Vijeće
Europske unije

Bruxelles, 22. ožujka 2022.
(OR. en)

7474/22

Međuinstitucijski predmet:
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

PRIJEDLOG

Od:	Glavna tajnica Europske komisije, potpisala direktorica Martine DEPREZ
Datum primitka:	22. ožujka 2022.
Za:	Jeppe TRANHOLM-MIKKELSEN, glavni tajnik Vijeća Europske unije
Br. dok. Kom.:	COM(2022) 122 final
Predmet:	Prijedlog UREDBE EUROPSKOG PARLAMENTA I VIJEĆA o mjerama za visoku zajedničku razinu kibersigurnosti u institucijama, tijelima, uredima i agencijama Unije

Za delegacije se u prilogu nalazi dokument COM(2022) 122 final.

Priloženo: COM(2022) 122 final

EUROPSKA
KOMISIJA

Bruxelles, 22.3.2022.
COM(2022) 122 final

2022/0085 (COD)

Prijedlog

UREDBE EUROPSKOG PARLAMENTA I VIJEĆA

o mjerama za visoku zajedničku razinu kibersigurnosti u institucijama, tijelima, uredima i agencijama Unije

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

OBRAZLOŽENJE

1. KONTEKST PRIJEDLOGA

• Razlozi i ciljevi prijedloga

Ovim prijedlogom uspostavlja se okvir za zajednička pravila i mjere za kibersigurnost u institucijama, tijelima i agencijama Unije. Cilj mu je dodatno poboljšati otpornost svih subjekata i njihove kapacitete za odgovor na incidente. U skladu je s prioritetima Komisije da Europu pripremi za digitalno doba i da izgradi gospodarstvo koje je u interesu građana i spremno za budućnost. Osim toga, sigurna i otporna javna uprava okosnica je digitalne transformacije društva u cjelini.

Ovaj se prijedlog temelji na Strategiji EU-a za sigurnosnu uniju (COM(2020) 605 final) i Strategiji EU-a za kibersigurnost za digitalno desetljeće (JOIN(2020) 18 final).

Prijedlogom se modernizira postojeći pravni okvir za CERT-EU te se uzimaju u obzir izmijenjena i rastuća digitalizacija institucija, tijela i agencija proteklih godina, kao i sve veće kiberprijetnje. Obje pojave dodatno su se intenzivirale od početka krize uzrokovane bolešću COVID-19, dok se broj incidenata i dalje povećava, a sve sofisticiraniji napadi dolaze iz raznih izvora.

U prijedlogu je CERT-EU preimenovan iz „tima za hitne računalne intervencije” u „Centar za kibersigurnost” institucija, tijela i agencija Unije u skladu s kretanjima u državama članicama i globalno, pri čemu su mnogi CERT-ovi preimenovani u centre za kibersigurnost, no zadržan je kratki naziv „CERT-EU” zbog prepoznatljivosti imena.

• Dosljednost s postojećim odredbama politike u tom području

Prijedlogom se nastoji povećati kiberotpornost institucija, tijela i agencija Unije na kiberprijetnje, uz usklađivanje s postojećim zakonodavstvom:

- Direktivom (EU) 2016/1148 o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije. Prijedlog je usklađen i s Prijedlogom direktive (EU) XXXX/XXXX o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije i stavljanju izvan snage Direktive (EU) 2016/1148 [prijedlog NIS 2];
- Uredbom (EU) 2019/881 o Agenciji Europske unije za kibersigurnost te o kibersigurnosnoj certifikaciji u području informacijske i komunikacijske tehnologije (Akt o kibersigurnosti);
- Prijedlog Uredbe (EU) XXXX/XXXX o sigurnosti podataka u institucijama, tijelima, uredima i agencijama Unije
- Preporukom Komisije od 23. lipnja 2021. o uspostavljanju Zajedničke jedinice za kibersigurnost;
- Preporukom Komisije (EU) 2017/1584 od 13. rujna 2017. o koordiniranom odgovoru na kiberincidente i kiberkrize velikih razmjera.

U Prilogu Preporuci Komisije (EU) 2017/1584 od 13. rujna 2017. o koordiniranom odgovoru na kiberincidente i kiberkrize velikih razmjera utvrđuje se plan za koordinirani odgovor na prekogranične kiberincidente i kiberkrize velikih razmjera.

U svojoj rezoluciji od 9. ožujka 2021. Vijeće Europske unije naglasilo je da je kibersigurnost ključna za funkcioniranje javne uprave i na nacionalnoj razini i na razini EU-a, kao i za društvo i gospodarstvo u cjelini te je istaknulo važnost čvrstog i dosljednog sigurnosnog okvira za zaštitu cjelokupnog osoblja, podataka, komunikacijskih mreža, informacijskih

sustava i postupaka donošenja odluka EU-a. Konkretno, to treba postići većom otpornošću i poboljšanom kulturom sigurnosti institucija, tijela i agencija Unije. Treba staviti na raspolaganje dostatne resurse i kapacitete, među ostalim u kontekstu jačanja mandata CERT-EU-a.

2. PRAVNA OSNOVA, SUPSIDIJARNOST I PROPORCIONALNOST

- **Pravna osnova**

Pravna osnova ove Uredbe jest članak 298. Ugovora o funkcioniranju Europske unije („UFEU”), kojim se određuje da u obavljanju svojih zadaća institucije, tijela, uredi i agencije Unije imaju potporu otvorene, učinkovite i neovisne europske administracije. U skladu s Pravilnikom o osoblju i Uvjetima zaposlenja donesenima na temelju članka 336., Europski parlament i Vijeće uredbama, u skladu s redovnim zakonodavnim postupkom, utvrđuju odredbe u tu svrhu.

Informacijska tehnologija omogućila je institucijama, tijelima i agencijama Unije nove načine rada, interakcije s građanima i poboljšanja svih operacija. S razvojem tehnologije razvijaju se i kiberprijetnje. Institucije, tijela i agencije Unije postale su vrlo privlačne mete sofisticiranih kibernapada. Čini se da uspostavljanje sustavâ i zahtjevâ kojima se postiže kibersigurnost pridonosi učinkovitosti i neovisnosti europske uprave, pa institucije, tijela, uredi i agencije Unije mogu učinkovitije obavljati svoje zadaće u digitalnom svijetu.

Nadalje, kako je objašnjeno u odjeljku 3. u nastavku, postojeće razlike u razini kibersigurnosti i pristupu tom pitanju među institucijama, tijelima i agencijama Unije dodatna su prepreka otvorenoj, učinkovitoj i neovisnoj europskoj upravi. Bez zajedničkog pristupa razina kibersigurnosti u institucijama, tijelima i agencijama Unije nastavila bi se razvijati u različitim smjerovima. Navedena je pravna osnova stoga prikladna s obzirom na to da se Uredbom želi stvoriti zajednički pravni okvir za kibersigurnost u institucijama, tijelima, uredima i agencijama Unije.

- **Supsidijarnost**

Uredba kojom se utvrđuju mjere za visoku zajedničku razinu kibersigurnosti u institucijama, tijelima, uredima i agencijama Unije u isključivoj je nadležnosti Unije.

- **Proporcionalnost**

Pravila predložena u ovoj Uredbi ne prelaze ono što je potrebno za zadovoljavajuće ostvarivanje specifičnih ciljeva. Predviđene mjere pridonijet će postizanju visoke zajedničke razine kibersigurnosti ne prelazeći ono što je potrebno za ostvarivanje cilja u kontekstu sve većih rizika s kojima se suočavaju.

- **Odabir instrumenta**

Odabir uredbe, koja je izravno primjenjiva, smatra se prikladnim pravnim instrumentom za definiranje i pojednostavnjenje obveza institucija, tijela i agencija Unije. Kako bi se omogućila ciljana poboljšanja, uredba je najprikladniji pravni instrument.

3. REZULTATI *EX ANTE* EVALUACIJA, SAVJETOVANJA S DIONICIMA I PROCJENA UČINKA

- ***Ex ante* evaluacije**

CERT-EU proveo je procjenu glavnih kiberprijetnji kojima su institucije, tijela i agencije Unije trenutačno izloženi ili će im vjerojatno biti izloženi u doglednoj budućnosti.

U analizi su korištene tri kategorije opažanja:

- pokušaji proboja u informatičku infrastrukturu institucija, tijela i agencija Unije (ako su uspješni, smatraju se incidentima, u ostalim slučajevima i dalje se bilježe kao otkriveni pokušaji),
- prijetnje otkrivene u blizini institucija, tijela i agencija Unije (npr. u njihovim povezanim sektorima, njihovim zajednicama dionika ili u Europi),
- glavni trendovi prijetnji uočeni na globalnoj razini.

Nadalje, u okviru analize razmatralo se kako velike promjene koje su u tijeku utječu na načine na koje institucije Unije upravljaju svojom informatičkom infrastrukturom i uslugama te kako ih upotrebljavaju. Te promjene obuhvaćaju:

- raširenији rad na daljinu,
- migraciju sustavâ u oblak,
- povećanu eksternalizaciju informatičkih usluga.

Od 2019. do 2021. broj ozbiljnih incidenata[1] koji pogađaju institucije, tijela i agencije Unije, čiji su počinitelji akteri iz kategorije naprednih kontinuiranih prijetnji (APT), znatno se povećao. U prvoj polovini 2021. zabilježen je isti broj ozbiljnih incidenata kao u cijeloj 2020. To se očituje i u broju forenzičkih prikaza (snimki sadržaja zahvaćenih sustava ili uređaja) koje je CERT-EU analizirao 2020., a koji se utrostručio u odnosu na 2019., dok se broj ozbiljnih incidenata od 2018. povećao za više od deset puta.

Upravljački odbor CERT-EU-a utvrdio je 2020. novi strateški cilj CERT-EU-a kako bi zajamčio sveobuhvatnu razinu kiberobrane odgovarajućeg opsega i temeljitosti za sve institucije, tijela i agencije te kontinuiranu prilagodbu postojećim ili predstojećim prijetnjama, uključujući napade na mobilne uređaje, okruženja u oblaku i umrežene internetske uređaje.

Komisija je kao dopunu CERT-EU-ovoj analizi prijetnji ocijenila funkcioniranje kibersigurnosti u 20 institucija, tijela i agencija Unije. Time je dobiven uvid u utvrđene kibersigurnosne prakse i sposobnosti upravljanja kibersigurnošću uz vanjsko ocjenjivanje određenih tehničkih sigurnosnih kontrola prema referentnim vrijednostima.

Ocjena se temeljila na upitnicima na koje su odgovorile predmetne institucije, tijela i agencije, javno dostupnim podacima i podacima koje su izravno dostavile same institucije, tijela i agencije Unije, a pruža dovoljno uvida u trenutačnu situaciju za sljedeće zaključke:

- razvijenost kibersigurnosti, veličina informatičke infrastrukture i razine sposobnosti u ocijenjenim institucijama, tijelima i agencijama Unije znatno se razlikuju,
- iako u mnogim institucijama, tijelima i agencijama Unije općenito postoje razvijene sposobnosti otkrivanja i reagiranja, razine integriranog upravljanja rizicima u njihovim sposobnostima upravljanja kibersigurnošću nisu ujednačene,
- iako su kibersigurnosni okviri (strategija, politika i osnova pravila) u ocijenjenim institucijama, tijelima i agencijama Unije općenito dobro uspostavljeni u ključnim područjima kibersigurnosti, navedenima u Prilogu I. Uredbi, u nekim institucijama, tijelima i agencijama Unije nedostaju promišljeno upravljanje kontinuitetom poslovanja, usklađenost, revizija i kontinuirano poboljšanje,

[1] „Ozbiljan incident” znači svaki incident, osim ako ima ograničen učinak i ako se njegova metoda ili tehnologija vjerojatno već dobro razumiju.

- utvrđeno je da ocijenjene institucije, tijela i agencije Unije nejednako primjenjuju tehničke mjere koje se smatraju najboljom praksom.

Ukratko, analiza 20 institucija, tijela i agencija Unije pokazuje niz znatnih razlika u njihovu upravljanju, kiberhigijeni, ukupnoj sposobnosti i razvijenosti. Stoga je zahtjev da sve institucije, tijela i agencije Unije uvedu osnovni okvir kibersigurnosnih mjera ključan za otklanjanje nejednakosti u razini razvijenosti i za postizanje visoke zajedničke razine kibersigurnosti u svim institucijama, tijelima i agencijama Unije.

Nijedan propis Unije dosad nije bio usmjeren na kibersigurnost institucija, tijela i agencija Unije niti se sveobuhvatno bavio kiberprijetnjama i novim informatičkim rizicima koje uzrokuje digitalizacija.

- **Savjetovanja s dionicima**

Komisija se savjetovala s dionicima u institucijama, tijelima i agencijama Unije te s predstavnicima država članica u Vijeću i dionicima u Europskom parlamentu. Predstavnici država članica i relevantni dionici iz institucija, tijela i agencija Unije sudjelovali su 25. lipnja 2021. u radionici koju je organizirala Komisija, na kojoj su raspravljali o sadržaju budućeg Prijedloga uredbe.

- **Procjena učinka**

Ovaj će prijedlog utjecati na institucije, tijela i agencije Unije. Zbog toga posebna procjena učinka nije potrebna jer se neće primjenjivati na države članice.

- **Temeljna prava**

Europska unija zalaže se za osiguravanje visokih standarda zaštite temeljnih prava. Sve informacije koje se razmjenjuju na temelju ove Uredbe razmjenjivale bi se u pouzdanom okruženju, uz potpuno poštovanje prava na zaštitu osobnih podataka, kako je utvrđeno u članku 8. Povelje Europske unije o temeljnim pravima i mjerodavnom zakonodavstvu u području zaštite podataka, posebno Uredbi (EU) 2018/1725 Europskog parlamenta i Vijeća.

4. UTJECAJ NA PRORAČUN

Tržišne referentne vrijednosti i studije[2] pokazuju da izravni izdaci za kibersigurnost obično iznose od 4 % do 7 % ukupnih rashoda organizacija za informacijske tehnologije. Međutim, analiza prijetnji koju je CERT-EU proveo kao potporu ovom zakonodavnom prijedlogu pokazuje da se međunarodna tijela i političke organizacije suočavaju s povećanim rizicima i stoga bi se činilo prikladnijim kibersigurnosti namijeniti 10 % izdataka za informacijske tehnologije. Točan trošak tih nastojanja ne može se utvrditi zbog nedostatka detaljnih informacija o rashodima institucija, tijela i agencija Unije za informacijske tehnologije i relevantnom udjelu izdataka za kibersigurnost.

Iako je, drugim riječima, vjerojatno da mnoge institucije, tijela i agencija Unije na kibersigurnost troše manje nego što bi trebali, ova Uredba neće sama po sebi prouzročiti povećanje tih tekućih rashoda. Čak i bez Uredbe svi bi subjekti morali zajamčiti odgovarajuću razinu kibersigurnosti. Uredbom se nastavlja prethodna suradnja u Upravljačkom odboru

[2] Izvor: Gartner, *Identifying the Real Information Security Budget* (Utvrđivanje stvarnog proračuna za sigurnost podataka) (2016.). To je dodatak neizravnim izdacima za informacijsku sigurnost, npr. za sigurnost mreže (vatrozidi, antivirusni programi) i za odgovornosti vlasnika sustava (procjena rizika, provedba sigurnosnih kontrola). U dokumentu iz 2020. vidljivo je da izdaci za kibersigurnost u financijskim institucijama iznose 10–11 % potrošnje za informacijske tehnologije, izvor: DI_2020-FS-ISAC-Cybersecurity.pdf (deloitte.com).

CERT-EU-a i formalizira se sloj razmjene informacija koji dijelom već postoji. Kako je navedeno u zakonodavnom financijskom izvještaju, CERT-EU trebat će dodatne resurse za obavljanje svojih proširenih zadaća, a ti bi se resursi trebali preraspodijeliti iz institucija, tijela i agencija Unije koje se koriste njegovim uslugama.

5. DRUGI ELEMENTI

- **Mehanizmi provedbe, praćenja, evaluacije i izvješćivanja**

Međuinstitucijski odbor za kibersigurnost (IICB) trebao bi, uz pomoć CERT-EU-a, preispitati funkcioniranje ove Uredbe, provesti procjene i podnijeti izvješće Komisiji o svojim zaključcima. Komisija bi trebala osigurati podnošenje redovitih izvješća Europskom parlamentu, Vijeću, Europskom gospodarskom i socijalnom odboru i Odboru regija.

CERT-EU može izraditi nacrt prijedloga smjernica ili preporuka, a IICB odlučuje o njihovu donošenju. Smjernice su savjetodavni dokument namijenjen svim institucijama, tijelima i agencijama Unije ili samo nekima od njih, dok je preporuka namijenjena pojedinačnim institucijama, tijelima i agencijama Unije. Poziv na djelovanje savjetodavni je dokument CERT-EU-a u kojem se opisuju hitne sigurnosne mjere koje institucije, tijela i agencije Unije trebaju poduzeti u zadanom roku.

- **Detaljno obrazloženje posebnih odredaba prijedloga**

Opće odredbe

Uredbom se utvrđuju mjere za visoku zajedničku razinu kibersigurnosti te se ona primjenjuje na institucije, tijela i agencije Unije kako bi im se omogućilo otvoreno, učinkovito i neovisno obavljanje zadaća (članci 1.–3. i 23.–25.).

Mjere za visoku zajedničku razinu kibersigurnosti

Institucije, tijela i agencije Unije dužni su uspostaviti unutarnji okvir za upravljanje, opće upravljanje i kontrolu kibersigurnosnih rizika, kojim se osigurava učinkovito i razborito upravljanje svim kibersigurnosnim rizicima. Osim toga, institucije, tijela i agencije donose osnovni okvir za kibersigurnost kako bi otklonili rizike utvrđene u skladu s unutarnjim okvirom, redovito ocjenjivali razvijenost kibersigurnosti i donijeli plan za kibersigurnost. (članci 4.–8.).

Međuinstitucijski odbor za kibersigurnost

Osniva se Međuinstitucijski odbor za kibersigurnost, koji je odgovoran za praćenje provedbe ove Uredbe u institucijama, tijelima i agencijama Unije, kao i za nadzor provedbe općih prioriteta i ciljeva koju obavlja CERT-EU i pružanje strateškog usmjerenja CERT-EU-u (članci 9.–11.).

CERT-EU

CERT-EU pridonosi sigurnosti informacijskog okruženja svih institucija, tijela i agencija Unije tako što ih savjetuje, pomaže im u sprečavanju, otkrivanju i ublažavanju incidenata i odgovoru na njih te djeluje kao koordinacijsko čvorište za razmjenu informacija o kibersigurnosti i odgovor na incidente (članci 12.–17.).

Obveze suradnje i izvješćivanja

Uredbom se osiguravaju suradnja i razmjena informacija između CERT-EU-a te institucija, tijela i agencija Unije kako bi se razvili povjerenje i pouzdanje. U tu svrhu CERT-EU može od institucija, tijela i agencija Unije tražiti da mu dostave relevantne informacije, a CERT-EU

može bez suglasnosti pogođene sastavnice s institucijama, tijelima i agencijama Unije razmjenjivati informacije o određenim incidentima kako bi olakšao otkrivanje sličnih kiberprijetnji ili incidenata. Informacije o određenim incidentima kojima se otkriva identitet mete kiberincidenta CERT-EU može razmjenjivati samo uz suglasnost pogođene sastavnice.

Sve institucije, tijela i agencije Unije dužne su obavijestiti CERT-EU o ozbiljnim kiberprijetnjama, znatnim ranjivostima i ozbiljnim incidentima bez nepotrebne odgode, a u svakom slučaju najkasnije 24 sata od saznanja o njima (članci 18.–22.).

2022/0085 (COD)

Prijedlog

UREDBE EUROPSKOG PARLAMENTA I VIJEĆA

o mjerama za visoku zajedničku razinu kibersigurnosti u institucijama, tijelima, uredima i agencijama Unije

EUROPSKI PARLAMENT I VIJEĆE EUROPSKE UNIJE,

uzimajući u obzir Ugovor o funkcioniranju Europske unije, a posebno njegov članak 298.,

uzimajući u obzir Ugovor o osnivanju Europske zajednice za atomsku energiju, a posebno njegov članak 106.a,

uzimajući u obzir prijedlog Europske komisije,

nakon prosljeđivanja nacrta zakonodavnog akta nacionalnim parlamentima,

u skladu s redovnim zakonodavnim postupkom,

budući da:

(1) U digitalnom dobu informacijska i komunikacijska tehnologija okosnica je otvorene, učinkovite i neovisne uprave u Uniji. Zbog napretka tehnologije te povećane složenosti i međusobne povezanosti digitalnih sustava kibersigurnosni rizici sve su veći, a uprava Unije osjetljivija je na kiberprijetnje i incidente, što u konačnici predstavlja prijetnju poslovnom kontinuitetu i sposobnosti uprave da zaštiti svoje podatke. Iako su povećana upotreba usluga u oblaku, sveprisutna upotreba informacijske tehnologije, visok stupanj digitalizacije, rad na daljinu te napredak tehnologije i povezanosti danas osnovne značajke svih aktivnosti upravnih tijela Unije, digitalna otpornost još nije dovoljno ukorijenjena u njihov rad.

(2) Kiberprijetnje s kojima se suočavaju institucije, tijela i agencije Unije stalno se mijenjaju. Taktike, tehnike i postupci prijetećih aktera neprestano se razvijaju, a glavni motivi tih napada, od krađe vrijednih neobjavljenih informacija do zarade, manipuliranja javnim mnijenjem ili ugrožavanja digitalne infrastrukture, ne mijenjaju se mnogo. Tempo kojim se provode kibernapadi stalno raste, a kampanje su sve sofisticiranije i automatiziranije, usmjerene su na prostore izložene napadu koji se stalno šire i brzo iskorištavaju ranjivosti.

(3) Informatička okruženja institucija, tijela i agencija Unije međuovisna su, imaju integrirane protoke podataka, a njihovi korisnici blisko surađuju. Ta međupovezanost znači da svaki poremećaj, čak i onaj koji je prvotno ograničen na jednu instituciju, tijelo ili agenciju Unije, može imati kaskadne učinke u širem smislu, što može dovesti do dalekosežnih i dugotrajnih negativnih učinaka na druge subjekte. Osim toga, informatička okruženja nekih institucija, tijela i agencija povezana su s informatičkim okruženjima država članica, zbog čega incident u jednom subjektu Unije predstavlja rizik za kibersigurnost informatičkog okruženja država članica i obratno.

(4) Institucije, tijela i agencije Unije privlačne su mete koje se suočavaju s vrlo vještim i dobro opremljenim prijetećim akterima i drugim prijetnjama. Istodobno, razina i razvijenost kiberotpornosti te sposobnost otkrivanja zlonamjernih kiberaktivnosti i

odgovora na njih znatno se razlikuju od subjekta do subjekta. Kako bi europska uprava funkcionirala, institucije, tijela i agencije Unije stoga moraju ostvariti visoku zajedničku razinu kibersigurnosti putem osnovnog okvira za kibersigurnost (skupa minimalnih pravila za kibersigurnost s kojima mrežni i informacijski sustavi te njihovi operateri i korisnici moraju biti usklađeni kako bi se kibersigurnosni rizici sveli na najmanju mjeru), kao i putem razmjene informacija i suradnje.

(5) Cilj je Direktive [prijedlog NIS 2] o mjerama za visoku zajedničku razinu kibersigurnosti u cijeloj Uniji dodatno poboljšanje kiberotpornosti javnih i privatnih subjekata, nadležnih nacionalnih tijela i institucija te Unije u cjelini kao i njihove sposobnosti odgovora na incidente. Stoga se institucije, tijela i agencije Unije moraju tome prilagoditi osiguravanjem pravila koja su u skladu s Direktivom [prijedlog NIS 2] i koja odražavaju njezinu razinu ambicije.

(6) Kako bi se postigla visoka zajednička razina kibersigurnosti, sve institucije, tijela i agencije Unije moraju uspostaviti unutarnji okvir za upravljanje, opće upravljanje i kontrolu kibersigurnosnih rizika, kojim se osigurava učinkovito i razborito upravljanje svim kibersigurnosnim rizicima te uzimaju u obzir kontinuitet poslovanja i upravljanje krizama.

(7) Zbog razlika među institucijama, tijelima i agencijama Unije pri provedbi je potrebna fleksibilnost jer ne postoji univerzalno rješenje. Mjere za visoku zajedničku razinu kibersigurnosti ne bi trebale obuhvaćati obveze koje izravno ometaju izvršavanje zadaća institucija, tijela i agencija Unije ili zadiru u njihovu institucijsku autonomiju. Stoga bi institucije, tijela i agencije trebali uspostaviti vlastite okvire za upravljanje, opće upravljanje i kontrolu kibersigurnosnih rizika te donijeti vlastite osnovne okvire i planove za kibersigurnost.

(8) Da bi se izbjeglo nerazmjerno financijsko i administrativno opterećenje za institucije, tijela i agencije Unije, zahtjevi za upravljanje kibersigurnosnim rizikom trebali bi biti razmjerni riziku kojem je izložen predmetni mrežni i informacijski sustav, uzimajući u obzir suvremenost mjera. Sve institucije, tijela i agencije Unije trebali bi nastojati odrediti odgovarajući postotak svojeg proračuna za informacijske tehnologije za poboljšanje svoje razine kibersigurnosti; dugoročno bi trebalo težiti cilju od 10 %.

(9) Kako bi se postigla visoka zajednička razina kibersigurnosti, ona mora biti pod nadzorom najviše rukovodeće razine svake institucije, tijela i agencije Unije, koja bi trebala odobriti osnovni okvir za kibersigurnost kojim bi se trebali otklanjati rizici utvrđeni u skladu s unutarnjim okvirom koji svaka institucija, tijelo i agencija mora uspostaviti. Bavljenje kulturom kibersigurnosti, tj. svakodnevna primjena kibersigurnosti, sastavni je dio osnovnog okvira za kibersigurnost u svim institucijama, tijelima i agencijama Unije.

(10) Institucije, tijela i agencije Unije trebali bi procijeniti rizike povezane s odnosima s dobavljačima i pružateljima usluga, uključujući pružatelje usluga pohrane i obrade podataka ili upravljanih sigurnosnih usluga, te poduzeti odgovarajuće mjere za njihovo otklanjanje. Te mjere trebale bi biti dio osnovnog okvira za kibersigurnost i trebalo bi ih pobliže definirati u smjernicama ili preporukama koje izdaje CERT-EU. Pri definiranju mjera i smjernica moraju se uzeti u obzir relevantno zakonodavstvo i politike EU-a, uključujući procjene rizika i preporuke koje je izdala Skupina za suradnju u području sigurnosti mrežnih i informacijskih sustava, kao što su usklađena procjena rizika na razini EU-a i paket instrumenata EU-a za kibersigurnost 5G mreža. Osim toga, moglo bi se zahtijevati certificiranje relevantnih IKT proizvoda, usluga i

procesa u okviru posebnih programa kibersigurnosne certifikacije EU-a donesenih na temelju članka 49. Uredbe (EU) 2019/881.

(11) U svibnju 2011. glavni tajnici institucija i tijela Unije odlučili su osnovati pretkonfiguracijski tim za hitne računalne intervencije europskih institucija, tijela i agencija (CERT-EU) pod nadzorom međuinstitucijskog upravljačkog odbora. U srpnju 2012. glavni tajnici potvrdili su praktične aranžmane i dogovorili se da će zadržati CERT-EU u obliku trajnog subjekta radi daljnjeg doprinosa poboljšanju ukupne razine sigurnosti informacijskih tehnologija u institucijama, tijelima i agencijama Unije kao primjer vidljive međuinstitucijske suradnje u području kibersigurnosti. U rujnu 2012. osnovan je CERT-EU kao radna skupina Europske komisije s međuinstitucijskim ovlastima. U prosincu 2017. institucije i tijela Unije sklopili su međuinstitucijski dogovor o organizaciji i djelovanju CERT-EU-a[3]. Taj bi dogovor trebalo kontinuirano prilagođavati radi pružanja potpore provedbi ove Uredbe.

(12) CERT-EU trebalo bi preimenovati iz „tima za hitne računalne intervencije” u „Centar za kibersigurnost” institucija, tijela i agencija Unije, u skladu s kretanjima u državama članicama i globalno, u okviru kojih su mnogi CERT-ovi preimenovani u centre za kibersigurnost, ali bi zbog prepoznatljivosti trebalo zadržati kratki naziv „CERT-EU”.

(13) Mnogi kibernapadi dio su širih kampanja usmjerenih na skupine institucija, tijela i agencija Unije ili interesnih zajednica koje uključuju institucije, tijela i agencije Unije. Kako bi omogućili proaktivne mjere za otkrivanje, odgovor na incidente ili ublažavanje, institucije, tijela i agencije Unije trebali bi obavijestiti CERT-EU o ozbiljnim kiberprijetnjama, znatnim ranjivostima i ozbiljnim incidentima te podijeliti odgovarajuće tehničke pojedinosti koje omogućuju otkrivanje ili ublažavanje sličnih kiberprijetnji, ranjivosti i incidenata u drugim institucijama, tijelima i agencijama Unije, kao i odgovor na njih. Na temelju istog pristupa kao što je onaj predviđen Direktivom [prijedlog NIS 2], ako subjekti dobiju informaciju o ozbiljnom incidentu, trebali bi biti dužni u roku od 24 sata dostaviti prvu obavijest CERT-EU-u. Ta razmjena informacija trebala bi omogućiti CERT-EU-u da te informacije proslijedi drugim institucijama, tijelima i agencijama Unije, kao i odgovarajućim partnerima, kako bi se pomoglo zaštititi sva informatička okruženja Unije i partnera Unije od sličnih incidenata, prijetnji i ranjivosti.

(14) Osim davanja većeg broja zadaća i važnije uloge CERT-EU-u, trebalo bi uspostaviti Međuinstitucijski odbor za kibersigurnost (IICB), koji bi trebao olakšati postizanje visoke zajedničke razine kibersigurnosti u institucijama, tijelima i agencijama Unije praćenjem provedbe ove Uredbe u institucijama, tijelima i agencijama Unije, nadzorom nad provedbom općih prioriteta i ciljeva koju obavlja CERT-EU i pružanjem strateškog usmjerenja CERT-EU-u. IICB bi trebao osigurati zastupljenost institucija te uključiti predstavnike agencija i tijela putem Mreže agencija Unije.

(15) CERT-EU trebao bi poduprijeti provedbu mjera za visoku zajedničku razinu kibersigurnosti prijedlozima za smjernice i preporuke IICB-u ili objavljivanjem poziva na djelovanje. IICB bi trebao odobriti te smjernice i preporuke. Prema potrebi, CERT-EU trebao bi objavljivati pozive na djelovanje u kojima se opisuju hitne sigurnosne mjere koje institucije, tijela i agencije Unije trebaju poduzeti u zadanom roku.

(16) IICB bi trebao nadzirati usklađenost s ovom Uredbom te pratiti smjernice, preporuke i pozive na djelovanje koje izdaje CERT-EU. IICB bi u tehničkim pitanjima trebalo

[3] SL C 12, 13.1.2018., str. 1.–11.

imati potporu tehničkih savjetodavnih skupina čiji sastav IICB određuje prema vlastitu nahođenju te koje bi prema potrebi trebale blisko surađivati s CERT-EU-om, institucijama, tijelima i agencijama Unije te drugim dionicima. Prema potrebi, IICB bi trebao izdavati neobvezujuća upozorenja i preporučivati revizije.

(17) Misija CERT-EU-a trebala bi biti pridonijeti sigurnosti informacijskog okruženja svih institucija, tijela i agencija Unije. CERT-EU trebao bi djelovati kao ekvivalent imenovanog koordinatora za institucije, tijela i agencije Unije u svrhu koordiniranog bilježenja ranjivosti u europskom registru ranjivosti kako je navedeno u članku 6. Direktive [prijedlog NIS 2].

(18) Upravljački odbor CERT-EU-a utvrdio je 2020. novi strateški cilj CERT-EU-a kako bi zajamčio sveobuhvatnu razinu kiberobrane odgovarajućeg opsega i temeljitosti za sve institucije, tijela i agencije Unije te kontinuiranu prilagodbu postojećim ili predstojećim prijetnjama, uključujući napade na mobilne uređaje, okruženja u oblaku i umrežene internetske uređaje. Strateški cilj obuhvaća i centre za sigurnosne operacije širokog spektra (SOC), koji nadziru mreže, i nadzor od 24 sata dnevno za vrlo ozbiljne prijetnje. Za veće institucije, tijela i agencije Unije CERT-EU trebao bi pružati potporu njihovim timovima za informatičku sigurnost, među ostalim prvom linijom nadzora 24 sata dnevno. Za manje i neke srednje velike institucije, tijela i agencije Unije CERT-EU trebao bi pružati sve usluge.

(19) CERT-EU trebao bi obavljati i ulogu koja mu je određena Direktivom [prijedlog NIS 2], a koja se odnosi na suradnju i razmjenu informacija s mrežom timova za odgovor na računalne sigurnosne incidente (CSIRT). Nadalje, u skladu s Preporukom Komisije (EU) 2017/1584[4] CERT-EU trebao bi surađivati i koordinirati odgovor s relevantnim dionicima. Kako bi pridonio visokoj razini kibersigurnosti u cijeloj Uniji, CERT-EU trebao bi s nacionalnim partnerima dijeliti informacije o određenim incidentima. CERT-EU trebao bi surađivati i s drugim javnim i privatnim partnerima, uključujući NATO, uz prethodno odobrenje IICB-a.

(20) Pri pružanju potpore operativnoj kibersigurnosti CERT-EU trebao bi koristiti raspoloživo stručno znanje Agencije Europske unije za kibersigurnost u okviru strukturirane suradnje kako je predviđeno Uredbom (EU) 2019/881 Europskog parlamenta i Vijeća[5]. Prema potrebi bi trebalo definirati namjenske aranžmane između ta dva subjekta kako bi se utvrdila praktična provedba takve suradnje i izbjeglo udvostručivanje aktivnosti. CERT-EU trebao bi surađivati s Agencijom Europske unije za kibersigurnost na analizi prijetnji i redovito izvješćivati Agenciju o stanju kiberprijetnji.

(21) Kao potpora Zajedničkoj jedinici za kibersigurnost koja je uspostavljena u skladu s Preporukom Komisije od 23. lipnja 2021.[6], CERT-EU trebao bi surađivati i razmjenjivati informacije s dionicima kako bi potaknuo operativnu suradnju i omogućio postojećim mrežama da ostvare svoj puni potencijal u zaštiti Unije.

---

4 Preporuka Komisije (EU) 2017/1584 od 13. rujna 2017. o koordiniranom odgovoru na kiberincidente i kiberkrize velikih razmjera (SL L 239, 19.9.2017., str. 36.).

5 Uredba (EU) 2019/881 Europskog parlamenta i Vijeća od 17. travnja 2019. o ENISA-i (Agencija Europske unije za kibersigurnost) te o kibersigurnosnoj certifikaciji u području informacijske i komunikacijske tehnologije i stavljanju izvan snage Uredbe (EU) br. 526/2013 (Akt o kibersigurnosti) (SL L 151, 7.6.2019., str. 15.).

6 Preporuka Komisije C(2021) 4520 od 23. lipnja 2021. o uspostavljanju Zajedničke jedinice za kibersigurnost.

(22) Obrada svih osobnih podataka na temelju ove Uredbe trebala bi biti u skladu sa zakonodavstvom o zaštiti podataka, uključujući Uredbu (EU) 2018/1725 Europskog parlamenta i Vijeća[7].

(23) Postupanje CERT-EU-a i institucija, tijela i agencija Unije s podacima trebalo bi biti u skladu s pravilima utvrđenima u Uredbi [predložena Uredba o sigurnosti podataka]. Kako bi se osigurala koordinacija u pitanjima sigurnosti, sve kontakte s CERT-EU-om koje pokrenu ili zatraže nacionalne sigurnosne i obavještajne službe trebalo bi bez nepotrebne odgode priopćiti Glavnoj upravi Komisije za sigurnost i predsjedniku IICB-a.

(24) Budući da su usluge i zadaće CERT-EU-a u interesu svih institucija, tijela i agencija Unije, sve institucije, tijela i agencije Unije s rashodima za informacijsku tehnologiju trebali bi razmjerno pridonositi tim uslugama i zadaćama. Ti doprinosi ne dovode u pitanje proračunsku autonomiju institucija, tijela i agencija Unije.

(25) IICB trebao bi, uz pomoć CERT-EU-a, preispitati i procijeniti funkcioniranje ove Uredbe te podnijeti izvješće Komisiji o svojim zaključcima. Na temelju tih informacija Komisija bi trebala podnijeti izvješće Europskom parlamentu, Vijeću, Europskom gospodarskom i socijalnom odboru i Odboru regija.

DONIJELI SU OVU UREDBU:

Poglavlje I.
OPĆE ODREDBE

Članak 1.
Predmet

Ovom se Uredbom utvrđuju:

(a) obveze institucija, tijela i agencija Unije da uspostave unutarnji okvir za upravljanje, opće upravljanje i kontrolu kibersigurnosnih rizika;

(b) obveze institucija, tijela i agencija Unije glede upravljanja kibersigurnosnim rizicima i izvješćivanja o njima;

(c) pravila o organizaciji i radu Centra za kibersigurnost institucija, tijela i agencija Unije (CERT-EU) te o organizaciji i radu Međuinstitucijskog odbora za kibersigurnost.

Članak 2.
Područje primjene

Ova se Uredba primjenjuje na upravljanje, opće upravljanje i kontrolu kibersigurnosnih rizika u svim institucijama, tijelima i agencijama Unije te na organizaciju i rad CERT-EU-a i Međuinstitucijskog odbora za kibersigurnost.

[7] Uredba (EU) 2018/1725 Europskog parlamenta i Vijeća od 23. listopada 2018. o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama, tijelima, uredima i agencijama Unije i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Uredbe (EZ) br. 45/2001 i Odluke br. 1247/2002/EZ (SL L 295, 21.11.2018., str. 39.).

Članak 3.
Definicije

Za potrebe ove Uredbe, primjenjuju se sljedeće definicije:

(1) „institucije, tijela i agencije Unije” znači institucije, tijela i agencije Unije koji su osnovani Ugovorom o Europskoj uniji, Ugovorom o funkcioniranju Europske unije ili Ugovorom o osnivanju Europske zajednice za atomsku energiju ili na temelju tih ugovora;

(2) „mrežni i informacijski sustav” znači mrežni i informacijski sustav u smislu članka 4. točke 1. Direktive [prijedlog NIS 2];

(3) „sigurnost mrežnih i informacijskih sustava” znači sigurnost mrežnih i informacijskih sustava u smislu članka 4. točke 2. Direktive [prijedlog NIS 2];

(4) „kibersigurnost” znači kibersigurnost u smislu članka 4. točke 3. Direktive [prijedlog NIS 2];

(5) „najviša rukovodeća razina” znači rukovoditelj, rukovodstvo ili koordinacijsko i nadzorno tijelo na najvišoj upravnoj razini, uzimajući u obzir sustave upravljanja na visokoj razini u svim institucijama, tijelima ili agencijama Unije;

(6) „incident” znači incident u smislu članka 4. točke 5. Direktive [prijedlog NIS 2];

(7) „ozbiljan incident” znači svaki incident, osim ako ima ograničen učinak i ako se njegova metoda ili tehnologija vjerojatno već dobro razumije;

(8) „veći napad” znači svaki incident za koji je potrebno više resursa nego što je dostupno u pogođenoj instituciji, tijelu ili agenciji Unije i CERT-EU-u;

(9) „rješavanje incidenta” znači rješavanje incidenta u smislu članka 4. točke 6. Direktive [prijedlog NIS 2];

(10) „kiberprijetnja” znači kiberprijetnja u smislu članka 2. točke 8. Uredbe (EU) 2019/881;

(11) „ozbiljna kiberprijetnja” znači kiberprijetnja s namjerom, mogućnošću i sposobnošću da uzrokuje ozbiljan incident;

(12) „ranjivost” znači ranjivost u smislu članka 4. točke 8. Direktive [prijedlog NIS 2];

(13) „znatna ranjivost” znači ranjivost koja će, ako se iskoristi, vjerojatno uzrokovati ozbiljan incident;

(14) „kibersigurnosni rizik” znači bilo koja razumno prepoznatljiva okolnost ili događaj koji ima potencijalan negativan učinak na sigurnost mrežnih i informacijskih sustava;

(15) „Zajednička jedinica za kibersigurnost” znači virtualna i fizička platforma za suradnju za razne zajednice za kibersigurnost u Uniji, prije svega za operativnu i tehničku koordinaciju protiv velikih prekograničnih kiberprijetnji i incidenata u smislu Preporuke Komisije od 23. lipnja 2021.;

(16) „osnovni okvir za kibersigurnost” znači skup minimalnih pravila za kibersigurnost s kojima mrežni i informacijski sustavi te njihovi operateri i korisnici moraju biti usklađeni kako bi se kibersigurnosni rizici sveli na najmanju mjeru.

Poglavlje II.
MJERE ZA VISOKU ZAJEDNIČKU RAZINU KIBERSIGURNOSTI

Članak 4.
Upravljanje, opće upravljanje i kontrola rizika

1. Sve institucije, tijela i agencije Unije uspostavljaju unutarnji okvir za upravljanje, opće upravljanje i kontrolu kibersigurnosnih rizika („okvir”) kojim se podupiru zadaće subjekta, pri čemu primjenjuju svoju institucijsku autonomiju. Provedbu nadzire najviša rukovodeća razina predmetnog subjekta kako bi se osiguralo učinkovito i razborito upravljanje svim kibersigurnosnim rizicima. Okvir se mora uspostaviti najkasnije do ... [15 mjeseci od stupanja na snagu ove Uredbe].

2. Okvir obuhvaća cjelokupno informatičko okruženje predmetne institucije, tijela ili agencije, uključujući sva lokalna informatička okruženja, eksternalizirana sredstva i usluge računalstva u oblaku ili one kojima treće strane pružaju usluge smještaja na poslužitelju, mobilne uređaje, korporacijske mreže, poslovne mreže koje nisu povezane s internetom i sve uređaje povezane s informatičkim okruženjem. U okviru se uzimaju u obzir kontinuitet poslovanja i upravljanje krizama te sigurnost lanca opskrbe i upravljanje ljudskim rizicima koji bi mogli utjecati na kibersigurnost predmetne institucije, tijela ili agencije Unije.

3. Najviša rukovodeća razina svih institucija, tijela i agencija Unije osigurava nadzor nad usklađenošću svoje organizacije s obvezama povezanima s upravljanjem, općim upravljanjem i kontrolom kibersigurnosnih rizika, bez dovođenja u pitanje formalnih odgovornosti ostalih rukovodećih razina u pogledu usklađenosti i upravljanja rizikom u područjima za koja su nadležne.

4. Sve institucije, tijela i agencije Unije dužne su imati uspostavljene učinkovite mehanizme kojima se osigurava da se odgovarajući postotak proračuna za informacijsku tehnologiju troši na kibersigurnost.

5. Sve institucije, tijela i agencije Unije imenuju lokalnog službenika za kibersigurnost ili jednakovrijednu funkciju koji djeluje kao njihova jedinstvena kontaktna točka za sve aspekte kibersigurnosti.

Članak 5.
Osnovni okvir za kibersigurnost

1. Najviša rukovodeća razina svake institucije, tijela i agencije Unije odobrava osnovni okvir za kibersigurnost svoje organizacije radi otklanjanja rizika utvrđenih u unutarnjem okviru iz članka 4. stavka 1. Time se podupiru zadaće organizacije i primjenjuje njezina institucijska autonomija. Osnovni okvir za kibersigurnost mora se utvrditi najkasnije do ... [18 mjeseci od stupanja na snagu ove Uredbe] i odnosi se na područja navedena u Prilogu I. i mjere navedene u Prilogu II.

2. Više rukovodstvo svih institucija, tijela i agencija Unije redovito sudjeluje u posebnim osposobljavanjima kako bi steklo dovoljno znanja i vještina da shvati i procijeni kibersigurnosne rizike i prakse upravljanja kibersigurnošću te njihov utjecaj na poslovanje organizacije.

Članak 6.
Procjene razvijenosti

Sve institucije, tijela i agencije Unije najmanje svake tri godine provode procjenu razvijenosti kibersigurnosti koja obuhvaća sve elemente njihovih informatičkih okruženja kako je opisano u članku 4., pri čemu uzimaju u obzir relevantne smjernice i preporuke donesene u skladu s člankom 13.

Članak 7.
Planovi za kibersigurnost

1. Na temelju zaključaka izvedenih iz procjene razvijenosti i s obzirom na sredstva i rizike utvrđene u skladu s člankom 4., najviša rukovodeća razina svih institucija, tijela i agencija Unije bez nepotrebne odgode odobrava plan za kibersigurnost nakon uspostave okvira za upravljanje, opće upravljanje i kontrolu rizika te osnovnog okvira za kibersigurnost. Planom se nastoji povećati ukupna kibersigurnost predmetnog subjekta i time pridonijeti postizanju ili poboljšanju visoke zajedničke razine kibersigurnosti u svim institucijama, tijelima i agencijama Unije. Kako bi se pružila potpora zadaćama subjekta na temelju njegove institucijske autonomije, plan obuhvaća barem područja navedena u Prilogu I., mjere navedene u Prilogu II. te mjere povezane s pripravnošću i odgovorom na incidente i oporavkom od njih, kao što su sigurnosni nadzor i vođenje evidencije. Plan se revidira najmanje svake tri godine na temelju procjena razvijenosti provedenih u skladu s člankom 6.
2. Plan za kibersigurnost sadržava dužnosti i zadaće članova osoblja koje se odnose na njegovu provedbu.
3. U planu za kibersigurnost u obzir se uzimaju sve primjenjive smjernice i preporuke koje je izdao CERT-EU.

Članak 8.
Provedba

1. Po završetku procjena razvijenosti institucije, tijela i agencije Unije dostavljaju procjene Međuinstitucijskom odboru za kibersigurnost. Po završetku izrade sigurnosnih planova institucije, tijela i agencije Unije o tome obavješćuju Međuinstitucijski odbor za kibersigurnost. Na zahtjev tog odbora izvješćuju o posebnim aspektima ovog poglavlja.
2. Smjernice i preporuke, izdane u skladu s člankom 13., podupiru provedbu odredbi utvrđenih u ovom poglavlju.

Poglavlje III.
MEĐUINSTITUCIJSKI ODBOR ZA KIBERSIGURNOST

Članak 9.
Međuinstitucijski odbor za kibersigurnost

1. Osniva se Međuinstitucijski odbor za kibersigurnost (IICB).
2. IICB je odgovoran za:
   (a) praćenje provedbe ove Uredbe u institucijama, tijelima i agencijama Unije;

(b) nadzor nad provedbom općih prioriteta i ciljeva koju obavlja CERT-EU i pružanje strateškog usmjerenja CERT-EU-u.

3. IICB se sastoji od tri predstavnika koje Mreža agencija Unije (EUAN) imenuje na prijedlog svojeg savjetodavnog odbora za IKT (ICTAC) da zastupaju interese agencija i tijela koja sama upravljaju svojim informatičkim okruženjem i po jednog predstavnika kojeg imenuje svako od sljedećih tijela:

(a) Europski parlament;

(b) Vijeće Europske unije;

(c) Europska komisija;

(d) Sud Europske unije;

(e) Europska središnja banka;

(f) Europski revizorski sud;

(g) Europska služba za vanjsko djelovanje;

(h) Europski gospodarski i socijalni odbor;

(i) Europski odbor regija;

(j) Europska investicijska banka;

(k) Agencija Europske unije za kibersigurnost.

Članovima može pomagati zamjenik. Predsjednik može pozvati druge predstavnike prethodno navedenih organizacija ili drugih institucija, tijela i agencija Unije da prisustvuju sastancima IICB-a bez prava glasa.

4. IICB donosi svoj unutarnji poslovnik.

5. U skladu sa svojim unutarnjim poslovnikom IICB iz redova svojih članova imenuje predsjednika na razdoblje od četiri godine. Njegov zamjenik postaje punopravni član IICB-a na isto razdoblje.

6. IICB se sastaje na inicijativu svojeg predsjednika, na zahtjev CERT-EU-a ili na zahtjev svojih članova.

7. Svaki član IICB-a ima jedan glas. Odluke IICB-a donose se običnom većinom, osim ako je ovom Uredbom drugačije određeno. Predsjednik ne smije glasovati osim u slučaju izjednačenog broja glasova kad može dati odlučujući glas.

8. IICB može djelovati po pojednostavnjenom pisanom postupku pokrenutom u skladu s unutarnjim poslovnikom IICB-a. Na temelju tog postupka relevantna odluka smatra se odobrenom u roku koji odredi predsjednik, osim ako se neki član protivi.

9. Voditelj CERT-EU-a ili njegov zamjenik sudjeluje na sastancima IICB-a osim ako IICB odluči drukčije.

10. Poslove tajništva za IICB obavlja Komisija.

11. Predstavnici koje EUAN imenuje na prijedlog savjetodavnog odbora za IKT prosljeđuju odluke IICB-a agencijama i zajedničkim poduzećima Unije. Sve agencije i tijela Unije imaju pravo s predstavnicima ili predsjednikom IICB-a pokrenuti sva pitanja za koja smatraju da bi trebalo uputiti IICB-u.

12. IICB može djelovati po pojednostavnjenom pisanom postupku koji pokreće predsjednik, a na temelju kojeg se relevantna odluka smatra odobrenom u roku koji odredi predsjednik, osim ako se neki član usprotivi.

13. IICB može imenovati izvršni odbor da mu pomaže u radu i delegirati mu neke svoje zadaće i ovlasti. IICB utvrđuje poslovnik izvršnog odbora, uključujući njegove zadaće i ovlasti te mandat njegovih članova.

Članak 10.
Zadaće IICB-a

Pri obavljanju svojih dužnosti IICB posebno:

(a) pregledava sva izvješća koja CERT-EU zatraži o stanju provedbe ove Uredbe u institucijama, tijelima i agencijama Unije;

(b) na temelju prijedloga voditelja CERT-EU-a odobrava godišnji program rada CERT-EU-a i prati njegovu provedbu;

(c) na temelju prijedloga voditelja CERT-EU-a odobrava katalog usluga CERT-EU-a;

(d) na temelju prijedloga voditelja CERT-EU-a odobrava godišnji financijski plan prihoda i rashoda, uključujući za osoblje, za aktivnosti CERT-EU-a;

(e) na temelju prijedloga voditelja CERT-EU-a odobrava modalitete sporazumâ o razini usluga;

(f) pregledava i odobrava godišnje izvješće koje sastavlja voditelj CERT-EU-a, a kojim su obuhvaćene aktivnosti CERT-EU-a i upravljanje njegovim sredstvima;

(g) odobrava i prati ključne pokazatelje uspješnosti CERT-EU-a definirane na prijedlog voditelja CERT-EU-a;

(h) odobrava dogovore o suradnji te sporazume ili ugovore o razini usluga između CERT-EU-a i drugih subjekata u skladu s člankom 17.;

(i) uspostavlja potreban broj tehničkih savjetodavnih skupina za pomoć u radu IICB-a, odobrava njihova pravila djelovanja i imenuje njihove predsjednike.

Članak 11.
Usklađenost

IICB prati kako institucije, tijela i agencije Unije provode ovu Uredbu i donesene smjernice, preporuke i pozive na djelovanje. Ako IICB utvrdi da institucije, tijela ili agencije Unije nisu učinkovito primjenjivali ili provodili ovu Uredbu ili smjernice, preporuke i pozive na djelovanje izdane na temelju ove Uredbe, može, ne dovodeći u pitanje unutarnje postupke relevantne institucije, tijela ili agencije Unije:

(a) izdati upozorenje; prema potrebi, pristup upozorenju na odgovarajući se način ograničava ako postoji uvjerljiv kibersigurnosni rizik;

(b) preporučiti mjerodavnoj revizorskoj službi da provede reviziju.

Poglavlje IV.
CERT-EU

Članak 12.
Misija i zadaće CERT-EU-a

1. Misija CERT-EU-a, autonomnog međuinstitucijskog centra za kibersigurnost svih institucija, tijela i agencija Unije, jest pridonijeti sigurnosti informacijskog okruženja svih institucija, tijela i agencija Unije pružanjem savjeta o kibersigurnosti, pomaganjem u sprečavanju, otkrivanju i ublažavanju incidenata i odgovoru na njih te preuzimanjem uloge njihova koordinacijskog čvorišta za razmjenu informacija o kibersigurnosti i za odgovor na incidente.

2. CERT-EU obavlja sljedeće zadaće za institucije, tijela i agencije Unije:

   (a) pruža im potporu u provedbi ove Uredbe i pridonosi koordinaciji primjene ove Uredbe putem mjera navedenih u članku 13. stavku 1.;

   (b) pruža im potporu paketom kibersigurnosnih usluga opisanih u njegovu katalogu usluga („osnovne usluge”);

   (c) održava mrežu kolega i partnera radi pružanja potpore uslugama kako je navedeno u člancima 16. i 17.;

   (d) skreće pozornost IICB-a na sva pitanja koja se odnose na provedbu ove Uredbe i provedbu smjernica, preporuka i poziva na djelovanje;

   (e) izvješćuje o kiberprijetnjama s kojima se suočavaju institucije, tijela i agencije Unije te pridonosi informiranosti o kibersigurnosnoj situaciji u EU-u.

3. CERT-EU pridonosi radu Zajedničke jedinice za kibersigurnost, osnovane u skladu s Preporukom Komisije od 23. lipnja 2021., među ostalim u sljedećim područjima:

   (a) pripravnost, koordinacija incidenata, razmjena informacija i odgovor na krize na tehničkoj razini u slučajevima povezanima s institucijama, tijelima i agencijama Unije;

   (b) operativna suradnja u pogledu mreže timova za odgovor na računalne sigurnosne incidente (CSIRT-ovi), uključujući međusobnu pomoć, i šire kibersigurnosne zajednice;

   (c) saznanja o prijetnjama, uključujući informiranost o situaciji;

   (d) sve teme za koje je potrebna tehnička stručnost CERT-EU-a u području kibersigurnosti.

4. CERT-EU sudjeluje u strukturiranoj suradnji s Agencijom Europske unije za kibersigurnost na izgradnji kapaciteta, operativnoj suradnji i dugoročnim strateškim analizama kiberprijetnji u skladu s Uredbom (EU) 2019/881 Europskog parlamenta i Vijeća.

5. CERT-EU može pružati sljedeće usluge koje nisu opisane u njegovu katalogu usluga („usluge uz naknadu”):

   (a) usluge kojima se podupire kibersigurnost informatičkog okruženja institucija, tijela i agencija Unije, osim onih iz stavka 2., na temelju sporazumâ o razini usluga i ovisno o dostupnim resursima;

(b) usluge kojima se podupiru kibersigurnosne operacije ili projekti institucija, tijela i agencija Unije koje ne služe za zaštitu njihovih informatičkih okruženja, na temelju pisanih sporazuma i uz prethodno odobrenje IICB-a;

(c) usluge kojima se podupire sigurnost informatičkog okruženja organizacija koje nisu institucije, tijela i agencije Unije, a koje blisko surađuju s institucijama, tijelima i agencijama Unije, na primjer zbog zadaća ili dužnosti dodijeljenih na temelju prava Unije, na temelju pisanih sporazuma i uz prethodno odobrenje IICB-a.

6. CERT-EU može organizirati vježbe u području kibersigurnosti ili preporučiti sudjelovanje u postojećim vježbama, u bliskoj suradnji s Agencijom Europske unije za kibersigurnost kad je to primjenjivo, kako bi se ispitala razina kibersigurnosti institucija, tijela i agencija Unije.

7. CERT-EU može pružiti pomoć institucijama, tijelima i agencijama Unije u pogledu incidenata u povjerljivim informatičkim okruženjima ako predmetna sastavnica to izričito zatraži.

Članak 13.
Smjernice, preporuke i pozivi na djelovanje

1. CERT-EU podupire provedbu ove Uredbe objavljivanjem:

(a) poziva na djelovanje u kojima se opisuju hitne sigurnosne mjere koje institucije, tijela i agencije Unije trebaju poduzeti u zadanom roku;

(b) prijedloga IICB-u za smjernice upućene svim institucijama, tijelima i agencijama Unije ili nekoj njihovoj podskupini;

(c) prijedloga IICB-u za preporuke upućene pojedinim institucijama, tijelima i agencijama Unije.

2. Smjernice i preporuke mogu sadržavati:

(a) modalitete za upravljanje kibersigurnosnim rizicima i osnovnim okvirom za kibersigurnost ili njihovo poboljšanje;

(b) modalitete za procjenu razvijenosti i planove za kibersigurnost; i

(c) prema potrebi, korištenje zajedničke tehnologije, arhitekture i povezane najbolje prakse radi postizanja interoperabilnosti i zajedničkih normi u smislu članka 4. točke 10. Direktive [prijedlog NIS 2].

3. IICB može donijeti smjernice ili preporuke na prijedlog CERT-EU-a.

4. IICB može uputiti CERT-EU da objavi, povuče ili izmijeni prijedlog smjernica ili preporuka ili poziv na djelovanje.

Članak 14.
Voditelj CERT-EU-a

Voditelj CERT-EU-a redovito podnosi izvješća IICB-u i predsjedniku IICB-a o uspješnosti CERT-EU-a, financijskom planiranju, prihodima, izvršenju proračuna, sklopljenim sporazumima o razini usluga i pisanim sporazumima, suradnji s ugovornim stranama i partnerima te službenim putovanjima osoblja, uključujući izvješća iz članka 10. stavka 1.

Članak 15.

Financijska pitanja i osoblje

1. Nakon što dobije jednoglasnu suglasnost IICB-a, Komisija imenuje voditelja CERT-EU-a. Savjetovanje s IICB-om obavezno je u svim fazama postupka prije imenovanja voditelja CERT-EU-a, posebno pri izradi obavijesti o slobodnom radnom mjestu, razmatranju prijava i imenovanju odbora za odabir za to radno mjesto.

2. Tijekom primjene upravnih i financijskih postupaka voditelj CERT-EU-a djeluje pod nadzorom Komisije.

3. Zadaće i aktivnosti CERT-EU-a, uključujući usluge koje CERT-EU u skladu s člankom 12. stavcima 2., 3., 4. i 6. te člankom 13. stavkom 1. pruža institucijama, tijelima i agencijama Unije financiranima iz naslova višegodišnjeg financijskog okvira namijenjenog europskoj javnoj upravi financiraju se iz posebne proračunske linije proračuna Komisije. Radna mjesta namijenjena CERT-EU-u detaljno se navode u bilješci uz plan radnih mjesta Komisije.

4. Institucije, tijela i agencije Unije osim onih iz stavka 3. daju godišnji financijski doprinos CERT-EU-u za pokrivanje usluga koje CERT-EU pruža u skladu s tim stavkom 3. Pojedini doprinosi temelje se na smjernicama koje je dao IICB i svi ih subjekti dogovaraju s CERT-EU-om u sporazumima o razini usluga. Doprinosi odgovaraju pravednom i razmjernom udjelu u ukupnim troškovima pruženih usluga. Zaprimaju se u posebnoj proračunskoj liniji iz stavka 3. kao namjenski prihod kako je predviđeno člankom 21. stavkom 3. točkom (c) Uredbe (EU, Euratom) 2018/1046 Europskog parlamenta i Vijeća[8].

5. Institucije, tijela i agencije Unije koji primaju usluge CERT-EU-a nadoknađuju troškove zadaća definiranih u članku 12. stavku 5. Prihodi se dodjeljuju proračunskim linijama kojima se financiraju navedeni troškovi.

Članak 16.

Suradnja CERT-EU-a s partnerima iz država članica

1. CERT-EU surađuje i razmjenjuje informacije s nacionalnim partnerima u državama članicama, uključujući CERT-ove, nacionalne centre za kibersigurnost, CSIRT-ove i jedinstvene kontaktne točke iz članka 8. Direktive [prijedlog NIS 2], o kiberprijetnjama, ranjivostima i incidentima, o mogućim protumjerama i o svim pitanjima važnima za poboljšanje zaštite informatičkog okruženja institucija, tijela i agencija Unije, među ostalim putem mreže CSIRT-ova iz članka 13. Direktive [prijedlog NIS 2].

2. CERT-EU može s nacionalnim partnerima u državama članicama razmjenjivati informacije o određenim incidentima bez suglasnosti pogođene sastavnice kako bi se olakšalo otkrivanje sličnih kiberprijetnji ili incidenata. Informacije o određenim incidentima kojima se otkriva identitet mete kiberincidenta CERT-EU može razmjenjivati samo uz suglasnost pogođene sastavnice.

---

[8] Uredba (EU, Euratom) 2018/1046 Europskog parlamenta i Vijeća od 18. srpnja 2018. o financijskim pravilima koja se primjenjuju na opći proračun Unije, o izmjeni uredaba (EU) br. 1296/2013, (EU) br. 1301/2013, (EU) br. 1303/2013, (EU) br. 1304/2013, (EU) br. 1309/2013, (EU) br. 1316/2013, (EU) br. 223/2014, (EU) br. 283/2014 i Odluke br. 541/2014/EU te o stavljanju izvan snage Uredbe (EU, Euratom) br. 966/2012 (SL L 193, 30.7.2018., str. 1.).

Članak 17.

Suradnja CERT-EU-a s partnerima iz trećih zemalja

1. CERT-EU može s partnerima iz trećih zemalja, uključujući partnere iz određenih industrijskih sektora, surađivati na pitanjima alata i metoda, kao što su tehnike, taktike, postupci i najbolja praksa, te na pitanjima kiberprijetnji i ranjivosti. Za suradnju s takvim partnerima, među ostalim u okvirima u kojima partneri koji nisu iz EU-a surađuju s nacionalnim partnerima iz država članica, CERT-EU mora zatražiti prethodno odobrenje IICB-a.
2. CERT-EU može surađivati s drugim partnerima, kao što su komercijalni subjekti, međunarodne organizacije, nacionalni subjekti izvan Europske unije ili pojedinačni stručnjaci, kako bi prikupio informacije o općim i specifičnim kiberprijetnjama, ranjivostima i mogućim protumjerama. Za širu suradnju s tim partnerima CERT-EU mora zatražiti prethodno odobrenje IICB-a.
3. Uz suglasnost sastavnice pogođene incidentom CERT-EU može informacije o incidentu podijeliti s partnerima koji mogu pridonijeti njegovoj analizi.

Poglavlje V.
OBVEZE SURADNJE I IZVJEŠĆIVANJA

Članak 18.

Postupanje s podacima

1. CERT-EU i institucije, tijela i agencije Unije moraju poštovati obvezu čuvanja poslovne tajne u skladu s člankom 339. Ugovora o funkcioniranju Europske unije ili jednakovrijednim primjenjivim okvirima.
2. Odredbe Uredbe (EZ) br. 1049/2001 Europskog parlamenta i Vijeća[9] primjenjuju se na zahtjeve za javni pristup dokumentima koje posjeduje CERT-EU, uključujući obvezu na temelju te uredbe u pogledu savjetovanja s drugim institucijama, tijelima i agencijama Unije kad se zahtjev odnosi na njihove dokumente.
3. Obrada osobnih podataka koja se provodi na temelju ove Uredbe podliježe Uredbi (EU) 2018/1725 Europskog parlamenta i Vijeća.
4. Postupanje CERT-EU-a i pripadajućih institucija, tijela i agencija Unije s podacima mora biti u skladu s pravilima utvrđenima u [predloženoj Uredbi o sigurnosti podataka].
5. Svi kontakti s CERT-EU-om koje pokrenu ili zatraže nacionalne sigurnosne i obavještajne službe priopćuju se bez nepotrebne odgode Glavnoj upravi Komisije za sigurnost i predsjedniku IICB-a.

Članak 19.

Obveze razmjene

1. Kako bi CERT-EU mogao koordinirati upravljanje ranjivostima i odgovor na incidente, može od institucija, tijela i agencija Unije zatražiti da mu iz svojih evidencija informatičkih sustava dostave informacije relevantne za pomoć koju pruža

[9] Uredba (EZ) br. 1049/2001 Europskog parlamenta i Vijeća od 30. svibnja 2001. o javnom pristupu dokumentima Europskog parlamenta, Vijeća i Komisije (SL L 145, 31.5.2001., str. 43.).

CERT-EU. Institucija, tijelo ili agencija kojoj je podnesen zahtjev bez nepotrebne odgode prenosi tražene informacije i sva njihova naknadna ažuriranja.

2. Institucije, tijela i agencije Unije na zahtjev CERT-EU-a i bez nepotrebne odgode dostavljaju CERT-EU-u digitalne informacije nastale upotrebom elektroničkih uređaja u predmetnim incidentima. CERT-EU može dodatno pojasniti koje su mu vrste tih digitalnih informacija potrebne za informiranost o stanju i odgovor na incident.

3. Informacije o određenim incidentima kojima se otkriva identitet institucije, tijela ili agencije Unije pogođene incidentom CERT-EU može razmjenjivati samo uz suglasnost tog subjekta. Informacije o određenim incidentima kojima se otkriva identitet mete kiberincidenta CERT-EU može razmjenjivati samo uz suglasnost subjekta pogođenog incidentom.

4. Obveze razmjene ne odnose se na klasificirane podatke EU-a (EUCI) ni na informacije koje je institucija, tijelo ili agencija Unije primila od sigurnosne ili obavještajne službe države članice ili tijela za izvršavanje zakonodavstva uz izričit uvjet da se one ne razmjenjuju s CERT-EU-om.

Članak 20.
Obveze obavješćivanja

1. Sve institucije, tijela i agencije Unije dostavljaju prvu obavijest CERT-EU-u o ozbiljnim kiberprijetnjama, znatnim ranjivostima i ozbiljnim incidentima bez nepotrebne odgode, a u svakom slučaju najkasnije 24 sata od saznanja o njima.

   U opravdanim slučajevima i u dogovoru s CERT-EU-om predmetna institucija, tijelo ili agencija Unije može odstupiti od roka utvrđenog u prethodnom stavku.

2. Osim toga, institucije, tijela i agencije Unije bez nepotrebne odgode obavješćuju CERT-EU o relevantnim tehničkim pojedinostima o kiberprijetnjama, ranjivostima i incidentima, a koje omogućuju poduzimanje mjera za otkrivanje, odgovor na incident ili ublažavanje. Obavijest obuhvaća, ako su dostupni:

   (a) relevantne pokazatelje ugroženosti;

   (b) relevantne mehanizme za otkrivanje;

   (c) mogući učinak;

   (d) relevantne mjere za ublažavanje.

3. CERT-EU jedanput mjesečno dostavlja ENISA-i sažeto izvješće koje uključuje anonimizirane i zbirne podatke o ozbiljnim kiberprijetnjama, znatnim ranjivostima i ozbiljnim incidentima prijavljenima u skladu sa stavkom 1.

4. IICB može izdati smjernice ili preporuke o modalitetima i sadržaju obavijesti. CERT-EU prosljeđuje odgovarajuće tehničke pojedinosti kako bi se institucijama, tijelima i agencijama Unije omogućilo poduzimanje proaktivnih mjera za otkrivanje, odgovor na incidente ili ublažavanje.

5. Obveze obavješćivanja ne odnose se na klasificirane podatke EU-a ni na informacije koje je institucija, tijelo ili agencija Unije primila od sigurnosne ili obavještajne službe države članice ili tijela za izvršavanje zakonodavstva uz izričit uvjet da se one ne dijele s CERT-EU-om.

Članak 21.

Koordinacija odgovora na incidente i suradnja na ozbiljnim incidentima

1. CERT-EU djeluje kao koordinacijsko čvorište za razmjenu informacija o kibersigurnosti i za odgovor na incidente te tako olakšava razmjenu informacija o kiberprijetnjama, ranjivostima i incidentima među:

   (a) institucijama, tijelima i agencijama Unije;

   (b) partnerima iz članaka 16. i 17.

2. CERT-EU olakšava koordinaciju odgovora na incidente među institucijama, tijelima i agencijama Unije, uključujući:

   (a) doprinos dosljednoj vanjskoj komunikaciji;

   (b) uzajamnu pomoć;

   (c) optimalnu upotrebu operativnih resursa;

   (d) koordinaciju s drugim mehanizmima za odgovor na krize na razini Unije.

3. CERT-EU pruža potporu institucijama, tijelima i agencijama Unije u pogledu informiranosti o kiberprijetnjama, ranjivostima i incidentima.

4. U slučaju ozbiljnih incidenata IICB izdaje smjernice o koordinaciji odgovora na incidente i suradnji. Ako se sumnja da je incident kaznene prirode, CERT-EU savjetuje o tome kako prijaviti incident tijelima za izvršavanje zakonodavstva.

Članak 22.

Veći napadi

1. CERT-EU koordinira odgovore na veće napade među institucijama, tijelima i agencijama Unije. Vodi evidenciju tehničkog stručnog znanja koje bi bilo potrebno za odgovor na incident u slučaju takvih napada.

2. Institucije, tijela i agencije Unije pridonose evidentiranju tehničkog stručnog znanja dostavljanjem popisa stručnjaka dostupnih u njihovim organizacijama; popis se ažurira jedanput godišnje, a sadržava pojedinosti o specifičnim tehničkim vještinama predmetnih stručnjaka.

3. U skladu s operativnim postupcima Zajedničke jedinice za kibersigurnost, CERT-EU uz odobrenje predmetnih institucija, tijela i agencija Unije može pozvati i stručnjake s popisa iz stavka 2. da pridonesu odgovoru na veći napad u državi članici.

Poglavlje VI.
ZAVRŠNE ODREDBE

Članak 23.

Početna preraspodjela proračunskih sredstava

Komisija predlaže preraspodjelu osoblja i financijskih sredstava iz relevantnih institucija, tijela i agencija Unije u proračun Komisije. Preraspodjela stupa na snagu istodobno s prvim proračunom koji se donese nakon stupanja na snagu ove Uredbe.

Članak 24.

Preispitivanje

1. IICB, uz pomoć CERT-EU-a, redovito izvješćuje Komisiju o provedbi ove Uredbe. IICB može Komisiji preporučiti i da predloži izmjene ove Uredbe.
2. Komisija Europskom parlamentu i Vijeću podnosi izvješće o provedbi ove Uredbe najkasnije 48 mjeseci od stupanja na snagu ove Uredbe, a nakon toga svake tri godine.
3. Komisija provodi evaluaciju ove Uredbe i podnosi izvješće Europskom parlamentu, Vijeću, Europskom gospodarskom i socijalnom odboru i Odboru regija najranije pet godina od stupanja na snagu ove Uredbe.

Članak 25.

Stupanje na snagu

Ova Uredba stupa na snagu dvadesetog dana od dana objave u *Službenom listu Europske unije*.

Ova je Uredba u cijelosti obvezujuća i izravno se primjenjuje u svim državama članicama.

Sastavljeno u Bruxellesu,

Za Europski parlament	*Za Vijeće*
Predsjednica	*Predsjednik*

ZAKONODAVNI FINANCIJSKI IZVJEŠTAJ

1. OKVIR PRIJEDLOGA/INICIJATIVE

1.1. Naslov prijedloga/inicijative

1.2. Predmetna područja politike

1.3. Prijedlog/inicijativa odnosi se na:

1.4. Ciljevi

1.4.1. Općí ciljevi

1.4.2. Posebni ciljevi

1.4.3. Očekivani rezultati i učinak

1.4.4. Pokazatelji uspješnosti

1.5. Osnova prijedloga/inicijative

1.5.1. Zahtjevi koje treba ispuniti u kratkoročnom ili dugoročnom razdoblju, uključujući detaljan vremenski plan provedbe inicijative.

1.5.2. Dodana vrijednost sudjelovanja Unije (može proizlaziti iz različitih čimbenika, npr. prednosti koordinacije, pravne sigurnosti, veće djelotvornosti ili komplementarnosti). Za potrebe ove točke „dodana vrijednost sudjelovanja Unije" vrijednost je koja proizlazi iz intervencije Unije i predstavlja dodatnu vrijednost u odnosu na vrijednost koju bi države članice inače ostvarile same.

1.5.3. Pouke iz prijašnjih sličnih iskustava

1.5.4. Usklađenost s višegodišnjim financijskim okvirom i moguće sinergije s drugim prikladnim instrumentima

1.5.5. Ocjena različitih dostupnih mogućnosti financiranja, uključujući mogućnost preraspodjele

1.6. Trajanje i financijski učinak prijedloga/inicijative

1.7. Predviđeni načini upravljanja

2. MJERE UPRAVLJANJA

2.1. Pravila praćenja i izvješćivanja

2.2. Sustavi upravljanja i kontrole

2.2.1. Obrazloženje načina upravljanja, mehanizama provedbe financiranja, načina plaćanja i predložene strategije kontrole

2.2.2. Informacije o utvrđenim rizicima i uspostavljenim sustavima unutarnje kontrole za ublažavanje rizika

2.2.3. Procjena i obrazloženje troškovne učinkovitosti kontrola (omjer troškova „kontrole i vrijednosti sredstava kojima se upravlja") i procjena očekivane razine rizika od pogreške (pri plaćanju i pri zaključenju)

2.3. Mjere za sprečavanje prijevara i nepravilnosti

3. PROCIJENJENI FINANCIJSKI UČINAK PRIJEDLOGA/INICIJATIVE

3.1. Naslovi višegodišnjeg financijskog okvira i proračunske linije rashoda na koje prijedlog/inicijativa ima učinak

3.2. Procijenjeni financijski učinak prijedloga na odobrena sredstva

3.2.1. Sažetak procijenjenog učinka na odobrena sredstva za poslovanje

3.2.2. Procijenjeni rezultati financirani odobrenim sredstvima za poslovanje

3.2.3. Sažetak procijenjenog učinka na administrativna odobrena sredstva

3.2.4. Usklađenost s aktualnim višegodišnjim financijskim okvirom

3.2.5. Doprinos trećih strana

3.3. Procijenjeni učinak na prihode

ZAKONODAVNI FINANCIJSKI IZVJEŠTAJ

1. OKVIR PRIJEDLOGA/INICIJATIVE

1.1. Naslov prijedloga/inicijative

Prijedlog uredbe Europskog parlamenta i Vijeća o mjerama za visoku zajedničku razinu kibersigurnosti u institucijama, tijelima, uredima i agencijama Unije

1.2. Predmetna područja politike

Europska javna uprava

Prijedlog se odnosi na mjere kojima se osigurava visoka zajednička razina kibersigurnosti u institucijama, tijelima i agencijama Unije

1.3. Prijedlog/inicijativa odnosi se na:

☑**novo djelovanje**

☐ **novo djelovanje nakon pilot-projekta/pripremnog djelovanja**[10]

☐ **produženje postojećeg djelovanja**

☑ **spajanje ili preusmjeravanje jednog ili više djelovanja u drugo/novo djelovanje**

1.4. Ciljevi

1.4.1. Opći ciljevi

– uspostaviti okvir za osiguravanje visoke zajedničke razine kibersigurnosti u institucijama, tijelima i agencijama Unije

– osigurati novu pravnu osnovu kako bi CERT-EU ojačao svoj mandat i financiranje

1.4.2. Posebni ciljevi

(1) utvrditi obveze institucija, tijela i agencija Unije da uspostave unutarnji okvir za upravljanje, opće upravljanje i kontrolu kibersigurnosnih rizika

(2) utvrditi obveze institucija, tijela i agencija Unije u pogledu izvješćivanja o unutarnjem okviru za upravljanje, opće upravljanje i kontrolu kibersigurnosnih rizika te o kiberincidentima

(3) utvrditi pravila o organizaciji i radu Centra za kibersigurnost institucija, tijela i agencija Unije (CERT-EU) te o organizaciji i radu Međuinstitucijskog odbora za kibersigurnost (IICB)

(4) pridonijeti Zajedničkoj jedinici za kibersigurnost

1.4.3. Očekivani rezultati i učinak

Navesti očekivane učinke prijedloga/inicijative na ciljane korisnike/skupine.

– unutarnji okviri za upravljanje, opće upravljanje i kontrolu kibersigurnosnih rizika, osnovni okviri za kibersigurnost, redovite procjene razvijenosti i planovi za kibersigurnost u institucijama, tijelima i agencijama Unije

[10] Kako je navedeno u članku 58. stavku 2. točkama (a) ili (b) Financijske uredbe.

– poboljšanje kiberotpornosti i sposobnosti odgovora na incidente u institucijama, tijelima i agencijama Unije – modernizacija CERT-EU-a – doprinos Zajedničkoj jedinici za kibersigurnost

1.4.4. Pokazatelji uspješnosti

Navesti pokazatelje za praćenje napretka i postignuća

– uspostavljeni okviri i osnovni okviri, redovite procjene razvijenosti i planovi za kibersigurnost u institucijama, tijelima i agencijama Unije – poboljšano rješavanje incidenata – bolja informiranost višeg rukovodstva institucija, tijela i agencija Unije o kibersigurnosnim rizicima – poravnanje izdataka za sigurnost IKT-a kao postotka ukupnih izdataka za IKT – kvalitetno vodstvo IICB-a i CERT-EU-a – povećana razmjena informacija među institucijama, tijelima i agencijama Unije i s relevantnim tijelima i dionicima u EU-u – pojačana suradnja u području kibersigurnosti s relevantnim tijelima i dionicima u EU-u putem CERT-EU-a i ENISA-e

1.5. Osnova prijedloga/inicijative

1.5.1. Zahtjevi koje treba ispuniti u kratkoročnom ili dugoročnom razdoblju, uključujući detaljan vremenski plan provedbe inicijative.

Prijedlogom se nastoji povećati razina kiberotpornosti institucija, tijela i agencija Unije, smanjiti nedosljednosti u otpornosti tih subjekata i poboljšati razina zajedničke informiranosti o situaciji i kolektivne sposobnosti za pripremu i odgovor. Prijedlog je u potpunosti dosljedan i usklađen s drugim povezanim inicijativama, a posebno s Prijedlogom direktive o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije i stavljanju izvan snage Direktive (EU) 2016/1148 [prijedlog NIS 2]. Prijedlog je bitan dio Strategije EU-a za sigurnosnu uniju i Strategije EU-a za kibersigurnost za digitalno desetljeće. Europska komisija trebala bi predložiti Uredbu u listopadu 2021., očekuje se da će je Europski parlament i Vijeće donijeti 2022., a odredbe će se primjenjivati od stupanja Uredbe na snagu. Predviđa se da će utjecaj na financijske i ljudske resurse naveden u ovom zakonodavnom financijskom izvještaju započeti 2023. Pripremno razdoblje već je započelo 2021., ali pripremne aktivnosti 2021. i 2022. nisu obuhvaćene financijskim učinkom prijedloga.

1.5.2. Dodana vrijednost sudjelovanja Unije (može proizlaziti iz različitih čimbenika, npr. prednosti koordinacije, pravne sigurnosti, veće djelotvornosti ili komplementarnosti). Za potrebe ove točke „dodana vrijednost sudjelovanja Unije" vrijednost je koja proizlazi iz intervencije Unije i predstavlja dodatnu vrijednost u odnosu na vrijednost koju bi države članice inače ostvarile same.

Razlozi za djelovanje na europskoj razini (*ex ante*)

Od 2019. do 2021. broj ozbiljnih incidenata koji pogađaju institucije, tijela i agencije Unije, a čiji su počinitelji akteri iz kategorije naprednih kontinuiranih prijetnji, znatno se povećao. U prvoj polovini 2021. zabilježen je isti broj ozbiljnih incidenata kao u cijeloj 2020. To se očituje i u broju forenzičkih prikaza (snimki sadržaja zahvaćenih sustava ili uređaja) koje je CERT-EU analizirao 2020., a koji se utrostručio u odnosu na 2019., dok se broj ozbiljnih incidenata od 2018. povećao za više od deset puta.

Razine razvijenosti kibersigurnosti znatno se razlikuju od tijela do tijela[11]. Ovom Uredbom osigurava se primjena osnovnog skupa sigurnosnih mjera u svim institucijama, tijelima i agencijama Unije te njihova međusobna suradnja u cilju otvorenog i učinkovitog funkcioniranja europske uprave.

Sustavi koje treba zaštititi u okviru su autonomije institucija, tijela i agencija Unije i oni tim sustavima upravljaju; države članice ne bi mogle poduzeti predložene radnje.

1.5.3. Pouke iz prijašnjih sličnih iskustava

Direktiva NIS prvi je horizontalni instrument unutarnjeg tržišta kojim se nastoji poboljšati otpornost mreža i sustava u Uniji na kibersigurnosne rizike. Od svojeg stupanja na snagu 2016. uvelike je pridonijela podizanju zajedničke razine kibersigurnosti među državama članicama. Prijedlogom direktive NIS2 te se mjere nastoje dodatno unaprijediti.

Uredbom se nastoje osigurati slične mjere za institucije, tijela i agencije Unije.

1.5.4. Usklađenost s višegodišnjim financijskim okvirom i moguće sinergije s drugim prikladnim instrumentima

Prijedlog je u skladu s višegodišnjim financijskim okvirom te je bitan dio Strategije EU-a za sigurnosnu uniju i Strategije EU-a za kibersigurnost za digitalno desetljeće.

Prijedlogom se predviđa primjena mjera za visoku zajedničku razinu kibersigurnosti na institucije, tijela i agencije Unije. Prijedlog je usklađen s Prijedlogom direktive o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije i stavljanju izvan snage Direktive (EU) 2016/1148 [prijedlog NIS 2].

1.5.5. Ocjena različitih dostupnih mogućnosti financiranja, uključujući mogućnost preraspodjele

Za upravljanje zadaćama CERT-EU-a potrebni su posebni profili i dodatno radno opterećenje koje se ne može podnijeti bez povećanja ljudskih i financijskih resursa.

[11] Referentni dokument: [Tematsko izvješće Europskog revizorskog suda o kibersigurnosti u institucijama, tijelima i agencijama Unije].

1.6. Trajanje i financijski učinak prijedloga/inicijative

☐ **ograničeno trajanje**

– ☐ na snazi od [DD/MM]GGGG do [DD/MM]GGGG

– ☐ financijski učinak od GGGG do GGGG za odobrena sredstva za preuzete obveze i od GGGG do GGGG za odobrena sredstva za plaćanje

☑ **neograničeno trajanje**

– financijski učinak trebao bi započeti prvim proračunom donesenim nakon stupanja Uredbe na snagu. Sredstva bi se iz proračuna institucija i glavnih tijela Unije preraspodijelila u proračun Komisije u prvoj godini, koja se smatra prijelaznom; ta i druga (pre)raspodjela sredstava odvijat će se u okviru godišnjih proračuna. Ako se Uredba donese 2022., financijska godina 2023. bit će prijelazno razdoblje, a 2024. odvijat će se u punom opsegu.

1.7. Predviđeni načini upravljanja[12]

☑ **izravno upravljanje** koje provodi Komisija i svaka institucija, tijelo i agencija Unije

– ☑ putem svojih službi, uključujući osoblje u delegacijama Unije

– ☐ putem izvršnih agencija

☐ **podijeljeno upravljanje** s državama članicama

☐ **neizravno upravljanje** povjeravanjem zadaća izvršenja proračuna:

– ☐ trećim zemljama ili tijelima koja su one odredile

– ☐ međunarodnim organizacijama i njihovim agencijama (navesti)

– ☐ EIB-u i Europskom investicijskom fondu

– ☐ tijelima iz članaka 70. i 71. Financijske uredbe

– ☐ tijelima javnog prava

– ☐ tijelima uređenima privatnim pravom koja pružaju javne usluge, u mjeri u kojoj daju odgovarajuća financijska jamstva

– ☐ tijelima uređenima privatnim pravom države članice kojima je povjerena provedba javno-privatnog partnerstva i koja daju odgovarajuća financijska jamstva

– ☐ osobama kojima je povjerena provedba određenih djelovanja u području ZVSP-a u skladu s glavom V. UEU-a i koje su navedene u odgovarajućem temeljnom aktu.

– *Ako je navedeno više načina upravljanja, potrebno je pojasniti u odjeljku „Napomene”.*

Napomene

Tijekom primjene upravnih i financijskih postupaka CERT-EU djeluje pod nadzorom Komisije.

[12] Informacije o načinima upravljanja i upućivanja na Financijsku uredbu dostupni su na internetskim stranicama BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx.

Dodatni resursi koji proizlaze iz nacrta Uredbe:

Provedba članaka 12. i 13. nacrta Uredbe rezultira proširenim katalogom usluga s dodatnim osnovnim uslugama. Kad se bude radilo u punom opsegu, bit će potrebni sljedeći dodatni resursi (do kraja VFO-a na kraju 2027.): 21 EPRV i 14,05 milijuna EUR.

Raspodjela dodatnih resursa u okviru proračuna prema različitim zadaćama:

(a) za obavljanje zadaća za institucije, tijela i agencije Unije navedene u članku 12. stavku 2. točkama (a), (b), (c) i (e): 13,75 EPRV-a i 11,275 milijuna EUR;

(b) za obavljanje zadaća navedenih u članku 12. stavku 3. (doprinos Zajedničkoj jedinici za kibersigurnost): 2 EPRV-a i 381 000 EUR;

(c) za obavljanje zadaća navedenih u članku 12. stavku 4. (strukturirana suradnja s ENISA-om): 0,25 EPRV-a i 236 000 EUR;

(d) za obavljanje zadaća navedenih u članku 12. stavku 6. (vježbe u području kibersigurnosti): 0,25 EPRV-a i 79 000 EUR;

(e) za obavljanje zadaća navedenih u članku 12. stavku 2. točki (d) i članku 13. (analiza i izvješćivanje o provedbi Uredbe, izrada smjernica, preporuka i poziva na djelovanje): 3,75 EPRV-a i 2,079 milijuna EUR;

(f) za obavljanje zadaća potpore tajništvu Međuinstitucijskog odbora za kibersigurnost (IICB): 1 EPRV.

Pregled trenutačnih resursa i prijelaz na puni opseg:

U rujnu 2021. CERT-EU poslovao je sa sljedećim resursima:

– stalna i upućena radna mjesta: 14 EPRV-a,

– ugovorno osoblje koje se financira u okviru sporazumâ o razini usluga: 24 EPRV-a,

– ukupno 38 EPRV-a.

Proračun CERT-EU-a za 2020. iznosio je: 250 000 EUR u okviru proračuna Komisije, 3,5 milijuna EUR iz namjenskih prihoda iz sporazumâ o razini usluga. Ukupno: 3,75 milijuna EUR. Riječ je o cijelom proračunu CERT-EU-a i on pokriva osposobljavanje, hardver, softver, službena putovanja, podršku, ugovorne agente i konferencije.

Nakon što Uredba stupi na snagu, predviđa se da će budući resursi CERT-EU-a iznositi:

– stalna radna mjesta: 34 EPRV-a,

– ugovorno osoblje: 15 EPRV-a,

– ukupno 49 EPRV-a, odnosno neto povećanje od 11 EPRV-a.

Promjenom u omjeru stalnih radnih mjesta i ugovornih agenata otklanja se kamen spoticanja u zapošljavanju i zadržavanju viših stručnjaka za kibersigurnost zbog njihove deficitarnosti na tržištu rada.

Osim toga, u Glavnoj upravi Komisije za informatiku bit će potreban 1 EPRV za ugovornog agenta za potporu IICB-u (Međuinstitucijski odbor za kibersigurnost).

Stoga će za provedbu Uredbe biti potreban ukupno 21 dodatni EPRV (20 EPRV-a za CERT-EU i 1 za Glavnu upravu Komisije za informatiku). To će se nadoknaditi istodobnim smanjenjem za 9 EPRV-a za ugovorne agente u CERT-EU-u za koje su se sredstva prethodno izdvajala iz namjenskog prihoda iz sporazumâ o razini usluga.

Nakon prijelaznog razdoblja proračun CERT-EU-a za 2024. koji nije namijenjen ljudskim resursima obuhvaćat će zadaće navedene u točkama od (a) do (e) i predviđeno je da će se financirati na sljedeći način:

– 8,921 milijun EUR godišnje od institucija Unije koje se financiraju u okviru naslova 7. proračuna Unije,

– 2,459 milijuna EUR od institucija, tijela i agencija Unije koje se financiraju u okviru naslova od 1. do 6. proračuna Unije,

– 2,670 milijuna EUR od institucija, tijela i agencija Unije koje se financiraju samostalno,

– ukupan proračun za CERT-EU: 14,05 milijuna EUR.

Zadaće navedene u članku 12. stavku 5. nisu opisane u katalogu usluga, riječ je o uslugama uz naknadu. To su pomoćne usluge koje predstavljaju relativno niske iznose, uglavnom su privremene, a troškovi tih usluga naplatit će se korisnicima usluga na temelju sporazumâ o razini usluga ili pisanih sporazuma.

Kad je riječ o doprinosima za osoblje CERT-EU-a: institucije i glavna tijela Unije pridonose pravednim udjelom koji je razmjeran odgovarajućem udjelu stalnih radnih mjesta razreda AD u predmetnoj organizaciji. Trebalo bi razmotriti mogu li i ECB i EIB dati pravedan doprinos upućivanjem stalnog osoblja.

2. MJERE UPRAVLJANJA

2.1. Pravila praćenja i izvješćivanja

Navesti učestalost i uvjete.

Komisija će, uz pomoć IICB-a i CERT-EU-a, povremeno preispitivati funkcioniranje Uredbe i izvješćivati Europski parlament i Vijeće, prvi put najkasnije 48 mjeseci od stupanja na snagu ove Uredbe, a nakon toga svake tri godine.

Izvori podataka koji se koriste za preispitivanja uglavnom bi bili iz IICB-a i CERT-EU-a. Osim toga, prema potrebi bi se mogli upotrebljavati specifični alati za prikupljanje podataka, npr. ankete institucija, tijela i agencija Unije, ENISA-e ili mreže CSIRT-ova.

2.2. Sustavi upravljanja i kontrole

2.2.1. Obrazloženje načina upravljanja, mehanizama provedbe financiranja, načina plaćanja i predložene strategije kontrole

Radnjama koje proizlaze iz Uredbe upravljat će se unutar svake institucije, tijela i agencije Unije u skladu s relevantnim primjenjivim pravilima i propisima svakog subjekta.

Administrativno i financijsko upravljanje aktivnostima CERT-EU-a integrirano je u administraciju Komisije te slijedi njezine primjenjive mehanizme upravljanja i provedbe, modalitete plaćanja i kontrole.

Unutarnji revizor Komisije ima iste ovlasti u odnosu na CERT-EU kao i u odnosu na službe Komisije.

2.2.2. Informacije o utvrđenim rizicima i uspostavljenim sustavima unutarnje kontrole za ublažavanje rizika

Vrlo nizak rizik, s obzirom na to da je CERT-EU administrativno već pridružen glavnom direktoru za informatiku kao radna skupina Komisije, a IICB je formiran po uzoru na sadašnji upravljački odbor CERT-EU-a. Ekosustav za financijsko upravljanje i unutarnju kontrolu stoga je već uspostavljen.

2.2.3. Procjena i obrazloženje troškovne učinkovitosti kontrola (omjer troškova „kontrole i vrijednosti sredstava kojima se upravlja”) i procjena očekivane razine rizika od pogreške (pri plaćanju i pri zaključenju)

Postupci za javnu nabavu, financijsko upravljanje i kontrolu već su uspostavljeni i dobro su ispitani. Troškovna učinkovitost kontrola i razine rizika od pogreške odgovaraju vrijednostima u svakoj instituciji, tijelu ili agenciji Unije te vrijednostima Komisije za aktivnosti CERT-EU-a.

2.3. Mjere za sprečavanje prijevara i nepravilnosti

Navesti postojeće ili predviđene mjere za sprečavanje i zaštitu, npr. iz strategije za borbu protiv prijevara.

Na aktivnosti CERT-EU-a primjenjuju se sustavi financijskog upravljanja i unutarnje kontrole Komisije.

Radi borbe protiv prijevara, korupcije i ostalih nezakonitih aktivnosti bez ograničenja se primjenjuju odredbe Uredbe (EU, Euratom) br. 883/2013 Europskog parlamenta i

Vijeća od 11. rujna 2013. o istragama koje provodi Europski ured za borbu protiv prijevara (OLAF).

3. PROCIJENJENI FINANCIJSKI UČINAK PRIJEDLOGA/INICIJATIVE

3.1. Naslovi višegodišnjeg financijskog okvira i proračunske linije rashoda na koje prijedlog/inicijativa ima učinak

- Postojeće proračunske linije

Prema redoslijedu naslova višegodišnjeg financijskog okvira i proračunskih linija.

Naslov višegodišnjeg financijskog okvira	Proračunska linija	Vrsta rashoda	Doprinos			
	Broj	dif./nedif.[13]	zemalja EFTA-e[14]	zemalja kandidatkinja[15]	trećih zemalja	u smislu članka 21. stavka 2. točke (b) Financijske uredbe
od 1. do 6.	Proračunske linije koje obuhvaćaju doprinos Unije decentraliziranim agencijama i tijelima	dif.	NE	NE	NE	NE
7.	Proračunske linije kojima se obuhvaćaju plaće osoblja, rashodi za IT i drugi administrativni rashodi u raznim odjeljcima proračuna EU-a	nedif.	NE	NE	NE	NE

- Zatražene nove proračunske linije

Prema redoslijedu naslova višegodišnjeg financijskog okvira i proračunskih linija.

Naslov višegodišnjeg financijskog okvira	Proračunska linija	Vrsta rashoda	Doprinos			
	Broj	dif./nedif.	zemalja EFTA-e	zemalja kandidatkinja	trećih zemalja	u smislu članka 21. stavka 2. točke (b) Financijske uredbe
	Nema		DA/NE	DA/NE	DA/NE	DA/NE

[13] Dif. = diferencirana odobrena sredstva; nedif. = nediferencirana odobrena sredstva.
[14] EFTA: Europsko udruženje slobodne trgovine.
[15] Zemlje kandidatkinje i, ako je primjenjivo, potencijalni kandidati sa zapadnog Balkana.

3.2. Procijenjeni financijski učinak prijedloga na odobrena sredstva

3.2.1. Sažetak procijenjenog učinka na odobrena sredstva za poslovanje

– ☐ Za prijedlog/inicijativu nisu potrebna odobrena sredstva za poslovanje.

– ☑ Za prijedlog/inicijativu potrebna su sljedeća odobrena sredstva za poslovanje:

U milijunima EUR (do 3 decimalna mjesta)

Naslov višegodišnjeg financijskog okvira	od 1. do 6.	Naslovi koji pokrivaju doprinose decentraliziranim agencijama i tijelima

Glavna uprava: više njih			Godina **2023.**	Godina **2024.**	Godina **2025.**	Godina **2026.**	Godina **2027.**	**UKUPNO**
○ Odobrena sredstva za poslovanje								
Proračunske linije koje obuhvaćaju doprinose Unije decentraliziranim agencijama (xx 10 xx xx)[16]	Obveze	(1a)	2,459	2,459	2,459	2,459	2,459	12,293
	Plaćanja	(2a)	2,459	2,459	2,459	2,459	2,459	12,293
Administrativna odobrena sredstva koja se financiraju iz omotnice za posebne programe[17]								
Proračunska linija		(3)						
UKUPNA odobrena sredstva za Glavnu upravu: više	Obveze	= 1a + 1b + 3	2,459	2,459	2,459	2,459	2,459	12,293
	Plaćanja	= 2a + 2b +3	2,459	2,459	2,459	2,459	2,459	12,293

[16] Prema službenoj proračunskoj nomenklaturi.

[17] Tehnička i/ili administrativna pomoć i rashodi za potporu provedbi programa i/ili djelovanja EU-a (prijašnje linije „BA”), neizravno istraživanje, izravno istraživanje.

○ UKUPNA odobrena sredstva za poslovanje	Obveze	(4)	2,459	2,459	2,459	2,459	2,459	12,293
	Plaćanja	(5)	2,459	2,459	2,459	2,459	2,459	12,293
○ UKUPNA administrativna odobrena sredstva koja se financiraju iz omotnice za posebne programe		(6)						
UKUPNA odobrena sredstva iz NASLOVA 1.–6. višegodišnjeg financijskog okvira	Obveze	= 4 + 6	2,459	2,459	2,459	2,459	2,459	12,293
	Plaćanja	= 5 + 6	2,459	2,459	2,459	2,459	2,459	12,293

Ako prijedlog/inicijativa utječe na više naslova za poslovanje, ponovite prethodni odjeljak:

○ UKUPNA odobrena sredstva za poslovanje (svi naslovi za poslovanje)	Obveze	(4)	2,459	2,459	2,459	2,459	2,459	12,293
	Plaćanja	(5)	2,459	2,459	2,459	2,459	2,459	12,293
UKUPNA administrativna odobrena sredstva koja se financiraju iz omotnice za posebne programe (svi naslovi za poslovanje)		(6)						
UKUPNA odobrena sredstva iz NASLOVA 1.–6. višegodišnjeg financijskog okvira (referentni iznos)	Obveze	= 4 + 6	2,459	2,459	2,459	2,459	2,459	12,293
	Plaćanja	= 5 + 6	2,459	2,459	2,459	2,459	2,459	12,293

Naslov višegodišnjeg financijskog okvira	7.	„Administrativni rashodi”

U ovaj se dio unose „administrativni proračunski podaci”, koji se najprije unose u prilog zakonodavnom financijskom izvještaju (Prilog V. internim pravilima), koji se učitava u sustav DECIDE za potrebe savjetovanja među službama.

U milijunima EUR (do 3 decimalna mjesta)

		Godina **2023.**	Godina **2024.**	Godina **2025.**	Godina **2026.**	**Godina 2027.**	**UKUPNO**
Glavna uprava: DIGIT (CERT-EU)							
○ Ljudski resursi		1,184	2,126	2,754	3,225	3,225	12,514
○ Ostali administrativni rashodi		7,938	8,921	8,921	8,921	8,921	43,622
UKUPNO GU DIGIT (CERT-EU)	Odobrena sredstva	9,122	11,047	11,675	12,146	12,146	56,136

UKUPNA odobrena sredstva iz NASLOVA 7. višegodišnjeg financijskog okvira	(ukupne obveze = ukupna plaćanja)	9,122	11,047	11,675	12,146	12,146	**56,136**

U milijunima EUR (do 3 decimalna mjesta)

		Godina 2023.	Godina 2024.	2025.	2026.	2027.	**UKUPNO**
UKUPNA odobrena sredstva iz NASLOVA 1.–7. višegodišnjeg financijskog okvira (*)	Obveze	11,581	13,506	14,134	14,605	14,605	68,429
	Plaćanja	11,581	13,506	14,134	14,605	14,605	68,429

(*) Doprinosi institucija, tijela i agencija Unije koji se financiraju samostalno procjenjuju se na 2,670 milijuna EUR godišnje (ukupno za pet godina 13,350 milijuna EUR). Ti će doprinosi biti namjenski prihodi za CERT-EU. Gornje tablice obuhvaćaju samo procijenjeni ukupni učinak na proračun Unije i ne obuhvaćaju te doprinose.

3.2.2. Procijenjeni rezultati financirani odobrenim sredstvima za poslovanje

Odobrena sredstva za preuzimanje obveza u milijunima EUR (do 3 decimalna mjesta)

Navesti ciljeve i rezultate ⇩			Godina **N**		Godina **N+1**		Godina **N+2**		Godina **N+3**		Unijeti onoliko godina koliko je potrebno za prikaz trajanja učinka (vidjeti točku 1.6.)						**UKUPNO**	
	REZULTATI																	
	Vrsta [18]	Prosječni trošak	Broj	Trošak	Broj	Trošak	Broj	Trošak	Broj	Trošak	Broj	Trošak	Broj	Trošak	Broj	Trošak	Ukupan broj	Ukupan trošak
POSEBNI CILJ br. 1[19]…																		
– Rezultat																		
– Rezultat																		
– Rezultat																		
Međuzbroj za posebni cilj br. 1																		
POSEBNI CILJ br. 2...																		
– Rezultat																		
Međuzbroj za posebni cilj br. 2																		
UKUPNO																		

[18] Rezultati se odnose na proizvode i usluge koji se isporučuju (npr.: broj financiranih studentskih razmjena, kilometri izgrađenih prometnica itd.).

[19] Kako je opisan u odjeljku 1.4.2. „Posebni ciljevi…".

3.2.3. Sažetak procijenjenog učinka na administrativna odobrena sredstva

– ☐ Za prijedlog/inicijativu nisu potrebna administrativna odobrena sredstva.

– ☑ Za prijedlog/inicijativu potrebna su sljedeća administrativna odobrena sredstva:

U milijunima EUR (do 3 decimalna mjesta)

	Godina 2023.	Godina 2024.	Godina 2025.	Godina 2026.	Godina 2027.	**UKUPNO**
NASLOV 7. višegodišnjeg financijskog okvira						
Ljudski resursi						
Stalno osoblje (razred AD)	1,099	2,041	2,669	3,14	3,14	12,089
Ugovorno osoblje	0,085	0,085	0,085	0,085	0,085	0,425
Ostali administrativni rashodi	7,938	8,921	8,921	8,921	8,921	43,622
Međuzbroj za NASLOV 7. višegodišnjeg financijskog okvira	9,122	11,047	11,675	12,146	12,146	56,136

Izvan NASLOVA 7.[20] of the multiannual financial framework						
Ljudski resursi						
Ostali administrativni rashodi						
Međuzbroj izvan NASLOVA 7. višegodišnjeg financijskog okvira						

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

Potrebna odobrena sredstva za ljudske resurse i ostale administrativne rashode pokrit će se odobrenim sredstvima glavne uprave koja su već dodijeljena za upravljanje djelovanjem i/ili su preraspodijeljena unutar glavne uprave te, prema potrebi, dodatnim sredstvima koja se mogu dodijeliti nadležnoj glavnoj upravi u okviru godišnjeg postupka dodjele sredstava uzimajući u obzir proračunska ograničenja.

[20] Tehnička i/ili administrativna pomoć i rashodi za potporu provedbi programa i/ili djelovanja EU-a (prijašnje linije „BA”), neizravno istraživanje, izravno istraživanje.

3.2.3.1. Procijenjene potrebe u pogledu ljudskih resursa

– ☐ Za prijedlog/inicijativu nisu potrebni ljudski resursi.

– ☑ Za prijedlog/inicijativu potrebni su sljedeći ljudski resursi:

Procjenu navesti u ekvivalentima punog radnog vremena

		Godina 2023.	Godina 2024.	Godina 2025.	Godina 2026.	Godina 2027.		
O Radna mjesta prema planu radnih mjesta (dužnosnici i privremeno osoblje)								
20 01 02 01 (sjedište i predstavništva Komisije)		7	13	17	20	20		
20 01 02 03 (delegacije)								
01 01 01 01 (neizravno istraživanje)								
01 01 01 11 (izravno istraživanje)								
Druge proračunske linije (navesti)								
O Vanjsko osoblje (u ekvivalentu punog radnog vremena: EPRV)[21]								
20 02 01 (UO, UNS, UsO iz „globalne omotnice")		1	1	1	1	1		
20 02 03 (UO, LO, UNS, UsO i MSD u delegacijama)								
XX 01 xx **yy zz** [22]	– u sjedištima							
	– u delegacijama							
01 01 01 02 (UO, UNS, UsO – neizravno istraživanje)								
01 01 01 12 (UO, UNS, UsO – izravno istraživanje)								
Druge proračunske linije (navesti)								
UKUPNO		**8**	**14**	**18**	**21**	**21**		

XX se odnosi na odgovarajuće područje politike ili glavu proračuna.

Potrebe za ljudskim resursima pokrit će se osobljem glavne uprave kojemu je već povjereno upravljanje djelovanjem i/ili koje je preraspoređeno unutar glavne uprave te, prema potrebi, resursima koji se mogu dodijeliti nadležnoj glavnoj upravi u okviru godišnjeg postupka dodjele sredstava uzimajući u obzir proračunska ograničenja.

Opis zadaća:

Dužnosnici i privremeno osoblje	Dužnosnici će provoditi zadaće i aktivnosti CERT-EU-a u skladu s Uredbom, a posebno poglavljima IV. i V.
Vanjsko osoblje	Ugovorni agent pomagat će u tajničkim funkcijama Međuinstitucijskog odbora za kibersigurnost.

[21] UO = ugovorno osoblje; LO = lokalno osoblje; UNS = upućeni nacionalni stručnjaci; UsO = ustupljeno osoblje; MSD = mladi stručnjaci u delegacijama.

[22] U okviru gornje granice za vanjsko osoblje iz odobrenih sredstava za poslovanje (prijašnje linije „BA").

3.2.4. Usklađenost s aktualnim višegodišnjim financijskim okvirom

Prijedlog/inicijativa:

– ☑ može se u potpunosti financirati preraspodjelom unutar relevantnog naslova višegodišnjeg financijskog okvira (VFO).

Objasniti o kakvom je reprogramiranju riječ te navesti predmetne proračunske linije i odgovarajuće iznose. U slučaju većeg reprogramiranja dostaviti tablicu u Excel formatu.

– ☐ zahtijeva upotrebu nedodijeljene razlike u okviru relevantnog naslova VFO-a i/ili upotrebu posebnih instrumenata kako su definirani u Uredbi o VFO-u.

Objasniti što je potrebno te navesti predmetne naslove i proračunske linije, odgovarajuće iznose te instrumente čija se upotreba predlaže.

– ☐ zahtijeva reviziju VFO-a.

Objasniti što je potrebno te navesti predmetne naslove i proračunske linije te odgovarajuće iznose.

3.2.5. Doprinos trećih strana

U prijedlogu/inicijativi:

– ☑ ne predviđa se sudjelovanje trećih strana u sufinanciranju[23].

– ☐ predviđa se sudjelovanje trećih strana u sufinanciranju prema sljedećoj procjeni:

Odobrena sredstva u milijunima EUR (do 3 decimalna mjesta)

	Godina **N**[24]	Godina **N+1**	Godina **N+2**	Godina **N+3**	Unijeti onoliko godina koliko je potrebno za prikaz trajanja učinka (vidjeti točku 1.6.)			Ukupno
Navesti tijelo koje sudjeluje u financiranju								
UKUPNO sufinancirana odobrena sredstva								

[23] Namjenski prihodi koji proizlaze iz povremenog pružanja usluga organizacijama koje nisu sastavnice predviđeni člankom 12. stavkom 5. točkom (c) nisu uzeti u obzir u procjeni jer bi trebali biti minimalni.

[24] Godina N jest godina početka provedbe prijedloga/inicijative. Umjesto „N” upisati predviđenu prvu godinu provedbe (na primjer: 2021.). Isto vrijedi i za ostale godine.

3.3. Procijenjeni učinak na prihode

– ☑ Prijedlog/inicijativa nema financijski učinak na prihode.

– ☐ Prijedlog/inicijativa ima sljedeći financijski učinak:

  – ☐ na vlastita sredstva

  – ☐ na ostale prihode

  – navesti jesu li prihodi namijenjeni proračunskim linijama rashoda ☐

U milijunima EUR (do 3 decimalna mjesta)

Proračunska linija prihoda:	Odobrena sredstva dostupna za tekuću financijsku godinu	Učinak prijedloga/inicijative[25]						
		Godina **N**	Godina **N+1**	Godina **N+2**	Godina **N+3**	Unijeti onoliko godina koliko je potrebno za prikaz trajanja učinka (vidjeti točku 1.6.)		
Članak …….								

Za namjenske prihode navesti odgovarajuće proračunske linije rashoda.

Ostale napomene (npr. metoda/formula za izračun učinka na prihode ili druge informacije)

[25] Kad je riječ o tradicionalnim vlastitim sredstvima (carine, pristojbe na šećer), navedeni iznosi moraju biti neto iznosi, to jest bruto iznosi nakon odbitka od 20 % na ime troškova naplate.