Svet
Evropske unije

Bruselj, 22. marec 2022
(OR. en)

7474/22

Medinstitucionalna zadeva:
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

PREDLOG

Pošiljatelj:	za generalno sekretarko Evropske komisije: direktorica Martine DEPREZ
Datum prejema:	22. marec 2022
Prejemnik:	generalni sekretar Sveta Evropske unije Jeppe TRANHOLM-MIKKELSEN
Št. dok. Kom.:	COM(2022) 122 final
Zadeva:	Predlog UREDBE EVROPSKEGA PARLAMENTA IN SVETA o določitvi ukrepov za visoko skupno raven kibernetske varnosti v institucijah, organih, uradih in agencijah Unije

Delegacije prejmejo priloženi dokument COM(2022) 122 final.

Priloga: COM(2022) 122 final

EVROPSKA
KOMISIJA

Bruselj, 22.3.2022
COM(2022) 122 final

2022/0085 (COD)

Predlog

UREDBA EVROPSKEGA PARLAMENTA IN SVETA

o določitvi ukrepov za visoko skupno raven kibernetske varnosti v institucijah, organih, uradih in agencijah Unije

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

OBRAZLOŽITVENI MEMORANDUM

1. OZADJE PREDLOGA

• Razlogi za predlog in njegovi cilji

Ta predlog vzpostavlja okvir za zagotavljanje skupnih pravil in ukrepov za kibernetsko varnost med institucijami, organi in agencijami Unije. Njegov namen je dodatno izboljšati odpornost vseh subjektov in njihove zmogljivosti za odzivanje na incidente. V skladu s prednostnimi nalogami Komisije se mora Evropa prilagoditi digitalni dobi in vzpostaviti gospodarstvo, pripravljeno na prihodnost, ki koristi ljudem. Poleg tega je zagotavljanje varne in odporne javne uprave temelj digitalne preobrazbe družbe kot celote.

Ta predlog temelji na strategiji EU za varnostno unijo (COM(2020) 605 final) in strategiji EU za kibernetsko varnost v digitalnem desetletju (JOIN(2020) 18 final).

Predlog posodablja obstoječi pravni okvir CERT-EU ter upošteva spremenjeno in večjo digitalizacijo institucij, organov in agencij v zadnjih letih ter razvijajoče se okolje kibernetskih groženj. Oboje se je od začetka krize zaradi COVID-19 še dodatno okrepilo, število incidentov pa se še naprej povečuje, pri čemer vse bolj izpopolnjeni napadi prihajajo iz različnih virov.

V predlogu je CERT-EU iz „skupine za odzivanje na računalniške grožnje “ preimenovan v „center za kibernetsko varnost“ za institucije, organe in agencije Unije, skladno z razvojem v državah članicah in v svetu, kjer je veliko skupin CERT preimenovanih v centre za kibernetsko varnost, vendar se kratica „CERT-EU“ ohranja zaradi prepoznavnosti imena.

• Skladnost z veljavnimi predpisi s področja zadevne politike

Ta predlog je namenjen izboljšanju kibernetske odpornosti institucij, organov in agencij Unije proti kibernetskim grožnjam, hkrati pa je skladen z obstoječo zakonodajo:

- Direktivo (EU) 2016/1148 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji. Skladen je tudi s predlogom Direktive (EU) XXXX/XXXX o ukrepih za visoko skupno raven kibernetske varnosti v Uniji in razveljavitvi Direktive (EU) 2016/1148 (predlog revidirane direktive o varnosti omrežij in informacijskih sistemov);
- Uredbo (EU) 2019/881 o Agenciji Evropske unije za kibernetsko varnost in o certificiranju informacijske in komunikacijske tehnologije na področju kibernetske varnosti (Akt o kibernetski varnosti);
- predlogom Uredbe (EU) XXXX/XXXX o informacijski varnosti v institucijah, organih, uradih in agencijah Unije;
- priporočilom Komisije z dne 23. junija 2021 o vzpostavitvi skupne kibernetske enote;
- Priporočilom Komisije (EU) 2017/1584 z dne 13. septembra 2017 o usklajenem odzivu na velike kibernetske incidente in krize.

Priloga k Priporočilu Komisije (EU) 2017/1584 z dne 13. septembra 2017 o usklajenem odzivu na velike kibernetske incidente in krize vsebuje načrt za usklajen odziv na velike čezmejne kibernetske incidente in krize.

Svet Evropske unije je v svoji resoluciji z dne 9. marca 2021 poudaril, da je kibernetska varnost ključna za delovanje javne uprave na nacionalni ravni in ravni EU ter za družbo in gospodarstvo kot celoti, pri čemer je poudaril pomen trdnega in skladnega varnostnega okvira

za zaščito vseh zaposlenih, podatkov, komunikacijskih omrežij, informacijskih sistemov in postopkov odločanja v EU. Zlasti se bo to doseglo z okrepljeno odpornostjo in boljšo varnostno kulturo institucij, organov in agencij Unije. Zagotovili naj bi se zadostni viri in zmogljivosti, tudi v okviru okrepitve pooblastil CERT-EU.

2. PRAVNA PODLAGA, SUBSIDIARNOST IN SORAZMERNOST

• Pravna podlaga

Pravna podlaga za to uredbo je člen 298 Pogodbe o delovanju Evropske unije (PDEU), ki določa, da institucije, organe, urade in agencije Unije pri izvajanju njihovih nalog podpira odprta, učinkovita in neodvisna evropska uprava. V skladu s kadrovskimi predpisi in pogoji za zaposlitev, sprejetimi na podlagi člena 336, Evropski parlament in Svet z uredbami, sprejetimi po rednem zakonodajnem postopku, v ta namen sprejmeta ustrezne določbe.

Informacijska tehnologija je institucijam, organom in agencijam Unije zagotovila nove načine dela, sodelovanja z državljani in izboljšanja splošnega delovanja. Hkrati z razvojem tehnologije se razvija tudi okolje kibernetskih groženj. Institucije, organi in agencije Unije so postali zelo privlačne tarče za izpopolnjene kibernetske napade. Zdi se, da vzpostavitev sistemov in zahtev za zagotavljanje kibernetske varnosti prispeva k učinkovitosti in neodvisnosti evropske uprave, tako da lahko institucije, organi in agencije Unije pri izvajanju svojih nalog v digitalnem svetu delujejo učinkoviteje.

Poleg tega so sedanje razlike med odnosom do kibernetske varnosti in pristopom na področju kibernetske varnosti, ki ju imajo institucije, organi in agencije Unije, kot je pojasnjeno v oddelku 3 v nadaljevanju, dodatne ovire za odprto, učinkovito in neodvisno evropsko upravo. Brez skupnega pristopa bi se odnos do kibernetske varnosti, ki ga imajo institucije, organi in agencije Unije, še naprej razvijal v različne smeri. Ta pravna podlaga je torej ustrezna glede na to, da je namen Uredbe vzpostaviti skupni pravni okvir za kibernetsko varnost v institucijah, organih, uradih in agencijah Unije.

• Subsidiarnost

Uredba o določitvi ukrepov za visoko skupno raven kibernetske varnosti v institucijah, organih, uradih in agencijah Unije spada v izključno pristojnost Unije.

• Sorazmernost

Pravila, predlagana v tej uredbi, ne presegajo tistega, kar je potrebno za zadovoljivo doseganje specifičnih ciljev. Predvideni ukrepi bodo prispevali k doseganju visoke skupne ravni kibernetske varnosti, ne da bi presegli tisto, kar je potrebno za doseganje cilja zaradi izpostavljenosti vse večjim tveganjem.

• Izbira instrumenta

Izbira Uredbe, ki se neposredno uporablja, se šteje za ustrezen pravni instrument za opredelitev in racionalizacijo obveznosti, naloženih institucijam, organom in agencijam Unije. Uredba je najustreznejši pravni instrument, da se omogočijo ciljno usmerjene izboljšave.

3. REZULTATI PREDHODNIH OCEN, POSVETOVANJ Z DELEŽNIKI IN OCEN UČINKA

• Predhodne ocene

CERT-EU je izvedel oceno glavnih kibernetskih groženj, ki so jim institucije, organi in agencije Unije trenutno izpostavljeni ali za katere obstaja verjetnost, da jim bodo izpostavljeni v bližnji prihodnosti.

V analizi so bile uporabljene tri kategorije opažanj:

- poskusi vdorov v infrastrukturo IT institucij, organov in agencij Unije (če so uspešni, se obravnavajo kot incidenti, v nasprotnem primeru pa se še vedno evidentirajo kot zaznani poskusi);
- grožnje, zaznane v bližini institucij, organov in agencij Unije (npr. v njihovih povezanih sektorjih, skupnostih njihovih deležnikov ali v Evropi);
- trendi velikih groženj, ugotovljeni na svetovni ravni.

Poleg tega je bilo v analizi preverjeno, kako večji stalni prehodi vplivajo na to, kako institucije Unije upravljajo in uporabljajo svojo infrastrukturo in storitve IT. Taki prehodi vključujejo:

- vse več dela na daljavo;
- migracijo sistemov v oblak;
- vse večje oddajanje storitev IT v zunanje izvajanje.

Med letoma 2019 in 2021 se je močno povečalo število pomembnih incidentov[1], ki so prizadeli institucije, organe in agencije Unije ter so jih izvedli akterji naprednih trajnih groženj. V prvi polovici leta 2021 se je zgodilo toliko pomembnih incidentov kot v vsem letu 2020. To dokazujejo tudi številni forenzični posnetki (posnetki vsebine prizadetih sistemov ali naprav), ki jih je CERT-EU analiziral v letu 2020 in so se v primerjavi z letom 2019 potrojili, število pomembnih incidentov pa se je od leta 2018 povečalo za več kot desetkrat.

Leta 2020 je usmerjevalni odbor CERT-EU določil nov strateški cilj za CERT-EU, da bi se zagotovila celovita ter ustrezno obsežna in poglobljena raven kibernetske obrambe za vse institucije, organe in agencije ter stalno prilagajanje sedanjim ali prihodnjim grožnjam, vključno z napadi na mobilne naprave, okolja v oblaku in naprave interneta stvari.

Komisija je kot dopolnitev k analizi groženj, ki jo je izvedel CERT-EU, izvedla oceno delovanja kibernetske varnosti 20 institucij, organov in agencij Unije. Tako je pridobila vpogled v ustaljene prakse na področju kibernetske varnosti in zmogljivosti za kibernetsko varnost z zunanjim primerjanjem nekaterih tehničnih varnostnih kontrol.

Ta ocena je temeljila na vprašalnikih, ki so jih izpolnile te institucije, organi in agencije, javno dostopnih podatkih ter podatkih, ki so jih neposredno zagotovili institucije, organi in agencije Unije. Zagotavlja dovolj dober vpogled v sedanjo situacijo za naslednje ugotovitve:

- zrelost kibernetske varnosti, velikost infrastrukture IT in ravni zmogljivosti se med ocenjenimi institucijami, organi in agencijami Unije močno razlikujejo;
- veliko institucij, organov in agencij Unije ima sicer na splošno zrele zmogljivosti za odkrivanje in odzivanje, vendar imajo v svojih zmogljivostih za upravljanje kibernetske varnosti različne ravni vgrajenega obvladovanja tveganj;
- okviri kibernetske varnosti (strategija, politika in baza pravil) ocenjenih institucij, organov in agencij Unije so na splošno dobro vzpostavljeni na ključnih področjih kibernetske varnosti, navedenih v Prilogi I k Uredbi, vendar nekatere institucije,

[1] „Pomembni incident“ pomeni vsak incident, razen če ima omejen učinek in obstaja verjetnost, da je z vidika metode ali tehnologije že dobro razumljen.

organi in agencije Unije nimajo zrelega upravljanja neprekinjenega poslovanja, skladnosti, revizije in stalnega izboljševanja;

- ugotovljeno je bilo, da so ocenjene institucije, organi in agencije Unije neenakomerno uporabljali tehnične ukrepe, ki se štejejo za dobre prakse.

Če povzamemo, analiza 20 institucij, organov in agencij Unije kaže, da se njihovo upravljanje, kibernetska higiena, splošna zmožnost in zrelost zelo razlikujejo. Zato je zahteva, da vse institucije, organi in agencije Unije izvedejo osnovne ukrepe za kibernetsko varnost, bistvena za obravnavo te razlike v zrelosti ter doseganje visoke skupne ravni kibernetske varnosti v vseh institucijah, organih in agencijah Unije.

Doslej še nobena zakonodaja Unije ni bila osredotočena na kibernetsko varnost institucij, organov in agencij Unije ter ni celovito obravnavala okolja kibernetskih groženj in nastajajočih tveganj za IT, ki so posledica digitalizacije.

- **Posvetovanja z deležniki**

Komisija se je posvetovala z deležniki iz vseh institucij, organov in agencij Unije ter predstavniki držav članic v Svetu in deležniki v Evropskem parlamentu. Predstavniki držav članic in ustrezni deležniki iz institucij, organov in agencij Unije so 25. junija 2021 sodelovali na delavnici, ki jo je organizirala Komisija in je bila namenjena razpravi o vsebini prihodnjega predloga uredbe.

- **Ocena učinka**

Učinek tega predloga bodo občutile institucije, organi in agencije Unije. Zaradi tega posebna ocena učinka ni potrebna, saj se ne bo uporabljal za države članice.

- **Temeljne pravice**

Evropska unija je zavezana zagotavljanju visokih standardov varstva temeljnih pravic. Vsa izmenjava informacij na podlagi te uredbe bi se izvajala v zaupanja vrednih okoljih ob popolnem spoštovanju pravice do varstva osebnih podatkov, kot je določena v členu 8 Listine Evropske unije o temeljnih pravicah in ustrezni zakonodaji o varstvu podatkov, zlasti Uredbi (EU) 2018/1725 Evropskega parlamenta in Sveta.

4. PRORAČUNSKE POSLEDICE

Tržna referenčna merila in študije[2] kažejo, da je neposredna poraba za kibernetsko varnost znašala 4–7 % skupnih izdatkov organizacij za IT. Vendar analiza groženj, ki jo je CERT-EU izvedel v podporo temu zakonodajnemu predlogu, kaže na to, da se mednarodni organi in politične organizacije srečujejo z večjimi tveganji, zato se zdi 10-odstotna raven porabe za IT za kibernetsko varnost ustreznejši cilj. Točnih stroškov takih prizadevanj ni mogoče določiti zaradi pomanjkanja podrobnih informacij o izdatkih institucij, organov in agencij Unije za IT ter ustreznem deležu porabe za kibernetsko varnost.

Torej je verjetno, da veliko institucij, organov in agencije Unije za kibernetsko varnost porabi manj, kot bi morali, vendar ta uredba ne bo povzročila velikega povečanja sedanjih izdatkov. Tudi brez Uredbe bi vsak subjekt moral zagotoviti ustrezno raven kibernetske varnosti. Z

[2] Vir: Gartner, „Identifying the Real Information Security Budget“ (Opredelitev dejanskega proračuna za informacijsko varnost) (2016). To je poleg posrednih izdatkov za varnost IT, na primer za varnost omrežja, kot so požarni zidovi, antivirusni programi in odgovornosti lastnika sistema, kot sta ocena tveganja in izvajanje varnostnih kontrol. V dokument iz leta 2020 je navedeno, da finančne institucij za kibernetsko varnost namenjajo 10–11 % porabe za IT, vir: DI_2020-FS-ISAC-Cybersecurity.pdf (deloitte.com).

Uredbo se nadaljuje prejšnje sodelovanje v usmerjevalnem odboru CERT-EU, v njej pa je formalizirana raven izmenjave informacij, ki delno obstaja že danes. Kot je podrobno navedeno v oceni finančnih posledic zakonodajnega predloga, bo CERT-EU potreboval dodatne vire za izpolnjevanje razširjene vloge, te vire pa bi bilo treba prerazporediti iz institucij, organov in agencij Unije, ki uporabljajo storitve CERT-EU.

5. DRUGI ELEMENTI

- **Ureditve izvajanja, spremljanja, ocenjevanja in poročanja**

Medinstitucionalni odbor za kibernetsko varnost (IICB) bi moral ob pomoči CERT-EU pregledati delovanje te uredbe, izvesti ocene in Komisiji predložiti poročilo z ugotovitvami. Komisija bi morala zagotoviti redno poročanje Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij.

CERT-EU lahko pripravi predlog smernic ali priporočilo, ki ga lahko IICB, če se tako odloči, sprejme. Smernice so posvetovalni dokument, namenjen vsem institucijam, organom in agencijam Unije ali njihovi podskupini, priporočilo pa je namenjeno posameznim institucijam, organom in agencijam Unije. Poziv k ukrepanje je posvetovalni dokument CERT-EU, ki opisuje nujne varnostne ukrepe, ki naj bi jih institucije, organi in agencije Unije nujno sprejeli v določenem časovnem obdobju.

- **Podrobnejša pojasnitev posameznih določb predloga**

Splošne določbe

Uredba določa ukrepe za zagotavljanje visoke skupne ravni kibernetske varnosti ter se uporablja za institucije, organe in agencije Unije, da bi ti lahko svoje naloge opravljali odprto, učinkovito in neodvisno (členi 1 do 3 in členi 23 do 25).

Ukrepi za visoko skupno raven kibernetske varnosti

Institucije, organi in agencije Unije morajo vzpostaviti notranji okvir za obvladovanje, upravljanje in nadzor tveganj za kibernetsko varnost, ki zagotavlja učinkovito in preudarno obvladovanje vseh tveganj za kibernetsko varnost. Poleg tega institucije, organi in agencije sprejmejo osnovne ukrepe za kibernetsko varnost za obravnavo tveganj, opredeljenih na podlagi okvira, izvajajo redne ocene zrelosti kibernetske varnosti in sprejmejo načrt za kibernetsko varnost (členi 4 do 8).

Medinstitucionalni odbor za kibernetsko varnost

Vzpostavi se Medinstitucionalni odbor za kibernetsko varnost, ki je odgovoren za spremljanje izvajanja te uredbe s strani institucij, organov in agencij Unije ter nadzor nad izvajanje splošnih prednostnih nalog in ciljev s strani CERT-EU, ki slednjemu zagotavlja tudi strateške usmeritve (členi 9 do 11).

CERT-EU

CERT-EU prispeva k varnosti okolja IT vseh institucij, organov in agencij Unije, tako da jim svetuje ter jim pomaga preprečiti, odkriti in ublažiti incidente in se odzivati nanje, deluje pa tudi kot njihovo vozlišče za izmenjavo informacij o kibernetski varnosti in za usklajevanje odzivanja na incidente (členi 12 do 17).

Obveznosti sodelovanja in poročanja

Uredba zagotavlja sodelovanje in izmenjavo informacij med CERT-EU ter institucijami, organi in agencijami Unije za ustvarjanje zaupanja. V ta namen lahko CERT-EU od institucij, organov in agencij Unije zahteva, naj mu zagotovijo ustrezne informacije, sam pa si lahko z

incidenti povezane informacije izmenjuje z institucijami, organi in agencijami Unije za olajšanje odkrivanja podobnih kibernetskih groženj ali incidentov brez soglasja prizadetega udeleženca. CERT-EU si lahko z incidenti povezane informacije, ki razkrivajo identiteto tarče kibernetskega incidenta, izmenjuje le s soglasjem prizadetega udeleženca.

Zlasti institucije, organi in agencije Unije CERT-EU nemudoma obvestijo o pomembnih kibernetskih grožnjah, pomembnih ranljivostih in pomembnih incidentih, vsekakor pa najpozneje 24 ur po seznanitvi z njimi (členi 18 do 22).

2022/0085 (COD)

Predlog

UREDBA EVROPSKEGA PARLAMENTA IN SVETA

o določitvi ukrepov za visoko skupno raven kibernetske varnosti v institucijah, organih, uradih in agencijah Unije

EVROPSKI PARLAMENT IN SVET EVROPSKE UNIJE STA –

ob upoštevanju Pogodbe o delovanju Evropske unije in zlasti člena 298 Pogodbe,

ob upoštevanju Pogodbe o ustanovitvi Evropske skupnosti za atomsko energijo in zlasti člena 106a Pogodbe,

ob upoštevanju predloga Evropske komisije,

po posredovanju osnutka zakonodajnega akta nacionalnim parlamentom,

v skladu z rednim zakonodajnim postopkom,

ob upoštevanju naslednjega:

(1) V digitalni dobi je informacijska in komunikacijska tehnologija temelj odprte, učinkovite in neodvisne uprave Unije. Razvijajoča se tehnologija ter vse večja kompleksnost in medsebojna povezanost digitalnih sistemov povečujejo tveganja za kibernetsko varnost, zaradi česar je uprava Unije ranljivejša za kibernetske grožnje in incidente, kar posledično ogroža neprekinjeno poslovanje uprave in zmogljivost zaščite podatkov. Večja uporaba storitev v oblaku, vsesplošna uporaba informacijskih tehnologij, visoka stopnja digitalizacije, delo na daljavo ter razvijajoča se tehnologija in povezljivost so danes ključne značilnosti vseh dejavnosti subjektov uprave Unije, vendar digitalna odpornost še ni zadostno vgrajena.

(2) Okolje kibernetskih groženj, ki so mu izpostavljeni institucije, organi in agencije Unije, se nenehno razvija. Taktike, tehnike in postopki, ki jih uporabljajo akterji groženj, se nenehno razvijajo, očitni motivi za take napade pa se le malo spreminjajo in zajemajo krajo dragocenih nerazkritih informacij, služenje denarja, manipulacijo z javnim mnenjem ali ogrožanje digitalne infrastrukture. Akterji kibernetske napade izvajajo vse pogosteje, njihove kampanje pa so vse bolj izpopolnjene in avtomatizirane, usmerjene v izpostavljene napadne površine, ki se širijo, ter hitro izkoriščajo ranljivosti.

(3) Okolja IT institucij, organov in agencij Unije so medsebojno povezana in imajo vgrajene podatkovne tokove, njihovi uporabniki pa tesno sodelujejo. Ta medsebojna povezava pomeni, da lahko ima vsaka motnja, tudi če je sprva omejena na eno institucijo, organ ali agencijo Unije, širše kaskadne učinke, ki lahko imajo daljnosežne in dolgotrajne negativne posledice za druge. Poleg tega so okolja IT nekaterih institucij, organov in agencij povezana z okolji IT držav članic, kar pomeni, da incident v enem subjektu Unije ogroža kibernetsko varnost okolij IT držav članic in obratno.

(4) Institucije, organi in agencije Unije so privlačne tarče, ki jih ogrožajo visoko usposobljeni in dobro podprti akterji groženj in tudi druge grožnje. Hkrati pa se raven

in zrelost kibernetske odpornosti ter sposobnost odkrivanja zlonamernih kibernetskih dejavnosti in odzivanja nanje med navedenimi subjekti močno razlikujejo. Zato je za delovanje evropske uprave nujno, da institucije, organi in agencije Unije dosežejo visoko skupno raven kibernetske varnosti z osnovnimi ukrepi za kibernetsko varnost (sklopom minimalnih pravil o kibernetski varnosti, ki jih morajo omrežja in informacijski sistemi ter njihovi upravljavci in uporabniki upoštevati, da čim bolj zmanjšajo tveganja za kibernetsko varnost), izmenjavo informacij in sodelovanjem.

(5) Cilj Direktive [predlog revidirane direktive o varnosti omrežij in informacijskih sistemov] o ukrepih za visoko skupno raven kibernetske varnosti v Uniji je nadalje izboljšati kibernetsko odpornost in zmogljivosti za odzivanje na incidente javnih in zasebnih subjektov, nacionalnih pristojnih organov in teles ter Unije kot celote. Zato morajo institucije, organi in agencije Unije temu slediti in zagotoviti pravila, ki so skladna z Direktivo [predlog revidirane direktive o varnosti omrežij in informacijskih sistemov] in izražajo njegovo raven ambicij.

(6) Za doseganje visoke skupne ravni kibernetske varnosti je nujno, da institucije, organi in agencije Unije vzpostavijo notranji okvir za obvladovanje, upravljanje in nadzor tveganj za kibernetsko varnost, ki zagotavlja učinkovito in preudarno obvladovanje vseh tveganj za kibernetsko varnost ter upošteva neprekinjeno poslovanje in krizno upravljanje.

(7) Zaradi razlik med institucijami, organi in agencijami Unije je potrebna prožnost v izvajanju, saj ena rešitev ne bo primerna za vse. Ukrepi za visoko skupno raven kibernetske varnosti ne bi smeli vključevati obveznosti, ki bi neposredno posegale v opravljanje nalog institucij, organov in agencij Unije ali posegale v njihovo institucionalno avtonomijo. Zato bi institucije, organi in agencije morali vzpostaviti lastne okvire za obvladovanje, upravljanje in nadzor tveganj za kibernetsko varnost ter sprejeti lastne osnovne ukrepe in načrte za kibernetsko varnost.

(8) Da institucijam, organom in agencijam Unije ne bi bilo naloženo nesorazmerno finančno in upravno breme, bi morale biti zahteve glede obvladovanja tveganj za kibernetsko varnost sorazmerne s tveganjem, ki ga pomenita zadevno omrežje in informacijski sistem, pri čemer bi bilo treba upoštevati dovršenost takih ukrepov. Institucije, organi in agencije Unije bi si morali za izboljšanje ravni kibernetske varnosti prizadevati za dodelitev ustreznega deleža proračuna za IT; dolgoročno bi si bilo treba prizadevati za cilj v višini 10 %.

(9) Za visoko skupno raven kibernetske varnosti mora imeti nadzor nad kibernetsko varnostjo najvišja raven upravljanja vsake institucije, organa in agencije Unije, ki bi morala odobriti osnovne ukrepe za kibernetsko varnost, ki bi morali obravnavati tveganja, opredeljena v okviru, ki ga vzpostavi vsaka institucija, organ in agencija. Obravnava kulture kibernetske varnosti, tj. dnevno izvajanje kibernetske varnosti, je sestavni del osnovnih ukrepov za kibernetsko varnost v vseh institucijah, organih in agencijah Unije.

(10) Institucije, organi in agencije Unije bi morali oceniti tveganja, povezana z odnosi z dobavitelji in ponudniki storitev, vključno s ponudniki shranjevanja podatkov, storitev obdelave ali upravljanih varnostnih storitev, ter sprejeti ustrezne ukrepe za njihovo obravnavo. Ti ukrepi bi morali biti del osnovnih ukrepov za kibernetsko varnost in podrobneje opredeljeni v smernicah ali priporočilih, ki jih izda CERT-EU. Pri pripravi ukrepov in smernic bi bilo treba ustrezno upoštevati zadevno zakonodajo in politike EU, vključno z ocenami tveganja in priporočili skupine za sodelovanje na področju varnosti omrežij in informacijskih sistemov, kot sta usklajena ocena tveganja v EU in

nabor orodij EU za kibernetsko varnost omrežij 5G. Poleg tega bi lahko bilo potrebno certificiranje ustreznih proizvodov, storitev in postopkov IKT, na podlagi specifičnih certifikacijskih shem za kibernetsko varnost EU, sprejetih v skladu s členom 49 Uredbe (EU) 2019/881.

(11) Generalni sekretarji institucij in organov Unije so maja 2011 sklenili, da bodo ustanovili predkonfiguracijsko skupino za skupino za odzivanje na računalniške grožnje za institucije, organe in agencije Unije (CERT-EU), ki jo bo nadziral medinstitucionalni usmerjevalni odbor. Julija 2012 so generalni sekretarji potrdili praktično ureditev in se dogovorili, da ohranijo CERT-EU kot stalno enoto, ki naj še naprej pomaga izboljševati splošno stopnjo varnosti informacijske tehnologije v institucijah, organih in agencijah Unije kot primer vidnega medinstitucionalnega sodelovanja na področju kibernetske varnosti. CERT-EU je bil septembra 2012 vzpostavljen kot projektna skupina Evropske komisije z medinstitucionalnimi pooblastili. Institucije in organi Unije so decembra 2017 sklenili medinstitucionalni dogovor o organizaciji in delovanju CERT-EU[3]. Ta ureditev bi se morala še naprej razvijati v podporo izvajanju te uredbe.

(12) CERT-EU bi bilo treba iz „skupine za odzivanje na računalniške grožnje “ preimenovati v „center za kibernetsko varnost“ za institucije, organe in agencije Unije, skladno z razvojem v državah članicah in v svetu, kjer je veliko skupin CERT preimenovanih v centre za kibernetsko varnost, vendar bi bilo treba kratico „CERT-EU“ ohraniti zaradi prepoznavnosti imena.

(13) Veliko kibernetskih napadov je del širših kampanj, usmerjenih v skupine institucij, organov in agencij Unije ali interesnih skupnosti, ki vključujejo institucije, organe in agencije Unije. Da bi omogočili proaktivno odkrivanje, odzivanje na incidente ali blažilne ukrepe, bi morali institucije, organi in agencije Unije CERT-EU obvestiti o pomembnih kibernetskih grožnjah, pomembnih ranljivostih in pomembnih incidentih ter deliti ustrezne tehnične podrobnosti, ki omogočajo odkrivanje ali blaženje podobnih kibernetskih groženj, ranljivosti in incidentov ter odzivanje nanje v drugih institucijah, organih in agencijah Unije. V skladu s pristopom, enakim tistemu, ki je predviden v Direktivi [predlog revidirane direktive o varnosti omrežij in informacijskih sistemov], bi morali subjekti, ko se seznanijo s pomembnim incidentom, v 24 urah CERT-EU predložiti začetno priglasitev. Taka izmenjava informacij bi morala CERT-EU omogočiti širjenje informacij drugim institucijam, organom in agencijam Unije ter tudi ustreznim sorodnim organom za pomoč pri zaščiti vseh okolij IT v Uniji in okolij IT sorodnih organov Unije pred podobnimi incidenti, grožnjami in ranljivostmi.

(14) Poleg tega, da se CERT-EU dodeli več nalog in razširjena vloga, bi moral biti ustanovljen tudi Medinstitucionalni odbor za kibernetsko varnost (IICB), ki bi moral olajšati doseganje visoke skupne ravni kibernetske varnosti med institucijami, organi in agencijami Unije s spremljanjem izvajanja te uredbe s strani institucij, organov in agencij Unije, nadzorovanjem izvajanja splošnih prednostnih nalog in ciljev s strani CERT-EU in zagotavljanjem strateških usmeritev CERT-EU. IICB bi moral zagotoviti zastopanost institucij ter vključevati predstavnike agencij in organov prek mreže agencij Unije.

(15) CERT-EU bi moral izvajanje ukrepov za visoko skupno raven kibernetske varnosti podpirati s predlogi za smernice in priporočila, naslovljenimi na IICB, ali z izdajo

[3] UL C 12, 13.1.2018, str. 1.

pozivov k ukrepanju. Take smernice in priporočila bi moral odobriti IICB. CERT-EU bi moral po potrebi izdati pozive k ukrepanju, ki opisujejo nujne varnostne ukrepe, ki naj bi jih institucije, organi in agencije Unije nujno sprejeli v določenem časovnem obdobju.

(16) IICB bi moral spremljati skladnost s to uredbo ter nadaljnje ukrepanje na podlagi smernic, priporočil in pozivov k ukrepanju, ki jih izda CERT-EU. V zvezi s tehničnimi vprašanji bi ga bilo treba podpreti s tehničnimi svetovalnimi skupinami, ki so sestavljene, kot se IICB zdi ustrezno, in ki bi morale tesno sodelovati s CERT-EU, institucijami, organi in agencijami Unije ter po potrebi z drugimi deležniki. IICB bi moral po potrebi izdati nezavezujoča opozorila in priporočiti revizije.

(17) CERT-EU bi moral imeti nalogo prispevati k varnosti okolja IT vseh institucij, organov in agencij Unije. Imeti bi moral vlogo, enakovredno imenovanemu koordinatorju za institucije, organe in agencije Unije, za namene usklajenega razkrivanja ranljivosti evropskemu registru ranljivosti iz člena 6 Direktive [predlog revidirane direktive o varnosti omrežij in informacijskih sistemov].

(18) Leta 2020 je usmerjevalni odbor CERT-EU določil nov strateški cilj za CERT-EU, da bi se zagotovila celovita ter ustrezno obsežna in poglobljena raven kibernetske obrambe za vse institucije, organe in agencije Unije ter stalno prilagajanje sedanjim ali prihodnjim grožnjam, vključno z napadi na mobilne naprave, okolja v oblaku in naprave interneta stvari. Strateški cilj vključuje tudi zelo različne centre za varnostne operacije, ki spremljajo omrežja, in spremljanje 24 ur na dan, sedem dni v tednu, za zelo resne grožnje. V zvezi z večjimi institucijami, organi in agencijami Unije bi moral CERT-EU podpirati njihove ekipe za varnost IT, vključno s primarnim spremljanjem 24 ur na dan, sedem dni v tednu. Manjšim in nekaj srednjim institucijam, organom in agencijam Unije bi CERT-EU moral zagotavljati vse storitve.

(19) CERT-EU bi moral tudi izpolnjevati vlogo, ki je zanj predvidena v Direktivi [predlog revidirane direktive o varnosti omrežij in informacijskih sistemov], v zvezi s sodelovanjem in izmenjavo informacij z mrežo skupin za odzivanje na incidente na področju računalniške varnosti (skupine CSIRT). Poleg tega bi moral CERT-EU v skladu s Priporočilom Komisije (EU) 2017/1584[4] sodelovati z zadevnimi deležniki in se z njimi usklajevati glede odzivanja. Za prispevanje k visoki ravni kibernetske varnosti v Uniji bi moral z nacionalnimi sorodnimi organi deliti informacije, povezane z incidenti. Prav tako bi moral sodelovati z drugimi javnimi in zasebnimi sorodnimi organi, tudi pri Natu, pri čemer sodelovanje predhodno odobri IICB.

(20) Pri podpori operativni kibernetski varnosti bi moral CERT-EU izkoriščati razpoložljivo strokovno znanje Agencije Evropske unije za kibernetsko varnost prek strukturiranega sodelovanja, kot je predvideno v Uredbi (EU) 2019/881 Evropskega parlamenta in Sveta[5]. Po potrebi bi bilo treba sprejeti posebne dogovore med tema dvema subjektoma, s katerimi bi določili praktično izvajanje takega sodelovanja in se izogibali podvajanju dejavnosti. CERT-EU bi moral z Agencijo Evropske unije za

[4] Priporočilo Komisije (EU) 2017/1584 z dne 13. septembra 2017 o usklajenem odzivu na velike kibernetske incidente in krize (UL L 239, 19.9.2017, str. 36).

[5] Uredba (EU) 2019/881 Evropskega parlamenta in Sveta z dne 17. aprila 2019 o Agenciji Evropske unije za kibernetsko varnost (ENISA) in o certificiranju informacijske in komunikacijske tehnologije na področju kibernetske varnosti ter razveljavitvi Uredbe (EU) št. 526/2013 (Akt o kibernetski varnosti) (UL L 151, 7.6.2019, str. 15).

kibernetsko varnost sodelovati v zvezi z analizo groženj in ji redno posredovati svoje poročilo o grožnjah.

(21) V podporo skupni kibernetski enoti, vzpostavljeni v skladu s priporočilom Komisije z dne 23. junija 2021[6], bi moral CERT-EU sodelovati z deležniki in si z njimi izmenjevati informacije, da bi se olajšalo operativno sodelovanje in se obstoječim mrežam omogočilo, da pri varovanju Unije uresničijo ves svoj potencial.

(22) Vsi osebni podatki, obdelani na podlagi te uredbe, bi se morali obdelovati v skladu z zakonodajo o varstvu podatkov, vključno z Uredbo (EU) 2018/1725 Evropskega parlamenta in Sveta[7].

(23) CERT-EU ter institucije, organi in agencije Unije bi morali z informacijami ravnati v skladu s pravili iz Uredbe [predlagana uredba o informacijski varnosti]. Za zagotavljanje usklajevanja glede varnostnih vprašanj bi bilo treba o vsakem stiku s CERT-EU, ki ga vzpostavijo ali nameravajo vzpostaviti nacionalne varnostne in obveščevalne službe, nemudoma obvestiti direktorat Evropske komisije za varnost in predsednika IICB.

(24) Ker so storitve in naloge CERT-EU v interesu vseh institucij, organov in agencij Unije, bi morala vsaka institucija, organ ali agencija Unije z izdatki za IT prispevati pravičen delež k tem storitvam in nalogam. Taki prispevki ne posegajo v proračunsko avtonomijo institucij, organov in agencij Unije.

(25) IICB bi moral ob pomoči CERT-EU pregledati in oceniti izvajanje te uredbe ter Komisiji poročati o svojih ugotovitvah. Na podlagi tega prispevka bi morala Komisija poročati Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij –

SPREJELA NASLEDNJO UREDBO:

Poglavje I
SPLOŠNE DOLOČBE

Člen 1
Predmet urejanja

Ta uredba določa:

(a) obveznosti za institucije, organe in agencije Unije, v skladu s katerimi morajo vzpostaviti notranji okvir za obvladovanje, upravljanje in nadzor tveganj za kibernetsko varnost;

(b) obveznosti za institucij, organe in agencije Unije glede obvladovanja tveganj za kibernetsko varnost in poročanja;

(c) pravila o organizaciji in delovanju centra za kibernetsko varnost za institucije, organe in agencije Unije (CERT-EU) ter o organizaciji in delovanju Medinstitucionalnega odbora za kibernetsko varnost.

---

[6] Priporočilo Komisije C(2021) 4520 z dne 23. junija 2021 o vzpostavitvi skupne kibernetske enote.

[7] Uredba (EU) 2018/1725 Evropskega parlamenta in Sveta z dne 23. oktobra 2018 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah, organih, uradih in agencijah Unije in o prostem pretoku takih podatkov ter o razveljavitvi Uredbe (ES) št. 45/2001 in Sklepa št. 1247/2002/ES (UL L 295, 21.11.2018, str. 39).

Člen 2

Področje uporabe

Ta uredba se uporablja za obvladovanje, upravljanje in nadzor tveganj za kibernetsko varnost, ki jih izvajajo vse institucije, organi in agencije Unije, ter za organizacijo in delovanje CERT-EU in Medinstitucionalnega odbora za kibernetsko varnost.

Člen 3

Opredelitev pojmov

V tej uredbi se uporabljajo naslednje opredelitve pojmov:

(1) „institucije, organi in agencije Unije“ pomeni institucije, organe in agencije Unije, ustanovljene s Pogodbo o Evropski uniji, Pogodbo o delovanju Evropske unije ali Pogodbo o ustanovitvi Evropske skupnosti za atomsko energijo ali na njihovi podlagi;

(2) „omrežje in informacijski sistem“ pomeni omrežje in informacijski sistem v smislu člena 4(1) Direktive [predlog revidirane direktive o varnosti omrežij in informacijskih sistemov];

(3) „varnost omrežij in informacijskih sistemov“ pomeni varnost omrežij in informacijskih sistemov v smislu člena 4(2) Direktive [predlog revidirane direktive o varnosti omrežij in informacijskih sistemov];

(4) „kibernetska varnost“ pomeni kibernetsko varnost v smislu člena 4(3) Direktive [predlog revidirane direktive o varnosti omrežij in informacijskih sistemov];

(5) „najvišja raven upravljanja“ pomeni vodjo, vodstvo ali organ za usklajevanje in nadzor na najvišji upravni ravni, ob upoštevanju ureditev upravljanja na visoki ravni v vsaki institucij, organu ali agenciji Unije;

(6) „incident“ pomeni incident v smislu člena 4(5) Direktive [predlog revidirane direktive o varnosti omrežij in informacijskih sistemov];

(7) „pomembni incident“ pomeni vsak incident, razen če ima omejen učinek in obstaja verjetnost, da je z vidika metode ali tehnologije že dobro razumljen;

(8) „večji napad“ pomeni vsak incident, ki zahteva več virov, kot jih imata na voljo prizadeta institucija, organ ali agencija Unije in CERT-EU;

(9) „obvladovanje incidentov“ pomeni obvladovanje incidenta v smislu člena 4(6) Direktive [predlog revidirane direktive o varnosti omrežij in informacijskih sistemov];

(10) „kibernetska grožnja“ pomeni kibernetsko grožnjo v smislu člena 2(8) Uredbe (EU) 2019/881;

(11) „pomembna kibernetska grožnja“ pomeni kibernetsko grožnjo z namenom, priložnostjo in zmožnostjo povzročiti pomemben incident;

(12) „ranljivost“ pomeni šibko točko v smislu člena 4(8) Direktive [predlog revidirane direktive o varnosti omrežij in informacijskih sistemov];

(13) „pomembna ranljivost“ pomeni ranljivost, ki bo, če bo izkoriščena, po vsej verjetnosti vodila do pomembnega incidenta;

(14) „tveganje za kibernetsko varnost“ pomeni vsako razumno določljivo okoliščino ali dogodek, ki ima lahko negativen učinek na varnost omrežja in informacijskih sistemov;

(15) „skupna kibernetska enota“ pomeni virtualno in fizično sodelovalno platformo za različne skupnosti za kibernetsko varnost v Uniji, s poudarkom na operativnem in tehničnem usklajevanju zoper večje čezmejne kibernetske grožnje in incidente v smislu priporočila Komisije z dne 23. junija 2021;

(16) „osnovni ukrepi za kibernetsko varnost“ pomeni sklop minimalnih pravil o kibernetski varnosti, ki jih morajo omrežja in informacijski sistemi ter njihovi upravljavci in uporabniki upoštevati, da zmanjšajo tveganja za kibernetsko varnost.

Poglavje II
UKREPI ZA VISOKO SKUPNO RAVEN KIBERNETSKE VARNOSTI

Člen 4
Obvladovanje, upravljanje in nadzor tveganj

1. Vsaka institucija, organ in agencija Unije vzpostavi lasten notranji okvir za obvladovanje, upravljanje in nadzor tveganj za kibernetsko varnost (v nadaljnjem besedilu: okvir) v podporo poslanstvu subjekta in izvajanju njegove institucionalne avtonomije. To delo nadzoruje najvišja raven upravljanja subjekta, da se zagotovi učinkovito in preudarno obvladovanje vseh tveganj za kibernetsko varnost. Okvir se vzpostavi najpozneje do …. [15 mesecev po začetku veljavnosti te uredbe].

2. Okvir zajema celotno okolje IT zadevne institucije, organa ali agencije, vključno z morebitnim okoljem IT v njenih prostorih, sredstvi in storitvami v okoljih računalništva v oblaku, ki jih upravlja zunanji izvajalec ali gostijo tretje osebe, mobilnimi napravami, korporativnimi omrežji, poslovnimi omrežji, ki niso povezana z internetom, in vsemi napravami, povezanimi z okoljem IT. Okvir upošteva neprekinjeno poslovanje in krizno upravljanje ter varnost dobavne verige in obvladovanje človeških tveganj, ki bi lahko vplivali na kibernetsko varnost zadevne institucije, organa ali agencije Unije.

3. Najvišja raven upravljanja vsake institucije, organa in agencije Unije zagotavlja nadzor nad skladnostjo svoje organizacije z obveznostmi, povezanimi z obvladovanjem, upravljanjem in nadzorom tveganj za kibernetsko varnost brez poseganja v dolžnosti drugih ravni upravljanja glede skladnosti in obvladovanja tveganja na njihovih področjih pristojnosti.

4. Vse institucije, organi in agencije Unije imajo vzpostavljene učinkovite mehanizme za zagotavljanje, da se za kibernetsko varnost nameni ustrezen delež proračuna za IT.

5. Vsaka institucija, organ in agencija Unije imenuje lokalnega uradnika za kibernetsko varnost ali enakovredno funkcijo, ki deluje kot njegova enotna kontaktna točka v zvezi z vsemi vidiki kibernetske varnosti.

Člen 5
Osnovni ukrepi za kibernetsko varnost

1. Najvišja raven upravljanja vsake institucije, organa in agencije Unije odobri osnovne ukrepe subjekta za kibernetsko varnost za obravnavo tveganj, opredeljenih v okviru iz člena 4(1). To stori v podporo svojemu poslanstvu in pri izvajanju svoje

institucionalne avtonomije. Osnovni ukrepi za kibernetsko varnost so vzpostavljeni najpozneje do ... [18 mesecev po začetku veljavnosti te uredbe] ter se nanašajo na področja iz Priloge I in ukrepe iz Priloge II.

2. Višje vodstvo vsake institucije, organa in agencije Unije redno opravlja posebno usposabljanje, da pridobi dovolj znanja in spretnosti za razumevanje in oceno tveganj za kibernetsko varnost in praks obvladovanja ter njihovega vpliva na delovanje organizacije.

Člen 6
Ocene zrelosti

Vsaka institucija, organ in agencija Unije najmanj vsaka tri leta izvede oceno kibernetskovarnostne zrelosti, ki vključuje vse elemente njenega okolja IT, kot je opisano v členu 4, ob upoštevanju ustreznih smernic in priporočil, sprejetih v skladu s členom 13.

Člen 7
Načrti za kibernetsko varnost

1. Najvišja raven upravljanja vsake institucije, organa in agencije Unije na podlagi sklepov ocene zrelosti in ob upoštevanju sredstev in tveganj, opredeljenih v skladu s členom 4, po vzpostavitvi okvira za obvladovanje, upravljanje in nadzor tveganj ter osnovnih ukrepov za kibernetsko varnost nemudoma odobri načrt za kibernetsko varnost. Cilj načrta je izboljšati splošno kibernetsko varnost zadevnega subjekta, s tem pa prispeva k doseganju ali zvišanju visoke skupne ravni kibernetske varnosti vseh institucij, organov in agencij Unije. V podporo poslanstvu subjekta na podlagi institucionalne avtonomije načrt vključuje najmanj področja, navedena v Prilogi I, ukrepe, navedene v Prilogi II, ter ukrepe v zvezi s pripravljenostjo na incidente, odzivanjem nanje in okrevanjem po njih, kot sta varnostno spremljanje in vodenje dnevnikov. Načrt se pregleda najmanj vsaka tri leta, in sicer na podlagi ocen zrelosti, izvedenih v skladu s členom 6.

2. Načrt za kibernetsko varnost vključuje vloge članov osebja in odgovornosti za njegovo izvajanje.

3. Načrt za kibernetsko varnost upošteva vse veljavne smernice in priporočila, ki jih izda CERT-EU.

Člen 8
Izvajanje

1. Institucije, organi in agencije Unije po zaključku ocen zrelosti te predložijo Medinstitucionalnemu odboru za kibernetsko varnost. Pripravijo varnostne načrte in Medinstitucionalni odbor za kibernetsko varnost obvestijo o njihovi pripravi. Na zahtevo odbora poročajo o posameznih vidikih tega poglavja.

2. Smernice in priporočila, izdani v skladu s členom 13, podpirajo izvajanje določb iz tega poglavja.

Poglavje III
MEDINSTITUCIONALNI ODBOR ZA KIBERNETSKO VARNOST

Člen 9
Medinstitucionalni odbor za kibernetsko varnost

1. Vzpostavi se Medinstitucionalni odbor za kibernetsko varnost (IICB).

2. IICB je odgovoren za:

   (a) spremljanje, kako institucije, organi in agencije Unije izvajajo to uredbo, ter

   (b) nadzor nad tem, kako CERT-EU izvaja splošne prednostne naloge in cilje, pri čemer IICB CERT-EU zagotavlja strateške usmeritve.

3. IICB sestavljajo trije predstavniki, ki jih imenuje mreža agencij Unije (EUAN) na predlog svojega svetovalnega odbora za IKT in ki zastopajo interese agencij in organov, ki upravljajo svoje okolje IT, ter po en predstavnik, ki ga imenuje vsak od spodaj navedenih:

   (a) Evropski parlament;

   (b) Svet Evropske unije;

   (c) Evropska komisija;

   (d) Sodišče Evropske unije;

   (e) Evropska centralna banka;

   (f) Evropsko računsko sodišče;

   (g) Evropska služba za zunanje delovanje;

   (h) Evropski ekonomsko-socialni odbor;

   (i) Evropski odbor regij;

   (j) Evropska investicijska banka;

   (k) Agencija Evropske unije za kibernetsko varnost.

   Članom lahko pomaga namestnik. Predsednik lahko povabi druge predstavnike zgoraj navedenih organizacij ali drugih institucij, organov in agencij Unije, da se udeležijo sestankov IICB brez pravice do glasovanja.

4. IICB sprejme svoj notranji poslovnik.

5. IICB v skladu z notranjim poslovnikom med svojimi člani imenuje predsednika za obdobje štirih let. Njegov namestnik postane polnopravni član IICB za enako obdobje.

6. IICB se sestane na pobudo predsednika, na zahtevo CERT-EU ali na zahtevo katerega koli člana.

7. Vsak član IICB ima en glas. IICB odločitve sprejema z navadno večino, razen če je v tej uredbi določeno drugače. Predsednik ne glasuje, razen v primeru neodločenega izida glasovanja, ko ima odločilni glas.

8. IICB lahko deluje po poenostavljenem pisnem postopku, ki se začne v skladu z notranjim poslovnikom IICB. V skladu s tem postopkom se zadevna odločitev šteje za odobreno v roku, ki ga določi predsednik, razen v primeru ugovora člana.

9. Vodja CERT-EU ali njegov ali njen namestnik se udeležuje sestankov IICB, razen če IICB odloči drugače.

10. Sekretariat IICB zagotavlja Komisija.

11. Predstavniki, ki jih mreža agencij Unije imenuje na predlog svetovalnega odbora za IKT, odločitve IICB posredujejo agencijam Unije ter skupnim podjetjem. Vsaka agencija in organ Unije ima pravico, da na predstavnike ali predsednika IICB naslovi katero koli vprašanje, za katero meni, da bi ga IICB moral obravnavati.

12. IICB lahko deluje po poenostavljenem pisnem postopku, ki ga začne predsednik, v skladu s katerim se zadevna odločitev šteje za odobreno v roku, ki ga določi predsednik, razen v primeru ugovora člana.

13. IICB lahko imenuje izvršni odbor, ki mu pomaga pri delu ter na katerega prenese nekaj svojih nalog in pooblastil. IICB določi poslovnik izvršnega odbora, vključno z njegovimi nalogami in pooblastili, ter mandat njegovih članov.

Člen 10
Naloge IICB

IICB pri izvrševanju svojih obveznosti zlasti:

(a) prouči vsa poročila, ki se zahtevajo od CERT-EU, o stanju izvajanja te uredbe s strani institucij, organov in agencij Unije;

(b) na podlagi predloga vodje CERT-EU odobri letni delovni program za CERT-EU in spremlja njegovo izvajanje;

(c) na podlagi predloga vodje CERT-EU odobri katalog storitev CERT-EU;

(d) na podlagi predloga, ki ga predloži vodja CERT-EU, odobri letno finančno načrtovanje prihodkov in izdatkov, vključno z osebjem, za dejavnosti CERT-EU;

(e) na podlagi predloga vodje CERT-EU odobri načine izvajanja sporazumov o ravni storitev;

(f) preveri in odobri letno poročilo, ki ga pripravi vodja CERT-EU ter zajema dejavnosti CERT-EU in upravljanje njegovih sredstev;

(g) odobri in spremlja ključne kazalnike uspešnosti za CERT-EU, opredeljene na predlog vodje CERT-EU;

(h) odobri dogovore o sodelovanju ter ureditve ali pogodbe o ravni storitev med CERT-EU in drugimi subjekti v skladu s členom 17;

(i) vzpostavi toliko tehničnih svetovalnih skupin, kot je potrebno za pomoč IICB pri njegovem delu, odobri njihov mandat in imenuje njihove predsednike.

Člen 11
Skladnost

IICB spremlja, kako institucije, organi in agencije Unije izvajajo to uredbo ter sprejete smernice, priporočila in pozive k ukrepanju. Kadar IICB ugotovi, da institucije, organi ali agencije Unije niso učinkovito uporabljale ali izvajale te uredbe ali smernic, priporočil in pozivov k ukrepanju, izdanih na podlagi te uredbe, lahko brez poseganja v notranje postopke zadevne institucije, organa ali agencije Unije:

(a) izda opozorilo; po potrebi zaradi velikega tveganja za kibernetsko varnost je krog prejemnikov opozorila ustrezno omejen;

(b) ustrezni službi za reviziji predlaga izvedbo revizije.

Poglavje IV
CERT-EU

Člen 12
Poslanstvo in naloge CERT-EU

1. Poslanstvo CERT-EU, samostojnega medinstitucionalnega centra za kibernetsko varnost za vse institucije, organe in agencije Unije, je prispevati k varnosti okolja netajnih podatkov IT vseh institucij, organov in agencij Unije, tako da jim svetuje glede kibernetske varnosti ter jim pomaga preprečiti, odkriti in ublažiti incidente ter se odzivati nanje, deluje pa tudi kot njihovo vozlišče za izmenjavo informacij o kibernetski varnosti in za usklajevanje odzivanja na incidente.

2. CERT-EU za institucije, organe in agencije Unije izvaja naslednje naloge:

   (a) podpira jih pri izvajanju te uredbe in prispeva k usklajevanju uporabe te uredbe z ukrepi iz člena 13(1) ali *ad hoc* poročili, ki jih zahteva IICB;

   (b) podpira jih s svežnjem storitev za kibernetsko varnost, opisanih v katalogu storitev CERT-EU (v nadaljnjem besedilu: osnovne storitve);

   (c) vzdržuje mrežo podobnih institucij, organov in agencij ter partnerjev za podporo storitev, kot so navedene v členih 16 in 17;

   (d) IICB opozori na katero koli vprašanje, ki se nanaša na izvajanje te uredbe ali smernic, priporočil in pozivov k ukrepanju;

   (e) poroča o kibernetskih grožnjah, ki so jim izpostavljeni institucije, organi in agencije Unije, ter prispeva k situacijskem zavedanju na področju kibernetske varnosti v EU.

3. CERT-EU prispeva k skupni kibernetski enoti, vzpostavljeni v skladu s priporočilom Komisije z dne 23. junija 2021, vključno na naslednjih področjih:

   (a) pripravljenost, obvladovanje incidentov, izmenjava informacij in odzivanje na krize na tehnični ravni v zvezi s primeri, povezanimi z institucijami, organi in agencijami Unije;

   (b) operativno sodelovanje v zvezi z mrežo skupin za odzivanje na incidente na področju računalniške varnosti (skupine CSIRT), vključno z vzajemno pomočjo, in širšo skupnostjo za kibernetsko varnost;

   (c) obveščevalni podatki o kibernetskih grožnjah, vključno s situacijskim zavedanjem;

   (d) vsaka tema, ki zahteva tehnično strokovno znanje CERT-EU na področju kibernetske varnosti.

4. CERT-EU strukturirano sodeluje z Agencijo Evropske unije za kibernetsko varnost pri krepitvi zmogljivosti, operativnem sodelovanju in dolgoročnih strateških analizah kibernetskih groženj v skladu z Uredbo (EU) 2019/881 Evropskega parlamenta in Sveta.

5. CERT-EU lahko zagotavlja naslednje storitve, ki niso opisane v njegovem katalogu storitev (v nadaljnjem besedilu: storitve, ki se zaračunajo):

   (a) storitve, ki podpirajo kibernetsko varnost okolja IT institucij, organov in agencij Unije, razen storitev iz odstavka 2, in sicer na podlagi sporazumov o ravni storitev in glede na razpoložljive vire;

   (b) storitve, ki podpirajo operacije ali projekte institucij, organov in agencij Unije za kibernetsko varnost, razen tistih za zaščito njihovih okolij IT, in sicer na podlagi pisnih dogovorov in s predhodno odobritvijo IICB;

   (c) storitve, ki podpirajo varnost okolja IT organizacij, ki niso institucije, organi in agencije Unije, ki tesno sodelujejo z institucijami, organi in agencijami Unije, ki so jim na primer bile dodeljene naloge ali odgovornosti v skladu s pravom Unije, na podlagi pisnih sporazumov in s predhodno odobritvijo IICB.

6. CERT-EU lahko organizira vaje na področju kibernetske varnosti ali priporoča udeležbo na obstoječih vajah, v tesnem sodelovanju z Agencijo Evropske unije za kibernetsko varnost, kadar se zdi primerno, da preizkusi raven kibernetske varnosti institucij, organov in agencij Unije.

7. CERT-EU lahko institucijam, organom in agencijam Unije zagotovi pomoč v zvezi z incidenti v tajnih okoljih IT, če to izrecno zahteva zadevni udeleženec.

Člen 13
Smernice, priporočila in pozivi k ukrepanju

1. CERT-EU podpira izvajanje te uredbe z izdajo:

   (a) pozivov k ukrepanju, ki opisujejo nujne varnostne ukrepe, ki naj bi jih institucije, organi in agencije Unije nujno sprejeli v določenem časovnem obdobju;

   (b) predlogov za IICB za smernice, naslovljene na vse ali podskupino institucij, organov in agencij Unije;

   (c) predlogov za IICB za priporočila, naslovljena na posamezne institucije, organe in agencije Unije.

2. Smernice in priporočila lahko vključujejo:

   (a) načine izvajanja obvladovanja tveganj za kibernetsko varnost in osnovnih ukrepov za kibernetsko varnost ali njihove izboljšave;

   (b) načine izvajanja ocen zrelosti in načrtov za kibernetsko varnost ter

   (c) kadar je primerno, uporabo skupne tehnologije, arhitekture in povezanih dobrih praks s ciljem doseganja interoperabilnosti in skupnih standardov v smislu člena 4(10) Direktive [predlog revidirane direktive o varnosti omrežij in informacijskih sistemov].

3. IICB lahko na predlog CERT-EU sprejme smernice ali priporočila.

4. IICB lahko CERT-EU naroči izdajo, umik ali spremembo predloga za smernice ali priporočila ali poziv k ukrepanju.

Člen 14
Vodja CERT-EU

Vodja CERT-EU IICB in njegovemu predsedniku redno posreduje poročila o delovanju CERT-EU, finančnem načrtovanju, prihodkih, izvrševanju proračuna, sporazumih o ravni storitev in sklenjenih pisnih sporazumih, sodelovanju s sorodnimi organi in partnerji ter službenih potovanjih osebja, vključno s poročili iz člena 10(1).

Člen 15
Finančne in kadrovske zadeve

1. Komisija po pridobitvi soglasne odobritve IICB imenuje vodjo CERT-EU. Posvetovanje z IICB se izvede v vseh fazah postopka pred imenovanjem vodje CERT-EU, zlasti pri pripravi razpisov prostega delovnega mesta, pregledovanju prijav in imenovanju izbirnih komisij v zvezi s tem delovnim mestom.

2. Pri uporabi upravnih in finančnih postopkov vodja CERT-EU deluje pod nadzorom Komisije.

3. Naloge in dejavnosti, vključno s storitvami, ki jih CERT-EU institucijam, organom in agencijam Unije zagotavlja v skladu s členom 12(2), (3), (4) in (6) ter členom 13(1) in so financirane iz razdelka večletnega finančnega okvira, namenjenega evropski javni upravi, se financirajo iz posebne proračunske vrstice proračuna Komisije. Delovna mesta, rezervirana za CERT-EU, se podrobneje opredelijo v opombi h kadrovskemu načrtu Komisije.

4. Institucije, organi in agencije Unije, razen tistih iz odstavka 3, CERT-EU zagotovijo letni finančni prispevek za kritje storitev, ki jih CERT-EU zagotavlja v skladu z odstavkom 3. Ustrezni prispevki temeljijo na usmeritvah IICB, o njih pa se vsak subjekt in CERT-EU dogovorita v sporazumih o ravni storitev. Prispevki pomenijo pravičen in sorazmeren delež skupnih stroškov zagotovljenih storitev. Zbirajo se na posebni proračunski vrstici iz odstavka 3 kot namenski prejemki, kot je določeno v členu 21(3), točka (c), Uredbe (EU, Euratom) 2018/1046 Evropskega parlamenta in Sveta[8].

5. Stroške nalog, opredeljenih v členu 12(5), krijejo institucije, organi in agencije Unije, ki prejemajo storitve CERT-EU. Prihodki se dodelijo proračunskim vrsticam, ki krijejo stroške.

Člen 16
Sodelovanje CERT-EU s sorodnimi organi iz držav članic

1. CERT-EU sodeluje in si izmenjuje informacije z nacionalnimi sorodnimi organi v državah članicah, vključno s skupinami CERT, nacionalnimi centri za kibernetsko varnost, skupinami CSIRT in enotnimi kontaktnimi točkami iz člena 8 Direktive [predlog revidirane direktive o varnosti omrežij in informacijskih sistemov], v zvezi s kibernetskimi grožnjami, ranljivostmi in incidenti, možnimi protiukrepi ter vsemi zadevami, pomembnimi za izboljšanje zaščite okolij IT institucij, organov in agencij

[8] Uredba (EU, Euratom) 2018/1046 Evropskega parlamenta in Sveta z dne 18. julija 2018 o finančnih pravilih, ki se uporabljajo za splošni proračun Unije, spremembi uredb (EU) št. 1296/2013, (EU) št. 1301/2013, (EU) št. 1303/2013, (EU) št. 1304/2013, (EU) št. 1309/2013, (EU) št. 1316/2013, (EU) št. 223/2014, (EU) št. 283/2014 in Sklepa št. 541/2014/EU ter razveljavitvi Uredbe (EU, Euratom) št. 966/2012 (UL L 193, 30.7.2018, str. 1).

Unije, vključno prek mreže skupin CSIRT iz člena 13 Direktive [predlog revidirane direktive o varnosti omrežij in informacijskih sistemov].

2. CERT-EU si lahko za olajšanje odkrivanja podobnih kibernetskih groženj in incidentov z nacionalnimi sorodnimi organi v državah članicah izmenjuje z incidenti povezane informacije brez soglasja prizadetega udeleženca. CERT-EU si lahko z incidenti povezane informacije, ki razkrivajo identiteto tarče kibernetskega incidenta, izmenjuje le s soglasjem prizadetega udeleženca.

Člen 17

Sodelovanje CERT-EU s sorodnimi organi, ki niso iz držav članic

1. CERT-EU lahko s sorodnimi organi, ki niso iz držav članic, vključno s sorodnimi organi iz posameznih industrijskih sektorjev, sodeluje v zvezi z orodji in metodami, kot so tehnike, taktike, postopki in dobre prakse, ter v zvezi s kibernetskimi grožnjami in ranljivostmi. Za vse sodelovanje s takimi sorodnimi organi, tudi kadar sorodni organi, ki niso iz EU, sodelujejo z nacionalnimi sorodnimi organi držav članic, CERT-EU pridobi predhodno soglasje IICB.

2. CERT-EU lahko za zbiranje informacij o splošnih in specifičnih kibernetskih grožnjah, ranljivostih in možnih protiukrepih sodeluje z drugimi partnerji, kot so komercialni subjekti, mednarodne organizacije, nacionalni subjekti, ki ne prihajajo iz Evropske unije, ali posamezni strokovnjaki. Za širše sodelovanje s takimi partnerji si CERT-EU pridobi predhodno soglasje IICB.

3. CERT-EU lahko s soglasjem udeleženca, ki ga je incident prizadel, partnerjem, ki lahko prispevajo k njegovi analizi, zagotovi z incidentom povezane informacije.

Poglavje V
OBVEZNOSTI SODELOVANJA IN POROČANJA

Člen 18

Ravnanje z informacijami

1. CERT-EU ter institucije, organi in agencije Unije spoštujejo obveznost varovanja poslovne skrivnosti v skladu s členom 339 Pogodbe o delovanju Evropske unije ali enakovrednimi veljavnimi okviri.

2. Določbe Uredbe (ES) št. 1049/2001 Evropskega parlamenta in Sveta[9] se uporabljajo v zvezi z zahtevami za dostop javnosti do dokumentov, ki jih ima CERT-EU, vključno z obveznostmi iz navedene Uredbe, da se je treba posvetovati z drugimi institucijami, organi in agencijami Unije, kadar se zahteva nanaša na njihove dokumente.

3. Obdelavo osebnih podatkov na podlagi te uredbe ureja Uredba (EU) 2018/1725 Evropskega parlamenta in Sveta.

4. CERT-EU ter njegove institucije, organi in agencije Unije s podatki ravnajo v skladu s pravili iz [predlagane uredbe o informacijski varnosti].

[9] Uredba (ES) št. 1049/2001 Evropskega parlamenta in Sveta z dne 30. maja 2001 o dostopu javnosti do dokumentov Evropskega parlamenta, Sveta in Komisije (UL L 145, 31.5.2001, str. 43).

5. O vsakem stiku s CERT-EU, ki ga vzpostavijo ali nameravajo vzpostaviti nacionalne varnostne in obveščevalne službe, se nemudoma obvestita direktorat Komisije za varnost in predsednik IICB.

Člen 19
Obveznosti izmenjave

1. Da bi CERT-EU lahko usklajeval obvladovanje ranljivosti in odzivanje na incidente, lahko institucije, organe in agencije Unije zaprosi za predložitev informacij iz njihovih zbirk sistemov IT, ki so pomembne za podporo CERT-EU. Zaprošena institucija, organ ali agencija nemudoma posreduje zahtevane informacije in vse njihove naknadne posodobitve.

2. Institucije, organi in agencije Unije na zahtevo CERT-EU nemudoma zagotovijo digitalne informacije, ustvarjene z elektronskimi napravami, uporabljenimi v zadevnih incidentih. CERT-EU lahko dodatno pojasni, katere vrste takih digitalnih informacij potrebuje za situacijsko zavedanje in odzivanje na incidente.

3. CERT-EU si lahko z incidenti povezane informacije, ki razkrivajo identiteto institucije, organa ali agencije Unije, ki jo je prizadel incident, izmenjuje le s soglasjem prizadetega subjekta. CERT-EU si lahko z incidenti povezane informacije, ki razkrivajo identiteto tarče kibernetskega incidenta, izmenjuje le s soglasjem subjekta, ki ga je prizadel incident.

4. Obveznosti izmenjave ne veljajo za tajne podatke EU in informacije, ki jih je institucija, organ ali agencija Unije prejela od varnostne ali obveščevalne službe ali organa kazenskega pregona države članice pod izrecnim pogojem, da se ne bodo delili s CERT-EU.

Člen 20
Obveznosti obveščanja

1. Vse institucije, organi in agencije Unije CERT-EU nemudoma predložijo začetno priglasitev o pomembnih kibernetskih grožnjah, pomembnih ranljivostih in pomembnih incidentih, vsekakor pa najpozneje 24 ur po seznanitvi z njimi.

   V ustrezno utemeljenih primerih in v dogovoru s CERT-EU lahko zadevna institucija, organ ali agencija Unije odstopa od roka, določenega v prejšnjem odstavku.

2. Institucije, organi in agencije Unije nadalje nemudoma obvestijo CERT-EU o ustreznih tehničnih podrobnostih o kibernetskih grožnjah, ranljivostih in incidentih, ki omogočajo odkrivanje, odzivanje na incidente ali blažilne ukrepe. Obvestilo vsebuje naslednje, če so na voljo:

   (a) ustrezne kazalnike ogroženosti;

   (b) ustrezne mehanizme odkrivanja;

   (c) možen učinek;

   (d) ustrezne blažilne ukrepe.

3. CERT-EU agenciji ENISA vsak mesec predloži zbirno poročilo, vključno z anonimiziranimi in zbirnimi podatki o pomembnih kibernetskih grožnjah, pomembnih ranljivostih in pomembnih incidentih, priglašenih v skladu z odstavkom 1.

4. IICB lahko izda smernice ali priporočila v zvezi z načini in vsebino obvestila. CERT-EU razširi ustrezne tehnične podrobnosti, da se institucijam, organom in agencijam Unije omogočijo proaktivno odkrivanje, odzivanje na incidente ali blažilni ukrepi.

5. Obveznosti obveščanja ne veljajo za tajne podatke EU in informacije, ki jih je institucija, organ ali agencija Unije prejela od varnostne ali obveščevalne službe ali organa kazenskega pregona države članice pod izrecnim pogojem, da se ne bodo delili s CERT-EU.

Člen 21

Usklajevanje odzivanja na incidente in sodelovanje pri pomembnih incidentih

1. CERT-EU, ki deluje kot vozlišče za izmenjavo informacij o kibernetski varnosti in usklajevanje odzivanja na incidente, olajša izmenjavo informacij v zvezi s kibernetskimi grožnjami, ranljivostmi in incidenti med:

   (a) institucijami, organi in agencijami Unije;

   (b) sorodnimi organi iz členov 16 in 17.

2. CERT-EU olajša usklajevanje med institucijami, organi in agencijami Unije v zvezi z odzivanjem na incidente, vključno s:

   (a) prispevkom k doslednemu zunanjemu komuniciranju;

   (b) medsebojno pomočjo;

   (c) optimalno uporabo operativnih virov;

   (d) usklajevanjem z drugimi mehanizmi za odzivanje na krize na ravni Unije.

3. CERT-EU podpira institucije, organe in agencije Unije v zvezi s situacijskim zavedanjem o kibernetskih grožnjah, ranljivostih in incidentih.

4. IICB izda smernice o usklajevanju odzivanja na incidente in sodelovanju pri pomembnih incidentih. Kadar obstaja sum, da je incident kaznivo dejanje, CERT-EU zagotovi smernice o tem, kako incident prijaviti organom kazenskega pregona.

Člen 22

Večji napadi

1. CERT-EU usklajuje odzive na večje napade med institucijami, organi in agencijami Unije. Vzdržuje zbirko tehničnega strokovnega znanja, ki bi bilo potrebno za odzivanje na incidente v primeru takih napadov.

2. Institucije, organi in agencije Unije prispevajo v zbirko tehničnega strokovnega znanja, tako da zagotovijo letno posodobljen seznam strokovnjakov, ki so na voljo v njihovih organizacijah, z navedbo posebnih tehničnih znanj in spretnosti strokovnjakov.

3. CERT-EU lahko z odobritvijo zadevnih institucij, organov in agencij Unije strokovnjake, navedene na seznamu iz odstavka 2, pozove, naj prispevajo k odzivanju na večji napad v državi članici, v skladu z operativnimi postopki skupne kibernetske enote.

Poglavje VI
KONČNE DOLOČBE

Člen 23
Začetne proračunske prerazporeditve

Komisija predlaga prerazporeditev osebja in finančnih virov iz zadevnih institucij, organov in agencij Unije v proračun Komisije. Prerazporeditev se izvede hkrati s sprejetjem prvega proračuna po začetku veljavnosti te uredbe.

Člen 24
Pregled

1. IICB ob pomoči CERT-EU redno poroča Komisiji o izvajanju te uredbe. IICB lahko Komisiji izda tudi priporočila, naj predlaga spremembe te uredbe.
2. Komisija poroča Evropskemu parlamentu in Svetu o izvajanju te uredbe najpozneje 48 mesecev po začetku veljavnosti te uredbe in nato vsaka tri leta.
3. Komisija oceni delovanje te uredbe in poroča Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij pet let po datumu začetka veljavnosti.

Člen 25
Začetek veljavnosti

Ta uredba začne veljati dvajseti dan po objavi v *Uradnem listu Evropske unije*.

Ta uredba je v celoti zavezujoča in se neposredno uporablja v vseh državah članicah.

V Bruslju,

Za Evropski parlament	*Za Svet*
predsednica	*predsednik*

OCENA FINANČNIH POSLEDIC ZAKONODAJNEGA PREDLOGA

1. OKVIR PREDLOGA/POBUDE

1.1. Naslov predloga/pobude

1.2. Zadevna področja

1.3. Ukrep, na katerega se predlog/pobuda nanaša

1.4. Cilji

1.4.1. Splošni cilji

1.4.2. Specifični cilji

1.4.3. Pričakovani rezultati in posledice

1.4.4. Kazalniki smotrnosti

1.5. Utemeljitev predloga/pobude

1.5.1. Potrebe, ki jih je treba zadovoljiti kratkoročno ali dolgoročno, vključno s podrobno časovnico za uvajanje ustreznih ukrepov za izvajanje pobude

1.5.2. Dodana vrednost ukrepanja Unije (ki je lahko posledica različnih dejavnikov, npr. boljšega usklajevanja, pravne varnosti, večje učinkovitosti ali dopolnjevanja). Za namene te točke je „dodana vrednost ukrepanja Unije“ vrednost, ki izhaja iz ukrepanja Unije in predstavlja dodatno vrednost poleg tiste, ki bi jo sicer ustvarile države članice same.

1.5.3. Spoznanja iz podobnih izkušenj v preteklosti

1.5.4. Skladnost z večletnim finančnim okvirom in možne sinergije z drugimi ustreznimi instrumenti

1.5.5. Ocena različnih razpoložljivih možnosti financiranja, vključno z možnostmi za prerazporeditev

1.6. Trajanje predloga/pobude in finančnih posledic

1.7. Načrtovani načini upravljanja

2. UKREPI UPRAVLJANJA

2.1. Pravila o spremljanju in poročanju

2.2. Upravljavski in kontrolni sistemi

2.2.1. Utemeljitev načinov upravljanja, mehanizmov financiranja, načinov plačevanja in predlagane strategije kontrol

2.2.2. Podatki o ugotovljenih tveganjih in vzpostavljenih sistemih notranjih kontrol za njihovo zmanjševanje

2.2.3. Ocena in utemeljitev stroškovne učinkovitosti kontrol (razmerje „stroški kontrol ÷ vrednost z njimi povezanih upravljanih sredstev“) ter ocena pričakovane stopnje tveganja napake (ob plačilu in ob zaključku)

2.3. Ukrepi za preprečevanje goljufij in nepravilnosti

3. OCENA FINANČNIH POSLEDIC PREDLOGA/POBUDE

3.1. Zadevni razdelki večletnega finančnega okvira in odhodkovne proračunske vrstice

3.2. Ocenjene finančne posledice predloga za odobritve

3.2.1. Povzetek ocenjenih posledic za odobritve za poslovanje

3.2.2. Ocenjene realizacije, financirane z odobritvami za poslovanje

3.2.3. Povzetek ocenjenih posledic za upravne odobritve

3.2.4. Skladnost z veljavnim večletnim finančnim okvirom

3.2.5. Udeležba tretjih oseb pri financiranju

3.3. Ocenjene posledice za prihodke

OCENA FINANČNIH POSLEDIC ZAKONODAJNEGA PREDLOGA

1. OKVIR PREDLOGA/POBUDE

1.1. Naslov predloga/pobude

Predlog uredbe Evropskega parlamenta in Sveta o določitvi ukrepov za visoko skupno raven kibernetske varnosti v institucijah, organih, uradih in agencijah Unije

1.2. Zadevna področja

Evropska javna uprava

Predlog se nanaša na ukrepe, ki zagotavljajo visoko skupno raven kibernetske varnosti v institucijah, organih in agencijah Unije.

1.3. Ukrep, na katerega se predlog/pobuda nanaša

☑**Nov ukrep**

☐ **Nov ukrep na podlagi pilotnega projekta / pripravljalnega ukrepa**[10]

☐ **Podaljšanje obstoječega ukrepa**

☑ **Združitev ali preusmeritev enega ali več ukrepov v drug/nov ukrep**

1.4. Cilji

1.4.1. Splošni cilji

– Vzpostaviti okvir za zagotavljanje visoke skupne ravni kibernetske varnosti v institucijah, organih in agencijah Unije.

– Zagotoviti novo pravno podlago za okrepitev pooblastil in financiranja CERT-EU.

1.4.2. Specifični cilji

(1) Določiti obveznosti za institucije, organe in agencije Unije v zvezi z vzpostavitvijo notranjega okvira za obvladovanje, upravljanje in nadzor tveganj za kibernetsko varnost.

(2) Določiti obveznosti za institucije, organe in agencije Unije za poročanje o njihovih okvirih za obvladovanje, upravljanje in nadzor tveganj za kibernetsko varnost ter o kibernetskih incidentih.

(3) Določiti pravila o organizaciji in delovanju centra za kibernetsko varnost za institucije, organe in agencije Unije (CERT-EU) ter o organizaciji in delovanju Medinstitucionalnega odbora za kibernetsko varnost (IICB).

(4) Prispevati k skupni kibernetski enoti.

1.4.3. Pričakovani rezultati in posledice

Navedite, kakšne učinke naj bi imel(-a) predlog/pobuda za upravičence/ciljne skupine.

– Notranji okviri za obvladovanje, upravljanje in nadzor tveganj za kibernetsko varnost, osnovni ukrepi za kibernetsko varnost, redne ocene zrelosti in načrti za kibernetsko varnost v institucijah, organih in agencijah Unije.

[10] Po členu 58(2)(a) oz. (b) finančne uredbe.

– Izboljšanje odpornosti kibernetske varnosti in zmogljivosti za odzivanje na incidente v institucijah, organih in agencijah Unije. – Posodobitev CERT-EU. – Prispevanje k skupni kibernetski enoti.

1.4.4. Kazalniki smotrnosti

Navedite, s katerimi kazalniki se bodo spremljali napredek in dosežki.

– Vzpostavljeni okviri in osnovni ukrepi, redne ocene zrelosti in načrti za kibernetsko varnost, izvedeni v institucijah, organih in agencijah Unije. – Izboljšano obvladovanje incidentov. – Večja ozaveščenost o tveganjih za kibernetsko varnost na višjih ravneh upravljanja v institucijah, organih in agencijah Unije. – Izravnava porabe za varnost IKT kot deleža skupne porabe za IKT. – Močno vodstvo IICB in CERT-EU. – Okrepljena izmenjava informacij med institucijami, organi in agencijami Unije ter z ustreznimi organi in deležniki v EU. – Boljše sodelovanje na področju kibernetske varnosti z ustreznimi organi in deležniki v EU prek CERT-EU in ENISA.

1.5. Utemeljitev predloga/pobude

1.5.1. Potrebe, ki jih je treba zadovoljiti kratkoročno ali dolgoročno, vključno s podrobno časovnico za uvajanje ustreznih ukrepov za izvajanje pobude

Cilj predloga je zvišati raven kibernetske odpornosti institucij, organov in agencij Unije, zmanjšati razlike v odpornosti med temi subjekti ter izboljšati raven skupnega situacijskega zavedanja in skupno zmogljivost za pripravo in odzivanje. Predlog je popolnoma skladen z drugimi povezanimi pobudami, zlasti s predlogom direktive o ukrepih za visoko skupno raven kibernetske varnosti v Uniji in razveljavitvi Direktive (EU) 2016/1148 [predlog revidirane direktive o varnosti omrežij in informacijskih sistemov]. Predlog je bistveni del strategije EU za varnostno unijo in strategije EU za kibernetsko varnost v digitalnem desetletju. Uredbo naj bi Evropska komisija predlagala oktobra 2021, Evropski parlament in Svet naj bi jo sprejela leta 2022, določbe pa se bodo uporabljale od začetka njene veljavnosti. Po predvidevanjih naj bi bil finančni in kadrovski učinek, začrtan v tej oceni finančnih posledic zakonodajnega predloga, viden v letu 2023. Pripravljalno obdobje se je že začelo leta 2021, vendar pripravljalne dejavnosti v letih 2021 in 2022 ne spadajo med finančne posledice predloga.

1.5.2. Dodana vrednost ukrepanja Unije (ki je lahko posledica različnih dejavnikov, npr. boljšega usklajevanja, pravne varnosti, večje učinkovitosti ali dopolnjevanja). Za namene te točke je „dodana vrednost ukrepanja Unije“ vrednost, ki izhaja iz ukrepanja Unije in predstavlja dodatno vrednost poleg tiste, ki bi jo sicer ustvarile države članice same.

Razlogi za ukrepanje na evropski ravni (predhodno)

Med letoma 2019 in 2021 se je močno povečalo število pomembnih incidentov, ki so prizadeli institucije, organe in agencije Unije ter so jih izvedli akterji naprednih trajnih groženj. V prvi polovici leta 2021 se je zgodilo toliko pomembnih incidentov kot v vsem letu 2020. To dokazujejo številni forenzični posnetki (posnetki vsebine prizadetih sistemov ali naprav), ki jih je CERT-EU analiziral v letu 2020 in so se v primerjavi z letom 2019 potrojili, število pomembnih incidentov pa se je od leta 2018 povečalo za več kot desetkrat.

Ravni zrelosti kibernetske varnosti se med subjekti zelo razlikujejo[11]. Ta uredba zagotavlja, da bodo vse institucije, organi in agencije Unije izvedli osnovne varnostne ukrepe in sodelovali drug z drugim s ciljem odprtega in učinkovitega delovanja uprave Unije.

Sistemi, ki se vzdržujejo, spadajo v okvir avtonomije institucij, organov in agencij Unije, ki jih tudi upravljajo; predlaganih ukrepov države članice ne morejo pripraviti.

1.5.3. Spoznanja iz podobnih izkušenj v preteklosti

Direktiva o varnosti omrežij in informacijskih sistemov je prvi horizontalni instrument notranjega trga, ki je namenjen povečanju odpornosti omrežij in sistemov v Uniji proti tveganjem za kibernetsko varnost. Od začetka veljavnosti leta 2016 je že veliko prispevala k zvišanju skupne ravni kibernetske varnosti v državah članicah. Namen predloga revidirane direktive o varnosti omrežij in informacijskih sistemov je še dodatno izboljšati te ukrepe.

Namen Uredbe je zagotoviti podobne ukrepe za institucije, organe in agencije Unije.

1.5.4. Skladnost z večletnim finančnim okvirom in možne sinergije z drugimi ustreznimi instrumenti

Predlog je skladen z večletnim finančnim okvirom ter je bistveni del strategije EU za varnostno unijo in strategije EU za kibernetsko varnost v digitalnem desetletju.

Predlog predvideva uporabo ukrepov za visoko skupno raven kibernetske varnosti za institucije, organe in agencije Unije. Predlog je skladen s predlogom direktive o ukrepih za visoko skupno raven kibernetske varnosti v Uniji in razveljavitvi Direktive (EU) 2016/1148 [predlog revidirane direktive o varnosti omrežij in informacijskih sistemov].

1.5.5. Ocena različnih razpoložljivih možnosti financiranja, vključno z možnostmi za prerazporeditev

Upravljanje nalog s strani CERT-EU zahteva posebne profile in dodatno delovno obremenitev, ki je ni mogoče prevzeti brez povečanja človeških in finančnih virov.

[11] Sklic: [posebno poročilo Evropskega računskega sodišča o kibernetski varnosti v institucijah, organih in agencijah Unije].

1.6. Trajanje predloga/pobude in finančnih posledic

☐ **Časovno omejeno**

– ☐ od [D. MMMM] LLLL do [D. MMMM] LLLL,

– ☐ finančne posledice med letoma LLLL in LLLL za odobritve za prevzem obveznosti ter med letoma LLLL in LLLL za odobritve plačil.

☑ **Časovno neomejeno**

– Finančne posledice bi se morale začeti s sprejetjem prvega proračuna po začetku veljavnosti Uredbe. Prerazporeditev virov z institucij in glavnih organov Unije na Komisijo bi bila izvedena v prvem letu, ki se šteje za prehodno leto; ta in druge (pre)razporeditve virov bodo izvedene v okviru letnih proračunov. Če bo Uredba sprejeta leta 2022, bo proračunsko leto 2023 prehodno obdobje, proračunsko leto 2024 pa se bo izvajalo v polnem obsegu.

1.7. Načrtovani načini upravljanja[12]

☑ **Neposredno upravljanje** s strani Komisije ter vsake institucije, organa in agencije Unije

– ☑ z lastnimi službami, vključno s svojim osebjem v delegacijah Unije,

– ☐ prek izvajalskih agencij.

☐ **Deljeno upravljanje** z državami članicami.

☐ **Posredno upravljanje**, tako da se naloge izvrševanja proračuna poverijo:

– ☐ tretjim državam ali organom, ki jih te imenujejo,

– ☐ mednarodnim organizacijam in njihovim agencijam (navedite),

– ☐ EIB in Evropskemu investicijskemu skladu,

– ☐ organom iz členov 70 in 71 finančne uredbe,

– ☐ subjektom javnega prava,

– ☐ subjektom zasebnega prava, ki opravljajo javne storitve, kolikor ti subjekti zagotavljajo ustrezna finančna jamstva,

– ☐ subjektom zasebnega prava države članice, ki so pooblaščeni za izvajanje javno-zasebnih partnerstev in ki zagotavljajo ustrezna finančna jamstva,

– ☐ osebam, pooblaščenim za izvajanje določenih ukrepov SZVP na podlagi naslova V PEU in opredeljenim v zadevnem temeljnem aktu.

– *Pri navedbi več kot enega načina upravljanja je treba to natančneje obrazložiti v oddelku „opombe“.*

Opombe

CERT-EU pri uporabi upravnih in finančnih postopkov deluje pod nadzorom Komisije. Dodatni viri, ki izhajajo iz osnutka uredbe: Zaradi izvajanja členov 12 in 13 osnutka uredbe se katalog storitev poveča z dodatnimi osnovnimi storitvami. Ob izvajanju v polnem obsegu bodo potrebni naslednji dodatni viri (do konca večletnega finančnega okvira konec leta 2027): 21 EPDČ in 14,05 milijona EUR.

[12] Pojasnila o načinih upravljanja in sklici na finančno uredbo so na voljo na spletišču BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx.

Razčlenitev dodatnih virov iz proračuna za različne naloge je naslednja:

(a) za opravljanje nalog za institucije, organe in agencije Unije, podrobno opredeljenih v členu 12(2), točke (a), (b), (c) in (e): 13,75 EPDČ in 11,275 milijona EUR;

(b) za opravljanje nalog, podrobno opredeljenih v členu 12(3) (prispevek za skupno kibernetsko enoto): 2 EPDČ in 381 000 EUR;

(c) za opravljanje nalog, podrobno opredeljenih v členu 12(4) (strukturirano sodelovanje z ENISA): 0,25 EPDČ in 236 000 EUR;

(d) za opravljanje nalog, podrobno opredeljenih v členu 12(6) (vaje na področju kibernetske varnosti): 0,25 EPDČ in 79 000 EUR;

(e) za opravljanje nalog, podrobno opredeljenih v členu 12(2), točka (d), in členu 13 (analiza in poročanje o izvajanju Uredbe, priprava smernic, priporočil in pozivov k ukrepanju): 3,75 EPDČ in 2,079 milijona EUR;

(f) za opravljanje nalog v podporo sekretariatu Medinstitucionalnega odbora za kibernetsko varnost (IICB): 1 EPDČ.

Pregled sedanjih virov in prehod na izvajanje v polnem obsegu:

Septembra 2021 je CERT-EU deloval z naslednjimi viri:

– stalna delovna mesta in delovna mesta za napoteno osebje: 14 EPDČ,

– pogodbeni uslužbenci, financirani iz sporazumov o ravni storitev: 24 EPDČ,

– skupaj 38 EPDČ.

Leta 2020 je proračun CERT-EU znašal: 250 000 EUR iz proračuna Komisije, 3,5 milijona EUR iz namenskih prejemkov na podlagi sporazumov o ravni storitev. Skupaj: 3,75 milijona EUR. To je pomenilo celoten proračun CERT-EU za usposabljanje, strojno in programsko opremo, službena potovanja, podporo, pogodbene uslužbence in konference.

Ko bo Uredba začela veljati, bodo predvideni prihodnji viri CERT-EU naslednji:

– stalna delovna mesta: 34 EPDČ,

– pogodbeni uslužbenci: 15 EPDČ,

– skupaj 49 EPDČ, kar pomeni neto povečanje za 11 EPDČ.

Sprememba v razmerju med stalnimi delovnimi mesti in pogodbenimi uslužbenci se nanaša na pomembno oviro pri zaposlovanju in zadržanju izkušenih strokovnjakov za kibernetsko varnost, ker jih je na trgu dela premalo.

Poleg tega bo v Generalnem direktoratu za informatiko Komisije potreben pogodbeni uslužbenec z 1 EPDČ za podporo IICB (Medinstitucionalni odbor za kibernetsko varnost).

Skupaj bo tako za izvajanje Uredbe potrebnih 21 dodatnih EPDČ (20 EPDČ za CERT-EU in en za Generalni direktorat za informatiko Komisije). To bo izravnano z vzporednim zmanjšanjem števila pogodbenih uslužbencev za 9 EPDČ, ki so se prej financirali iz namenskih prejemkov na podlagi sporazumov o ravni storitev.

Proračun CERT-EU za vire, ki niso človeški viri, bo leta 2024 po prehodnem obdobju kril naloge, navedene zgoraj v točkah (a) do (e), financiral pa naj bi se, kot sledi:

– 8,921 milijona EUR na leto iz institucij Unije, financiranih iz razdelka 7 proračuna Unije;

– 2,459 milijona EUR iz institucij, organov in agencij Unije, financiranih iz razdelkov 1 do 6 proračuna Unije;

– 2,670 milijona EUR iz institucij, organov in agencij Unije, ki se financirajo sami;

– skupni proračun CERT-EU: 14,05 milijona EUR.

Naloge iz člena 12(5) niso opisane v katalogu storitev CERT-EU; to so storitve, ki se zaračunajo. Te storitve so pomožne, pomenijo sorazmerno nizke zneske in so večinoma začasne, stroške teh storitev pa bodo krili upravičenci storitev na podlagi sporazumov o ravni storitev ali pisnih sporazumov.

Kar zadeva prispevke za osebje CERT-EU: institucije in glavni organi Unije prispevajo pravičen delež, ki je sorazmeren ustreznemu deležu stalnih delovnih mest v razredu AD organizacije. Preveriti bi bilo treba, ali lahko pravičen delež prispevata tudi ECB in EIB z napotitvijo stalnega osebja.

2. UKREPI UPRAVLJANJA

2.1. Pravila o spremljanju in poročanju

Navedite pogostost in pogoje.

Komisija bo s pomočjo IICB in CERT-EU redno pregledovala delovanje Uredbe ter poročala Evropskemu parlamentu in Svetu, in sicer prvič najpozneje 48 mesecev po začetku veljavnosti te uredbe in nato vsaka tri leta.

Viri podatkov, uporabljeni za preglede, bi izhajali predvsem iz IICB in CERT-EU. Poleg tega bi bilo mogoče po potrebi uporabiti posebna orodja za zbiranje podatkov, na primer ankete za institucije, organe in agencije Unije, agencijo ENISA ali mrežo skupin CSIRT.

2.2. Upravljavski in kontrolni sistemi

2.2.1. Utemeljitev načinov upravljanja, mehanizmov financiranja, načinov plačevanja in predlagane strategije kontrol

Ukrepi, ki izhajajo iz Uredbe, se bodo upravljali znotraj vsake institucije, organa in agencije Unije v skladu z ustreznimi pravili in predpisi.

Upravno in finančno upravljanje dejavnosti CERT-EU je del uprave Komisije ter poteka v skladu z njenimi veljavnimi mehanizmi upravljanja in izvajanja, načini plačevanja in kontrolami.

Notranji revizor Komisije ima za CERT-EU enaka pooblastila kot za službe Komisije.

2.2.2. Podatki o ugotovljenih tveganjih in vzpostavljenih sistemih notranjih kontrol za njihovo zmanjševanje

Zelo majhno tveganje, saj je CERT-EU kot projektna skupina Komisije upravno že povezan z Generalnim direktoratom za informatiko, IICB pa je vzpostavljen po vzoru sedanjega usmerjevalnega odbora CERT-EU. Ekosistem za finančno poslovodenje in notranjo kontrolo je tako že vzpostavljen.

2.2.3. Ocena in utemeljitev stroškovne učinkovitosti kontrol (razmerje „stroški kontrol ÷ vrednost z njimi povezanih upravljanih sredstev“) ter ocena pričakovane stopnje tveganja napake (ob plačilu in ob zaključku)

Postopki za javno naročanje, finančno poslovodenje in kontrole so že vzpostavljeni in dobro preizkušeni. Stroškovna učinkovitost kontrol in stopnje tveganja napake ustrezajo tistim v vsaki instituciji, organu ali agenciji Unije ter tistim, ki jih Komisija uporablja za dejavnosti CERT-EU.

2.3. Ukrepi za preprečevanje goljufij in nepravilnosti

Navedite obstoječe ali načrtovane preprečevalne in zaščitne ukrepe, npr. iz strategije za boj proti goljufijam.

Finančno poslovodenje in sistemi notranjih kontrol Komisije se uporabljajo za dejavnosti CERT-EU.

Za boj proti goljufijam, korupciji in drugim nezakonitim dejavnostim se brez omejitev uporabljajo določbe Uredbe (EU, Euratom) št. 883/2013 Evropskega parlamenta in Sveta z dne 11. septembra 2013 o preiskavah, ki jih izvaja Evropski urad za boj proti goljufijam (OLAF).

3. OCENA FINANČNIH POSLEDIC PREDLOGA/POBUDE

3.1. Zadevni razdelki večletnega finančnega okvira in odhodkovne proračunske vrstice

- Obstoječe proračunske vrstice

<u>Po vrstnem redu</u> razdelkov večletnega finančnega okvira in proračunskih vrstic

Razdelek večletnega finančnega okvira	Proračunska vrstica	Vrsta odhodkov	Prispevek			
	številka	dif./nedif.[13]	držav Efte[14]	držav kandidatk[15]	tretjih držav	po členu 21(2)(b) finančne uredbe
1 do 6	Proračunske vrstice, ki zajemajo prispevke Unije za decentralizirane agencije in organe	dif.	NE	NE	NE	NE
7	Proračunske vrstice, ki zajemajo prejemke osebja, izdatke za IT in druge upravne odhodke v različnih oddelkih proračuna EU	nedif.	NE	NE	NE	NE

- Zahtevane nove proračunske vrstice

<u>Po vrstnem redu</u> razdelkov večletnega finančnega okvira in proračunskih vrstic

Razdelek večletnega finančnega okvira	Proračunska vrstica	Vrsta odhodkov	Prispevek			
	številka	dif./nedif.	držav Efte	držav kandidatk	tretjih držav	po členu 21(2)(b) finančne uredbe
	je ni		DA/NE	DA/NE	DA/NE	DA/NE

[13] Dif. = diferencirana sredstva / nedif. = nediferencirana sredstva.
[14] Efta: Evropsko združenje za prosto trgovino.
[15] Države kandidatke in po potrebi potencialne kandidatke z Zahodnega Balkana.

3.2. Ocenjene finančne posledice predloga za odobritve

3.2.1. Povzetek ocenjenih posledic za odobritve za poslovanje

– ☐ Za predlog/pobudo niso potrebne odobritve za poslovanje.

– ☑ Za predlog/pobudo so potrebne odobritve za poslovanje, kot je pojasnjeno v nadaljevanju:

v mio. EUR (na tri decimalna mesta natančno)

Razdelek večletnega finančnega okvira	1 do 6	Razdelek, ki zajema prispevke za decentralizirane agencije in organe

GD več			Leto **2023**	Leto **2024**	Leto **2025**	Leto **2026**	Leto **2027**	**SKUPAJ**
○ Odobritve za poslovanje								
Proračunske vrstice, ki zajemajo prispevke Unije za decentralizirane agencije (xx 10 xx xx)[16]	obveznosti	(1a)	2,459	2,459	2,459	2,459	2,459	12,293
	plačila	(2a)	2,459	2,459	2,459	2,459	2,459	12,293
Odobritve za upravne zadeve, ki se financirajo iz sredstev določenih programov[17]								
Proračunska vrstica		(3)						
Odobritve za GD <…….> za GD: več, SKUPAJ	obveznosti	= 1a + 1b + 3	2,459	2,459	2,459	2,459	2,459	12,293
	plačila	= 2a + 2b + 3	2,459	2,459	2,459	2,459	2,459	12,293

[16] Po uradni proračunski nomenklaturi.

[17] Tehnična in/ali upravna pomoč ter odhodki za podporo izvajanja programov in/ali ukrepov EU (prej vrstice BA), posredne raziskave, neposredne raziskave.

○ Odobritve za poslovanje SKUPAJ	obveznosti	(4)	2,459	2,459	2,459	2,459	2,459	12,293
	plačila	(5)	2,459	2,459	2,459	2,459	2,459	12,293
○ Odobritve za upravne zadeve, ki se financirajo iz sredstev določenih programov, SKUPAJ		(6)						
Odobritve iz RAZDELKOV 1 do 6 SKUPAJ	obveznosti	= 4 + 6	2,459	2,459	2,459	2,459	2,459	12,293
	plačila	= 5 + 6	2,459	2,459	2,459	2,459	2,459	12,293

<u>Če ima predlog/pobuda posledice za več razdelkov za poslovanje, ponovite zgornji odsek:</u>

○ Odobritve za poslovanje SKUPAJ (vsi razdelki za poslovanje)	obveznosti	(4)	2,459	2,459	2,459	2,459	2,459	12,293
	plačila	(5)	2,459	2,459	2,459	2,459	2,459	12,293
Odobritve za upravne zadeve, ki se financirajo iz sredstev določenih programov, SKUPAJ (vsi razdelki za poslovanje)		(6)						
Odobritve iz RAZDELKOV 1 do 6 SKUPAJ (referenčni znesek)	obveznosti	= 4 + 6	2,459	2,459	2,459	2,459	2,459	12,293
	plačila	= 5 + 6	2,459	2,459	2,459	2,459	2,459	12,293

Razdelek večletnega finančnega okvira	**7**	„Upravni odhodki“

Ta oddelek se izpolni s „proračunskimi podatki upravne narave“, ki jih je treba najprej vnesti v Prilogo k oceni finančnih posledic zakonodajnega predloga (Priloga V k notranjim pravilom), ki se prenese v sistem DECIDE za namene posvetovanj med službami.

v mio. EUR (na tri decimalna mesta natančno)

		Leto **2023**	Leto **2024**	Leto **2025**	Leto **2026**	**Leto 2027**	**SKUPAJ**
GD DIGIT (CERT-EU)							
○ Človeški viri		1,184	2,126	2,754	3,225	3,225	12,514
○ Drugi upravni odhodki		7,938	8,921	8,921	8,921	8,921	43,622
GD DIGIT (CERT-EU) SKUPAJ	odobritve	9,122	11,047	11,675	12,146	12,146	56,136

Odobritve iz RAZDELKA 7 večletnega finančnega okvira **SKUPAJ**	(obveznosti skupaj = plačila skupaj)	9,122	11,047	11,675	12,146	12,146	**56,136**

v mio. EUR (na tri decimalna mesta natančno)

		Leto 2023	Leto 2024	Leto 2025	Leto 2026	Leto 2027	**SKUPAJ**
Odobritve iz RAZDELKOV 1 do 7 SKUPAJ (*)	obveznosti	11,581	13,506	14,134	14,605	14,605	68,429
	plačila	11,581	13,506	14,134	14,605	14,605	68,429

(*) Prispevki institucij, organov in agencij Unije, ki se financirajo sami, so ocenjeni na 2,670 milijona EUR na leto (skupaj za pet let 13,350 milijona EUR). Prispevki bodo pomenili namenske prejemke za CERT-EU. Zgornje preglednice vključujejo le ocenjene skupne posledice za proračun Unije in ne vključujejo navedenih prejemkov.

3.2.2. Ocenjene realizacije, financirane z odobritvami za poslovanje

odobritve za prevzem obveznosti v mio. EUR (na tri decimalna mesta natančno)

Cilji in realizacije ⇩			Leto **N**		Leto **N+1**		Leto **N+2**		Leto **N+3**		Vstavite ustrezno število let glede na trajanje posledic (gl. točko 1.6)						**SKUPAJ**	
	REALIZACIJE																	
	vrsta[18]	povprečni stroški	število	stroški	število	stroški	število	stroški	število	stroški	število	stroški	število	stroški	število	stroški	število realizacij skupaj	stroški realizacij skupaj
SPECIFIČNI CILJ št. 1[19] …																		
– realizacija																		
– realizacija																		
– realizacija																		
Seštevek za specifični cilj št. 1																		
SPECIFIČNI CILJ št. 2 …																		
– realizacija																		
Seštevek za specifični cilj št. 2																		
SKUPAJ																		

[18] Realizacije so dobavljeni proizvodi in opravljene storitve (npr. število financiranih izmenjav študentov, število kilometrov novozgrajenih cest …).

[19] Kakor je opisan v točki 1.4.2 „Specifični cilji …“.

3.2.3. Povzetek ocenjenih posledic za upravne odobritve

– ☐ Za predlog/pobudo niso potrebne odobritve za upravne zadeve.

– ☑ Za predlog/pobudo so potrebne odobritve za upravne zadeve, kot je pojasnjeno v nadaljevanju:

v mio. EUR (na tri decimalna mesta natančno)

	Leto 2023	Leto 2024	Leto 2025	Leto 2026	Leto 2027	**SKUPAJ**
RAZDELEK 7 večletnega finančnega okvira						
Človeški viri						
Stalno osebje (razredi AD)	1,099	2,041	2,669	3,14	3,14	12,089
Pogodbeni uslužbenci	0,085	0,085	0,085	0,085	0,085	0,425
Drugi upravni odhodki	7,938	8,921	8,921	8,921	8,921	43,622
Seštevek za RAZDELEK 7 večletnega finančnega okvira	9,122	11,047	11,675	12,146	12,146	56,136

Odobritve zunaj RAZDELKA 7[20] večletnega finančnega okvira						
Človeški viri						
Drugi upravni odhodki						
Seštevek za odobritve zunaj RAZDELKA 7 večletnega finančnega okvira						

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

Potrebe po odobritvah za človeške vire in druge upravne odhodke se krijejo z odobritvami GD, ki so že dodeljene za upravljanje ukrepa in/ali so bile prerazporejene znotraj GD, po potrebi skupaj z dodatnimi viri, ki se lahko pristojnemu GD dodelijo v postopku letne dodelitve virov glede na proračunske omejitve.

[20] Tehnična in/ali upravna pomoč ter odhodki za podporo izvajanja programov in/ali ukrepov EU (prej vrstice BA), posredne raziskave, neposredne raziskave.

3.2.3.1. Ocenjene potrebe po človeških virih

– ☐ Za predlog/pobudo niso potrebni človeški viri.

– ☑ Za predlog/pobudo so potrebni človeški viri, kot je pojasnjeno v nadaljevanju:

ocena, izražena v ekvivalentu polnega delovnega časa

	Leto 2023	Leto 2024	Leto 2025	Leto 2026	Leto 2027		
O Delovna mesta v skladu s kadrovskim načrtom (uradniki in začasni uslužbenci)							
20 01 02 01 (sedež in predstavništva Komisije)	7	13	17	20	20		
20 01 02 03 (delegacije)							
01 01 01 01 (posredne raziskave)							
01 01 01 11 (neposredne raziskave)							
Druge proračunske vrstice (navedite)							
O Zunanji sodelavci (v ekvivalentu polnega delovnega časa: EPDČ)[21]							
20 02 01 (PU, NNS, ZU iz splošnih sredstev)	1	1	1	1	1		
20 02 03 (PU, LU, NNS, ZU in MSD na delegacijah)							
XX 01 xx **yy zz** [22] – na sedežu							
XX 01 xx **yy zz** [22] – na delegacijah							
01 01 01 02 (PU, NNS, ZU za posredne raziskave)							
01 01 01 12 (PU, NNS, ZU za neposredne raziskave)							
Druge proračunske vrstice (navedite)							
SKUPAJ	**8**	**14**	**18**	**21**	**21**		

XX je zadevno področje ali naslov v proračunu.

Potrebe po človeških virih se krijejo z osebjem GD, ki je že dodeljeno za upravljanje ukrepa in/ali je bilo prerazporejeno znotraj GD, po potrebi skupaj z dodatnimi viri, ki se lahko pristojnemu GD dodelijo v postopku letne dodelitve virov glede na proračunske omejitve.

Opis nalog:

Uradniki in začasni uslužbenci	Uradniki bodo naloge in dejavnosti CERT-EU opravljali v skladu z Uredbo, zlasti poglavjema IV in V.
Zunanji sodelavci	Pogodbeni uslužbenec bo pomagal pri tajniških nalogah Medinstitucionalnega odbora za kibernetsko varnost.

[21] PU = pogodbeni uslužbenec; LU = lokalni uslužbenec; NNS = napoteni nacionalni strokovnjak; ZU = začasni uslužbenec; MSD = mladi strokovnjak na delegaciji.

[22] Dodatna zgornja meja za zunanje sodelavce v okviru odobritev za poslovanje (prej vrstice BA).

3.2.4. Skladnost z veljavnim večletnim finančnim okvirom

Predlog/pobuda:

– ☑ se lahko v celoti financira s prerazporeditvijo znotraj zadevnega razdelka večletnega finančnega okvira;

Pojasnite zahtevano spremembo ter navedite zadevne proračunske vrstice in ustrezne zneske. V primeru pomembnejših sprememb med programi predložite Excelovo tabelo.

– ☐ zahteva uporabo nedodeljene razlike do zgornje meje v zadevnem razdelku večletnega finančnega okvira in/ali uporabo posebnih instrumentov, kot so opredeljeni v uredbi o večletnem finančnem okviru;

Pojasnite te zahteve ter navedite zadevne razdelke in proračunske vrstice, ustrezne zneske in instrumente, ki naj bi bili uporabljeni.

– ☐ zahteva spremembo večletnega finančnega okvira.

Pojasnite te zahteve ter navedite zadevne razdelke in proračunske vrstice ter ustrezne zneske.

3.2.5. Udeležba tretjih oseb pri financiranju

V predlogu/pobudi:

– ☑ ni načrtovano sofinanciranje tretjih oseb[23]

– ☐ je načrtovano sofinanciranje, kot je ocenjeno v nadaljevanju:

odobritve v mio. EUR (na tri decimalna mesta natančno)

	Leto **N**[24]	Leto **N+1**	Leto **N+2**	Leto **N+3**	Vstavite ustrezno število let glede na trajanje posledic (gl. točko 1.6)			Skupaj
Navedite organ, ki bo sofinanciral predlog/pobudo								
Sofinancirane odobritve SKUPAJ								

[23] Namenski prejemki, ki izhajajo iz občasnega zagotavljanja storitev organizacijam, ki niso udeleženci, kot so predvidene v členu 12(5), točka (c), niso bili ocenjeni, ker bi morali biti zanemarljivi.

[24] Leto N je leto začetka izvajanja predloga/pobude. Nadomestite „N“ s pričakovanim prvim letom izvajanja (na primer: 2021). Naredite isto za naslednja leta.

3.3. Ocenjene posledice za prihodke

– ☑ Predlog/pobuda nima finančnih posledic za prihodke.

– ☐ Predlog/pobuda ima finančne posledice, kot je pojasnjeno v nadaljevanju:

  – ☐ za lastna sredstva,

  – ☐ za druge prihodke.

  – navedite, ali so prihodki dodeljeni za odhodkovne vrstice ☐

v mio. EUR (na tri decimalna mesta natančno)

Prihodkovna proračunska vrstica	Odobritve na voljo za tekoče proračunsko leto	Posledice predloga/pobude[25]						
		Leto **N**	Leto **N+1**	Leto **N+2**	Leto **N+3**	Vstavite ustrezno število let glede na trajanje posledic (gl. točko 1.6)		
Člen …….								

Za namenske prejemke navedite zadevne odhodkovne proračunske vrstice.

Druge opombe (npr. metoda/formula za izračun posledic za prihodke ali druge informacije).

[25] Pri tradicionalnih lastnih sredstvih (carine, prelevmani na sladkor) se navedejo neto zneski, tj. bruto zneski po odbitku 20 % stroškov pobiranja.