1. Po dokončení posúdení vyspelosti inštitúcie, orgány a agentúry Únie predložia tieto posúdenia Medziinštitucionálnej rade pre kybernetickú bezpečnosť. Po dokončení plánov bezpečnosti inštitúcie, orgány a agentúry Únie oznámia Medziinštitucionálnej rade pre kybernetickú bezpečnosť ich dokončenie. Na žiadosť rady podajú správu o osobitných aspektoch tejto kapitoly.

2. Vykonávanie ustanovení stanovených v tejto kapitole sa podporí usmerňovacími dokumentmi a odporúčaniami vydanými v súlade s článkom 13.

Kapitola III
MEDZIINŠTITUCIONÁLNA RADA PRE KYBERNETICKÚ BEZPEČNOSŤ

Článok 9
Medziinštitucionálna rada pre kybernetickú bezpečnosť

1. Zriaďuje sa Medziinštitucionálna rada pre kybernetickú bezpečnosť (IICB).

2. IICB zodpovedá za:

   a) monitorovanie vykonávania tohto nariadenia inštitúciami, orgánmi a agentúrami Únie;

   b) dohľad nad vykonávaním všeobecných priorít a cieľov centrom CERT-EU, ako aj strategické riadenie CERT-EU.

3. IICB sa skladá z troch zástupcov vymenovaných sieťou agentúr Únie na návrh jej poradného výboru pre IKT, ktorí zastupujú záujmy agentúr a orgánov, ktoré prevádzkujú vlastné prostredie IT, a z jedného zástupcu vymenovaného každým z týchto subjektov:

   a) Európsky parlament;

   b) Rada Európskej únie;

   c) Európska komisia;

   d) Súdny dvor Európskej únie;

   e) Európska centrálna banka;

   f) Európsky dvor audítorov;

   g) Európska služba pre vonkajšiu činnosť;

   h) Európsky hospodársky a sociálny výbor;

   i) Európsky výbor regiónov;

   j) Európska investičná banka;

   k) Agentúra Európskej únie pre kybernetickú bezpečnosť.

Členom môže pomáhať náhradník. Predseda môže pozvať iných zástupcov uvedených organizácií alebo zástupcov iných inštitúcií, orgánov a agentúr Únie, aby sa zúčastnili na zasadnutiach IICB bez hlasovacieho práva.

4. IICB prijíma svoj vnútorný rokovací poriadok.

5. IICB v súlade so svojím vnútorným rokovacím poriadkom vymenuje spomedzi svojich členov predsedu na obdobie štyroch rokov. Jeho náhradník sa na rovnaké obdobie stáva riadnym členom IICB.

6. IICB zasadá z iniciatívy predsedu, na žiadosť CERT-EU alebo na žiadosť niektorého z členov.

7. Každý člen IICB má jeden hlas. Rozhodnutia IICB sa prijímajú jednoduchou väčšinou, ak v tomto nariadení nie je stanovené inak. Predseda hlasuje iba v prípade rovnosti hlasov, v ktorom môže odovzdať rozhodujúci hlas.

8. IICB môže konať v rámci zjednodušeného písomného postupu, ktorý sa začne v súlade s vnútorným rokovacím poriadkom IICB. V rámci tohto postupu sa príslušné rozhodnutie považuje za schválené v časovom rámci stanovenom predsedom s výnimkou prípadu, keď niektorý člen namieta.

9. Vedúci CERT-EU alebo jeho náhradník sa zúčastňuje na zasadnutiach IICB s výnimkou prípadu, keď IICB rozhodne inak.

10. Sekretariát IICB zabezpečuje Komisia.

11. Zástupcovia vymenovaní sieťou agentúr EÚ na návrh poradného výboru pre IKT oznamujú rozhodnutia IICB agentúram Únie a spoločným podnikom. Ktorákoľvek agentúra a ktorýkoľvek orgán Únie majú právo predložiť zástupcom alebo predsedovi IICB každú záležitosť, na ktorú by sa podľa ich názoru mala upozorniť IICB.

12. IICB môže konať v rámci zjednodušeného písomného postupu, ktorý začne predseda a v ktorom sa príslušné rozhodnutie považuje za schválené v časovom rámci stanovenom predsedom s výnimkou prípadu, keď niektorý člen namieta.

13. IICB môže vymenovať výkonný výbor, ktorý jej pomáha pri práci, a postúpiť mu niektoré svoje úlohy a právomoci. IICB stanoví rokovací poriadok výkonného výboru vrátane jeho úloh a právomocí a funkčného obdobia jeho členov.

Článok 10
Úlohy IICB

IICB pri plnení svojich úloh predovšetkým:

(a) preskúmava všetky správy vyžiadané od CERT-EU o stave vykonávania tohto nariadenia inštitúciami, orgánmi a agentúrami Únie;

(b) na základe návrhu vedúceho CERT-EU schvaľuje ročný pracovný program CERT-EU a monitoruje jeho vykonávanie;

(c) na základe návrhu vedúceho CERT-EU schvaľuje katalóg služieb CERT-EU;

(d) na základe návrhu predloženého vedúcim CERT-EU schvaľuje ročný finančný plán príjmov a výdavkov vrátane počtu zamestnancov v súvislosti s činnosťami CERT-EU;

(e) na základe návrhu vedúceho CERT-EU schvaľuje postupy v súvislosti s dohodami o úrovni poskytovaných služieb;

(f) preskúmava a schvaľuje výročnú správu vypracovanú vedúcim CERT-EU, ktorá sa týka činností CERT-EU a správy jeho finančných prostriedkov;

(g) schvaľuje a monitoruje kľúčové ukazovatele výkonnosti CERT-EU vymedzené na návrh vedúceho CERT-EU;

(h) schvaľuje dohody o spolupráci, dojednania alebo zmluvy o úrovni poskytovaných služieb medzi CERT-EU a inými subjektmi podľa článku 17;

(i) zriaďuje potrebný počet technických poradných skupín, ktoré pomáhajú IICB pri práci, schvaľuje ich mandát a vymenúva jednotlivých predsedov.

Článok 11
Súlad

IICB monitoruje vykonávanie tohto nariadenia a prijatých usmerňovacích dokumentov, odporúčaní a výziev na činnosť inštitúciami, orgánmi a agentúrami Únie. Keď IICB zistí, že inštitúcie, orgány a agentúry Únie toto nariadenie alebo usmerňovacie dokumenty, odporúčania a výzvy na činnosť vydané podľa tohto nariadenia účinne neuplatňujú alebo nevykonávajú, bez toho, aby boli dotknuté vnútorné postupy príslušných inštitúcií, orgánov alebo agentúr Únie, môže:

(a) vydať varovanie; v prípade potreby sa vzhľadom na závažné kybernetickobezpečnostné riziko náležite obmedzí cieľová skupina varovania;

(b) odporučiť príslušnému útvaru pre audit, aby vykonal audit.

Kapitola IV
CERT-EU

Článok 12
Poslanie a úlohy CERT-EU

1. Poslaním CERT-EU, autonómneho medziinštitucionálneho centra kybernetickej bezpečnosti pre všetky inštitúcie, orgány a agentúry Únie, je prispievať k bezpečnosti verejne prístupného prostredia IT všetkých inštitúcií, orgánov a agentúr Únie tým, že im poskytuje poradenstvo v oblasti kybernetickej bezpečnosti, pomáha im predchádzať incidentom, odhaľovať ich, zmierňovať a reagovať na ne a vystupuje ako centrum na výmenu informácií a koordináciu reakcie na incidenty v oblasti kybernetickej bezpečnosti.

2. CERT-EU plní pre inštitúcie, orgány a agentúry Únie tieto úlohy:

   a) podporuje ich pri vykonávaní tohto nariadenia a prispieva ku koordinácii uplatňovania tohto nariadenia prostredníctvom opatrení uvedených v článku 13 ods. 1 alebo prostredníctvom správ *ad hoc*, o ktoré požiada IICB;

   b) podporuje ich pomocou balíka služieb v oblasti kybernetickej bezpečnosti opísaných v jeho katalógu služieb (ďalej len „základné služby“);

   c) spravuje sieť partnerov na podporu služieb, ako sa uvádza v článkoch 16 a 17;

   d) upozorňuje IICB na záležitosti súvisiace s vykonávaním tohto nariadenia a vykonávaním usmerňovacích dokumentov, odporúčaní a výziev na činnosť;

e) oznamuje kybernetické hrozby, ktorým čelia inštitúcie, orgány a agentúry Únie, a prispieva k situačnej informovanosti v EÚ v kybernetickej oblasti.

3. CERT-EU prispieva k činnosti spoločnej kybernetickej jednotky zriadenej v súlade s odporúčaním Komisie z 23. júna 2021, a to aj v týchto oblastiach:

a) pripravenosť, koordinácia pri incidentoch, výmena informácií a reakcia na krízu na technickej úrovni v prípadoch súvisiacich s inštitúciami, orgánmi a agentúrami Únie;

b) operačná spolupráca v súvislosti so sieťou jednotiek pre riešenie počítačových bezpečnostných incidentov (CSIRT) vrátane vzájomnej pomoci a so širšou komunitou v oblasti kybernetickej bezpečnosti;

c) spravodajské informácie o kybernetických hrozbách vrátane situačnej informovanosti;

d) akákoľvek téma, ktorá si vyžaduje odborné technické znalosti CERT-EU v oblasti kybernetickej bezpečnosti.

4. CERT-EU štruktúrovane spolupracuje s Agentúrou Európskej únie pre kybernetickú bezpečnosť v oblasti budovania kapacít, operačnej spolupráce a dlhodobých strategických analýz kybernetických hrozieb v súlade s nariadením Európskeho parlamentu a Rady (EÚ) 2019/881.

5. CERT-EU môže poskytovať tieto služby, ktoré nie sú opísané v jeho katalógu služieb (ďalej len „spoplatnené služby“):

a) služby na podporu kybernetickej bezpečnosti prostredia IT inštitúcií, orgánov a agentúr Únie iné ako služby uvedené v odseku 2 na základe dohôd o úrovni poskytovaných služieb a v súlade s dostupnými zdrojmi;

b) služby na podporu činností alebo projektov inštitúcií, orgánov a agentúr Únie v oblasti kybernetickej bezpečnosti iné ako služby na ochranu prostredia IT na základe písomných dohôd a s predchádzajúcim súhlasom IICB;

c) služby na podporu bezpečnosti prostredia IT organizácií iných ako inštitúcie, orgány a agentúry Únie, ktoré úzko spolupracujú s inštitúciami, orgánmi a agentúrami Únie, napr. majú pridelené úlohy alebo povinnosti podľa práva Únie, na základe písomných dohôd a s predchádzajúcim súhlasom IICB.

6. CERT-EU môže usporiadať cvičenia v oblasti kybernetickej bezpečnosti alebo odporučiť účasť na existujúcich cvičeniach, a to vo vhodnom prípade v úzkej spolupráci s Agentúrou Európskej únie pre kybernetickú bezpečnosť, s cieľom otestovať úroveň kybernetickej bezpečnosti inštitúcií, orgánov a agentúr Únie.

7. CERT-EU môže poskytnúť pomoc inštitúciám, orgánom a agentúram Únie v súvislosti s incidentmi v utajených prostrediach IT, ak o to dotknutá zložka výslovne požiada.

Článok 13

Usmerňovacie dokumenty, odporúčania a výzvy na činnosť

1. CERT-EU podporuje vykonávanie tohto nariadenia vydávaním:

a) výziev na činnosť, v ktorých sa opisujú naliehavé bezpečnostné opatrenia a v ktorých sa inštitúcie, orgány a agentúry Únie naliehavo vyzývajú, aby prijali tieto opatrenia v stanovenom časovom rámci;

b) návrhov usmerňovacích dokumentov pre IICB adresovaných všetkým inštitúciám, orgánom a agentúram Únie alebo len ich časti;

c) návrhov odporúčaní pre IICB adresovaných jednotlivým inštitúciám, orgánom a agentúram Únie.

2. Usmerňovacie dokumenty a odporúčania môžu zahŕňať:

a) postupy alebo zlepšenia v súvislosti s riadením kybernetickobezpečnostných rizík a základných kybernetickobezpečnostných pravidiel;

b) postupy v súvislosti s posudzovaním vyspelosti a plánmi kybernetickej bezpečnosti a

c) vo vhodnom prípade využívanie spoločných technológií, architektúry a súvisiacich najlepších postupov s cieľom dosiahnuť interoperabilitu a spoločné normy v zmysle článku 4 bodu 10 smernice [návrh smernice NIS 2].

3. IICB môže na návrh CERT-EU prijímať usmerňovacie dokumenty alebo odporúčania.

4. IICB môže dať CERT-EU pokyn na vydanie, zrušenie alebo zmenu návrhu usmerňovacích dokumentov alebo odporúčaní alebo výzvy na činnosť.

Článok 14
Vedúci CERT-EU

Vedúci CERT-EU pravidelne predkladá správy IICB a predsedovi IICB, pokiaľ ide o výkonnosť CERT-EU, finančné plánovanie, príjmy, plnenie rozpočtu, dohody o úrovni poskytovaných služieb a písomné dohody, ktoré uzavrelo, spoluprácu s náprotivkami a partnermi a služobné cesty zamestnancov, vrátane správ uvedených v článku 10 ods. 1.

Článok 15
Finančné a personálne záležitosti

1. Komisia vymenúva vedúceho CERT-EU po jednohlasnom schválení IICB. Konzultácie s IICB sa uskutočňujú vo všetkých fázach postupu pred vymenovaním vedúceho CERT-EU, najmä pri vypracúvaní oznámení o voľnom pracovnom mieste, posudzovaní prihlášok a vymenúvaní výberových komisií v súvislosti s týmto miestom.

2. V prípade uplatňovania administratívnych a finančných postupov koná vedúci CERT-EU pod vedením Komisie.

3. Úlohy a činnosti CERT-EU vrátane služieb, ktoré poskytuje CERT-EU podľa článku 12 ods. 2, 3, 4 a 6 a podľa článku 13 ods. 1 inštitúciám, orgánom a agentúram Únie financovaným v rámci okruhu viacročného finančného rámca určeného na Európsku verejnú správu, sa financujú prostredníctvom samostatného rozpočtového riadka v rozpočte Komisie. Miesta vyčlenené pre CERT-EU sa podrobne uvádzajú v poznámke pod čiarou plánu pracovných miest Komisie.

4. Inštitúcie, orgány a agentúry Únie iné ako tie, ktoré sa uvádzajú v odseku 3, poskytujú CERT-EU ročný finančný príspevok na úhradu služieb, ktoré CERT-EU poskytuje podľa odseku 3. Jednotlivé príspevky vychádzajú z usmernení, ktoré poskytne IICB, a každý subjekt si ich dohodne s CERT-EU v dohodách o úrovni poskytovaných služieb. Príspevky predstavujú spravodlivý a primeraný podiel z celkových nákladov na poskytnuté služby. Započítajú sa do samostatného

rozpočtového riadka uvedeného v odseku 3 ako pripísané príjmy, ako sa stanovuje v článku 21 ods. 3 písm. c) nariadenia Európskeho parlamentu a Rady (EÚ, Euratom) 2018/1046[8].

5. Náklady na úlohy vymedzené v článku 12 ods. 5 uhrádzajú inštitúcie, orgány a agentúry Únie, ktorým CERT-EU služby poskytlo. Príjmy sa pripíšu do rozpočtových riadkov na podporu nákladov.

Článok 16

Spolupráca CERT-EU s náprotivkami v členských štátoch

1. CERT-EU spolupracuje a vymieňa si informácie s vnútroštátnymi náprotivkami v členských štátoch vrátane tímov CERT, vnútroštátnych centier pre kybernetickú bezpečnosť, jednotiek CSIRT a jednotných kontaktných miest uvedených v článku 8 smernice [návrh smernice NIS 2] v súvislosti s kybernetickými hrozbami, so zraniteľnosťami a s incidentmi, s možnými protiopatreniami a so všetkými záležitosťami relevantnými z hľadiska zlepšenia ochrany prostredia IT inštitúcií, orgánov a agentúr Únie, a to aj prostredníctvom siete jednotiek CSIRT uvedenej v článku 13 smernice [návrh smernice NIS 2].

2. CERT-EU si s vnútroštátnymi náprotivkami v členských štátoch môže vymieňať informácie o konkrétnom incidente s cieľom uľahčiť odhaľovanie podobných kybernetických hrozieb alebo incidentov bez súhlasu dotknutej zložky. CERT-EU môže informácie o konkrétnom incidente, v rámci ktorých sa uvádza identita cieľa kybernetickobezpečnostného incidentu, poskytovať iba so súhlasom dotknutej zložky.

Článok 17

Spolupráca CERT-EU s náprotivkami z tretích krajín

1. CERT-EU môže spolupracovať s náprotivkami z tretích krajín vrátane náprotivkov z konkrétnych odvetví v oblasti nástrojov a metód, ako sú techniky, taktiky, postupy a najlepšie postupy, ako aj v oblasti kybernetických hrozieb a zraniteľností. V každom prípade spolupráce s týmito náprotivkami, a to aj v rámcoch, v ktorých náprotivky z tretích krajín spolupracujú s vnútroštátnymi náprotivkami z členských štátov, si CERT-EU vždy vyžiada predchádzajúci súhlas IICB.

2. CERT-EU môže spolupracovať s inými partnermi, ako sú obchodné subjekty, medzinárodné organizácie, vnútroštátne subjekty z tretích krajín alebo jednotliví odborníci, s cieľom zhromažďovať informácie o všeobecných a špecifických kybernetických hrozbách, zraniteľnostiach a možných protiopatreniach. V prípade širšej spolupráce s týmito partnermi si CERT-EU vyžiada predchádzajúci súhlas IICB.

3. CERT-EU so súhlasom zložky dotknutej incidentom môže poskytnúť informácie týkajúce sa incidentu partnerom, ktorí môžu prispieť k jeho analýze.

---

[8] Nariadenie Európskeho parlamentu a Rady (EÚ, Euratom) 2018/1046 z 18. júla 2018 o rozpočtových pravidlách, ktoré sa vzťahujú na všeobecný rozpočet Únie, o zmene nariadení (EÚ) č. 1296/2013, (EÚ) č. 1301/2013, (EÚ) č. 1303/2013, (EÚ) č. 1304/2013, (EÚ) č. 1309/2013, (EÚ) č. 1316/2013, (EÚ) č. 223/2014, (EÚ) č. 283/2014 a rozhodnutia č. 541/2014/EÚ a o zrušení nariadenia (EÚ, Euratom) č. 966/2012 (Ú. v. EÚ L 193, 30.7.2018, s. 1).

Kapitola V
SPOLUPRÁCA A OZNAMOVACIE POVINNOSTI

Článok 18
Zaobchádzanie s informáciami

1. CERT-EU a inštitúcie, orgány a agentúry Únie rešpektujú povinnosť služobného tajomstva v súlade s článkom 339 Zmluvy o fungovaní Európskej únie alebo rovnocennými uplatniteľnými rámcami.

2. V súvislosti so žiadosťami o prístup verejnosti k dokumentom v držbe CERT-EU sa uplatňujú ustanovenia nariadenia Európskeho parlamentu a Rady (ES) č. 1049/2001[9] vrátane povinnosti podľa daného nariadenia poradiť sa s inými inštitúciami, orgánmi a agentúrami Únie vždy, keď sa žiadosť týka ich dokumentov.

3. Na spracúvanie osobných údajov vykonané podľa tohto nariadenia sa vzťahuje nariadenie Európskeho parlamentu a Rady (EÚ) 2018/1725.

4. Zaobchádzanie s údajmi zo strany CERT-EU a inštitúcií, orgánov a agentúr Únie je v súlade s pravidlami stanovenými v [navrhovanom nariadení o informačnej bezpečnosti].

5. Ak dôjde k nadviazaniu kontaktu alebo k snahe o nadviazanie kontaktu s CERT-EU zo strany vnútroštátnych bezpečnostných a spravodajských služieb, bez zbytočného odkladu sa to oznámi riaditeľstvu Komisie pre bezpečnosť a predsedovi IICB.

Článok 19
Povinnosti v oblasti poskytovania informácií

1. S cieľom umožniť CERT-EU koordinovať riadenie zraniteľností a reakciu na incidenty môže CERT-EU požiadať inštitúcie, orgány a agentúry Únie, aby mu poskytli informácie zo svojich príslušných inventárov systémov IT, ktoré sú relevantné pre podporu zo strany CERT-EU. Dožiadaná inštitúcia, orgán alebo agentúra poskytne požadované informácie a všetky ich ďalšie aktualizácie bez zbytočného odkladu.

2. Inštitúcie, orgány a agentúry Únie na žiadosť CERT-EU a bez zbytočného odkladu poskytnú CERT-EU digitálne informácie vytvorené pomocou elektronických zariadení zapojených do príslušných incidentov. CERT-EU môže ďalej objasniť, ktoré druhy takýchto digitálnych informácií na účel situačnej informovanosti a reakcie na incidenty požaduje.

3. CERT-EU môže informácie o konkrétnom incidente, v rámci ktorých sa uvádza identita inštitúcie, orgánu alebo agentúry Únie dotknutej incidentom, poskytovať iba so súhlasom daného subjektu. CERT-EU môže informácie o konkrétnom incidente, v rámci ktorých sa uvádza identita cieľa kybernetickobezpečnostného incidentu, poskytovať iba so súhlasom subjektu dotknutého incidentom.

4. Povinnosti v oblasti poskytovania informácií sa nevzťahujú na utajované skutočnosti EÚ a na informácie, ktoré inštitúcia, orgán alebo agentúra Únie prijali od

[9] Nariadenie Európskeho parlamentu a Rady (ES) č. 1049/2001 z 30. mája 2001 o prístupe verejnosti k dokumentom Európskeho parlamentu, Rady a Komisie (Ú. v. ES L 145, 31.5.2001, s. 43).

bezpečnostnej alebo spravodajskej služby alebo orgánu presadzovania práva členského štátu pod výslovnou podmienkou, že sa neposkytnú CERT-EU.

Článok 20

Oznamovacie povinnosti

1. Všetky inštitúcie, orgány a agentúry Únie vykonajú prvotné oznámenie významných kybernetických hrozieb, významných zraniteľností a významných incidentov CERT-EU bez zbytočného odkladu a v každom prípade najneskôr 24 hodín potom, ako sa o nich dozvedia.

   V náležite odôvodnených prípadoch a po dohode s CERT-EU sa inštitúcia, orgán alebo agentúra Únie môže odchýliť od lehoty stanovenej v predchádzajúcom odseku.

2. Inštitúcie, orgány a agentúry Únie ďalej bez zbytočného odkladu oznámia CERT-EU primerané technické podrobnosti o kybernetických hrozbách, zraniteľnostiach a incidentoch, ktoré umožňujú odhaľovanie, reakciu na incidenty alebo prijímanie zmierňujúcich opatrení. Takéto oznámenie v prípade dostupnosti zahŕňa:

   a) relevantné ukazovatele kompromitácie;

   b) relevantné mechanizmy odhaľovania;

   c) potenciálny vplyv;

   d) relevantné zmierňujúce opatrenia.

3. CERT-EU predkladá agentúre ENISA mesačnú súhrnnú správu, ktorá zahŕňa anonymizované a súhrnné údaje o významných kybernetických hrozbách, významných zraniteľnostiach a významných incidentoch oznámených v súlade s odsekom 1.

4. IICB môže vydávať usmerňovacie dokumenty alebo odporúčania v súvislosti s postupmi a obsahom oznámenia. CERT-EU poskytuje primerané technické podrobnosti s cieľom umožniť inštitúciám, orgánom a agentúram Únie proaktívne odhaľovanie, reakciu na incidenty alebo prijímanie zmierňujúcich opatrení.

5. Oznamovacie povinnosti sa nevzťahujú na utajované skutočnosti EÚ a na informácie, ktoré inštitúcia, orgán alebo agentúra Únie prijala od bezpečnostnej alebo spravodajskej služby alebo orgánu presadzovania práva členského štátu pod výslovnou podmienkou, že sa neposkytnú CERT-EU.

Článok 21

Koordinácia reakcie na incidenty a spolupráca v súvislosti s významnými incidentmi

1. CERT-EU ako centrum na výmenu informácií a koordináciu reakcie na incidenty v oblasti kybernetickej bezpečnosti uľahčuje výmenu informácií o kybernetických hrozbách, zraniteľnostiach a incidentoch medzi:

   a) inštitúciami, orgánmi a agentúrami Únie;

   b) náprotivkami uvedenými v článkoch 16 a 17.

2. CERT-EU uľahčuje koordináciu reakcie inštitúcií, orgánov a agentúr Únie na incidenty vrátane:

   a) prispievania k sústavnej vonkajšej komunikácii;

   b) vzájomnej pomoci;

c) optimálneho využívania operačných zdrojov;

d) koordinácie s inými mechanizmami reakcie na krízu na úrovni Únie.

3. CERT-EU podporuje inštitúcie, orgány a agentúry Únie v súvislosti so situačnou informovanosťou o kybernetických hrozbách, zraniteľnostiach a incidentoch.

4. IICB vydáva usmernenie ku koordinácii reakcie na incidenty a k spolupráci v tejto oblasti v prípade významných incidentov. Ak vznikne podozrenie, že incident má trestnoprávnu povahu, CERT-EU poskytne poradenstvo k tomu, ako incident oznámiť orgánom presadzovania práva.

Článok 22
Významné útoky

1. CERT-EU koordinuje reakcie inštitúcií, orgánov a agentúr Únie na významné útoky. Vedie súpis odborných technických znalostí, ktoré by boli potrebné na účel reakcie na incidenty v prípade takýchto útokov.

2. Inštitúcie, orgány a agentúry Únie prispievajú k súpisu odborných technických znalostí tým, že každoročne poskytujú aktualizovaný zoznam odborníkov dostupných v rámci jednotlivých organizácií s podrobným uvedením ich konkrétnych technických zručností.

3. So súhlasom dotknutých inštitúcií, orgánov a agentúr Únie môže CERT-EU takisto vyzvať odborníkov zo zoznamu uvedeného v odseku 2, aby prispeli k reakcii na významný útok v členskom štáte v súlade s operačnými postupmi spoločnej kybernetickej jednotky.

Kapitola VI
ZÁVEREČNÉ USTANOVENIA

Článok 23
Počiatočné prerozdelenie rozpočtových prostriedkov

Komisia navrhne prerozdelenie zamestnancov a finančných zdrojov z príslušných inštitúcií, orgánov a agentúr Únie do rozpočtu Komisie. Prerozdelenie nadobudne účinnosť súčasne s prvým rozpočtom prijatým po nadobudnutí účinnosti tohto nariadenia.

Článok 24
Preskúmanie

1. IICB s pomocou CERT-EU pravidelne Komisii podáva správy o vykonávaní tohto nariadenia. IICB môže Komisii takisto odporučiť, aby navrhla zmeny tohto nariadenia.

2. Komisia podáva správu o vykonávaní tohto nariadenia Európskemu parlamentu a Rade najneskôr 48 mesiacov po nadobudnutí účinnosti tohto nariadenia a potom každé tri roky.

3. Komisia prehodnocuje fungovanie tohto nariadenia a podáva o tom správu Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov najskôr päť rokov po dátume nadobudnutia účinnosti.

Článok 25

Nadobudnutie účinnosti

Toto nariadenie nadobúda účinnosť dvadsiatym dňom po jeho uverejnení v *Úradnom vestníku Európskej únie*.

Toto nariadenie je záväzné v celom rozsahu a priamo uplatniteľné vo všetkých členských štátoch.

V Bruseli

Za Európsky parlament	*Za Radu*
predsedníčka	*predseda*

LEGISLATÍVNY FINANČNÝ VÝKAZ

1. RÁMEC NÁVRHU/INICIATÍVY

1.1. Názov návrhu/iniciatívy

1.2. Príslušné oblasti politiky

1.3. Návrh/iniciatíva sa týka:

1.4. Ciele

1.4.1. Všeobecné ciele

1.4.2. Špecifické ciele

1.4.3. Očakávané výsledky a vplyv

1.4.4. Ukazovatele výkonnosti

1.5. Dôvody návrhu/iniciatívy

1.5.1. Požiadavky, ktoré sa majú splniť v krátkodobom alebo dlhodobom horizonte vrátane podrobného harmonogramu prvotnej fázy vykonávania iniciatívy.

1.5.2. Prínos zapojenia Únie (môže byť výsledkom rôznych faktorov, napr. lepšej koordinácie, právnej istoty, väčšej účinnosti alebo komplementárnosti). Na účely tohto bodu je „prínos zapojenia Únie“ hodnota vyplývajúca zo zásahu Únie, ktorá dopĺňa hodnotu, ktorú by inak vytvorili len samotné členské štáty.

1.5.3. Poznatky získané z podobných skúseností v minulosti

1.5.4. Zlučiteľnosť s viacročným finančným rámcom a možná synergia s inými vhodnými nástrojmi

1.5.5. Posúdenie rôznych disponibilných možností financovania vrátane možnosti prerozdelenia

1.6. Trvanie a finančný vplyv návrhu/iniciatívy

1.7. Plánovaný spôsob riadenia

2. OPATRENIA V OBLASTI RIADENIA

2.1. Zásady monitorovania a predkladania správ

2.2. Systémy riadenia a kontroly

2.2.1. Opodstatnenie navrhovaných spôsobov riadenia, mechanizmov vykonávania financovania, spôsobov platby a stratégie kontroly

2.2.2. Informácie o zistených rizikách a systémoch vnútornej kontroly zavedených na ich zmierňovanie

2.2.3. Odhad a opodstatnenie nákladovej účinnosti kontrol (pomer medzi nákladmi na kontroly a hodnotou súvisiacich riadených finančných prostriedkov) a posúdenie očakávaných úrovní rizika chyby (pri platbe a uzavretí)

2.3. Opatrenia na predchádzanie podvodom a nezrovnalostiam

3. ODHADOVANÝ FINANČNÝ VPLYV NÁVRHU/INICIATÍVY

3.1. Príslušné okruhy viacročného finančného rámca a rozpočtové riadky výdavkov

3.2. Odhadovaný finančný vplyv návrhu na rozpočtové prostriedky

3.2.1. Zhrnutie odhadovaného vplyvu na operačné rozpočtové prostriedky

3.2.2. Odhadované výsledky financované z operačných rozpočtových prostriedkov

3.2.3. Zhrnutie odhadovaného vplyvu na administratívne rozpočtové prostriedky

3.2.4. Súlad s platným viacročným finančným rámcom

3.2.5. Príspevky od tretích strán

3.3. Odhadovaný vplyv na príjmy

LEGISLATÍVNY FINANČNÝ VÝKAZ

1. RÁMEC NÁVRHU/INICIATÍVY

1.1. Názov návrhu/iniciatívy

Návrh nariadenia Európskeho parlamentu a Rady, ktorým sa stanovujú opatrenia na zaistenie vysokej spoločnej úrovne kybernetickej bezpečnosti v inštitúciách, orgánoch, úradoch a agentúrach Únie

1.2. Príslušné oblasti politiky

Európska verejná správa

Návrh sa týka opatrení, ktorými sa zaistí vysoká spoločná úroveň kybernetickej bezpečnosti v inštitúciách, orgánoch a agentúrach Únie

1.3. Návrh/iniciatíva sa týka:

☑ **novej akcie**

☐ **novej akcie, ktorá nadväzuje na pilotný projekt/prípravnú akciu[10]**

☐ **predĺženia trvania existujúcej akcie**

☑ **zlúčenia jednej alebo viacerých akcií do ďalšej/novej akcie alebo presmerovania jednej alebo viacerých akcií na ďalšiu/novú akciu**

1.4. Ciele

1.4.1. Všeobecné ciele

– vytvoriť rámec na zaistenie vysokej spoločnej úrovne kybernetickej bezpečnosti v inštitúciách, orgánoch a agentúrach Únie,

– poskytnúť nový právny základ CERT-EU s cieľom posilniť jeho mandát a financovanie.

1.4.2. Špecifické ciele

1. stanoviť povinnosti inštitúcií, orgánov a agentúr Únie, pokiaľ ide o vytvorenie vnútorného rámca riadenia, správy a kontroly kybernetickobezpečnostných rizík;
2. stanoviť povinnosti inštitúcií, orgánov a agentúr Únie, pokiaľ ide o predkladanie správ o ich rámci riadenia, správy a kontroly kybernetickobezpečnostných rizík, ako aj o kybernetickobezpečnostných incidentoch;
3. stanoviť pravidlá organizácie a činnosti Centra kybernetickej bezpečnosti pre inštitúcie, orgány a agentúry Únie (CERT-EU), ako aj organizácie a činnosti Medziinštitucionálnej rady pre kybernetickú bezpečnosť (IICB);
4. prispieť k činnosti spoločnej kybernetickej jednotky.

1.4.3. Očakávané výsledky a vplyv

Uveďte, aký vplyv by mal mať návrh/iniciatíva na prijímateľov/cieľové skupiny.

[10] Podľa článku 58 ods. 2 písm. a) alebo b) nariadenia o rozpočtových pravidlách.

– vnútorné rámce riadenia, správy a kontroly kybernetickobezpečnostných rizík, základné kybernetickobezpečnostné pravidlá, pravidelné posúdenia vyspelosti a plány kybernetickej bezpečnosti v inštitúciách, orgánoch a agentúrach Únie, – zlepšenie odolnosti v oblasti kybernetickej bezpečnosti a kapacít na reakciu na incidenty v inštitúciách, orgánoch a agentúrach Únie, – modernizácia CERT-EU, – príspevok k činnosti spoločnej kybernetickej jednotky.

1.4.4. Ukazovatele výkonnosti

Uveďte ukazovatele na monitorovanie pokroku a dosiahnutých výsledkov.

– zavedené rámce a základné pravidlá, pravidelné posúdenia vyspelosti a plány kybernetickej bezpečnosti vykonané v inštitúciách, orgánoch a agentúrach Únie, – lepšie riešenie incidentov, – zvýšená informovanosť o kybernetickobezpečnostných rizikách na úrovni vrcholového manažmentu inštitúcií, orgánov a agentúr Únie, – stanovenie úrovne výdavkov na bezpečnosť IKT ako percentuálneho podielu celkových výdavkov na IKT, – silné vedenie IICB a CERT-EU, – posilnená výmena informácií medzi inštitúciami, orgánmi a agentúrami Únie a relevantným orgánmi a zainteresovanými stranami v EÚ, – rozšírená spolupráca v oblasti kybernetickej bezpečnosti s relevantnými orgánmi a so zainteresovanými stranami v EÚ prostredníctvom CERT-EU a agentúry ENISA.

1.5. Dôvody návrhu/iniciatívy

1.5.1. Požiadavky, ktoré sa majú splniť v krátkodobom alebo dlhodobom horizonte vrátane podrobného harmonogramu prvotnej fázy vykonávania iniciatívy.

Cieľom návrhu je zvýšiť úroveň kybernetickej odolnosti inštitúcií, orgánov a agentúr Únie, zmenšiť rozdiely v odolnosti medzi týmito subjektmi a zlepšiť úroveň spoločnej situačnej informovanosti a spoločnej schopnosti pripraviť sa a reagovať. Návrh je v plnej miere zosúladený a koherentný s inými súvisiacimi iniciatívami, najmä s návrhom smernice o opatreniach na zaistenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii a o zrušení smernice (EÚ) 2016/1148 [návrh smernice NIS 2]. Návrh je kľúčovou súčasťou Stratégie EÚ pre bezpečnostnú úniu a stratégie kybernetickej bezpečnosti EÚ v digitálnej dekáde. Európska komisia má naradenie navrhnúť v októbri 2021, pričom prijatie nariadenia Európskym parlamentom a Radou sa očakáva v roku 2022 a ustanovenia budú uplatniteľné od nadobudnutia účinnosti nariadenia. Predpokladá sa, že finančný vplyv a vplyv v oblasti ľudských zdrojov uvedený v tomto legislatívnom finančnom výkaze sa začne prejavovať v roku 2023. Prípravné obdobie sa začalo už v roku 2021, ale prípravné činnosti v rokoch 2021 a 2022 nie sú zahrnuté do finančného vplyvu návrhu.

1.5.2. Prínos zapojenia Únie (môže byť výsledkom rôznych faktorov, napr. lepšej koordinácie, právnej istoty, väčšej účinnosti alebo komplementárnosti). Na účely tohto bodu je „prínos zapojenia Únie“ hodnota vyplývajúca zo zásahu Únie, ktorá dopĺňa hodnotu, ktorú by inak vytvorili len samotné členské štáty.

Dôvody na akciu na európskej úrovni (*ex ante*)

V rokoch 2019 až 2021 sa výrazne zvýšil počet významných incidentov ovplyvňujúcich inštitúcie, orgány a agentúry Únie, ktorých pôvodcami boli aktéri označovaní ako pokročilé pretrvávajúce hrozby (advanced persistent threat). V prvej polovici roka 2021 došlo k rovnakému počtu významných incidentov ako počas celého roka 2020. To sa prejavuje aj v počte forenzných obrázkov (momentkových snímok obsahu dotknutých systémov alebo zariadení), ktoré CERT-EU analyzovalo v roku 2020, ktorý sa v porovnaní s rokom 2019 strojnásobil, zatiaľ čo počet významných incidentov od roku 2018 vzrástol viac než desaťnásobne.

Úroveň vyspelosti v oblasti kybernetickej bezpečnosti sa medzi jednotlivými subjektmi výrazne líši[11]. Týmto nariadením sa zabezpečuje, že všetky inštitúcie, orgány a agentúry Únie budú vykonávať základné bezpečnostné opatrenia a navzájom spolupracovať, ako aj jeho cieľ, ktorým je otvorené a efektívne fungovanie európskej správy.

Systémy, ktoré sa majú zachovať, patria do autonómie inštitúcií, orgánov a agentúr Únie, ktoré ich prevádzkujú. Navrhované akcie by nebolo možné dosiahnuť na úrovni členských štátov.

1.5.3. Poznatky získané z podobných skúseností v minulosti

Smernica NIS je prvým horizontálnym nástrojom vnútorného trhu zameraným na zlepšenie odolnosti sietí a systémov v Únii proti kybernetickobezpečnostným rizikám. Od nadobudnutia účinnosti v roku 2016 už významne prispela k zvýšeniu spoločnej úrovne kybernetickej bezpečnosti členských štátov. V návrhu smernice NIS 2 sa vyvíjajú snahy o ďalšie zlepšenie týchto opatrení.

Účelom nariadenia je poskytnúť podobné opatrenia pre inštitúcie, orgány a agentúry Únie.

1.5.4. Zlučiteľnosť s viacročným finančným rámcom a možná synergia s inými vhodnými nástrojmi

Návrh je v súlade s viacročným finančným rámcom a je kľúčovou súčasťou Stratégie EÚ pre bezpečnostnú úniu, ako aj stratégie kybernetickej bezpečnosti EÚ v digitálnej dekáde.

V návrhu sa stanovuje uplatňovanie opatrení na zaistenie vysokej spoločnej úrovne kybernetickej bezpečnosti v inštitúciách, orgánoch a agentúrach Únie Návrh je v súlade s návrhom smernice o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii a o zrušení smernice (EÚ) 2016/1148 [návrh smernice NIS 2].

[11] Odkaz: [osobitná správa EDA o kybernetickej bezpečnosti v inštitúciách, orgánoch a agentúrach Únie].

1.5.5. Posúdenie rôznych disponibilných možností financovania vrátane možnosti prerozdelenia

Riadenie úloh zo strany CERT-EU si vyžaduje osobitné profily a doplnkové pracovné zaťaženie, ktoré nemožno zvládnuť bez zvýšenia ľudských a finančných zdrojov.

1.6. Trvanie a finančný vplyv návrhu/iniciatívy

☐ **obmedzené trvanie**

– ☐ v platnosti od [DD/MM]RRRR do [DD/MM]RRRR

– ☐ Finančný vplyv na viazané rozpočtové prostriedky od RRRR do RRRR a na platobné rozpočtové prostriedky od RRRR do RRRR.

☑ **neobmedzené trvanie**

– Finančný vplyv by sa mal začať prejavovať pri prvom rozpočte prijatom po nadobudnutí účinnosti nariadenia. V prvom roku, ktorý sa považuje za prechodný rok, sa vykoná prerozdelenie zdrojov z inštitúcií a hlavných orgánov Únie na Komisiu. Toto a ďalšie (pre)rozdelenia zdrojov sa uskutočnia v rámci ročných rozpočtov. Ak sa nariadenie prijme v roku 2022, rozpočtový rok 2023 bude prechodným obdobím a v roku 2024 bude pôsobiť v plnom rozsahu.

1.7. Plánovaný spôsob riadenia[12]

☑ **Priame riadenie** prostredníctvom Komisie a jednotlivých inštitúcií, orgánov a agentúr Únie

– ☑ prostredníctvom jej útvarov vrátane zamestnancov v delegáciách Únie

– ☐ prostredníctvom výkonných agentúr

☐ **Zdieľané riadenie** s členskými štátmi

☐ **Nepriame riadenie**, pri ktorom sa plnením rozpočtu poveria:

– ☐ tretie krajiny alebo subjekty, ktoré tieto krajiny určili,

– ☐ medzinárodné organizácie a ich agentúry (uveďte),

– ☐ Európska investičná banka (EIB) a Európsky investičný fond,

– ☐ subjekty uvedené v článkoch 70 a 71 nariadenia o rozpočtových pravidlách,

– ☐ verejnoprávne subjekty,

– ☐ súkromnoprávne subjekty poverené vykonávaním verejnej služby, pokiaľ tieto subjekty poskytujú dostatočné finančné záruky,

– ☐ súkromnoprávne subjekty spravované právom členského štátu, ktoré sú poverené vykonávaním verejno-súkromného partnerstva a ktoré poskytujú primerané finančné záruky,

– ☐ osoby poverené vykonávaním osobitných činností v oblasti SZBP podľa hlavy V Zmluvy o Európskej únii a určené v príslušnom základnom akte.

– *V prípade viacerých spôsobov riadenia uveďte v oddiele „Poznámky“ presnejšie vysvetlenie.*

Poznámky:

V prípade uplatňovania administratívnych a finančných postupov CERT-EU koná pod vedením Komisie.

Dodatočné zdroje vyplývajúce z návrhu nariadenia:

[12] Vysvetlenie spôsobov riadenia a odkazy na nariadenie o rozpočtových pravidlách sú k dispozícii na webovej stránke BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx.

Vykonávanie článkov 12 a 13 návrhu nariadenia vedie k rozsiahlejšiemu katalógu služieb s ďalšími základnými službami. Pri pôsobení v plnom rozsahu budú potrebné tieto dodatočné zdroje (do konca VFR na konci roka 2027): 21 ekvivalentov plného pracovného času a 14,05 milióna EUR.

Rozčlenenie dodatočných zdrojov v rámci rozpočtu podľa jednotlivých úloh je takéto:

(a) na plnenie úloh inštitúcií, orgánov a agentúr Únie podrobne uvedených v článku 12 ods. 2 písm. a), b), c) a e): 13,75 ekvivalentu plného pracovného času a 11,275 milióna EUR;

(b) na plnenie úloh podrobne uvedených v článku 12 ods. 3 (prispievanie k činnosti spoločnej kybernetickej jednotky): 2 ekvivalenty plného pracovného času a 381 000 EUR;

(c) na plnenie úloh podrobne uvedených v článku 12 ods. 4 (štruktúrovaná spolupráca s agentúrou ENISA): 0,25 ekvivalentu plného pracovného času a 236 000 EUR;

(d) na plnenie úloh podrobne uvedených v článku 12 ods. 6 (cvičenia v oblasti kybernetickej bezpečnosti): 0,25 ekvivalentu plného pracovného času a 79 000 EUR;

(e) na plnenie úloh podrobne uvedených v článku 12 ods. 2 písm. d) a článku 13 (analýza a predkladanie správ o vykonávaní nariadenia, vypracovanie usmerňovacích dokumentov, odporúčaní a výziev na činnosť): 3,75 ekvivalentu plného pracovného času a 2,079 milióna EUR;

(f) na plnenie úloh na podporu sekretariátu Medziinštitucionálnej rady pre kybernetickú bezpečnosť (IICB): 1 ekvivalent plného pracovného času.

Prehľad aktuálnych zdrojov a prechodu na plné pôsobenie:

v septembri 2021 CERT-EU fungoval s týmito zdrojmi:

– stále pracovné miesta a miesta vyslaných pracovníkov: 14 ekvivalentov plného pracovného času,

– zmluvní zamestnanci financovaní v rámci dohôd o úrovni poskytovaných služieb: 24 ekvivalentov plného pracovného času,

– celkovo 38 ekvivalentov plného pracovného času.

Rozpočet CERT-EU na rok 2020 predstavoval: 250 000 EUR v rámci rozpočtu Komisie, 3,5 milióna EUR prostredníctvom pripísaných príjmov v rámci dohôd o úrovni poskytovaných služieb. Spolu: 3,75 milióna EUR. Táto suma predstavovala celý rozpočet CERT-EU, z ktorého sa financovala odborná príprava, hardvér, softvér, služobné cesty, podpora, zmluvní zamestnanci a konferencie.

Plánuje sa, že po nadobudnutí účinnosti nariadenia budú budúce zdroje CERT-EU takéto:

– stále pracovné miesta: 34 ekvivalentov plného pracovného času,

– zmluvní zamestnanci: 15 ekvivalentov plného pracovného času,

– celkovo 49 ekvivalentov plného pracovného času, čo predstavuje čistý nárast o 11 ekvivalentov plného pracovného času.

Zmenou pomeru medzi stálymi pracovnými miestami a zmluvnými zamestnancami sa rieši súvisiaci vážny problém s prijímaním a udržaním samostatných odborníkov v oblasti kybernetickej bezpečnosti spôsobený ich nedostatkom na trhu práce.

Okrem toho bude potrebný zmluvný zamestnanec zodpovedajúci jednému ekvivalentu plného pracovného času v rámci Generálneho riaditeľstva Komisie pre informatiku na podporu IICB (Medziinštitucionálnej rady pre kybernetickú bezpečnosť).

Celkovo bude teda na vykonanie nariadenia potrebných dodatočných 21 ekvivalentov plného pracovného času (20 ekvivalentov plného pracovného času pre CERT-EU a jeden pre Generálne riaditeľstvo Komisie pre informatiku). To sa bude kompenzovať súčasným znížením počtu zmluvných zamestnancov v CERT-EU zodpovedajúcim deviatim ekvivalentom plného pracovného času, ktorí sa predtým financovali z pripísaných príjmov z dohôd o úrovni poskytovaných služieb.

Rozpočet CERT-EU na iné ako ľudské zdroje na rok 2024 po prechodnom období sa bude vzťahovať na úlohy uvedené pod písmenami a) až e) a plánuje sa, že sa bude financovať takto:

– 8,921 milióna EUR ročne z inštitúcií Únie financovaných v rámci okruhov rozpočtu Únie 7,

– 2,459 milióna EUR z inštitúcií, orgánov a agentúr Únie financovaných v rámci okruhov rozpočtu Únie 1 až 6,

– 2,670 milióna EUR z inštitúcií, orgánov a agentúr Únie, ktoré sa financujú samy,

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

Úlohy uvedené v článku 12 ods. 5 nie sú opísané v jeho katalógu služieb, pričom ide o spoplatnené služby. Sú doplnkové, predstavujú pomerne nízke sumy, sú zväčša dočasné a náklady na tieto služby uhradia príjemcovia služieb prostredníctvom dohôd o úrovni poskytovaných služieb alebo písomných dohôd.

Pokiaľ ide o príspevky na zamestnancov CERT-EU: inštitúcie a hlavné orgány Únie prispievajú spravodlivým podielom, ktorý je v pomere k príslušnému podielu stálych pracovných miest AD organizácie. Malo by sa zistiť, či aj ECB a EIB môžu prispieť spravodlivým podielom prostredníctvom vyslania stálych zamestnancov.

2. OPATRENIA V OBLASTI RIADENIA

2.1. Zásady monitorovania a predkladania správ

Uveďte frekvenciu a podmienky, ktoré sa vzťahujú na tieto opatrenia.

Komisia s pomocou IICB a CERT-EU pravidelne preskúma fungovanie nariadenia a predloží správy Európskemu parlamentu a Rade, prvýkrát najneskôr 48 mesiacov po nadobudnutí účinnosti tohto nariadenia a potom každé tri roky.

Zdroje údajov použité pri preskúmaní by zväčša pochádzali od IICB a CERT-EU. V prípade potreby by sa okrem toho mohli použiť osobitné nástroje na zhromažďovanie údajov, napr. prieskumy v inštitúciách, orgánoch a agentúrach Únie, v agentúre ENISA alebo v rámci siete jednotiek CSIRT.

2.2. Systémy riadenia a kontroly

2.2.1. Opodstatnenie navrhovaných spôsobov riadenia, mechanizmov vykonávania financovania, spôsobov platby a stratégie kontroly

Opatrenia vyplývajúce z nariadenia sa budú riadiť v rámci jednotlivých inštitúcií, orgánov a agentúr Únie v súlade s ich príslušnými uplatniteľnými pravidlami a právnymi predpismi.

Administratívne a finančné riadenie činností CERT-EU je včlenené v správe Komisie a využívajú sa v ňom jej uplatniteľné mechanizmy riadenia a vykonávania, spôsoby platby a kontroly.

Vnútorný audítor Komisie má vo vzťahu k CERT-EU rovnaké právomoci ako vo vzťahu k útvarom Komisie.

2.2.2. Informácie o zistených rizikách a systémoch vnútornej kontroly zavedených na ich zmierňovanie

Veľmi nízke riziko, keďže CERT-EU je už ako pracovná skupina Komisie administratívne pričlenené ku Generálnemu riaditeľstvu pre informatiku a IICB je vytvorená podľa modelu aktuálnej riadiacej rady CERT-EU. Ekosystém finančného riadenia a vnútornej kontroly je teda už zavedený.

2.2.3. Odhad a opodstatnenie nákladovej účinnosti kontrol (pomer medzi nákladmi na kontroly a hodnotou súvisiacich riadených finančných prostriedkov) a posúdenie očakávaných úrovní rizika chyby (pri platbe a uzavretí)

Postupy obstarávania, finančného riadenia a kontroly sú už zavedené a dobre odskúšané. Nákladová účinnosť kontrol a úrovne rizika chyby zodpovedajú tým v jednotlivých inštitúciách, orgánoch alebo agentúrach Únie a tým v Komisii v prípade činností CERT-EU.

2.3. Opatrenia na predchádzanie podvodom a nezrovnalostiam

Uveďte existujúce alebo plánované preventívne a ochranné opatrenia, napr. zo stratégie na boj proti podvodom.

Na činnosti CERT-EU sa uplatňujú systémy finančného riadenia a vnútornej kontroly Komisie.

Na účely boja proti podvodom, korupcii a iným nezákonným činnostiam sa bez obmedzenia uplatňujú ustanovenia nariadenia Európskeho parlamentu a Rady (EÚ,

Euratom) č. 883/2013 z 11. septembra 2013 o vyšetrovaniach vykonávaných Európskym úradom pre boj proti podvodom (OLAF).

3. ODHADOVANÝ FINANČNÝ VPLYV NÁVRHU/INICIATÍVY

3.1. Príslušné okruhy viacročného finančného rámca a rozpočtové riadky výdavkov

- Existujúce rozpočtové riadky

V poradí, v akom za sebou nasledujú okruhy viacročného finančného rámca a rozpočtové riadky.

Okruh viacročného finančného rámca	Rozpočtový riadok	Druh výdavkov	Príspevky			
	Číslo	DRP/NRP [13]	krajín EZVO[14]	kandidátskych krajín[15]	tretích krajín	v zmysle článku 21 ods. 2 písm. b) nariadenia o rozpočtových pravidlách
1 až 6	Rozpočtové riadky, ktoré sa vzťahujú na príspevky Únie na decentralizované agentúry a orgány	DRP	NIE	NIE	NIE	NIE
7	Rozpočtové riadky, ktoré sa vzťahujú na odmenu zamestnancov, výdavky v oblasti IT a iné administratívne výdavky v iných oddieloch rozpočtu EÚ	NRP	NIE	NIE	NIE	NIE

- Požadované nové rozpočtové riadky

V poradí, v akom za sebou nasledujú okruhy viacročného finančného rámca a rozpočtové riadky.

Okruh viacročného finančného rámca	Rozpočtový riadok	Druh výdavkov	Príspevky			
	Číslo	DRP/NRP	krajín EZVO	kandidátskych krajín	tretích krajín	v zmysle článku 21 ods. 2 písm. b) nariadenia o rozpočtových pravidlách
	Žiadne		ÁNO/NIE	ÁNO/NIE	ÁNO/NIE	ÁNO/NIE

[13] DRP = diferencované rozpočtové prostriedky/NRP = nediferencované rozpočtové prostriedky.
[14] EZVO: Európske združenie voľného obchodu.
[15] Kandidátske krajiny a prípadne potenciálni kandidáti zo západného Balkánu.

3.2. Odhadovaný finančný vplyv návrhu na rozpočtové prostriedky

3.2.1. Zhrnutie odhadovaného vplyvu na operačné rozpočtové prostriedky

– ☐ Návrh/iniciatíva si nevyžaduje použitie operačných rozpočtových prostriedkov.

– ☑ Návrh/iniciatíva si vyžaduje použitie týchto operačných rozpočtových prostriedkov:

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

Okruh viacročného finančného rámca	1 až 6	Okruhy, ktoré sa vzťahujú na príspevky na decentralizované agentúry a orgány

GR: viaceré			Rok **2023**	Rok **2024**	Rok **2025**	Rok **2026**	Rok **2027**	**SPOLU**
○ Operačné rozpočtové prostriedky								
Rozpočtové riadky, ktoré sa vzťahujú na príspevky Únie na decentralizované agentúry (xx 10 xx xx)[16]	Záväzky	(1a)	2,459	2,459	2,459	2,459	2,459	12,293
	Platby	(2a)	2,459	2,459	2,459	2,459	2,459	12,293
Administratívne rozpočtové prostriedky financované z finančného krytia na vykonávanie osobitných programov[17]								
Rozpočtový riadok		(3)						
Rozpočtové prostriedky pre GR: viaceré	Záväzky	= 1a + 1b + 3	2,459	2,459	2,459	2,459	2,459	12,293
	Platby	= 2a + 2b + 3	2,459	2,459	2,459	2,459	2,459	12,293

16 Podľa oficiálnej rozpočtovej nomenklatúry.

17 Technická a/alebo administratívna pomoc a výdavky na podporu vykonávania programov a/alebo akcií EÚ (pôvodné rozpočtové riadky „BA“), nepriamy výskum, priamy výskum.

○ Operačné rozpočtové prostriedky SPOLU	Záväzky	(4)	2,459	2,459	2,459	2,459	2,459	12,293
	Platby	(5)	2,459	2,459	2,459	2,459	2,459	12,293
○ Administratívne rozpočtové prostriedky financované z finančného krytia na vykonávanie osobitných programov SPOLU		(6)						
Rozpočtové prostriedky OKRUHOV 1 až 6 viacročného finančného rámca **SPOLU**	Záväzky	= 4 + 6	2,459	2,459	2,459	2,459	2,459	12,293
	Platby	= 5 + 6	2,459	2,459	2,459	2,459	2,459	12,293

Ak má návrh/iniciatíva vplyv na viaceré operačné okruhy, zopakujte oddiel uvedený vyššie:

○ Operačné rozpočtové prostriedky SPOLU (všetky operačné okruhy)	Záväzky	(4)	2,459	2,459	2,459	2,459	2,459	12,293
	Platby	(5)	2,459	2,459	2,459	2,459	2,459	12,293
Administratívne rozpočtové prostriedky financované z finančného krytia na vykonávanie osobitných programov SPOLU (všetky operačné okruhy)		(6)						
Rozpočtové prostriedky OKRUHOV 1 až 6 viacročného finančného rámca **SPOLU** (referenčná suma)	Záväzky	= 4 + 6	2,459	2,459	2,459	2,459	2,459	12,293
	Platby	= 5 + 6	2,459	2,459	2,459	2,459	2,459	12,293

Okruh viacročného finančného rámca	**7**	„Administratívne výdavky“

Tento oddiel treba vyplniť s použitím rozpočtových údajov administratívnej povahy, ktoré sa najprv uvedú v prílohe k legislatívnemu finančnému výkazu (príloha V k interným pravidlám), ktorá sa na účely medziútvarovej konzultácie nahrá do aplikácie DECIDE.

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

	Rok	Rok	Rok	Rok	**Rok**	**SPOLU**

		2023	2024	2025	2026	2027	
GR: DIGIT (CERT-EU)							
○ Ľudské zdroje		1,184	2,126	2,754	3,225	3,225	12,514
○ Ostatné administratívne výdavky		7,938	8,921	8,921	8,921	8,921	43,622
GR DIGIT (CERT-EU) SPOLU	Rozpočtové prostriedky	9,122	11,047	11,675	12,146	12,146	56,136

Rozpočtové prostriedky OKRUHU 7 viacročného finančného rámca **SPOLU**	(Záväzky spolu = Platby spolu)	9,122	11,047	11,675	12,146	12,146	**56,136**

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

		Rok 2023	Rok 2024	Rok 2025	Rok 2026	Rok 2027	**SPOLU**
Rozpočtové prostriedky OKRUHOV 1 až 7 viacročného finančného rámca **SPOLU** (*)	Záväzky	11,581	13,506	14,134	14,605	14,605	68,429
	Platby	11,581	13,506	14,134	14,605	14,605	68,429

(*) Odhaduje sa, že príspevky inštitúcií, orgánov a agentúr Únie, ktoré sa financujú samy, budú predstavovať 2,670 milióna EUR ročne (celkovo počas piatich rokov 13,350 milióna EUR). Príspevky budú predstavovať pripísané príjmy pre CERT-EU. Uvedené tabuľky zahŕňajú len odhadovaný celkový vplyv na rozpočet Únie a nezahŕňajú tieto príspevky.

3.2.2. Odhadované výsledky financované z operačných rozpočtových prostriedkov

viazané rozpočtové prostriedky v mil. EUR (zaokrúhlené na 3 desatinné miesta)

Uveďte ciele a výstupy			Rok **N**	Rok **N + 1**	Rok **N + 2**	Rok **N + 3**	Uveďte všetky roky, počas ktorých vplyv trvá (pozri bod 1.6)	**SPOLU**
	VÝSTUPY							

⇩	Druh[18]	Priemerné náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet spolu	Náklady spolu
ŠPECIFICKÝ CIEĽ č. 1[19]…																		
– Výstup																		
– Výstup																		
– Výstup																		
Špecifický cieľ č. 1 medzisúčet																		
ŠPECIFICKÝ CIEĽ č. 2…																		
– Výstup																		
Špecifický cieľ č. 2 medzisúčet																		
SPOLU																		

[18] Výstupy sú produkty, ktoré sa majú dodať, a služby, ktoré sa majú poskytnúť (napr.: počet financovaných výmen študentov, vybudované cesty v km atď.).

[19] Ako je uvedené v bode 1.4.2. „Špecifické ciele...“.

3.2.3. Zhrnutie odhadovaného vplyvu na administratívne rozpočtové prostriedky

– ☐ Návrh/iniciatíva si nevyžaduje použitie administratívnych rozpočtových prostriedkov

– ☑ Návrh/iniciatíva si vyžaduje použitie týchto administratívnych rozpočtových prostriedkov:

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

	Rok 2023	Rok 2024	Rok 2025	Rok 2026	Rok 2027	**SPOLU**
OKRUH 7 viacročného finančného rámca						
Ľudské zdroje						
Stáli zamestnanci (triedy AD)	1,099	2,041	2,669	3,14	3,14	12,089
Zmluvní zamestnanci	0,085	0,085	0,085	0,085	0,085	0,425
Ostatné administratívne výdavky	7,938	8,921	8,921	8,921	8,921	43,622
Medzisúčet OKRUHU 7 viacročného finančného rámca	9,122	11,047	11,675	12,146	12,146	56,136

Mimo OKRUHU 7[20] viacročného finančného rámca						
Ľudské zdroje						
Ostatné administratívne výdavky						
Medzisúčet mimo OKRUHU 7 viacročného finančného rámca						

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

Rozpočtové prostriedky potrebné na ľudské zdroje a na ostatné administratívne výdavky budú pokryté rozpočtovými prostriedkami GR, ktoré už boli pridelené na riadenie akcie a/alebo boli prerozdelené v rámci GR, a v prípade potreby budú doplnené zdrojmi, ktoré sa môžu prideliť riadiacemu GR v rámci ročného postupu prideľovania zdrojov a v závislosti od rozpočtových obmedzení.

[20] Technická a/alebo administratívna pomoc a výdavky na podporu vykonávania programov a/alebo akcií EÚ (pôvodné rozpočtové riadky „BA“), nepriamy výskum, priamy výskum.

3.2.3.1. Odhadované potreby ľudských zdrojov

– ☐ Návrh/iniciatíva si nevyžaduje použitie ľudských zdrojov.

– ☑ Návrh/iniciatíva si vyžaduje použitie týchto ľudských zdrojov:

odhady sa vyjadrujú v jednotkách ekvivalentu plného pracovného času

	Rok 2023	Rok 2024	Rok 2025	Rok 2026	Rok 2027		
O Plán pracovných miest (úradníci a dočasní zamestnanci)							
20 01 02 01 (ústredie a zastúpenia Komisie)	7	13	17	20	20		
20 01 02 03 (delegácie)							
01 01 01 01 (nepriamy výskum)							
01 01 01 11 (priamy výskum)							
Iné rozpočtové riadky (uveďte)							
O Externí zamestnanci (ekvivalent plného pracovného času: FTE)[21]							
20 02 01 (ZZ, VNE, DAZ z celkového finančného krytia)	1	1	1	1	1		
20 02 03 (ZZ, MZ, VNE, DAZ, PED v delegáciách)							
XX 01 xx **yy zz** [22] – ústredie							
XX 01 xx **yy zz** [22] – delegácie							
01 01 01 02 (ZZ, DAZ, VNE – nepriamy výskum)							
01 01 01 12 (ZZ, DAZ, VNE – priamy výskum)							
Iné rozpočtové riadky (uveďte)							
SPOLU	**8**	**14**	**18**	**21**	**21**		

XX predstavuje príslušnú oblasť politiky alebo rozpočtovú hlavu.

Potreby ľudských zdrojov budú pokryté úradníkmi GR, ktorí už boli pridelení na riadenie akcie a/alebo boli interne prerozdelení v rámci GR, a v prípade potreby budú doplnené zdrojmi, ktoré sa môžu prideliť riadiacemu GR v rámci ročného postupu prideľovania zdrojov a v závislosti od rozpočtových obmedzení.

Opis úloh, ktoré sa majú vykonať:

Úradníci a dočasní zamestnanci	Úradníci budú vykonávať úlohy a činnosti CERT-EU v súlade s nariadením, najmä s kapitolami IV a V.
Externí zamestnanci	Zmluvný zamestnanec bude poskytovať pomoc pri plnení funkcií sekretariátu Medziinštitucionálnej rady pre kybernetickú bezpečnosť.

[21] ZZ = zmluvný zamestnanec; MZ = miestny zamestnanec; VNE = vyslaný národný expert; DAZ = dočasný agentúrny zamestnanec; PED = pomocný expert v delegácii.

[22] Čiastkový strop pre externých zamestnancov financovaných z operačných rozpočtových prostriedkov (pôvodné rozpočtové riadky „BA“).

3.2.4. Súlad s platným viacročným finančným rámcom

Návrh/iniciatíva:

– ☑ môže byť v plnej miere financovaná prerozdelením v rámci príslušného okruhu viacročného finančného rámca (VFR).

Vysvetlite požadovanú zmenu v plánovaní a uveďte príslušné rozpočtové riadky a zodpovedajúce sumy. V prípade väčšieho preprogramovania poskytnite tabuľku vo formáte Excel.

– ☐ si vyžaduje použitie nepridelenej rezervy v rámci príslušného okruhu VFR a/alebo použitie osobitných nástrojov vymedzených v nariadení o VFR.

Vysvetlite potrebu a uveďte príslušné okruhy, rozpočtové riadky, zodpovedajúce sumy a nástroje, ktorých použitie sa navrhuje.

– ☐ si vyžaduje revíziu VFR.

Vysvetlite potrebu a uveďte príslušné okruhy, rozpočtové riadky a zodpovedajúce sumy.

3.2.5. Príspevky od tretích strán

Návrh/iniciatíva:

– ☑ nezahŕňa spolufinancovanie tretími stranami[23]

– ☐ zahŕňa spolufinancovanie tretími stranami, ako je odhadnuté v nasledujúcej tabuľke:

rozpočtové prostriedky v mil. EUR (zaokrúhlené na 3 desatinné miesta)

	Rok **N**[24]	Rok **N + 1**	Rok **N + 2**	Rok **N + 3**	Uveďte všetky roky, počas ktorých vplyv trvá (pozri bod 1.6)			Spolu
Uveďte spolufinancujúci subjekt								
Prostriedky zo spolufinancovania SPOLU								

[23] Pripísané príjmy vyplývajúce z občasného poskytovania služieb organizáciám, ktoré nie sú zložkami, ako sa stanovuje v článku 12 ods. 5 písm. c), neboli predmetom odhadu, pretože by mali byť nepatrné.

[24] Rok N je rokom, v ktorom sa návrh/iniciatíva začína vykonávať. Nahraďte „N“ očakávaným prvým rokom vykonávania (napríklad: 2021). To isté urobte aj pri nasledujúcich rokoch.

3.3. Odhadovaný vplyv na príjmy

– ☑ Návrh/iniciatíva nemá finančný vplyv na príjmy.

– ☐ Návrh/iniciatíva má tento finančný vplyv na príjmy:

– ☐ vplyv na vlastné zdroje

– ☐ vplyv na iné príjmy

– uveďte, či sú príjmy pripísané rozpočtovým riadkom výdavkov ☐

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

Rozpočtový riadok príjmov:	Rozpočtové prostriedky k dispozícii v bežnom rozpočtovom roku	Vplyv návrhu/iniciatívy[25]						
		Rok **N**	Rok **N + 1**	Rok **N + 2**	Rok **N + 3**	Uveďte všetky roky, počas ktorých vplyv trvá (pozri bod 1.6)		
Článok …….								

V prípade pripísaných príjmov uveďte príslušné rozpočtové riadky výdavkov.

Ďalšie poznámky (napr. spôsob/vzorec použitý na výpočet vplyvu na príjmy alebo akékoľvek ďalšie informácie).

[25] Pokiaľ ide o tradičné vlastné zdroje (clá, odvody z produkcie cukru), uvedené sumy musia predstavovať čisté sumy, t. j. hrubé sumy po odčítaní 20 % na náklady na výber.