



Dokument s plenarne sjednice

A9-0064/2023

10.3.2023

*****|**

IZVJEŠĆE

o Prijedlogu uredbe Europskog parlamenta i Vijeća o mjerama za visoku zajedničku razinu kibersigurnosti u institucijama, tijelima, uredima i agencijama Unije
(COM(2022)0122 – C9-0122/2022 – 2022/0085(COD))

Odbor za industriju, istraživanje i energetiku

Izvjestiteljica: Henna Virkkunen

Izvjestitelj za mišljenje pridruženog odbora u skladu s člankom 57. Poslovnika:
Tomas Tobé, Odbor za građanske slobode, pravosuđe i unutarnje poslove

Oznake postupaka

- * Postupak savjetovanja
- *** Postupak suglasnosti
- ***I Redovni zakonodavni postupak (prvo čitanje)
- ***II Redovni zakonodavni postupak (drugo čitanje)
- ***III Redovni zakonodavni postupak (treće čitanje)

(Navedeni se postupak temelji na pravnoj osnovi predloženoj u nacrtu akta.)

Izmjene nacrta akta

Amandmani Parlamenta u obliku dvaju stupaca

Brisanja su označena **podebljanim kurzivom** u lijevom stupcu. Izmjene su označene **podebljanim kurzivom** u obama stupcima. Novi tekst označen je **podebljanim kurzivom** u desnom stupcu.

U prvom i drugom retku zaglavlja svakog amandmana naznačen je predmetni odlomak iz nacerta akta koji se razmatra. Ako se amandman odnosi na postojeći akt koji se želi izmijeniti nacrtom akta, zaglavljे sadrži i treći redak u kojem se navodi postojeći akt te četvrti redak u kojem se navodi odredba akta na koju se izmjena odnosi.

Amandmani Parlamenta u obliku pročišćenog teksta

Novi dijelovi teksta označuju se **podebljanim kurzivom**. Brisani dijelovi teksta označuju se oznakom █ ili su precrtni. Izmjene se naznačuju tako da se novi tekst označi **podebljanim kurzivom**, a da se zamjenjeni tekst izbriše ili precrta.

Iznimno, izmjene stroga tehničke prirode koje unesu nadležne službe prilikom izrade konačnog teksta ne označuju se.

SADRŽAJ

	Stranica
NACRT ZAKONODAVNE REZOLUCIJE EUROPSKOG PARLAMENTA	5
OBRAZLOŽENJE	47
MIŠLJENJE ODBORA ZA GRAĐANSKE SLOBODE, PRAVOSUDE I UNUTARNJE POSLOVE	49
MIŠLJENJE ODBORA ZA PRORAČUNE.....	64
MIŠLJENJE ODBORA ZA USTAVNA PITANJA	81
POSTUPAK U NADLEŽNOM ODBORU.....	120
POIMENIČNO KONAČNO GLASOVANJE U NADLEŽNOM ODBORU	121

NACRT ZAKONODAVNE REZOLUCIJE EUROPSKOG PARLAMENTA

**o Prijedlogu uredbe Europskog parlamenta i Vijeća o mjerama za visoku zajedničku razinu kibersigurnosti u institucijama, tijelima, uredima i agencijama Unije
(COM(2022)0122 – C9-0122/2022 – 2022/0085(COD))**

(Redovni zakonodavni postupak: prvo čitanje)

Europski parlament,

- uzimajući u obzir Prijedlog Komisije upućen Europskom parlamentu i Vijeću (COM(2022)0122),
 - uzimajući u obzir članak 294. stavak 2. i članak 298. Ugovora o funkcioniranju Europske unije, u skladu s kojima je Komisija podnijela Prijedlog Parlamentu (C9-0122/2022),
 - uzimajući u obzir članak 294. stavak 3. Ugovora o funkcioniranju Europske unije,
 - uzimajući u obzir članak 59. Poslovnika,
 - uzimajući u obzir mišljenja Odbora za građanske slobode, pravosuđe i unutarnje poslove, Odbora za proračune te Odbora za ustavna pitanja
 - uzimajući u obzir izvješće Odbora za industriju, istraživanje i energetiku (A9-0064/2023),
1. usvaja sljedeće stajalište u prvom čitanju;
 2. poziva Komisiju da predmet ponovno uputi Parlamentu ako zamijeni, bitno izmijeni ili namjerava bitno izmijeniti svoj Prijedlog;
 3. nalaže svojoj predsjednici da stajalište Parlamenta proslijedi Vijeću, Komisiji i nacionalnim parlamentima.

Izmjena 1

AMANDMANI EUROPSKOG PARLAMENTA*

na Prijedlog Komisije

2022/0085 (COD)

Prijedlog

UREDJE EUROPSKOG PARLAMENTA I VIJEĆA

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

EUROPSKI PARLAMENT I VIJEĆE EUROPSKE UNIJE,

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

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

uzimajući u obzir prijedlog Europske komisije,

nakon prosljeđivanja nacrta zakonodavnog akta nacionalnim parlamentima,

u skladu s redovnim zakonodavnim postupkom,

budući da:

- (1) U digitalnom dobu informacijska i komunikacijska tehnologija okosnica je otvorene, učinkovite i neovisne uprave u Uniji. Zbog napretka tehnologije te povećane složenosti i međusobne povezanosti digitalnih sustava kibersigurnosni rizici sve su veći, a uprava Unije osjetljivija je na kiberprijetnje i incidente, što u konačnici predstavlja prijetnju

* Amandmani: novi ili izmijenjeni tekst označava se podebljanim kurzivom, a brisani tekst oznakom █.

poslovnom kontinuitetu i sposobnosti uprave da zaštiti svoje podatke. Iako su povećana upotreba usluga u oblaku, sveprisutna upotreba *informacijske i komunikacijske tehnologije (IKT)*, visok stupanj digitalizacije, rad na daljinu te napredak tehnologije i povezanosti danas osnovne značajke svih aktivnosti upravnih tijela Unije, digitalna otpornost još nije dovoljno ukorijenjena u njihov rad.

- (2) Kiberprijetnje s kojima se suočavaju *subjekti* Unije stalno se mijenjaju. Taktike, tehnike i postupci prijetećih aktera neprestano se razvijaju, a glavni motivi tih napada, od krađe vrijednih neobjavljenih informacija do zarade, manipuliranja javnim mnijenjem ili ugrožavanja digitalne infrastrukture, ne mijenjaju se mnogo. Tempo kojim se provode kibernapadi stalno raste, a kampanje su sve sofisticirane i automatizirane, usmjerene su na prostore izložene napadu koji se stalno šire i brzo iskorištavaju ranjivosti.
- (3) *Informacijska i komunikacijska* okruženja *subjekata* Unije međuvisna su, imaju integrirane protoke podataka, a njihovi korisnici blisko surađuju. Ta međupovezanost znači da svaki poremećaj, čak i onaj koji je prvotno ograničen na jednog *subjekta* Unije, može imati kaskadne učinke u širem smislu, što može dovesti do dalekosežnih i dugotrajnih negativnih učinaka na druge subjekte. Osim toga, *informacijska i komunikacijska* okruženja nekih *subjekata* povezana su s *informacijskim i komunikacijskim* okruženjima država članica, zbog čega incident u jednom subjektu Unije predstavlja rizik za kibersigurnost *informacijskog i komunikacijskog* okruženja država članica i obratno.
- (4) *Subjekti* Unije privlačne su mete koje se suočavaju s vrlo vještim i dobro opremljenim prijetećim akterima i drugim prijetnjama. Istodobno, razina i razvijenost kiberotpornosti te sposobnost otkrivanja zlonamjernih kiberaktivnosti i odgovora na njih znatno se razlikuju od subjekta do subjekta. Kako bi europska uprava funkcionalala, *subjekti Unije* stoga moraju ostvariti visoku zajedničku razinu kibersigurnosti *provedbom mjera upravljanja* kibersigurnosnim *rizicima koje su razmjerne relevantnim rizicima* ┌, razmjenom informacija i suradnjom.
- (5) ┌ Cilj je Direktive (EU) 2022/2555 Evropskog parlamenta i Vijeća¹ dodatno poboljšanje kiberotpornosti javnih i privatnih subjekata, nadležnih nacionalnih tijela i

¹ Direktiva (EU) 2022/2555 Evropskog parlamenta i Vijeća od 14. prosinca 2022. o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije, izmjeni Uredbe

institucija te Unije u cjelini kao i njihove sposobnosti odgovora na incidente. Stoga se subjekti Unije moraju tome prilagoditi osiguravanjem pravila koja su u skladu s Direktivom (EU) 2022/2555 i koja odražavaju njezinu razinu ambicije.

- (6) Kako bi se postigla visoka zajednička razina kibersigurnosti, svaki *subjekt* Unije uspostavlja okvir za upravljanje, opće upravljanje i kontrolu kibersigurnosnih rizika te *postupanje u slučaju incidenata*, kojim se osigurava učinkovito i razborito upravljanje svim kibersigurnosnim rizicima te uzimaju u obzir kontinuitet poslovanja i upravljanje krizama. *Tim bi se okvirom trebale utvrditi kibersigurnosne politike i prioriteti za sigurnost mrežnih i informacijskih sustava koji obuhvaćaju cjelokupno okruženje IKT-a. Okvir bi se trebao redovito preispitivati i to najmanje svake tri godine.*
- (7) Zbog razlika među *subjektima* Unije pri provedbi je potrebna fleksibilnost jer ne postoji univerzalno rješenje. Mjere za visoku zajedničku razinu kibersigurnosti ne bi trebale obuhvaćati obveze koje izravno ometaju izvršavanje zadaća *subjekata* Unije ili zadiru u njihovu institucijsku autonomiju. *Stoga* bi ti *subjekti* trebali uspostaviti vlastite okvire za upravljanje kibersigurnosnim rizicima, *postupanje u slučaju incidenata*, upravljanje i kontrolu te donijeti vlastite mjere upravljanja kibersigurnosnim rizicima i planove za kibersigurnost *koji obuhvaćaju cjelokupno okruženje IKT-a subjekta. Subjekti Unije trebali bi kontinuirano ocjenjivati učinkovitost donesenih mjer za upravljanje rizicima i njihovu proporcionalnost u odnosu na utvrđene rizike te prema potrebi na odgovarajući način prilagođavati i revidirati svoje okvire i planove na temelju rezultata procjena razvijenosti kibersigurnosti.*
- (7.a) *Opetovana obveza provedbe procjena razvijenosti u području kibersigurnosti mogla bi stvoriti dodatno i nerazmjerne opterećenje za male subjekte Unije s ograničenim resursima IKT-a. Ovom bi se Uredbom stoga trebala predvidjeti mogućnost da dva ili više subjekata Unije osnivaju zajedničke timove za provedbu procjena kibersigurnosne razvijenosti te da kombiniraju resurse i stručno znanje.*
- (8) Da bi se izbjeglo nerazmjerne financijsko i administrativno opterećenje za *subjekte* Unije, zahtjevi za upravljanje kibersigurnosnim rizikom trebali bi biti razmjerni riziku kojem je izložen predmetni mrežni i informacijski sustav, uzimajući u obzir

(EU) br. 910/2014 i Direktive (EU) 2018/1972 i stavljaju izvan snage Direktive (EU) 2016/1148 (Direktiva NIS 2) (SL L 333, 27.12.2022., str. 80.).

suvremenost mjera. Svi **subjekti** Unije trebali bi nastojati odrediti odgovarajući postotak svojeg proračuna za *informacijske i komunikacijske tehnologije* za poboljšanje svoje razine kibersigurnosti; dugoročno bi trebalo težiti cilju od **najmanje** 10 %.

- (9) Kako bi se postigla visoka zajednička razina kibersigurnosti, ona mora biti pod nadzorom najviše rukovodeće razine svakog **subjekta** Unije, koji bi trebao **nadgledati provedbu odredaba ove Uredbe i odobriti uspostavu i sve naknadne revizije okvira za upravljanje i kontrolu rizika, odgovarajuće mjere upravljanja** kibersigurnosnim **rizicima kojima se otklanjaju** rizici utvrđeni u okviru te **planove za kibersigurnost** svakog **subjekta Unije**. Bavljenje kulturom kibersigurnosti, tj. svakodnevna primjena kibersigurnosti, sastavni je dio okvira za **upravljanje** kibersigurnosnim **rizicima, upravljanje i kontrolu i odgovarajućih mera za upravljanje kibersigurnosnim rizicima** u svim **subjektima** Unije.
- (10) **Subjekti** Unije trebali bi procijeniti rizike povezane s odnosima s dobavljačima i pružateljima usluga, uključujući pružatelje usluga pohrane i obrade podataka ili upravljenih sigurnosnih usluga, te poduzeti odgovarajuće mjere za njihovo otklanjanje. Te bi mjere **za upravljanje** kibersigurnosnim **rizicima** trebalo pobliže definirati u smjernicama ili preporukama koje izdaje CERT-EU. Pri definiranju mera i smjernica moraju se uzeti u obzir relevantno **pravo** i politike **Unije**, uključujući procjene rizika i preporuke koje je izdala **Skupina za suradnju uspostavljena Direktivom (EU) 2022/2555**, kao što su usklađena procjena rizika na razini EU-a i paket instrumenata EU-a za kibersigurnost 5G mreža. Osim toga, **s obzirom na prijetnje i važnost jačanja otpornosti za subjekte Unije, mora** se zahtijevati certificiranje relevantnih IKT proizvoda, usluga i procesa u okviru posebnih programa kibersigurnosne certifikacije **Unije** donesenih na temelju članka 49. Uredbe (EU) 2019/881.
- (11) U svibnju 2011. glavni tajnici institucija i tijela Unije odlučili su osnovati pretkonfiguracijski tim za hitne računalne intervencije europskih institucija, tijela i agencija (CERT-EU) pod nadzorom međuinstitucijskog upravljačkog odbora. U srpnju 2012. glavni tajnici potvrdili su praktične aranžmane i dogovorili se da će zadržati CERT-EU u obliku trajnog subjekta radi dalnjeg doprinosa poboljšanju ukupne razine sigurnosti informacijskih tehnologija u institucijama, tijelima i agencijama Unije kao primjer vidljive međuinstitucijske suradnje u području kibersigurnosti. U rujnu 2012. osnovan je CERT-EU kao radna skupina Europske komisije s međuinstitucijskim

ovlastima. U prosincu 2017. institucije i tijela Unije sklopili su međuinstitucijski dogovor o organizaciji i djelovanju CERT-EU-a². **Taj** bi dogovor trebalo kontinuirano prilagodavati radi pružanja potpore provedbi ove Uredbe *te bi ga trebalo redovito ocjenjivati s obzirom na buduće pregovore o dugoročnim proračunskim okvirima kojima će se omogućiti donošenje dalnjih odluka u pogledu funkcioniranja i institucionalne uloge CERT-EU-a, uključujući moguću uspostavu CERT-EU-a kao ureda Unije.*

- (12) CERT-EU trebalo bi preimenovati iz „tima za hitne računalne intervencije” u „Centar za kibersigurnost” **subjekata** Unije, u skladu s kretanjima u državama članicama i globalno, u okviru kojih su mnogi CERT-ovi preimenovani u centre za kibersigurnost, ali bi zbog prepoznatljivosti trebalo zadržati kratki naziv „CERT-EU”.
- (13) Mnogi kibernapadi dio su širih kampanja usmjerenih na skupine **subjekata** Unije ili interesnih zajednica koje uključuju **subjekte** Unije. Kako bi omogućili proaktivne mjere za otkrivanje, odgovor na incidente ili ublažavanje *i oporavak od ozbiljnih incidenata, subjekti Unije* trebali bi obavijestiti CERT-EU o ozbiljnim kiberprijetnjama, znatnim ranjivostima, *izbjegnutim incidentima* i ozbiljnim incidentima te podijeliti odgovarajuće tehničke pojedinosti koje omogućuju otkrivanje ili ublažavanje sličnih █ incidenata u drugim **subjektima** Unije, kao i odgovor na *i oporavak od* njih. Na temelju istog pristupa kao što je onaj predviđen Direktivom **(EU) 2022/2555**, ako subjekti dobiju informaciju o ozbiljnog incidentu, trebali bi biti dužni u roku od 24 sata dostaviti **rano upozorenje** CERT-EU-u. Ta razmjena informacija trebala bi omogućiti CERT-EU-u da te informacije proslijedi drugim **subjektima** Unije, kao i odgovarajućim partnerima, kako bi se pomoglo zaštiti sva **informacijska i komunikacijska** okruženja Unije i partnera Unije od sličnih incidenata, prijetnji i ranjivosti.
- (13. a) *Ovom se Uredbom utvrđuje pristup izvješćivanju o ozbiljnim incidentima u više faza kako bi se uspostavila prava ravnoteža između, s jedne strane, brzog izvješćivanja koje pridonosi ublažavanju potencijalnog širenja incidenata i omogućuje subjektima Unije da traže pomoć te, s druge strane, detaljnog izvješćivanja kojim se iz pojedinačnih incidenata izvlače vrijedne pouke i s vremenom poboljšava otpornost pojedinačnih subjekata Unije te doprinosi povećanju opće razine kibersigurnosti*

² SL C 12, 13.1.2018., str. 1 █ .

uprave Unije. U tom pogledu ova bi Uredba trebala uključivati i izvješćivanje o incidentima koji bi, na temelju početne procjene koju dotični subjekt provodi, mogli uzrokovati ozbiljne poremećaje u funkciranju usluga ili finansijske gubitke za taj subjekt Unije ili utjecati na druge fizičke ili pravne osobe uzrokovanjem znatne materijalne ili nematerijalne štete. U takvoj početnoj procjeni trebalo bi uzeti u obzir, među ostalim, pogodene mrežne i informacijske sustave, posebno njihovu važnost za funkciranje i operacije dotičnog subjekta Unije, ozbiljnost i tehničke značajke kiberprijetnje i sve temeljne ranjivosti koje se iskorištavaju, kao i iskustvo dotičnog subjekta Unije sa sličnim incidentima. Pokazatelji kao što su mjera u kojoj je ugroženo funkciranje subjekta Unije, trajanje incidenta ili broj korisnika na koje je incident utjecao mogli bi imati važnu ulogu u utvrđivanju toga je li poremećaj u funkciranju usluge ozbiljan.

- (14) Osim davanja većeg broja zadaća i važnije uloge CERT-EU-u, trebalo bi uspostaviti Međuinstitucijski odbor za kibersigurnost (IICB), koji bi trebao olakšati postizanje visoke zajedničke razine kibersigurnosti u **subjektima** Unije praćenjem provedbe ove Uredbe u **subjektima** Unije, nadzorom nad provedbom općih prioriteta i ciljeva koju obavlja CERT-EU i pružanjem strateškog usmjerenja CERT-EU-u. IICB bi trebao osigurati zastupljenost institucija te uključiti predstavnike agencija i tijela putem Mreže agencija Unije.
- (14.a) *Cilj je IICB-a poduprijeti subjekte u podizanju njihovih kibersigurnosnih stavova provedbom ove Uredbe. Kako bi se pružila potpora subjektima Unije, IICB bi trebao donijeti smjernice i preporuke potrebne za procjene pripremljenosti subjekata Unije u području kibersigurnosti i planove za kibersigurnost, preispitati moguću međusobnu povezanost IKT okruženja subjekata Unije i poduprijeti osnivanje skupine službenika za kibersigurnost u okviru ENISA-e koja se sastoji od lokalnih službenika za kibersigurnost svih subjekata Unije s ciljem olakšavanja razmjene najboljih praksi i iskustava stečenih provedbom ove Uredbe.*
- (14.b) *Kako bi se osigurala usklađenost s Direktivom (EU) 2022/2555, IICB bi mogao donijeti preporuke na temelju rezultata koordiniranih procjena rizika ključnih lanaca opskrbe na razini EU-a iz članka 22. Direktive (EU) 2022/2555 za potporu subjektima Unije u donošenju učinkovitih i razmjernih mjera upravljanja rizicima koje se odnose na sigurnost lanca opskrbe i izraditi smjernice za mehanizme razmijene informacija*

subjekata Unije u vezi s dobrovoljnim obavlješćivanjem CERT-EU-a o kiberprijetnjama, izbjegnutim incidentima i incidentima.

- (15) CERT-EU trebao bi poduprijeti provedbu mjera za visoku zajedničku razinu kibersigurnosti prijedlozima za smjernice i preporuke IICB-u ili objavljivanjem poziva na djelovanje. IICB bi trebao odobriti te smjernice i preporuke. Prema potrebi, CERT-EU trebao bi objavljivati pozive na djelovanje u kojima se opisuju hitne sigurnosne mjere koje **subjekti** Unije trebaju poduzeti u zadanom roku.
- (16) IICB bi trebao nadzirati uskladenost s ovom Uredbom te pratiti smjernice, preporuke i pozive na djelovanje koje izdaje CERT-EU. IICB bi u tehničkim pitanjima trebalo imati potporu tehničkih savjetodavnih skupina čiji sastav IICB određuje prema vlastitu nahođenju te koje bi, *kada je to prikladno*, trebale blisko surađivati s CERT-EU-om, **subjektima** Unije te drugim dionicima. Prema potrebi, IICB bi trebao izdavati █ upozorenja i *zahtjeve za revizije*.
- (16.a) *Ako IICB utvrdi da subjekti Unije nisu učinkovito primijenili ili proveli ovu Uredbu, mogao bi, ne dovodeći u pitanje interne postupke dotičnog subjekta Unije, zatražiti relevantnu i dostupnu dokumentaciju koja se odnosi na učinkovitu provedbu odredaba ove Uredbe, dostaviti obrazloženo mišljenje s uočenim nedostacima u provedbi ove Uredbe, pozvati dotičnog subjekta Unije da dostavi samoprocjenu u pogledu njegova obrazloženog mišljenja i u suradnji s CERT-EU-om izdati smjernice za usklađivanje njihova okvira za upravljanje rizicima, upravljanje i kontrolu, mjera za upravljanje kibersigurnosnim rizicima, planova za kibersigurnost i obveza izvješćivanja s ovom Uredbom.*
- (17) Misija CERT-EU-a trebala bi biti pridonijeti sigurnosti *informacijskog i komunikacijskog* okruženja svih **subjekata** Unije. *Prema potrebi i u koordinaciji sa subjektima Unije CERT-EU može podnijeti IICB-u na odobrenje prijedlog koordinirane police kiberosiguranja koja bi obuhvaćala subjekte Unije kako bi se uspostavila pokrivenost policom osiguranja od štete i nezgode i policom osiguranja od odgovornosti prema trećima radi rješavanja mogućeg učinka incidenata.* CERT-EU trebao bi djelovati kao █ imenovani koordinator za **subjekte** Unije u svrhu koordiniranog bilježenja ranjivosti u europskoj *bazi podataka* o ranjivosti kako je navedeno u članku 12. Direktive (EU) 2022/2555.

- (18) Upravljački odbor CERT-EU-a utvrdio je 2020. novi strateški cilj CERT-EU-a kako bi zajamčio sveobuhvatnu razinu kiberobrane odgovarajućeg opsega i temeljitosti za sve *subjekte* Unije te kontinuiranu prilagodbu postojećim ili predstojećim prijetnjama, uključujući napade na mobilne uređaje, okruženja u oblaku i umrežene internetske uređaje. Strateški cilj obuhvaća i centre za sigurnosne operacije širokog spektra (SOC), koji nadziru mreže, i nadzor od 24 sata dnevno za vrlo ozbiljne prijetnje. Za veće *subjekte* Unije CERT-EU trebao bi pružati potporu njihovim timovima za *informacijsku i komunikacijsku* sigurnost, među ostalim prvom linijom nadzora 24 sata dnevno. Za manje i neke srednje velike *subjekte* Unije CERT-EU trebao bi pružati sve usluge.
- (19) CERT-EU trebao bi obavljati i ulogu koja mu je određena Direktivom **(EU) 2022/2555**, a koja se odnosi na suradnju i razmjenu informacija s mrežom timova za odgovor na računalne sigurnosne incidente (CSIRT). Nadalje, u skladu s Preporukom Komisije (EU) 2017/1584³ CERT-EU trebao bi surađivati i koordinirati odgovor s relevantnim dionicima. Kako bi pridonio visokoj razini kibersigurnosti u cijeloj Uniji, CERT-EU trebao bi s nacionalnim partnerima dijeliti informacije o određenim incidentima. CERT-EU trebao bi surađivati i s drugim javnim i privatnim partnerima, uključujući NATO, uz prethodno odobrenje IICB-a.
- (20) Pri pružanju potpore operativnoj kibersigurnosti CERT-EU trebao bi se koristiti raspoloživim stručnim znanjem Agencije Europske unije za kibersigurnost **(ENISA)** u okviru strukturirane suradnje kako je predviđeno Uredbom (EU) 2019/881 Europskog parlamenta i Vijeća⁴. Trebalo bi definirati namjenske aranžmane između ta dva subjekta kako bi se *u roku od dvije godine od datuma stupanja na snagu ove Uredbe* utvrdila praktična provedba takve suradnje i izbjeglo udvostručivanje aktivnosti. CERT-EU trebao bi surađivati s **ENISA-om** na analizi prijetnji i redovito izvješčivati Agenciju o stanju kiberprijetnji.

³ Preporuka Komisije (EU) 2017/1584 od 13. rujna 2017. o koordiniranom odgovoru na kiberincidente i kiberkrize velikih razmjera (SL L 239, 19.9.2017., str. 36.).

⁴ Uredba (EU) 2019/881 Europskog parlamenta i Vijeća od 17. travnja 2019. o ENISA-i (Agencija Europske unije za kibersigurnost) te o kibersigurnosnoj certifikaciji u području informacijske i komunikacijske tehnologije i stavljanju izvan snage Uredbe (EU) br. 526/2013 (Akt o kibersigurnosti) (SL L 151, 7.6.2019., str. 15.).

- (21) Kao potpora Zajedničkoj jedinici za kibersigurnost koja je uspostavljena u skladu s Preporukom Komisije od 23. lipnja 2021.⁵, CERT-EU trebao bi surađivati i razmjenjivati informacije s dionicima kako bi potaknuo operativnu suradnju i omogućio postojećim mrežama da ostvare svoj puni potencijal u zaštiti Unije.
- (22) Obrada svih osobnih podataka na temelju ove Uredbe trebala bi biti u skladu sa **zakonom** o zaštiti podataka, uključujući Uredbu (EU) 2018/1725 Europskog parlamenta i Vijeća **█**.⁶ *Ova Uredba ne bi trebala utjecati na primjenu prava Unije kojim se uređuje obrada osobnih podataka, uključujući zadaće i ovlasti Europskog nadzornika za zaštitu podataka (EDPS). CERT-EU i IICB trebali bi blisko surađivati s Europskim nadzornikom za zaštitu podataka i osobljem specijaliziranim za zaštitu podataka u subjektima Unije kako bi se osigurala potpuna usklađenost s pravom Unije o zaštiti podataka.*
- (22.a) *Kibersigurnosni sustavi i usluge uključeni u sprečavanje, otkrivanje i odgovor na kiberprijetnje trebali bi biti u skladu s pravom o zaštiti podataka i privatnosti te bi trebali uključivati relevantne tehničke i organizacijske zaštitne mjere kako bi se osiguralo postizanje te usklađenosti na odgovoran način.*
- (22.b) *Alati i aplikacije za kibersigurnost otvorenog koda mogu pridonijeti većem stupnju otvorenosti. Otvoreni standardi olakšavaju interoperabilnost između sigurnosnih alata, pogodujući sigurnosti dionika. Alati i aplikacije za kibersigurnost otvorenog koda mogu utjecati na šиру zajednicu programera, omogućujući diversifikaciju dobavljača. Otvoreni kod može dovesti do transparentnijeg procesa provjere alata koji se odnose na kibersigurnost i procesa otkrivanja ranjivosti koji pokreće zajednica. Subjekti Unije stoga bi trebali moći promicati usvajanje softvera otvorenog koda i otvorenih standarda provođenjem politika koje se odnose na korištenje otvorenih podataka i otvorenog koda kao dijela sigurnosti pomoću transparentnosti.*

⁵ Preporuka Komisije C(2021) 4520 od 23. lipnja 2021. o uspostavljanju Zajedničke jedinice za kibersigurnost.

⁶ Uredba (EU) 2018/1725 Europskog parlamenta i Vijeća od 23. listopada 2018. o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama, tijelima, uredima i agencijama Unije i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Uredbe (EZ) br. 45/2001 i Odluke br. 1247/2002/EZ (SL L 295, 21.11.2018., str. 39.).

- (23) Postupanje CERT-EU-a i *subjekata* Unije s podacima trebalo bi biti u skladu s pravilima o sigurnosti podataka, posebno onima utvrđenima u Uredbi [predložena Uredba o sigurnosti podataka]. Kako bi se osigurala koordinacija u pitanjima sigurnosti, sve kontakte s CERT-EU-om koje pokrenu ili zatraže nacionalne sigurnosne i obavještajne službe trebalo bi bez nepotrebne odgode priopćiti Glavnoj upravi Komisije za sigurnost i predsjedniku IICB-a.
- (24) Budući da su usluge i zadaće CERT-EU-a u interesu svih *subjekata* Unije, svi *subjekti* Unije s rashodima za *informacijsku i komunikacijsku tehnologiju* trebali bi razmjerno pridonositi tim uslugama i zadaćama. Ti doprinosi ne dovode u pitanje proračunsku autonomiju *subjekata* Unije.
- (24.a) *Međutim, ovom bi se Uredbom trebalo uzeti u obzir da, osim institucija Unije, većina subjekata Unije, a posebno mali subjekti, nemaju potrebne finansijske i ljudske resurse za dodatne zadaće u području kibersigurnosti.*
- (25) IICB trebao bi, uz pomoć CERT-EU-a, preispitati i procijeniti funkcioniranje ove Uredbe te podnijeti izvješće Komisiji o svojim zaključcima. Na temelju tih informacija Komisija bi trebala podnijeti izvješće Europskom parlamentu, Vijeću, Europskom gospodarskom i socijalnom odboru i Odboru regija.

DONIJELI SU OVU UREDBU:

Poglavlje I.
OPĆE ODREDBE

Članak 1.

Predmet

Ovom se Uredbom utvrđuju mjere kojima se nastoji postići visoka zajednička razina kibersigurnosti u subjektima Unije. U tu svrhu, ovom se Uredbom utvrđuju:

- (a) obveze *koje obvezuju subjekte Unije* da uspostave okvir za upravljanje, opće upravljanje i kontrolu kibersigurnosnih rizika te *postupanje u slučaju incidenata*;

- (b) obveze ***subjekata*** Unije glede upravljanja kibersigurnosnim rizicima i izvješćivanja o njima;
- (ba) ***pravila na kojima se temelje obveze razmjene informacija i olakšavanje dobrovoljnih aranžmana za razmjenu informacija u pogledu subjekata Unije;***
- (c) pravila o organizaciji, ***zadaćama*** i radu Centra za kibersigurnost ***subjekata*** Unije (CERT-EU) te o ***funkcioniranju***, organizaciji i radu Međuinstitucijskog odbora za kibersigurnost (***IICB***).

Članak 2.

Područje primjene

Ova se Uredba primjenjuje na **█** sve ***subjekte*** Unije te na ***funkcioniranje***, organizaciju i rad CERT-EU-a i ***IICB-a***.

Članak 3.

Definicije

Za potrebe ove Uredbe, primjenjuju se sljedeće definicije:

- (1) „***subjekti*** Unije” znači institucije, tijela, ***uredi*** i agencije Unije koji su osnovani Ugovorom o Europskoj uniji, Ugovorom o funkcioniranju Europske unije ili Ugovorom o osnivanju Europske zajednice za atomsku energiju ili na temelju tih ugovora;
- (2) „mrežni i informacijski sustav” znači mrežni i informacijski sustav ***kako je definiran u članku 6. točki 1.*** Direktive (EU) 2022/2555;
- (3) „sigurnost mrežnih i informacijskih sustava” znači sigurnost mrežnih i informacijskih sustava ***kako je definirana u članku 6. točki 2.*** Direktive (EU) 2022/2555;
- (4) „kibersigurnost” znači kibersigurnost ***kako je definirana u članku 2. točki 1. Uredbe (EU) 2019/881***;
- (5) „najviša rukovodeća razina” znači rukovoditelj, rukovodstvo ili koordinacijsko i nadzorno tijelo ***odgovorno za funkcioniranje dotičnog subjekta Unije*** na najvišoj upravnoj razini ***s mandatom za donošenje ili autoriziranje odluka u skladu s***

aranžmanima upravljanja na visokoj razini *dотичног subjekta Unije, ne dovodeći u pitanje formalne odgovornosti drugih rukovodećih razina za upravljanje uskladenošću i rizicima u njihovim područjima odgovornosti;*

- (5.a) „*izbjegnuti incident*” znači *izbjegnuti incident kako je definiran u članku 6. točki 5. Direktive (EU) 2022/2555;*
- (6) „*incident*” znači incident *kako je definiran člankom 6. točkom 6. Direktive (EU) 2022/2555;*
- |
- (8) „veći *incident*” znači incident *čiji disruptivni učinak premašuje sposobnost pogodenog subjekta Unije i CERT-EU-a da na njega odgovore ili koji ima ozbiljan učinak na najmanje dva subjekta Unije, ili u kojem kiberincident velikih razmjera iz članka 6. točke 7. Direktive (EU) 2022/2555 ima ozbiljan učinak na najmanje jedan subjekt Unije;*
- (9) „*rješavanje incidenta*” znači rješavanje incidenta *kako je definirano u članku 6. točki 8. Direktive (EU) 2022/2555;*
- (10) „*kiberprijetnja*” znači kiberprijetnja *kako je definirana u članku 2. točki 8. Uredbe (EU) 2019/881;*
- (11) „*ozbiljna kiberprijetnja*” znači kiberprijetnja *kako je definirana u članku 6. točki 11. Direktive (EU) 2022/2555;*
- (12) „*ranjivost*” znači ranjivost *kako je definirana* u članku **6. točki 15. Direktive (EU) 2022/2555;**
- (13) „*znatna ranjivost*” znači ranjivost koja će, ako se iskoristi, vjerojatno uzrokovati ozbiljan incident;
- (14) „*rizik*” znači *rizik kako je definiran u članku 6. točki 9. Direktive (EU) 2022/2555;*
- (14.a) „*norma*” znači *norma definirana u članku 2. točki 1. Uredbe (EU) br. 1025/2012 Europskog parlamenta i Vijeća⁸;*

⁸ *Uredba (EU) br. 1025/2012 Europskog parlamenta i Vijeća od 25. listopada 2012. o europskoj normizaciji, o izmjeni direktiva Vijeća 89/686/EEZ i 93/15/EEZ i direktiva 94/9/EZ, 94/25/EZ, 95/16/EZ, 97/23/EZ, 98/34/EZ, 2004/22/EZ, 2007/23/EZ,*

- (14.b) „tehnička specifikacija” znači tehnička specifikacija kako je definirana u članku 2. točki 4. Uredbe (EU) br. 1025/2012;
- (14.c) „IKT proizvod” znači IKT proizvod kako je definiran u članku 2. točki 12. Uredbe (EU) 2019/881;
- (14.d) „IKT usluga” znači IKT usluga kako je definirana u članku 2. točki 13. Uredbe (EU) 2019/881;
- (14.e) „IKT proces” znači IKT proces kako je definiran u članku 2. točki 14. Uredbe (EU) 2019/881;
- (14.f) „IKT okruženje” znači svaki lokalni ili virtualni IKT proizvod, IKT usluga i IKT proces, svaki mrežni i informacijski sustav, bez obzira na to je li u vlasništvu i pod upravljanjem subjekta ili u vlasništvu i pod upravljanjem treće strane, uključujući mobilne uređaje, korporativne mreže i poslovne mreže koje nisu povezane s internetom i sve uređaje povezane s IKT okruženjem te sve decentralizirane prostore i decentralizirane urede, kao što su uredi za vezu, predstavništva ili lokalni uredi;
- (15) „Zajednička jedinica za kibersigurnost” znači virtualna i fizička platforma za suradnju za razne zajednice za kibersigurnost u Uniji, prije svega za operativnu i tehničku koordinaciju protiv velikih prekograničnih kiberprijetnji i incidenata u smislu Preporuke Komisije od 23. lipnja 2021.;
- (16) „kibersigurnosne **mjere**” znači skup minimalnih pravila *i mjera* za kibersigurnost s kojima mrežni i informacijski sustavi te njihovi operateri i korisnici moraju biti usklađeni kako bi se kibersigurnosni rizici sveli na najmanju mjeru.

Poglavlje II.

MJERE ZA VISOKU ZAJEDNIČKU RAZINU KIBERSIGURNOSTI

Članak 4.

Okvir za upravljanje rizicima, *postupanje u slučaju incidenata*, opće upravljanje i kontrolu

2009/23/EZ i 2009/105/EZ Europskog parlamenta i Vijeća te o stavljanju izvan snage Odluke Vijeća 87/95/EEZ i Odluke br. 1673/2006/EZ Europskog parlamenta i Vijeća (OJL 316, 14.11.2012., str. 12.).

1. *Na temelju kibersigurnosne revizije* svi *subjekti* Unije uspostavljaju unutarnji █ okvir za upravljanje, opće upravljanje, *postupanje u slučaju incidenta* i kontrolu kibersigurnosnih rizika („okvir“) kojim se podupiru zadaće subjekta *Unije*, pri čemu primjenjuju svoju institucijsku autonomiju. *Uspostavu okvira* nadzire najviša rukovodeća razina subjekta Unije *te je odgovorna* za osiguravanje učinkovitog i razboritog upravljanja svim kibersigurnosnim rizicima. Okvir se mora *uspostaviti* najkasnije do ... █ [15 mjeseci od *datuma* stupanja na snagu ove Uredbe].
 2. Okvir obuhvaća cijelokupno *IKT* okruženje predmetnog *subjekta Unije* █ . U okviru se uzimaju u obzir kontinuitet poslovanja i upravljanje krizama te sigurnost lanca opskrbe i upravljanje ljudskim rizicima *te svi drugi relevantni tehnički, operativni i organizacijski rizici* koji bi mogli *imati* utjecaj *na* kibersigurnost *doticnog subjekta* █ Unije.
- 2.a *Okvirom iz stavka 1. definiraju se strateški ciljevi za osiguravanje visoke razine kibersigurnosti u subjektima Unije. Tim se okvirom utvrđuju kibersigurnosne politike za sigurnost mrežnih i informacijskih sustava koje obuhvaćaju cijelokupno okruženje IKT-a i definiraju uloge i odgovornosti osoblja subjekata Unije čija je zadaća osigurati učinkovitu provedbu ove Uredbe. Okvir uključuje i ključne pokazatelje uspješnosti za mjerjenje učinkovitosti provedbe na temelju popisa ključnih pokazatelja uspješnosti iz članka 12. stavka 2. točke (eb).*
- 2.b *Okvir iz stavka 1. redovito se preispituje i to najmanje svake tri godine. Prva revizija provodi se najkasnije ... [3 godine od datuma stupanja na snagu ove Uredbe]. Prema potrebi i na zahtjev IICB-a, okvir subjekta Unije ažurira se u skladu sa smjernicama CERT-EU-a o utvrđenim incidentima ili mogućim nedostacima uočenima u provedbi ove Uredbe.*
3. Najviša rukovodeća razina svakog *subjekta* Unije *zadužena je za provedbu i nadzire* usklađenost *i funkcioniranje svoje* organizacije s obvezama povezanima s *okvirom*, ne dovodeći u pitanje formalne odgovornosti ostalih rukovodećih razina u pogledu usklađenosti i upravljanja rizikom u područjima za koja su nadležne, *poput zaštite podataka*.

4. Svi *subjekti* Unije dužni su imati uspostavljene učinkovite mehanizme kojima se osigurava da se odgovarajući postotak proračuna za *informacijsku i komunikacijsku tehnologiju* troši na kibersigurnost.
5. Svi *subjekti* Unije imenuju lokalnog službenika za kibersigurnost ili jednakovrijednu funkciju koji djeluje kao njihova jedinstvena kontaktna točka za sve aspekte kibersigurnosti. *Nekoliko subjekata Unije može dijeliti iste lokalne službenike za kibersigurnost.*

Članak 5.

Mjere upravljanja kibersigurnosnim rizicima

1. Najviša rukovodeća razina svakog *subjekta* Unije odobrava unutarnji okvir subjekta *Unije* u pogledu *mjera upravljanja* kibersigurnosnim *rizikom* radi otklanjanja rizika utvrđenih u unutarnjem okviru iz članka 4. stavka 1. *u skladu sa svim smjernicama i preporukama IICB-a i CERT-EU-a. Uzimajući u obzir najmodernije i, ako je primjenjivo, relevantne europske i međunarodne norme ili dostupne europske kibersigurnosne certifikate kako su definirani u članku 2. točki 11. Uredbe (EU) 2019/881, tím se mjerama upravljanja rizikom osigurava razina sigurnosti mrežnih i informacijskih sustava u cijelokupnom IKT okruženju koja je razmjerna rizicima utvrđenima u okviru iz članka 4. stavka 1. Pri procjeni razmjernosti tih mjeru u obzir se uzima stupanj izloženosti subjekta Unije rizicima, njegova veličina, vjerojatnost pojave incidenata i njihova ozbiljnost, uključujući njihov društveni, gospodarski i međuinstitucijski učinak.*
- 1.a *Subjekti Unije u provedbu mjera upravljanja kibersigurnosnim rizicima uključuju barem sljedeća područja:*
 - (a) *kibersigurnosnu politiku, uključujući mjere potrebne za postizanje ciljeva i prioriteta iz članka 4. i stavka 2.a ovog članka;*
 - (b) *ciljeve politike u pogledu korištenja usluga računalstva u oblaku kako su definirane u članku 6. točki 30. Direktive (EU) 2022/2555 i tehničke mehanizme za omogućivanje i održavanje rada na daljinu;*
 - (c) *kako bi se procijenilo imaju li subjekti Unije dovoljnu kontrolu nad sigurnošću svojih IKT sustava, cijelovito početno preispitivanje kibersigurnosti,*

uključujući procjenu rizika, osjetljivosti i prijetnji te penetracijsko ispitivanje IKT sustava i uređaja subjekata Unije koje će provesti vodeća i provjerena treća strana izvan subjekata Unije, kao što je vodeće poduzeće za kibersigurnost, na... [datum stupanja na snagu ove Uredbe] i svake sljedeće godine nakon toga, pri čemu se uzimaju u obzir zahtjevi u pogledu informacijske sigurnosti relevantnih institucija;

- (d) *s obzirom na preispitivanja iz točke (c), ublažavanje prijavljenih rizika i ranjivosti u ažuriranjima u području kibersigurnosti te provedba preporuka s pomoću kibersigurnosne politike koja može uključivati zamjenu zaraženih sustava IKT-a;*
- (e) *organizacija kibersigurnosti, uključujući definiranje uloga i odgovornosti;*
- (f) *upravljanje okruženjem IKT-a, uključujući popis imovine i mrežnu kartografiju IKT-a;*
- (g) *kontrolu pristupa, upravljanje identitetom i upravljanje povlaštenim pristupom;*
- (h) *sigurnost operacija i sigurnost ljudskih resursa;*
- (i) *sigurnost komunikacija;*
- (j) *nabava, razvoj, održavanje sustava i transparentnost izvornog koda;*
- (k) *revizije kibersigurnosti;*
- (l) *radno opterećenje osoblja u području IKT-a i ukupno zadovoljstvo osoblja;*
- (m) *sigurnost lanca opskrbe i odnose s dobavljačima između subjekata Unije i njezinih izravnih dobavljača i pružatelja usluga;*
- (n) *rješavanje incidenata, uključujući pristupe za poboljšanje spremnosti, otkrivanja, analiziranja i stavljanja pod kontrolu incidenata, odgovor na incidente i oporavak od njih te suradnju s CERT-EU-om, što se primjerice odnosi na održavanje nadzora nad sigurnošću i vodenje evidencije o njoj;*
- (o) *upravljanje kontinuitetom poslovanja i upravljanje krizama; te*
- (p) *vještine, educiranje, informiranje, programe osposobljavanja i vježbe.*

2. Više rukovodstvo svakog *subjekta Unije te sve relevantno osoblje zaduženo za provedbu mjera upravljanja kibersigurnosnim rizicima i obveza utvrđenih u ovoj Uredbi* redovito sudjeluje u posebnim osposobljavanjima kako bi steklo dovoljno znanja i vještina da shvati i procijeni kibersigurnosne rizike i prakse upravljanja kibersigurnošću te njihov utjecaj na poslovanje *subjekta Unije*.
- 2.a *Pri provedbi mjera upravljanja kibersigurnosnim rizicima te u svojim planovima za kibersigurnost subjekti Unije bavit će se barem sljedećim specifičnim mjerama i podkontrolama, u skladu sa smjernicama i preporukama IICB-a:*
- (a) *konkretnim koracima prema uspostavi arhitekture nultog povjerenja, u smislu sigurnosnog modela koji se sastoji od skupa načela za projektiranje sustava te koordinirane strategije za kibersigurnost i upravljanje sustavom koji se temelje na priznavanju postojanja prijetnji unutar i izvan tradicionalnih granica mreže;*
 - (b) *primjenom dvostrukе autentifikacije kao norme u mrežnim i informacijskim sustavima;*
 - (c) *primjenom kriptografije i šifriranja, a posebno šifriranja s kraja na kraj, šifriranja pri prijenosu i šifriranja u mirovanju te sigurnih digitalnih potpisa;*
 - (d) *sigurnim slanjem glasovnih, video i tekstuálnih poruka te sigurnim sustavima za komunikaciju u slučaju opasnosti, kada je to primjерено;*
 - (e) *uvodenjem čestih i ad hoc mogućnosti skeniranja krajnjih uređaja i drugih komponenti okruženja IKT-a za otkrivanje i uklanjanje zlonamjernih softvera kao što su špijunski softveri;*
 - (f) *osiguravanjem integrirane privatnosti (privacy by design) i poboljšane sigurnosti svih osobnih podataka;*
 - (g) *uspostavljanjem sigurnosti lanca opskrbe softverom s pomoću kriterija za siguran razvoj i evaluaciju softvera;*
 - (h) *redovitim osposobljavanjem osoblja u području kibersigurnosti;*
 - (i) *sudjelovanjem u analizama rizika u pogledu međupovezanosti subjekata Unije;*

- (j) *poboljšanjem pravila javne nabave kako bi se olakšalo postizanje visoke zajedničke razine kibersigurnosti:*
- (i) *uklanjanjem ugovornih prepreka koje pružateljima informacijskih i komunikacijskih usluga otežavaju razmjenu informacija o incidentima, ranjivostima i kiberprijetnjama s CERT-EU-om;*
 - (ii) *ugovornom obvezom prijavljivanja incidenata, ranjivosti, izbjegnutih incidenata i kiberprijetnji te uspostavljanja odgovarajućeg odgovora na incidente i praćenja incidenata.*
- (k) *uspostavljanjem i donošenjem programa za osposobljavanje u području kibersigurnosti koji odgovara predvidenim zadaćama i očekivanim sposobnostima najvišeg rukovodstva te tehničkog i operativnog osoblja.*
- 2.b *IICB može preporučiti tehničke i metodološke zahtjeve za područja i mjere upravljanja kibersigurnosnim rizikom iz stavaka 1.a i 2.a ovog članka te, prema potrebi, preporučiti prilagodbe kao odgovor na promjene u metodama kibernapada, kiberprijetnjama i tehnološkom napretku, za potrebe preispitivanja iz članka 24.*

Članak 6.

Procjene razvijenosti u području *kibersigurnosti*

1. Svaki *subjekt* Unije najkasnije *do ... /18 mjeseci nakon datuma stupanja na snagu ove Uredbej* te najmanje svake *dvije* godine *nakon toga* provode procjenu razvijenosti kibersigurnosti koja obuhvaća sve elemente njihovih *IKT* okruženja kako je opisano u članku 4., pri čemu uzimaju u obzir relevantne smjernice i preporuke donesene u skladu s člankom 13.
2. *Mali subjekti Unije sa sličnim zadaćama ili strukturom mogu provoditi kombiniranu procjenu razvijenosti kibersigurnosti.*
3. *Nakon savjetovanja s Agencijom Europske unije za kibersigurnost (ENISA) i nakon primanja smjernica CERT-EU-a, IICB do... /godinu dana nakon datuma stupanja na snagu ove Uredbej* subjektima iz Unije izdaje smjernice za provedbu procjena razvijenosti u području kibersigurnosti. Procjena razvijenosti u području kibersigurnosti temelji se na revizijama kibersigurnosti.

4. *Na zahtjev IICB-a i uz izričitu suglasnost dotični subjekti Unije, o rezultatima procjene razvijenosti u području kibersigurnosti može se raspravljati unutar IICB-a ili u okviru uspostavljene mreže lokalnih službenika za kibersigurnost kako bi se izvukle pouke iz iskustava u provedbi ove Uredbe i razmijenile najbolje prakse i rezultati primjene.*

Članak 7.

Planovi za kibersigurnost

1. Na temelju zaključaka izvedenih iz procjene razvijenosti **kibersigurnosti** i s obzirom na [] rizike utvrđene u skladu s člankom 4., najviša rukovodeća razina svakog **subjekta** Unije bez nepotrebne odgode odobrava plan za kibersigurnost nakon uspostave okvira [] i **mjera za upravljanje** kibersigurnosnim **rizikom**. Planom za **kibersigurnost** nastoji se povećati ukupna kibersigurnost **dotičnog** subjekta **Unije** i time doprinijeti poboljšanju visoke zajedničke razine kibersigurnosti u svim subjektima **unutar** Unije []. Kako bi se pružila potpora misiji subjekta **Unije** na temelju njihove institucijske autonomije, **kibersigurnosni** plan obuhvaća barem mjere **upravljanja kibersigurnosnim rizicima** iz članka 5. stavaka 1.a i 2.a. Plan za **kibersigurnost** revidira se najmanje svake **dvije** godine **ili, prema potrebi, nakon svake znatne revizije okvira** iz članka 4., nakon procjena **kibersigurnosne** razvijenosti provedenih u skladu s člankom 6.
2. Plan za kibersigurnost sadržava dužnosti, **potrebnu razinu kompetencija** i zadaće **relevantnih** članova osoblja, koje se odnose na njegovu provedbu, **uključujući detaljne opise radnih mjeseta za tehničko i operativno osoblje te sve relevantne procese na kojima se temelji evaluacija uspješnosti**.
- 2.a **Plan za kibersigurnost uključuje plan subjekta Unije za upravljanje kiberkrizama za velike incidente.**
3. U planu za kibersigurnost u obzir se uzimaju sve primjenjive smjernice i preporuke koje je izdao CERT-EU **u skladu s člankom 13. i svim primjenjivim ili ciljanim preporukama** koje su izdali IICB i CERT-EU.
- 3.a **Subjekti Unije podnose svoje planove za kibersigurnost IICB-u.**

Članak 8.

Provedba

1. Po završetku *svojih* procjena razvijenosti u području *kibersigurnosti iz članka 6. i planova za kibersigurnost iz članka 7., subjekti* Unije dostavljaju *ih IICB-u*. ┌ Na zahtjev *IICB-a* izvješćuju o posebnim aspektima ovog poglavlja.
2. Smjernice i preporuke, izdane u skladu s člankom 13., podupiru provedbu odredbi utvrđenih u ovom poglavlju.

Poglavlje III.

IICB

Članak 9.

IICB

1. Osniva se ┌ IICB ┌ .
2. IICB je odgovoran za:
 - (a) praćenje provedbe ove Uredbe u *subjektima* Unije *te izdavanje preporuka za postizanje zajedničke visoke razine kibersigurnosti*;
 - (b) nadzor nad provedbom općih prioriteta i ciljeva koju obavlja CERT-EU i pružanje strateškog usmjerenja CERT-EU-u.
3. IICB se sastoji od:
 - (a) *dva* predstavnika ┌ koje imenuje svako od sljedećih tijela:
 - (i.) Europski parlament;
 - ii. Vijeće Europske unije;
 - iii. Europska komisija;
 - (b) *jednog predstavnika* kojeg imenuje svako od sljedećih tijela:
 - (i.) Sud Europske unije;
 - (ii.) Europska središnja banka;

- (iii.) Evropski revizorski sud;
 - (iv.) Evropska služba za vanjsko djelovanje;
 - (v.) Evropski gospodarski i socijalni odbor;
 - (vi.) Evropski odbor regija;
 - (vii.) Evropska investicijska banka;
 - (viii.) **ENISA;**
 - (ix.) **Evropski nadzornik za zaštitu podataka;**
 - (x.) **Evropski stručni centar za industriju, tehnologiju i istraživanja u području kibersigurnosti;**
 - (xi.) **Agencija Evropske unije za svemirski program;**
- (c) *jedan predstavnik kojeg imenuje Mreža agencija Unije (EUAN) na prijedlog svojeg Savjetodavnog odbora za IKT, a koji zastupa interes agencija, ureda i tijela koji nisu navedeni u točkama (b) vii., x. i xi., i koji upravlja vlastitim IKT okruženjem.*

Među imenovanim predstavnicima teži se cilju rodne ravnoteže.

- 3.a Članovima može pomagati zamjenik. Predsjednik može pozvati druge predstavnike prethodno navedenih organizacija ili drugih *subjekata* Unije da prisustvuju sastancima IICB-a bez prava glasa.
- 3.b *Voditelj CERT-EU-a i predsjednici Skupine za suradnju, mreže CSIRT-ova i EU-CyCLONe-a iz članaka 14., 15. i 16. Direktive (EU) 2022/2555 ili njihovi zamjenici mogu sudjelovati na sastancima IICB-a kao promatrači. U iznimnim slučajevima i u skladu s unutarnjim poslovnikom IICB-a, IICB može odlučiti drugčije.*
- 4. IICB donosi svoj unutarnji poslovnik.
- 5. U skladu sa svojim unutarnjim poslovnikom IICB iz redova svojih članova imenuje predsjednika na razdoblje od četiri godine. Njegov zamjenik postaje punopravni član IICB-a s *pravom glasovanja* na isto razdoblje.

6. IICB se sastaje na inicijativu svojeg predsjednika, *i to barem dvaput godišnje*, na zahtjev CERT-EU-a ili na zahtjev svojih članova.
7. Svaki član IICB-a ima jedan glas. Odluke IICB-a donose se običnom većinom, osim ako je ovom Uredbom drugačije određeno. Predsjednik ne smije glasovati osim u slučaju izjednačenog broja glasova kad može dati odlučujući glas.
8. IICB može djelovati po pojednostavljenom pisanom postupku pokrenutom u skladu s unutarnjim poslovnikom IICB-a. Na temelju tog postupka relevantna odluka smatra se odobrenom u roku koji odredi predsjednik, osim ako se neki član protivi.

|

10. Poslove tajništva za IICB obavlja Komisija.
11. *Predstavnici* koje EUAN | imenuje prosljeđuju odluke IICB-a agencijama i zajedničkim poduzećima Unije. Sve agencije i tijela Unije imaju pravo s predstavnicima ili predsjednikom IICB-a pokrenuti sva pitanja za koja smatraju da bi trebalo uputiti IICB-u.

|

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

Članak 10.

Zadaće IICB-a

Pri obavljanju svojih dužnosti IICB posebno:

- (-a) *podupire subjekte Unije pri provedbi ove Uredbe s ciljem podizanja razine kibersigurnosti;*
- (-aa) *efektivno prati provedbu obveza iz ove Uredbe u subjektima Unije, ne dovodeći pritom u pitanje njihovu institucionalnu autonomiju i opću institucionalnu ravnotežu;*
- (-ab) *pruža strateške smjernice voditelju CERT-EU-a;*
- (a) *traži izvješća | koja CERT-EU o stanju provedbe ove Uredbe u subjektima Unije;*

- (aa) na temelju prijedloga voditelja CERT-EU-a odobrava preporuke za postizanje zajedničke visoke razine kibersigurnosti namijenjene jednom ili više subjekata Unije;
 - (ab) uspostavlja okvir za provođenje usporednih analiza za subjekte Unije s ciljem učenja iz zajedničkih iskustava, jačanja uzajamnog povjerenja, postizanja visoke zajedničke razine kibersigurnosti te povećanja sposobnosti subjekata iz Unije, koje trebaju provoditi tehnički stručnjaci za kibersigurnost koje imenuje subjekt različit od subjekta koji se ocjenjuje;
- (b) na temelju prijedloga voditelja CERT-EU-a odobrava godišnji program rada CERT-EU-a i prati njegovu provedbu;
- (c) na temelju prijedloga voditelja CERT-EU-a odobrava katalog usluga CERT-EU-a;
- (d) na temelju prijedloga voditelja CERT-EU-a odobrava godišnji finansijski plan prihoda i rashoda, uključujući za osoblje, za aktivnosti CERT-EU-a;
- (e) na temelju prijedloga voditelja CERT-EU-a odobrava modalitete sporazumâ o razini usluga;
- (f) pregledava i odobrava godišnje izvješće koje sastavlja voditelj CERT-EU-a, a kojim su obuhvaćene aktivnosti CERT-EU-a i upravljanje njegovim sredstvima;
- (g) odobrava i prati *ključne pokazatelje uspješnosti* CERT-EU-a definirane na prijedlog voditelja CERT-EU-a;
- (h) odobrava dogovore o suradnji te sporazume ili ugovore o razini usluga između CERT-EU-a i drugih subjekata u skladu s člankom 17.;
- (ha) donosi smjernice ili preporuke na osnovu prijedloga CERT-EU-a;
- (hb) kada je to potrebno, nalaže CERT-EU da objavi, povuče ili izmjeni prijedlog smjernica ili preporuka, ili poziv na djelovanje;
- (i) uspostavlja tehničke savjetodavne skupine, s **konkretnim zadaćama** za pomoć u radu IICB-a, odobrava njihova pravila djelovanja i imenuje njihove predsjednike;
- (ia) preispituje i, na zahtjev, u skladu s relevantnim smjernicama CERT-EU-a, subjektima Unije pruža povratne informacije o procjenama kibersigurnosne razvijenosti iz članka 6. i planovima za kibersigurnost iz članka 7.;

- (ib) *olakšava razmjenu najboljih praksi među lokalnim službenicima za kibersigurnost; daje, prema potrebi, preporuke o njihovoj ulozi u subjektima Unije;*
- (ic) *preispituje moguće medupovezanosti okruženja IKT-a subjekata Unije te vodi evidenciju zajedničkih komponenti IKT proizvoda, IKT usluga i IKT procesa;*
- (id) *prema potrebi donosi preporuke o interoperabilnosti IKT okruženja ili IKT komponenti subjekata Unije;*
- (ie) *podupire osnivanje Skupine službenika za kibersigurnost, koju će koordinirati ENISA, koja okuplja lokalne službenike za kibersigurnost svih subjekata Unije s ciljem olakšavanja razmjene najboljih praksi i iskustava stecenih provedbom ove Uredbe;*
- (if) *razraduje plan za incidente i za odgovor na velike incidente i koordinira donošenje planova za upravljanje kiberkrizama pojedinačnih subjekata Unije iz članka 7. stavka 2.a;*
- (ig) *donosi preporuke na temelju rezultata koordiniranih procjena sigurnosnih rizika ključnih lanaca opskrbe na razini Unije iz članka 22. Direktive (EU) 2022/2555 za potporu subjektima Unije u donošenju učinkovitih i razmernih mjera upravljanja kibersigurnosnim rizicima koje se odnose na sigurnost lanca opskrbe iz članka 5. stavka 1.ai točke (m);*
- (ih) *izrađuje smjernice za mehanizme razmjene informacija iz članka 19.*

Članak 11.

Usklađenost

1. IICB prati kako **subjekti** Unije provode ovu Uredbu i donešene smjernice, preporuke i pozive na djelovanje. Ako IICB utvrdi da **subjekti** Unije nisu učinkovito primjenjivali ili provodili ovu Uredbu ili smjernice, preporuke i pozive na djelovanje izdane na temelju ove Uredbe, može, ne dovodeći u pitanje unutarnje postupke relevantnog **subjekta** Unije:
 - (-a) *zatražiti relevantnu i dostupnu dokumentaciju o dotičnom subjektu Unije;*
 - (-aa) *dostaviti obrazloženo mišljenje dotičnom subjektu Unije u kojem navodi uočene nedostatke u provedbi ove Uredbe;*

(-ab) pozvati dotičnog subjekta Unije da u određenom roku dostavi samoprocjenu na temelju obrazloženog mišljenja;

(-ac) nakon savjetovanja s CERT-EU-om izdati smjernice namijenjene pojedinim subjektima Unije s ciljem da se njihov okvir, mjere upravljanja kibersigurnosnim rizicima, planovi za kibersigurnost i obveze izvješćivanja u utvrđenom roku usklade s ovom Uredbom;

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

(b) **zatražiti** od mjerodavne revizorske službe da provede reviziju;

(ba) obavijestiti Revizorski sud o navodnoj neusklađenosti.

Sva upozorenja i preporuke upućuju se najvišoj rukovodećoj razini predmetnog subjekta Unije.

2. *Ako mali subjekti Unije obavijeste da nisu u mogućnosti poštovati rokove iz članka 4. stavka 1. i članka 5. stavka 1., IICB može u iznimnim slučajevima odobriti njihovo produljenje i određuje rokove za usklađivanje.*

Poglavlje IV.

CERT-EU

Članak 12.

Misija i zadaće CERT-EU-a

1. Misija CERT-EU-a, autonomnog međuinstitucijskog centra za kibersigurnost svih **subjekata** Unije, jest pridonositi sigurnosti neklasificiranog **IKT** okruženja svih **subjekata** Unije *i pružati im usluge analogne CSIRT-ovima koje su države članice osnovale u skladu s Direktivom 2022/2555, posebno* pružanjem savjeta o kibersigurnosti, pomaganjem u sprečavanju, otkrivanju, **obradivanju** i ublažavanju incidenata, odgovoru na njih *i oporavku od njih* te preuzimanjem uloge njihova koordinacijskog čvorišta za razmjenu informacija o kibersigurnosti i za odgovor na incidente.
2. CERT-EU obavlja sljedeće zadaće za **subjekte** Unije:

- (a) pruža im potporu u provedbi ove Uredbe i pridonosi koordinaciji primjene ove Uredbe putem mjera navedenih u članku 13. *stavku 1.*; ili putem ad hoc izvješća koja je zatražio IICB;
 - (b) pruža im potporu paketom kibersigurnosnih usluga opisanih u njegovu katalogu usluga („osnovne usluge”);
 - (ba) za subjekte Unije koji za to sami nemaju kapacitete upravlja Centrom za sigurnosne operacije širokog spektra (SOC) koji prati mreže, što uključuje prvu liniju nadzora 24 sata dnevno sedam dana u tjednu u slučaju vrlo ozbiljnih prijetnji;
 - (c) održava mrežu kolega i partnera radi pružanja potpore uslugama kako je navedeno u člancima 16. i 17.;
 - (d) skreće pozornost IICB-a na sva pitanja koja se odnose na provedbu ove Uredbe i provedbu smjernica iz članka 13. i podnošenje prijedloga za preporuke;
 - (e) izvješćuje subjekte Unije o relevantnim kiberprijetnjama █ i pridonosi informiranosti o kibersigurnosnoj situaciji u Uniji, uzimajući u obzir mišljenje ENISA-e, te ta izvješća podnosi IICB-u, mreži CSIRT-ova iz članka 15. Direktive (EU) 2022/2555 i Obavještajnom i situacijskom centru EU-a (EU-INTCEN);
- (ea) djeluje kao imenovani koordinator za subjekte Unije u svrhu koordiniranog bilježenja ranjivosti u europskoj bazi podataka o ranjivosti navedenoj u članku 12. Direktive (EU) 2022/2555;
 - (eb) nakon savjetovanja s ENISA-om predlaže IICB-u sigurnosne kriterije, popis mogućih ključnih pokazatelja uspješnosti i razmjere okvira za kibersigurnost koje koriste subjekti Unije;
 - (ec) nakon savjetovanja s ENISA-om predlaže IICB-u područja kibersigurnosti i kibersigurnosne mjere koje subjekti Unije trebaju uzeti u obzir u svojem okviru za kibersigurnost te određuje prioritete u pogledu tih područja i mjera;
 - (ed) subjektima Unije pruža jedan ili više modela razvijenosti kibersigurnosti koji će se upotrebljavati u njihovim okvirima za kibersigurnost i koji odražavaju njihovu veličinu i područja kibersigurnosti kojima se koriste;

- (ee) pruža usluge kojima se, uz visoku razinu transparentnosti i pouzdanosti, podupire razmjena informacija, posebno u pogledu obavijesti koje subjekti Unije dostavljaju CERT-EU-u.
- (ef) provodi redovitu analizu rizika u pogledu međupovezanosti subjekata Unije radi podupiranja zadaća IICB-a.
3. CERT-EU pridonosi radu Zajedničke jedinice za kibersigurnost, osnovane u skladu s Preporukom Komisije od 23. lipnja 2021., među ostalim u sljedećim područjima:
- (a) pripravnost, koordinacija incidenata, razmjena informacija i odgovor na krize na tehničkoj razini u slučajevima povezanim sa **subjektima** Unije;
 - (b) operativna suradnja u pogledu mreže timova za odgovor na računalne sigurnosne incidente (CSIRT-ovi), uključujući međusobnu pomoć, i šire kibersigurnosne zajednice;
 - (ba) koordinacija upravljanja većim incidentima i krizama na operativnoj razini te redovita razmjena relevantnih informacija među državama članicama i subjektima Unije u okviru Europske mreže organizacija za vezu za kiberkrize (EU-CyCLONe);
 - (c) saznanja o prijetnjama, uključujući informiranost o situaciji;
 - (ca) proaktivno skeniranje mrežnih i informacijskih sustava;
 - (d) sve teme za koje je potrebna tehnička stručnost CERT-EU-a u području kibersigurnosti.
4. CERT-EU sudjeluje u strukturiranoj suradnji s **ENISA-om** na izgradnji kapaciteta, operativnoj suradnji i dugoročnim strateškim analizama kiberprijetnji u skladu s Uredbom (EU) 2019/881. **CERT-EU može surađivati i razmjenjivati informacije s Europolovim Centrom za kiberkriminalitet.**
5. CERT-EU **subjektima Unije** može pružati sljedeće usluge koje nisu opisane u njegovu katalogu usluga („usluge uz naknadu”):
- (a) usluge kojima se podupire kibersigurnost **IKT** okruženja **subjekata** Unije, osim onih iz stavka 2., na temelju sporazumâ o razini usluga i ovisno o dostupnim resursima, **uključujući, putem svojeg Centra za sigurnosne operacije iz stavka**

- 2. točke (ba), praćenje mreža i prvu liniju nadzora 24 sata dnevno sedam dana u tjednu u slučaju vrlo ozbiljnih prijetnji za veće subjekte Unije;*
- (b) usluge kojima se podupiru kibersigurnosne operacije ili projekti subjekata Unije koje ne služe za zaštitu njihovih **IKT** okruženja, na temelju pisanih sporazuma i uz prethodno odobrenje IICB-a;
- (c) usluge kojima se podupire sigurnost **IKT** okruženja organizacija koje nisu **subjekti** Unije, a koje blisko surađuju sa **subjektima** Unije, na primjer zbog zadaća ili dužnosti dodijeljenih na temelju prava Unije, na temelju pisanih sporazuma i uz prethodno odobrenje IICB-a.
6. CERT-EU *organizira* vježbe u području kibersigurnosti ili preporučiti sudjelovanje u postojećim vježbama, u bliskoj suradnji s **ENISA-om** kad je to primjenjivo, kako bi se *redovito* ispitivala razina kibersigurnosti **subjekata** Unije.
7. CERT-EU *pruža* pomoć **subjektima** Unije u pogledu incidenata u povjerljivim **IKT** okruženjima ako predmetna sastavnica to izričito zatraži. *Odredbe i obveze svih subjekata Unije utvrđene u poglavljju V. ne primjenjuju se na incidente u povjerljivim okruženjima IKT-a osim ako ih određeni subjekt Unije izričito i dobrovoljno ne primjeni kako bi zatražila praktičnu pomoć CERT-EU-a ili na drugi način doprinijela informiranosti o stanju na razini Unije.*
- 7.a *CERT-EU Europskom parlamentu podnosi godišnje izvješće o svojim aktivnostima pod odgovarajućim uvjetima povjerljivosti. To izvješće uključuje relevantne i precizne informacije o većim incidentima i načinu na koji su riješeni.*
- 7.b *CERT-EU surađuje s Europskim nadzornikom za zaštitu podataka kako bi pružio potporu subjektima Unije u incidentima koji uključuju povredu osobnih podataka kako je definirana u članku 3. točki 16. Uredbe (EU) 2018/1725.*
- 7.c *Obrada osobnih podataka koju provodi CERT-EU na temelju ove Uredbe podliježe Uredbi (EU) 2018/1725.*
- 7.d *CERT-EU može pružati pomoć subjektima Unije u provedbi odgovarajuće suradnje u području kibersigurnosti među njima, u pogledu znanja, osoblja i resursa IKT-a u području kibersigurnosti te stručnog znanja u području kibersigurnosti.*

- 7.e CERT-EU obavljačuje Europskog nadzornika za zaštitu podataka o rješavanju znatnih ranjivosti, ozbiljnih incidenata ili velikih napada koji bi mogli dovesti do povreda osobnih podataka i/ili povrede povjerljivosti električkih komunikacija.*
- 7.f CERT-EU obavljačuje EDPS o preventivnim aktivnostima u području kibersigurnosti koje će rezultirati prikupljanjem osobnih podataka.*

Članak 13.

Smjernice, preporuke i pozivi na djelovanje

1. CERT-EU podupire provedbu ove Uredbe objavljinjem:
 - (a) poziva na djelovanje u kojima se opisuju hitne sigurnosne mjere koje *subjekti* Unije trebaju poduzeti u zadnom roku;
 - (b) prijedloga IICB-u za smjernice upućene svim *subjektima* Unije ili nekoj njihovoj podskupini;
 - (c) prijedloga IICB-u za preporuke upućene pojedinim *ili svim subjektima Unije*.
2. Smjernice i preporuke mogu sadržavati:
 - (a) modalitete za upravljanje kibersigurnosnim rizicima i **mjerama za upravljanje kibersigurnosnim** rizicima ili njihovo poboljšanje;
 - (b) *načine* za procjenu razvijenosti *kibersigurnosti* i planove za kibersigurnost; te
 - (c) prema potrebi, korištenje zajedničke tehnologije, arhitekture *otvorenog koda* i povezane najbolje prakse radi postizanja interoperabilnosti i zajedničkih normi;
 - (ca) *prema potrebi, olakšavanje zajedničke nabave relevantnih IKT usluga i IKT proizvoda.*

Članak 14.

Voditelj CERT-EU-a

Nakon što dobije dvotrećinsku suglasnost članova IICB-a, Komisija imenuje voditelja CERT-EU-a. Savjetovanje s IICB-om obavezno je u svim fazama postupka prije imenovanja

voditelja CERT-EU-a, posebno pri izradi obavijesti o slobodnom radnom mjestu, razmatranju prijava i imenovanju odbora za odabir za to radno mjesto. Na konačnom popisu kandidata nalazi se najmanje jedan muškarac i jedna žena.

Voditelj CERT-EU-a **barem jednom godišnje** podnosi izvješća IICB-u i predsjedniku IICB-a o *aktivnostima i uspješnosti CERT-EU-a tijekom referentnog razdoblja, uključujući o izvršenju proračuna, sklopljenim sporazumima o razini usluga i pisanim sporazumima, suradnji s ugovornim stranama i partnerima te službenim putovanjima osoblja, uključujući izvješća iz članka 10. . Ta izvješća uključuju program rada za sljedeće razdoblje, financijsko planiranje prihoda i rashoda, uključujući zapošljavanje osoblja, planirano ažuriranje kataloga usluga CERT-EU-a i procjenu očekivanog učinka koji bi takva ažuriranja mogla imati u pogledu financijskih i ljudskih resursa.*

Voditelj CERT-EU-a također podnosi ad hoc izvješća IICB-u na njegov zahtjev.

Članak 15.

Financijska pitanja i osoblje

1. *CERT-EU je kao autonoman međuinstitucijski pružatelj usluga svim subjektima Unije, uključen u administrativnu strukturu glavne uprave Komisije kako bi se ostvarila korist od Komisijinih administrativnih, financijskih, upravljačkih i računovodstvenih potpornih struktura. Komisija obavješćuje IICB o administrativnom položaju CERT-EU-a i svim promjenama tog položaja. Taj se pristup treba redovito evaluirati kako bi se omogućilo poduzimanje odgovarajućih mjera, uključujući moguće osnivanje CERT-EU-a kao ureda Unije.*
1.a Sve odluke povezane sa zapošljavanjem i dodjelom proračunskih sredstava CERT-EU-a podnose se IICB-u na službeno odobrenje.
2. Tijekom primjene upravnih i financijskih postupaka voditelj CERT-EU-a djeluje **pod nadzorom Komisije i IICB-a**.
3. Zadaće i aktivnosti CERT-EU-a, uključujući usluge koje CERT-EU u skladu s člankom 12. stavcima 2., 3., 4. i 6. te člankom 13. stavkom 1. pruža **subjektima** Unije financiranim iz naslova višegodišnjeg financijskog okvira namijenjenog europskoj

javnoj upravi financiraju se iz posebne proračunske linije proračuna Komisije. Radna mjesta namijenjena CERT-EU-u detaljno se navode u bilješci uz plan radnih mjesta Komisije.

4. **Subjekti** Unije osim onih iz stavka 3. daju godišnji finansijski doprinos CERT-EU-u za pokrivanje usluga koje CERT-EU pruža u skladu s tim stavkom 3. Pojedini doprinosi temelje se na smjernicama koje je dao IICB i svi ih subjekti dogovaraju s CERT-EU-om u sporazumima o razini usluga. Doprinosi odgovaraju pravednom i razmjernom udjelu u ukupnim troškovima pruženih usluga. Zaprimaju se u posebnoj proračunskoj liniji iz stavka 3. kao namjenski prihod kako je predviđeno člankom 21. stavkom 3. točkom (c) Uredbe (EU, Euratom) 2018/1046 Europskog parlamenta i Vijeća⁹.
5. **Subjekti** Unije koji primaju usluge CERT-EU-a nadoknađuju troškove zadaća definiranih u članku 12. stavku 5. Prihodi se dodjeljuju proračunskim linijama kojima se financiraju navedeni troškovi.

Članak 16.

Suradnja CERT-EU-a s partnerima iz država članica

1. CERT-EU surađuje i razmjenjuje informacije s nacionalnim partnerima u državama članicama, uključujući CERT-ove, nacionalne centre za kibersigurnost, CSIRT-ove i jedinstvene kontaktne točke iz članka 8. Direktive (EU) 2022/2555, o kiberprijetnjama, ranjivostima, incidentima, *izbjegnutim incidentima*, mogućim protumjerama *te najboljim praksama* i o svim pitanjima važnim za poboljšanje zaštite *informacičkog i komunikacijskog* okruženja *subjekata* Unije, među ostalim putem mreže CSIRT-ova iz članka 15. Direktive (EU) 2022/2555. **CERT-EU podupire Komisiju u okviru mreže EU-CyCLONe iz članka 16. Direktive 2022/2555 o koordiniranom upravljanju većim incidentima i krizama.**

⁹ Uredba (EU, Euratom) 2018/1046 Europskog parlamenta i Vijeća od 18. srpnja 2018. o finansijskim pravilima koja se primjenjuju na opći proračun Unije, o izmjeni uredaba (EU) br. 1296/2013, (EU) br. 1301/2013, (EU) br. 1303/2013, (EU) br. 1304/2013, (EU) br. 1309/2013, (EU) br. 1316/2013, (EU) br. 223/2014, (EU) br. 283/2014 i Odluke br. 541/2014/EU te o stavljanju izvan snage Uredbe (EU, Euratom) br. 966/2012 (SL L 193, 30.7.2018., str. 1.).

2. CERT-EU može s nacionalnim partnerima u državama članicama razmjenjivati informacije o određenim incidentima bez ***odobrenja*** pogodene sastavnice kako bi se olakšalo otkrivanje sličnih kiberprijetnji ili incidenata, ***pod uvjetom da su osobni podaci zaštićeni u skladu s primjenjivim odredbama Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća***¹⁰. Informacije o određenim incidentima kojima se otkriva identitet mete kiberincidenta CERT-EU može razmjenjivati samo uz ***odobrenje pogodene*** sastavnice ***te u skladu s primjenjivim odredbama Uredbe (EU) 2016/679.***

Članak 17.

Suradnja CERT-EU-a s partnerima iz trećih zemalja

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

Poglavlje V.

¹⁰ ***Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) (SL L 119, 4.5.2016., str. 1.).***

OBVEZE SURADNJE I IZVJEŠĆIVANJA

Članak 18.

Postupanje s podacima

1. CERT-EU i *subjekti* Unije moraju poštovati obvezu čuvanja poslovne tajne u skladu s člankom 339. Ugovora o funkcioniranju Europske unije ili jednakovrijednim primjenjivim okvirima.
2. Odredbe Uredbe (EZ) br. 1049/2001 Europskog parlamenta i Vijeća¹¹ primjenjuju se na zahtjeve za javni pristup dokumentima koje posjeduje CERT-EU, uključujući obvezu na temelju te uredbe u pogledu savjetovanja s drugim *subjektima* Unije, *ili, prema potrebi državama članicama*, kad se zahtjev odnosi na njihove dokumente.
3. Obrada osobnih podataka koja se provodi na temelju ove Uredbe podliježe Uredbi (EZ) 2018/1725 ┌ .

Svaka obrada, razmjena, prikupljanje ili zadržavanje osobnih podataka koje provode CERT-EU, IIICB i subjekti Unije ograničena je na obradu, razmjenu, prikupljanje ili zadržavanje koje je nužno potrebno i provodi se isključivo u svrhu ispunjavanja njihovih obveza na temelju ove Uredbe.

- 3.a *Komisija do... [jedna godina nakon datuma stupanja na snagu ove Uredbe] u skladu s člankom 24.a donosi delegirani akt kojim se određuje koje su aktivnosti obrade osobnih podataka dopuštene ovom Uredbom, uključujući svrhu obrade, kategorije osobnih podataka, kategorije ispitanika, uvjete obrade podataka, maksimalna razdoblja zadržavanja, definiciju voditelja obrade i izvršitelja obrade te primatelje u slučaju prijenosa.*

Delegiranim aktom iz prvog podstavka aktivnosti obrade ograničavaju se na one koje su nužno potrebne i njime se zahtijeva da takve aktivnosti obrade budu što je moguće usmjerene i da ne uključuju neselektivno zadržavanje podataka o prometu ili sadržaju.

¹¹ Uredba (EZ) br. 1049/2001 Europskog parlamenta i Vijeća od 30. svibnja 2001. o javnom pristupu dokumentima Europskog parlamenta, Vijeća i Komisije (SL L 145, 31.5.2001., str. 43.).

Komisija mijenja delegirani akt iz prvog podstavka ako utvrdi znatne promjene u pogledu nužnosti ili posebnih svrha ili subjekata uključenih u obradu osobnih podataka za potrebe ove Uredbe.

4. Postupanje CERT-EU-a i pripadajućih **subjekata** Unije s podacima mora biti u skladu s pravilima utvrđenima u [predloženoj Uredbi o sigurnosti podataka]. *I pri suradnji s drugim partnerima CERT-EU pravila o postupanju s informacijama trebala bi biti ista.*
5. Svi kontakti s CERT-EU-om koje pokrenu ili zatraže nacionalne sigurnosne i obavještajne službe priopćuju se bez nepotrebne odgode Glavnoj upravi Komisije za sigurnost, **Europolu** i predsjedniku IICB-a.
 - 5.a *Informacije o završetku izrade sigurnosnih planova subjekata Unije dijele se s tijelima nadležnima za davanje razrješnice.*
 - 5.b *Smjernice i preporuke te pozivi na djelovanje koje izdaje IICB dijele se s tijelima nadležnima za davanje razrješnice.*

Članak 19.

Mehanizmi i obveze za razmjenu informacija o kibersigurnosti

- 1. *Subjekti Unije mogu dobrovoljno obavijestiti CERT-EU o kiberprijetnjama, incidentima, izbjegnutim incidentima i ranjivostima koji na njih utječu i dostaviti informacije o njima. CERT-EU osigurava donošenje učinkovitih mjera kako bi se osigurala povjerljivost i odgovarajuća zaštita informacija koje pruža subjekt Unije koji izvješćuje. CERT-EU osigurava dostupnost učinkovitih sredstava komunikacije u svrhu olakšavanja razmjene informacija sa subjektima Unije. Pri obradi obavijesti, CERT-EU obradi obveznih obavijesti može dati prednost pred obradom obavijesti na dobrovoljnoj osnovi. Subjektu koji je obavijest podnio dobrovoljno ne smiju se zbog tog obavješćivanja Unije nametati dodatne obveze kojima ne bi podlijegao da nije podnio tu obavijest.*
1. Kako bi CERT-EU mogao *djelotvorno izvršiti misiju i zadaće utvrđene u članku 12. ove Uredbe, posebice* koordinirati upravljanje ranjivostima █, može od **subjekata** Unije zatražiti da mu iz svojih evidencija **IKT** sustava dostave informacije relevantne za █ pomoć koju pruža CERT-EU. **Subjekt Unije** kojem je podnesen zahtjev bez

nepotrebne odgode *može prenijeti* tražene informacije i sva njihova naknadna ažuriranja.

Ne dovodeći u pitanje Uredbu (EU) 2018/1725, svaka razmjena podataka između CERT-EU-a i subjekata Unije provodi se u skladu s načelima jasnih zaštitnih mjera za posebne slučajevе upotrebe i upotrebljava ugovore o uzajamnoj pravnoj pomoći i druge sporazume kako bi se osigurala visoka razina zaštite prava pri obradi zahtjeva za prekogranični pristup podacima.

|

3. Informacije o određenim incidentima kojima se otkriva identitet *subjekta* Unije pogodenog incidentom CERT-EU može razmjenjivati samo uz suglasnost tog subjekta. Informacije o određenim incidentima kojima se otkriva identitet mete kiberincidenta CERT-EU može razmjenjivati samo uz suglasnost subjekta pogodenog incidentom. *S obzirom na svoje nadzorne zadaće, Europski parlament može zatražiti te informacije i bez suglasnosti subjekta Unije. Ako Europski parlament zatraži informacije bez suglasnosti dotičnog subjekta, njegove rasprave ne smiju biti javne, a svi relevantni dokumenti razmatraju se samo na temelju nužnosti pristupa informacijama.*
4. Obveze *i uvjeti* o razmjeni *kibersigurnosnih informacija* ne odnose se na klasificirane podatke EU-a (EUCI) ni na informacije koje je *subjekt* Unije primio od sigurnosne ili obavještajne službe države članice ili tijela za izvršavanje zakonodavstva, *osim ako dotična sigurnosna ili obavještajna služba države članice ili tijelo za izvršavanje zakonodavstva dopusti da se te informacije* razmjenjuju s CERT-EU-om.

Članak 20.

Obveze *izvješćivanja*

1. Svi *subjekti* Unije *izvješćuju* CERT-EU u *skladu sa stavkom 1.d o svakom incidentu koji ima znatan učinak. Incident se smatra značajnim:*
 - (a) *ako je uzrokovao ili može uzrokovati ozbiljne poremećaje u funkcioniranju usluga ili financijske gubitke za predmetni subjekt;*

(b) ako je utjecao ili može utjecati na druge fizičke ili pravne osobe uzrokovanjem znatne materijalne ili nematerijalne štete.

- 1.a Subjekti Unije izvješćuju, među ostalim, o svim informacijama koje CERT-EU-u omogućuju da utvrdi učinak incidenta na ostale subjekte, učinak na državu članicu domaćina ili prekogranični učinak nakon značajnog incidenta. Subjekt Unije koji obavlja obavešćenje ne podliježe samo zbog toga povećanoj odgovornosti.
- 1.b Prema potrebi, subjekti Unije bez nepotrebne odgode obavješćuju korisnike pogodjenih mrežnih i informacijskih sustava ili drugih komponenti IKT okruženja na koje bi mogao utjecati ozbiljan incident ili ozbiljna kiberprijetnja o svim mjerama ili postupcima koji se mogu poduzeti kao odgovor na taj incident ili prijetnju. O samoj prijetnji korisnika obavješćuju, prema potrebi, subjekte Unije.
- 1.c Ako ozbiljan incident ili ozbiljna kiberprijetnja utječe na mrežni i informacijski sustav ili komponentu IKT okruženja subjekta Unije koja je svjesno povezana s IKT okruženjem drugog subjekta Unije, CERT-EU bez nepotrebne odgode obavješćuje pogodjeni subjekt Unije.
- 1.d Svi subjekti Unije podnose CERT-EU-u:
- (a) bez nepotrebne odgode, a u svakom slučaju u roku od 24 sata od kad su saznali za ozbiljan incident, rano upozorenje u kojem se, prema potrebi, navodi sumnja li se da je ozbiljan incident uzrokovan nezakonitim ili zlonamernim djelovanjem te bi li mogao imati učinak na subjekte ili prekogranični učinak;
 - (b) bez nepotrebne odgode, a u svakom slučaju u roku od 72 sata od kad su saznali za ozbiljan incident, izvješće o incidentu kojom se, prema potrebi, ažuriraju informacije iz točke (a) i navodi početna procjena ozbiljnog incidenta, njegove ozbiljnosti i učinka te, ako su dostupni, pokazatelje kompromisa;
 - (c) na zahtjev CERT-EU-a, privremeno izvješće o relevantnim ažuriranjima statusa.
2. Osim toga, subjekti Unije podnosi CERT-EU-u završeno izvješće, najkasnije jedan mjesec nakon podnošenja izvješća o incidentu iz stavka 1.d točke (b). u slučajevima ozbiljnih incidenta koji su u tijeku u trenutku podnošenja završnog izvješća, izvješće o napretku u tom trenutku i završno izvješće podnose se u roku od mjesec

dana nakon što je incident riješen. Izvješće o incidentu sadržava barem sljedeće informacije, ako su dostupne:

- (a) *detaljni opis incidenta, uključujući njegovu ozbiljnost i učinak;*
- (b) *vrstu prijetnje ili temeljnog uzroka koji je vjerojatno prouzročio incident;*
- (c) *mjere za ublažavanje koje su provedene ili se provode;*
- (d) *ako je primjenjivo, potencijalni utjecaj incidenta na druge subjekte Unije ili prekogranični utjecaj.*

- 2.a *U opravdanim slučajevima i u dogovoru s CERT-EU-om predmetni subjekt Unije može odstupiti roka utvrđenog u stavku 2. Ako je postignut dogovor o izuzeću, predmetni subjekt Unije dostavlja izvješće o napretku u roku za podnošenje završnog izvješća.*
- 2.b *Subjekti Unije na zahtjev CERT-EU-a i bez nepotrebne odgode dostavljaju CERT-EU-u digitalne informacije nastale upotrebom elektroničkih uređaja u predmetnim incidentima. CERT-EU može dodatno pojasniti koje su mu vrste tih digitalnih informacija potrebne za informiranost o stanju i odgovor na incident.*
3. CERT-EU jedanput mjesечно dostavlja ENISA-i sažeto izvješće koje uključuje anonimizirane i zbirne podatke o ozbiljnim *incidentima*, kiberprijetnjama, *incidentima, izbjegnutim incidentima i ranjivostima* prijavljenima u skladu sa stavkom 1.d ovog članka i s člankom 19. stavkom -1.
4. *Najkasnije ... [jednu godinu nakon datuma stupanja na snagu Uredbe] CERT-EU izdaje smjernice ili preporuke o uvjetima koji se odnose na izvješća i njihovu sadržaju. Pri pripremi takvih smjernica ili preporuka, CERT-EU uzima u obzir specifikacije iz provedbenih akata koje je donijela Komisija, a kojima se određuje vrsta informacija, oblik i postupak za obavijesti podnesene u skladu s člankom 23. stavkom 11. Direktive (EU) 2022/2555. CERT-EU prosljeđuje odgovarajuće tehničke pojedinosti kako bi se *subjektima* Unije omogućilo poduzimanje proaktivnih mjera za otkrivanje, odgovor na incidente ili ublažavanje.*
5. Obveze *izvješćivanja* ne odnose se na klasificirane podatke EU-a ni na informacije koje je *subjekt* Unije primio od sigurnosne ili obavještajne službe države članice ili

tijela za izvršavanje zakonodavstva uz izričit uvjet da se one ne dijele s CERT-EU-om.

Članak 21.

Koordinacija odgovora na incidente i suradnja

1. CERT-EU djeluje kao koordinacijsko čvorište za razmjenu informacija o kibersigurnosti i za odgovor na incidente te tako olakšava razmjenu informacija o kiberprijetnjama, ranjivostima, ***izbjegnutim incidentima*** i incidentima među:
 - (a) ***subjektima*** Unije;
 - (b) partnerima iz članaka 16. i 17.
2. CERT-EU olakšava koordinaciju odgovora na incidente među ***subjektima*** Unije, uključujući:
 - (a) doprinos dosljednoj vanjskoj komunikaciji;
 - (b) uzajamnu pomoć;
 - (c) optimalnu upotrebu operativnih resursa;
 - (d) koordinaciju s drugim mehanizmima za odgovor na krize na razini Unije.
3. CERT-EU, *u suradnji s ENISA-om*, pruža potporu ***subjektima*** Unije u pogledu informiranosti o kiberprijetnjama, ranjivostima, ***izbjegnutim incidentima*** i incidentima *te pruža informacije o najnovijim zbivanjima u području kibersigurnosti*.
4. *Najkasnije ... /jednu godinu nakon datuma stupanja na snagu Uredbe/* IICB izdaje smjernice o koordinaciji odgovora na incidente i suradnji U slučaju ozbiljnih incidenata. Ako se sumnja da je incident kaznene prirode, ***IICB i CERT-EU bez nepotrebnog odgadanja*** savjetuju o tome kako prijaviti incident tijelima za izvršavanje zakonodavstva.

Članak 22.

Veći *incidenti*

1. CERT-EU koordinira *upravljanje* većim *napadima* među *subjektima* Unije. *U tom pogledu* vodi evidenciju *dostupnog* tehničkog stručnog znanja koje bi bilo potrebno za odgovor na incident u slučaju takvih *većih incidenata i pomaže IICB-u u koordinaciji planova za upravljanje kiberkrizama subjekata Unije za veće incidente iz članka 7. točke (2.a).*
2. *Subjekti* Unije pridonose evidentiranju tehničkog stručnog znanja dostavljanjem popisa stručnjaka dostupnih u njihovim organizacijama; popis se ažurira jedanput godišnje, a sadržava pojedinosti o specifičnim tehničkim vještinama predmetnih stručnjaka.
3. U skladu s █ operativnim postupcima mreže *EU CyCLONe*, CERT-EU uz odobrenje █ *predmetnih subjekata* Unije može pozvati i stručnjake s popisa iz stavka 2. da pridonesu odgovoru na veći *incident* u državi članici. *IICB na prijedlog CERT EU-a odobrava posebna pravila o pristupu tehničkim stručnjacima iz subjekata Unije i njihovom djelovanju.*

Poglavlje VI.

ZAVRŠNE ODREDBE

Članak 23.

Početni proračunski *aranžmani*

1. *U svojem prijedlogu za donošenje prvog proračuna nakon... [datum stupanja na snagu ove Uredbe] Komisija uzima u obzir povećane potrebe za proračunom i osobljem svih subjekata Unije, posebno malih subjekata Unije, koji su povezani s obvezama koje proizlaze iz ove Uredbe.*
2. *Kako bi se osiguralo pravilno i stabilno funkcioniranje CERT-EU-a, Komisija može predložiti preraspodjelu osoblja i finansijskih sredstava █ u proračun Komisije za upotrebu u operacijama CERT-EU-a iz proračuna za IKT određenih subjekata Unije na temelju jasnih kriterija i ne dovodeći u pitanje njihovu kibersigurnost.* Preraspodjela stupa na snagu istodobno s prvim proračunom koji se donese nakon stupanja na snagu ove Uredbe.

Članak 24.

Preispitivanje

1. IICB, uz pomoć CERT-EU-a, **barem jednom godišnje**, izvješćuje Komisiju o provedbi ove Uredbe. IICB može Komisiji preporučiti i da predloži izmjene ove Uredbe.
2. Komisija **ocjenjuje i** izvješćuje Europski parlament i Vijeće o provedbi ove Uredbe **i iskustvu stečenom na strateškoj i operativnoj razini do... /36 mjeseci od datuma stupanja ove Uredbe na snagu/** i nakon toga svake **dvije** godine.
- 2.a **U izvješćima iz stavka 2. ovog članka ocjenjuje se, uzimajući u obzir članak 15. stavak 1.a, mogućnost uspostave CERT-EU-a kao ureda Unije.**
3. Komisija provodi evaluaciju ove Uredbe i podnosi izvješće Europskom parlamentu, Vijeću, Europskom gospodarskom i socijalnom odboru i Odboru regija najranije pet godina od stupanja na snagu ove Uredbe.

Članak 24.a

Izvršavanje delegiranja ovlasti

1. **Ovlast za donošenje delegiranih akata dodjeljuje se Komisiji podložno uvjetima utvrđenima u ovom članku.**
2. **Ovlast za donošenje delegiranih akata iz članka 18. članka 3.a dodjeljuje se Komisiji na neodređeno razdoblje počevši od ... [jedan dan nakon datuma stupanja na snagu ove Uredbe].**
3. **Europski parlament ili Vijeće u svakom trenutku mogu opozvati delegiranje ovlasti iz članka 18. stavka 3.a. Odlukom o opozivu prekida se delegiranje ovlasti koje je u njoj navedeno. Opoziv počinje proizvoditi učinke sljedećeg dana od dana objave spomenute odluke u Službenom listu Europske unije ili na kasniji dan naveden u spomenutoj odluci. On ne utječe na valjanost delegiranih akata koji su već na snazi.**
4. **Čim doneše delegirani akt, Komisija ga istodobno priopćuje Europskom parlamentu i Vijeću.**
5. **Delegirani akt donesen u skladu s člankom 18. stavkom 3.a stupa na snagu samo ako se tome ne usprotive ni Europski parlament ni Vijeće u roku od dva mjeseca od**

priopćenja Europskom parlamentu i Vijeću o tom aktu ili ako su prije isteka tog roka i Europski parlament i Vijeće obavijestili Komisiju da se ne protive. Taj se rok prodljuje za dva mjeseca na inicijativu Europskog parlamenta ili Vijeća.

Članak 25.

Stupanje na snagu

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

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

Sastavljeno u ...

Za Europski parlament

Predsjednik/Predsjednica

Za Vijeće

Predsjednik/Predsjednica

OBRAZLOŽENJE

KONTEKST

KONTEKST

U svojem prijedlogu o mjerama za visoku zajedničku razinu kibersigurnosti u institucijama, tijelima, uredima i agencijama Unije Komisija je utvrdila mjere za sve subjekte Unije kako bi uspostavili okvir za zajednička pravila i mjere u području kibersigurnosti radi poboljšanja njihove otpornosti i sposobnosti odgovora na incidente. Riječ je o prvom zakonodavnom aktu Unije usmjerenom na kibersigurnost institucija, tijela, ureda i agencija Unije.

Cilj je prijedloga poboljšati otpornost i sposobnost subjekata Unije za odgovor na incidente te proširiti mandat i financiranje CERT-EU-a, koji će se preimenovati iz „Tima za hitne računalne intervencije” u „Centar za kibersigurnost”. Prijedlogom se osniva i Međuinstitucijski odbor za kibersigurnost (IICB), koji je zadužen za praćenje načina na koji institucije, tijela, uredi i agencije Unije provode Uredbu te za nadziranje načina na koji CERT-EU provodi opće prioritete i ciljeve.

IZVJESTITELJICA

Izvjestiteljica pozdravlja prijedlog Komisije i slaže se s izborom uredbe kao pravog instrumenta za suočavanje s rastućim trendom kiberprijetnji s obzirom na to da se broj ozbiljnih incidenata koji utječu na institucije, tijela, uredi i agencije EU-a, a čiji su počinitelji akteri iz kategorije naprednih kontinuiranih prijetnji (APT) znatno povećao između 2019. i 2021. Stoga bi trebalo posvetiti više pozornosti pitanjima kibersigurnosti te bi za tu svrhu trebalo namijeniti odgovarajuća proračunska sredstva.

Izvjestiteljica smatra da je ovaj prijedlog ključan kako bi se poboljšala otpornost i zaštita javne uprave EU-a s obzirom na sve veći broj kibersigurnosnih prijetnji, koje su sve sofisticirane. U tom kontekstu međuinstitucijska suradnja korisna je za otkrivanje, sprečavanje, praćenje i odgovor na kiberprijetnje i povezane rizike. Institucije, tijela, uredi i agencije Unije trebaju razviti svoje kibersigurnosne mјere i odgovore na kiberprijetnje te potencijalne napade. Stoga je potreban zajednički pristup.

Izvjestiteljica smatra da bi institucijama, tijelima, uredima i agencijama EU-a trebalo osigurati odgovarajuće resurse za suočavanje s izazovima sve češćih kibersigurnosnih prijetnji. Konkretno, trebalo bi zaštititi znanje i vještine u području kibersigurnosti u institucijama, tijelima, uredima i agencijama Unije.

U prijedlogu se pitanje ljudskih resursa nastoji riješiti centraliziranjem resursa u okviru CERT-EU-a. Cilj predloženog centraliziranog modela jest poboljšati postupak zapošljavanja stručnjaka u institucijama, tijelima, uredima i agencijama Unije. Izvjestiteljica pozdravlja jačanje mandata CERT-EU-a i smatra da je potrebno osigurati resurse koji su potrebni za ispunjavanje tog mandata te da bi u budućnosti trebalo pažljivo razmotriti njegovu strukturu.

Institucije, tijela, uredi i agencije Unije znatno se razlikuju po veličini i ulozi. Neki od njih imaju značajne međunarodne mreže. Izvjestiteljica stoga ističe da bi im trebalo omogućiti

dostatnu razinu fleksibilnosti i pristup koji se temelji na riziku kako bi mogli izvršavati svoje zadaće. Istodobno bi trebalo pronaći jedinstven pristup za borbu protiv kibersigurnosnih prijetnji jer su sve institucije, tijela, uredi i agencije Unije međusobno povezani i ne bi smjelo biti slabih karika u lancu.

1.3.2023

MIŠLJENJE ODBORA ZA GRAĐANSKE SLOBODE, PRAVOSUĐE I UNUTARNE POSLOVE

upućeno Odboru za industriju, istraživanje i energetiku

o prijedlogu uredbe Europskog parlamenta i Vijeća o mjerama za visoku zajedničku razinu kibersigurnosti u institucijama, tijelima, uredima i agencijama Unije (COM(2022)0122 – C9-0122/2022 – 2022/0085(COD))

Izvjestitelj za mišljenje (*): Tomas Tobé

(*) Pridruženi odbor – članak 57. Poslovnika

AMANDMANI

Odbor za građanske slobode, pravosuđe i unutarnje poslove poziva Odbor za industriju, istraživanje i energetiku da kao nadležni odbor uzme u obzir sljedeće amandmane:

Amandman 1

Prijedlog uredbe Uvodna izjava 4.

Tekst koji je predložila Komisija

(4) Institucije, tijela i agencije Unije privlačne su mete koje se suočavaju s vrlo vještim i dobro opremljenim prijetećim akterima i drugim prijetnjama. Istodobno, razina i razvijenost kiberotpornosti te sposobnost otkrivanja zlonamjernih kberaktivnosti i odgovora na njih znatno se razlikuju od subjekta do subjekta. Kako bi europska uprava funkcionalala, institucije, tijela i agencije Unije stoga moraju ostvariti visoku zajedničku razinu kibersigurnosti putem osnovnog okvira za kibersigurnost (skupa minimalnih pravila za kibersigurnost s kojima mrežni i informacijski sustavi te njihovi operateri i

Izmjena

(4) Institucije, tijela i agencije Unije **bile su i** jesu privlačne mete koje se suočavaju s vrlo vještim i dobro opremljenim prijetećim akterima i drugim prijetnjama. Istodobno, razina i razvijenost kiberotpornosti te sposobnost otkrivanja zlonamjernih kberaktivnosti i odgovora na njih znatno se razlikuju od subjekta do subjekta. Kako bi europska uprava funkcionalala, institucije, tijela i agencije Unije stoga moraju ostvariti visoku zajedničku razinu kibersigurnosti putem osnovnog okvira za kibersigurnost (skupa minimalnih pravila za kibersigurnost s kojima mrežni i informacijski sustavi te

korisnici moraju biti usklađeni kako bi se kibersigurnosni rizici sveli na najmanju mjeru), kao i putem razmjene informacija i suradnje.

njihovi operateri i korisnici moraju biti usklađeni kako bi se kibersigurnosni rizici sveli na najmanju mjeru), kao i putem razmjene informacija i suradnje.

Amandman 2

Prijedlog uredbe Uvodna izjava 5.

Tekst koji je predložila Komisija

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

Izmjena

(5) Cilj je Direktive [prijeđlog NIS 2] o mjerama za visoku zajedničku razinu kibersigurnosti u cijeloj Uniji dodatno poboljšanje kiberotpornosti javnih i privatnih subjekata, nadležnih nacionalnih tijela i institucija te Unije u cjelini kao i njihove sposobnosti odgovora na incidente. Stoga se institucije, tijela i agencije Unije moraju tome prilagoditi osiguravanjem pravila koja su u skladu s Direktivom [prijeđlog NIS 2] i koja odražavaju njezinu razinu ambicije. ***Sigurnosni zahtjevi trebali bi biti barem jednaki minimalnim sigurnosnim zahtjevima subjekata obuhvaćenih Direktivom (EU) 2022/2555 ili viši od njih.***

Amandman 3

Prijedlog uredbe Uvodna izjava 6.a (nova)

Tekst koji je predložila Komisija

Izmjena

(6.a) Institucijama, tijelima, uredima i agencijama Unije trebalo bi osigurati odgovarajuća sredstva i alate za jačanje njihove kiberotpornosti. Stoga je ključno osigurati uspostavu odgovarajućih mehanizama koordinacije kako bi se odluke donosile na učinkovit i djelotvoran način.

Amandman 4

Prijedlog uredbe Uvodna izjava 22.

Tekst koji je predložila Komisija

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

Izmjena

(22) Obrada svih osobnih podataka na temelju ove Uredbe trebala bi biti u skladu sa zakonodavstvom **Unije** o zaštiti podataka, uključujući Uredbu (EU) 2018/1725 Europskog parlamenta i Vijeća⁷. **Ova Uredba ne bi trebala utjecati na primjenu prava Unije kojim se uređuje obrada osobnih podataka, uključujući zadaće i ovlasti Europskog nadzornika za zaštitu podataka. CERT-EU i IICB trebali bi blisko suradivati s Europskim nadzornikom za zaštitu podataka i osobljem specijaliziranim za zaštitu podataka u institucijama, tijelima, uredima i agencijama Unije kako bi se osigurala potpuna usklađenost s pravom Unije o zaštiti podataka.**

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

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

Amandman 5

Prijedlog uredbe Uvodna izjava 22.a (nova)

Tekst koji je predložila Komisija

Izmjena

(22.a) Kibersigurnosni sustavi i usluge uključeni u sprečavanje, otkrivanje i odgovor na kiberprijetnje trebali bi biti u skladu s pravom o zaštiti podataka i privatnosti te bi trebali uključivati

relevantne tehničke i organizacijske zaštitne mjere kako bi se osiguralo postizanje te usklađenosti na odgovoran način.

Amandman 6

Prijedlog uredbe Uvodna izjava 23.

Tekst koji je predložila Komisija

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

Izmjena

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

Amandman 7

Prijedlog uredbe Uvodna izjava 25.a (nova)

Tekst koji je predložila Komisija

Izmjena

(25.a) Provedeno je savjetovanje s Europskim nadzornikom za zaštitu podataka u skladu s člankom 42. stavkom 1. Uredbe (EU) 2018/1725 te je on dao mišljenje 17. svibnja 2022.,

Amandman 8

Prijedlog uredbe Članak 4. – stavak 5.

Tekst koji je predložila Komisija

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

Izmjena

5. Sve institucije, tijela i agencije Unije imenuju lokalnog službenika za kibersigurnost ili jednakovrijednu funkciju koji djeluje kao njihova jedinstvena kontaktna točka za sve aspekte kibersigurnosti. *Lokalni službenik za kibersigurnost surađuje sa službenikom za zaštitu podataka imenovanim u skladu s člankom 43. Uredbe (EU) 2018/1725 kada je riječ o aktivnostima koje se preklapaju, kao što su primjena tehničke i integrirane zaštite podataka na kibersigurnosne mjere i odabir kibersigurnosnih mjera koje uključuju zaštitu osobnih podataka, integrirano upravljanje rizicima i integrirano rješavanje sigurnosnih incidenata.*

Amandman 9

Prijedlog uredbe

Članak 9. – stavak 3. – podstavak 1. – točka ka (nova)

Tekst koji je predložila Komisija

Izmjena

(ka) Europski nadzornik za zaštitu podataka;

Amandman 10

Prijedlog uredbe

Članak 9. – stavak 3. – podstavak 1. – točka kb (nova)

Tekst koji je predložila Komisija

Izmjena

(kb) Agencija Europske unije za suradnju tijela za izvršavanje zakonodavstva.

Amandman 11

Prijedlog uredbe

Članak 12. – stavak 2. – točka ea (nova)

Tekst koji je predložila Komisija

Izmjena

(ea) obavljačeće Europskog nadzornika za zaštitu podataka o svim naznakama kršenja obveza utvrđenih ovom Uredbom od strane institucije, tijela, ureda ili agencije Unije koje obuhvaća nezakonitu obradu osobnih podataka;

Amandman 12

Prijedlog uredbe

Članak 12. – stavak 2. – točka eb (nova)

Tekst koji je predložila Komisija

Izmjena

(eb) blisko surađuje s Europskim nadzornikom za zaštitu podataka u rješavanju incidenata koji za posljedicu imaju povrede osobnih podataka ili povrede povjerljivosti elektroničke komunikacije.

Amandman 13

Prijedlog uredbe

Članak 12. – stavak 7.a (novi)

Tekst koji je predložila Komisija

Izmjena

7.a CERT-EU obavljačeće Europskog nadzornika za zaštitu podataka o rješavanju znatnih ranjivosti, ozbiljnih incidenata ili velikih napada koji bi mogli dovesti do povreda osobnih podataka ili povreda povjerljivosti elektroničkih komunikacija.

Amandman 14

Prijedlog uredbe

Članak 18. – stavak 2.

Tekst koji je predložila Komisija

2. Odredbe Uredbe (EZ) br. 1049/2001 Europskog parlamenta i Vijeća⁹ primjenjuju se na zahtjeve za javni pristup dokumentima koje posjeduje CERT-EU, uključujući obvezu na temelju te uredbe u pogledu savjetovanja s drugim institucijama, tijelima i agencijama Unije kad se zahtjev odnosi na njihove dokumente.

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

Izmjena

2. Odredbe Uredbe (EZ) br. 1049/2001 Europskog parlamenta i Vijeća⁹ primjenjuju se na zahtjeve za javni pristup dokumentima koje posjeduje CERT-EU, uključujući obvezu na temelju te uredbe u pogledu savjetovanja s drugim institucijama, tijelima i agencijama Unije *ili, po potrebi, s državama članicama*, kad se zahtjev odnosi na njihove dokumente.

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

Amandman 15

Prijedlog uredbe

Članak 18. – stavak 13. – podstavak 1.a (novi)

Tekst koji je predložila Komisija

Izmjena

Svaka obrada, razmjena, prikupljanje ili zadržavanje osobnih podataka koje provode CERT-EU, IICB i institucije, tijela, uredi i agencije Unije ograničena je na obradu, razmjenu, prikupljanje ili zadržavanje koje je nužno potrebno i provodi se isključivo u svrhu ispunjavanja njihovih obveza na temelju ove Uredbe.

Amandman 16

Prijedlog uredbe

Članak 18. – stavak 3.a (novi)

Tekst koji je predložila Komisija

Izmjena

3.a Komisija do... [1 godina nakon datuma stupanja na snagu ove Uredbe] donosi delegirani akt kojim se određuje koje su aktivnosti obrade osobnih

podataka dopuštene ovom Uredbom, uključujući svrhu obrade, kategorije osobnih podataka, kategorije ispitanika, uvjete obrade podataka, maksimalna razdoblja zadržavanja, definiciju voditelja obrade i izvršitelja obrade te primatelje u slučaju prijenosa.

Delegiranim aktom iz prvog podstavka aktivnosti obrade ograničavaju se na one koje su nužno potrebne i njime se zahtijeva da takve aktivnosti obrade budu što je moguće usmjerene i da ne uključuju neselektivno zadržavanje podataka o prometu ili sadržaju.

Komisija mijenja delegirani akt iz prvog podstavka ako utvrdi znatne promjene u pogledu nužnosti ili posebnih svrha ili subjekata uključenih u obradu osobnih podataka za potrebe ove Uredbe.

Amandman 17

Prijedlog uredbe

Članak 18. – stavak 4.

Tekst koji je predložila Komisija

4. Postupanje CERT-EU-a i pripadajućih institucija, tijela i agencija Unije s podacima mora biti u skladu s pravilima utvrđenima u [predloženoj Uredbi o sigurnosti podataka].

Izmjena

4. Postupanje CERT-EU-a i institucija, tijela i agencija Unije s podacima trebalo bi biti u skladu s pravilima **Unije o sigurnosti podataka, posebno onima** utvrđenima u [predloženoj Uredbi o sigurnosti podataka].

Amandman 18

Prijedlog uredbe

Članak 18. – stavak 5.

Tekst koji je predložila Komisija

5. Svi kontakti s CERT-EU-om koje pokrenu ili zatraže nacionalne sigurnosne i obavlještajne službe priopćuju se bez nepotrebne odgode Glavnoj upravi

Izmjena

5. Svi kontakti s CERT-EU-om koje pokrenu ili zatraže nacionalne sigurnosne i obavlještajne službe priopćuju se bez nepotrebne odgode Glavnoj upravi

Komisije za sigurnost i predsjedniku IICB-a.

Komisije za sigurnost, *Europolu* i predsjedniku IICB-a.

Amandman 19

Prijedlog uredbe

Članak 19. – naslov

Tekst koji je predložila Komisija

Izmjena

Obveze razmjene

Razmjena *informacija*

Amandman 20

Prijedlog uredbe

Članak 19. – stavak 1.

Tekst koji je predložila Komisija

Izmjena

1. Kako bi CERT-EU mogao koordinirati upravljanje ranjivostima i odgovor na incidente, *može od institucija, tijela i agencija* Unije *zatražiti da mu iz svojih evidencija informatičkih sustava dostave informacije relevantne za pomoć koju pruža CERT-EU. Institucija, tijelo ili agencija kojoj* je podnesen zahtjev bez nepotrebne odgode prenosi tražene informacije i sva njihova naknadna ažuriranja.

1. Kako bi CERT-EU mogao *izvršavati zadaće utvrđene u članku 12., posebno* koordinirati upravljanje ranjivostima i odgovor na incidente, *institucije, tijela ili agencije* Unije *na zahtjev CERT-EU-a* iz svojih evidencija *IKT* sustava *dostavljaju CERT-EU-u* informacije relevantne za *CERT-EU, uključujući sve izmjene u svojem informacijskom okruženju. Subjekt kojem* je podnesen zahtjev bez nepotrebne odgode prenosi tražene informacije i sva njihova naknadna ažuriranja.

Ne dovodeći u pitanje Uredbu (EU) 2018/1725, svaka razmjena podataka između CERT-EU-a i institucija, tijela, ureda ili agencija Unije provodi se u skladu s načelima jasnih zaštitnih mjera za posebne slučajevе upotrebe i upotrebljava ugovore o uzajamnoj pravnoj pomoći i druge sporazume kako bi se osigurala visoka razina zaštite prava pri obradi zahtjeva za prekogranični pristup podacima.

Amandman 21

Prijedlog uredbe
Članak 19. – stavak 1.a (novi)

Tekst koji je predložila Komisija

Izmjena

1.a Institucije, tijela, uredi i agencije Unije mogu CERT-EU-u dobrovoljno dostaviti informacije o kiberprijetnjama i incidentima, izbjegnutim incidentima i ranjivostima koji na njih utječu. Od CERT-EU-a mogu zatražiti i dodatnu tehničku pomoć i savjete za borbu protiv kiberincidenta i većih napada. CERT-EU može dati prednost obradi obveznih obavijesti u odnosu na dobrovoljne obavijesti, osim u slučaju propisno obrazloženih i hitnih dobrovoljnih zahtjeva institucija, tijela, ureda i agencija Unije.

Amandman 22

Prijedlog uredbe
Članak 19. – stavak 3.

Tekst koji je predložila Komisija

Izmjena

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

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

Ako je to potrebno za izvršavanje njegovih zadaća, CERT-EU može razmjenjivati informacije o incidentima, među ostalim i u nedostatku odobrenja institucije, tijela, ureda ili agencije Unije pogodene incidentom. Institucija, tijelo, ured ili agencija Unije unaprijed se obavješćuje o svakoj takvoj razmjeni informacija.

Amandman 23

Prijedlog uredbe Članak 19. – stavak 4.

Tekst koji je predložila Komisija

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

Izmjena

4. Obveze razmjene ne odnose se na klasificirane podatke EU-a (EUCI) ni na informacije koje je institucija, tijelo ili agencija Unije primila od sigurnosne ili obavještajne službe države članice ili tijela za izvršavanje zakonodavstva, **osim ako sigurnosna ili obavještajna služba države članice ili tijelo za izvršavanje zakonodavstva dopusti** da se **te informacije** razmjenjuju s CERT-EU-om.

Amandman 24

Prijedlog uredbe Članak 20. – stavak 3.

Tekst koji je predložila Komisija

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

Izmjena

3. CERT-EU jedanput mjesečno dostavlja ENISA-i sažeto izvješće koje uključuje anonimizirane i zbirne podatke o ozbiljnim kiberprijetnjama, znatnim ranjivostima i ozbiljnim incidentima prijavljenima u skladu sa stavkom 1. **To se izvješće objavljuje u skladu s relevantnim pravilima Unije o informacijskoj sigurnosti, posebno onima utvrđenima u [predloženoj uredbi o informacijskoj sigurnosti].**

Amandman 25

Prijedlog uredbe Članak 20. – stavak 5.

Tekst koji je predložila Komisija

5. Obveze obavješćivanja ne odnose se na klasificirane podatke EU-a ni na

Izmjena

5. Obveze obavješćivanja ne odnose se na klasificirane podatke EU-a ni na

informacije koje je institucija, tijelo ili agencija Unije primila od sigurnosne ili obavještajne službe države članice ili tijela za izvršavanje zakonodavstva *uz izričit uvjet* da se *one ne* dijele s CERT-EU-om.

informacije koje je institucija, tijelo ili agencija Unije primila od sigurnosne ili obavještajne službe države članice ili tijela za izvršavanje zakonodavstva, *osim ako dotična sigurnosna ili obavještajna služba države članice ili tijelo za izvršavanje zakonodavstva dopusti* da se *te informacije* dijele s CERT-EU-om.

Amandman 26

Prijedlog uredbe Članak 21. – stavak 4.

Tekst koji je predložila Komisija

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

Izmjena

4. U slučaju ozbiljnih incidenata IICB izdaje smjernice o koordinaciji odgovora na incidente i suradnji. Ako se sumnja da je incident kaznene prirode, CERT-EU *ili IICB bez nepotrebne odgode prijavljuje* incident tijelima za izvršavanje zakonodavstva.

Amandman 27

Prijedlog uredbe Članak 24.a (novi)

Tekst koji je predložila Komisija

Izmjena

Članak 24.a

Delegiranje ovlasti

1. *Ovlast za donošenje delegiranih akata dodjeljuje se Komisiji u skladu s uvjetima utvrđenima u ovom članku.*

2. *Ovlast za donošenje delegiranih akata iz članka 18. članka 3.a dodjeljuje se Komisiji na neodređeno razdoblje počevši od ... [jedan dan nakon datuma stupanja na snagu ove Uredbe].*

3. *Europski parlament ili Vijeće u svakom trenutku mogu opozvati delegiranje ovlasti iz članka 18. stavka 3.a. Odlukom o opozivu prekida se*

delegiranje ovlasti koje je u njoj navedeno. Opoziv počinje proizvoditi učinke sljedećeg dana od dana objave spomenute odluke u Službenom listu Europske unije ili na kasniji dan naveden u spomenutoj odluci. Opoziv ne utječe na valjanost delegiranih akata koji su već na snazi.

4. Čim doneše delegirani akt, Komisija ga istodobno priopćuje Europskom parlamentu i Vijeću.

5. Delegirani akt donesen u skladu s člankom 18. stavkom 3.a stupa na snagu samo ako se tome ne usprotive ni Europski parlament ni Vijeće u roku od dva mjeseca od priopćenja Europskom parlamentu i Vijeću o tom aktu ili ako su prije isteka tog roka i Europski parlament i Vijeće obavijestili Komisiju da se ne protive. Taj se rok produljuje za dva mjeseca na inicijativu Europskog parlamenta ili Vijeća.

Amandman 28

Prijedlog uredbe

Prilog II. – stavak 1. – točka 2.a (nova)

Tekst koji je predložila Komisija

Izmjena

(2.a) primjenom šifriranja u mirovanju, šifriranja pri prijenosu i šifriranja s kraja na kraj, ako je to moguće;

POSTUPAK U ODBORU KOJI DAJE MIŠLJENJE

Naslov	Uspostava mjera za visoku zajedničku razinu kibersigurnosti u institucijama, tijelima, uredima i agencijama Unije
Referentni dokumenti	COM(2022)0122 – C9-0122/2022 – 2022/0085(COD)
Nadležni odbor Datum objave na plenarnoj sjednici	ITRE 4.4.2022
Odbori koji su dali mišljenje Datum objave na plenarnoj sjednici	LIBE 4.4.2022
Pridruženi odbori - datum objave na plenarnoj sjednici	15.9.2022
Izvjestitelj(ica) za mišljenje Datum imenovanja	Tomas Tobé 12.12.2022
Razmatranje u odboru	31.1.2023
Datum usvajanja	1.3.2023
Rezultat konačnog glasovanja	+: -: 0: 62 0 1
Zastupnici nazočni na konačnom glasovanju	Magdalena Adamowicz, Abir Al-Sahlani, Malik Azmani, Katarina Barley, Pietro Bartolo, Vladimír Bilčík, Vasile Blaga, Ioan-Rareş Bogdan, Karolin Braunsberger-Reinhold, Patrick Breyer, Saskia Bricmont, Patricia Chagnon, Caterina Chinnici, Clare Daly, Lena Düpont, Lucia Ďuriš Nicholsonová, Maria Grapini, Sylvie Guillaume, Andrzej Halicki, Evin Incir, Sophia in 't Veld, Patryk Jaki, Marina Kaljurand, Assita Kanko, Fabienne Keller, Łukasz Kohut, Moritz Körner, Alice Kuhnke, Jeroen Lenaers, Juan Fernando López Aguilar, Erik Marquardt, Nuno Melo, Maite Pagazaurtundúa, Karlo Ressler, Diana Riba i Giner, Birgit Sippel, Sara Skyttedal, Vincenzo Sofo, Tineke Strik, Ramona Strugariu, Annalisa Tardino, Tomas Tobé, Yana Toom, Milan Uhrík, Tom Vandendriessche, Jadwiga Wiśniewska
Zamjenici nazočni na konačnom glasovanju	Susanna Ceccardi, Gwendoline Delbos-Corfield, Lucas Fourlas, Beata Kempa, Philippe Olivier, Dragoš Tudorache, Petar Vitanov, Tomáš Zdechovský
Zamjenici nazočni na konačnom glasovanju prema čl. 209. st. 7.	Gheorghe Falcă, Jean-François Jalkh, Petra Kammerevert, Marisa Matias, Martina Michels, Ljudmila Novak, Stanislav Polčák, Mick Wallace, Bernhard Zimniok

POIMENIČNO KONAČNO GLASOVANJE U ODBORU KOJI DAJE MIŠLJENJE

62	+
ECR	Patryk Jaki, Assita Kanko, Beata Kempa, Vincenzo Sofo, Jadwiga Wiśniewska
ID	Susanna Ceccardi, Patricia Chagnon, Jean-François Jalkh, Philippe Olivier, Annalisa Tardino, Tom Vandendriessche, Bernhard Zimniok
PPE	Magdalena Adamowicz, Vladimír Bilčík, Vasile Blaga, Ioan-Rareş Bogdan, Karolin Braunsberger-Reinhold, Lena Düpont, Gheorghe Falcă, Lucas Fourlas, Andrzej Halicki, Jeroen Lenaers, Nuno Melo, Ljudmila Novak, Stanislav Polčák, Karlo Ressler, Sara Skyttedal, Tomas Tobé, Tomáš Zdechovský
Renew	Abir Al-Sahlani, Malik Azmani, Lucia Ďuriš Nicholsonová, Sophia in 't Veld, Fabienne Keller, Moritz Körner, Maite Pagazaurtundúa, Ramona Strugariu, Yana Toom, Dragoş Tudorache
S&D	Katarina Barley, Pietro Bartolo, Caterina Chinnici, Maria Grapini, Sylvie Guillaume, Evin Incir, Marina Kaljurand, Petra Kammerevert, Łukasz Kohut, Juan Fernando López Aguilar, Birgit Sippel, Petar Vitanov
The Left	Clare Daly, Marisa Matias, Martina Michels, Mick Wallace
Verts/ALE	Patrick Breyer, Saskia Bricmont, Gwendoline Delbos-Corfield, Alice Kuhnke, Erik Marquardt, Diana Riba i Giner, Tineke Strik

0	-

1	0
NI	Milan Uhrík

Korišteni znakovi:

- + : za
- : protiv
- 0 : suzdržani

13.7.2022

MIŠLJENJE ODBORA ZA PRORAČUNE

upućeno Odboru za industriju, istraživanje i energetiku

o Prijedlogu uredbe Europskog parlamenta i Vijeća o mjerama za visoku zajedničku razinu kibersigurnosti u institucijama, tijelima, uredima i agencijama Unije
(COM(2022)0122 – C9-0122/2022 – 2022/0085(COD))

Izvjestitelj za mišljenje: Nils Ušakovs

KRATKO OBRAZLOŽENJE

Izvjestitelj pozdravlja prijedlog Komisije o mjerama za visoku zajedničku razinu kibersigurnosti u institucijama, tijelima, uredima i agencijama Unije. Smatra da je ovaj prijedlog potreban kako bi se poboljšala otpornost i sigurnost javne uprave EU-a s obzirom na sve veći broj kibersigurnosnih prijetnji, koje su sve sofisticirane. To je tim više evidentno ako se uzme u obzir trenutačni geopolitički kontekst.

Izvjestitelj smatra da je međuinsticujska suradnja ključna kako bi se na odgovarajući način spriječilo, otkrilo i pratio prijetnje i rizike te odgovorilo na njih. Sve institucije, tijela, uredi i agencije Unije, bez obzira na njihovu veličinu, imaju zadaću i odgovornost da zaštite te organe Unije od kibernapada jer samo jedan mali propust u jednom od njih može ugroziti i sve ostale. Izvjestitelj stoga podržava ideju osnovnog okvira kibersigurnosnih mjera. Nadalje, smatra da bi se u okviru međuinsticuionalne suradnje, povrh toga što će se institucijama, tijelima, uredima i agencijama Unije omogućiti da povećaju svoju informatičku kibersigurnost i odgovor na kibernapade, trebale razmotriti i potencijalne sinergije u metodama rada i komunikacijskim kanalima u cilju smanjenja administrativnog opterećenja, izbjegavanja udvostručavanja napora i poboljšanja pripravnosti i zaštite.

Suprotno prijedlogu Komisije, izvjestitelj smatra da su potrebna 42 radna mjesta umjesto 21, kako bi CERT-EU mogao funkcionirati s kompletiranim i naјsvremenijim službama. Ne slaže se s prijedlogom Komisije o djelomičnoj nadoknadi dodatnih radnih mjesta namijenjenih CERT-EU-u smanjenjem broja ugovornih djelatnika.

Izvjestitelj se zalaže za to da bi Europski parlament, s obzirom na njegovu relativnu veličinu i njegov zahtjev za dodatna radna mjesta u području kibersigurnosti u svojem izvještaju o procjenama za 2023., trebao dodijeliti prvih 48 radnih mjesta CERT-EU-u u prvom proračunu donesenom nakon stupanja na snagu ove Uredbe. U sljedeće tri godine 14 od tih radnih mjesta bit će godišnje preraspoređeno Parlamentu kako bi na kraju šest radnih mjesta trajno ostalo u CERT-EU-u. Tim postupnim vraćanjem omogućit će se stabilnost u pogledu osoblja i upravljanja znanjem. Istodobno će nakon prve godine druge relevantne institucije, tijela, uredi

i agencije Unije postupno dodijeliti radna mjesta CERT-EU-u. Time će se od samog početka omogućiti stvaranje grupe od 42 nova stalna zaposlenika u CERT-EU-u.

Izvjestitelj predlaže poboljšanje postojećih mehanizama u pogledu sporazuma o razini usluga za usluge uz naknadu, kao što je Europski revizorski sud preporučio u svojem tematskom izvješću 05/2022¹ kako bi se osiguralo bolje upravljanje novčanim tokovima i smanjio administrativni rad.

Naposljetku, izvjestitelj preporučuje da se u institucijama, tijelima, uredima i agencijama Unije ulaganja i radna mjesta za kibersigurnost posebno rezerviraju. Time će se omogućiti prepoznavanje i razmjena najboljih praksi i potencijalnih potreba za financiranjem na razini institucija, tijela, ureda i agencija Unije.

¹ Tematsko izvješće br. 05/2022: Kibersigurnost institucija, tijela i agencija EU-a: razina pripravnosti općenito nije razmjerna prijetnjama

AMANDMANI

Odbor za proračune poziva Odbor za industriju, istraživanje i energetiku da kao nadležni odbor uzme u obzir sljedeće amandmane:

Amandman 1

Prijedlog uredbe

Uvodna izjava 7.

Tekst koji je predložila Komisija

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

Izmjena

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

Obrazloženje

Od male agencije ili tijela ne može se očekivati isti doprinos kao i od institucije Unije.

Amandman 2

Prijedlog uredbe

Uvodna izjava 8.

Tekst koji je predložila Komisija

(8) Da bi se izbjeglo nerazmjerne financijsko i administrativno opterećenje za institucije, tijela i agencije Unije, zahtjevi za upravljanje kibersigurnosnim rizikom trebali bi biti razmjerni riziku kojem je izložen predmetni mrežni i informacijski sustav, uzimajući u obzir suvremenost mjera. Sve institucije, tijela i agencije Unije trebali bi nastojati odrediti **odgovarajući postotak** svojeg proračuna za

Izmjena

(8) Da bi se izbjeglo nerazmjerne financijsko i administrativno opterećenje za institucije, tijela i agencije Unije, zahtjevi za upravljanje kibersigurnosnim rizikom trebali bi biti razmjerni riziku kojem je izložen predmetni mrežni i informacijski sustav, uzimajući u obzir suvremenost mjera. Sve institucije, tijela i agencije Unije trebali bi nastojati odrediti **odgovarajuće resurse iz** svojeg proračuna

informacijske tehnologije za poboljšanje svoje razine kibersigurnosti; dugoročno bi *trebalo težiti cilju od 10 %.*

za informacijske tehnologije za poboljšanje svoje razine kibersigurnosti *i osiguravanje barem minimalne razine kibersigurnosti koja odgovara procjeni rizika.* Trošak osiguravanja kibersigurnosti ovisi o nekoliko čimbenika kao što su veličina subjekta, potreba za osiguravanjem posebne zaštite, površina napada i profil prijetnji te uključuje fiksne troškove i varijabilni dio. Zbog sve većih prijetnji dugoročno bi moglo biti potrebno do 10 % proračuna subjekta kako bi se osigurala odgovarajuća razina sigurnosti u skladu s industrijskim standardima. U skladu s preporukom Europskog nadzornika za zaštitu podataka utvrđenom u njegovu mišljenju 8/2022 od 17. svibnja 2022. minimalni sigurnosni zahtjevi utvrđeni ovom Uredbom trebali bi biti jednaki tim minimalnim sigurnosnim zahtjevima u pogledu subjekata iz prijedloga Direktive NIS i NIS 2.0 ili viši od njih.

Obrazloženje

Prema industrijskim standardima, 10 % ukupnog proračuna za informacijske i komunikacijske tehnologije (IKT) trebalo bi se trošiti na kibersigurnost. Proračun za informacijske tehnologije trebao bi biti razmjeran rizicima u svim institucijama, tijelima, uredima i agencijama Unije u skladu s njihovim vanjskim i unutarnjim okruženjem. U svojem Mišljenju 8/2022 Europski nadzornik za zaštitu podataka preporučuje da se u prijedlog doda da bi minimalni sigurnosni zahtjevi trebali biti jednakim minimalnim sigurnosnim zahtjevima u pogledu subjekata iz prijedloga Direktive NIS i NIS 2.0 ili viši od njih.

Amandman 3

Prijedlog uredbe Uvodna izjava 8.a (nova)

Tekst koji je predložila Komisija

Izmjena

(8a) Kako bi pokrio troškove usluga uz naknadu naplatom od institucija, tijela i agencija Unije koji se koriste tim uslugama, CERT-EU trebao bi se pobrinuti za to da se sporazumima o razini usluga, iz kojih proizlazi više od 90 % proračuna CERT-EU-a za 2020., ne

stvara nepotrebno administrativno opterećenje i da oni budu koristan alat za planiranje budućih prihoda od novčanih tokova.

Obrazloženje

Prema tematskom izvješću Europskog revizorskog suda br. 05/2022 „Sporazumi o razini usluga trebaju se zasebno obnavljati svake godine. To stvara administrativno opterećenje te uzrokuje probleme s novčanim tokom jer CERT-EU ne dobiva finansijska sredstva predviđena svim sporazumima o razini usluga u isto vrijeme. Agencije mogu raskinuti sporazume o razini usluge u bilo kojem trenutku, što stvara rizik od začaranog kruga u kojem će zbog izgubljenih prihoda CERT-EU morati smanjiti opseg svojih usluga i neće moći odgovoriti na potražnju, što će pak potaknuti druge institucije, tijela i agencije Unije da raskinu svoje sporazume o razini usluga i prebace se na privatne pružatelje usluga. Stoga, trenutačni model financiranja nije idealan za to da se zajamči stabilna i optimalna razina usluga.

Amandman 4

Prijedlog uredbe Uvodna izjava 8.b (nova)

Tekst koji je predložila Komisija

Izmjena

(8b) Kako bi se mogao zajamčiti učinkovit okvir za kibersigurnost i pružiti širok raspon usluga institucijama, tijelima i agencijama Unije, CERT-EU-u je potrebno stabilno, visokokvalificirano i specijalizirano osoblje. Osim toga, kako bi se osiguralo učinkovito upravljanje znanjem, velik udio osoblja CERT-EU-a trebao bi biti stalno osoblje. To bi osoblje trebalo imati pristup programima kontinuiranog osposobljavanja.

Obrazloženje

Trebalo bi dodijeliti 42 dodatna stalna radna mjesta CERT-EU-u kako bi se znanje zadržalo unutar CERT-EU-a. Europski parlament trebao bi dodijeliti prvih 48 radnih mjesta CERT-EU-u u prvom proračunu donesenom nakon stupanja na snagu ove Uredbe. U sljedeće tri godine, 14 od tih radnih mjesta bit će godišnje preraspoređeno Parlamentu, nakon čega bi šest radnih mjesta trajno ostalo u CERT-EU-u. Istodobno će nakon prve godine druge relevantne institucije, tijela, uredi i agencije Unije postupno dodijeliti radna mjesta CERT-EU-u. Ovim će se mehanizmom od samog početka omogućiti stvaranje 42 stalna radna mjesta, uz odgovarajući pristup programima osposobljavanja.

Amandman 5

Prijedlog uredbe Uvodna izjava 8.c (nova)

Tekst koji je predložila Komisija

Izmjena

(8c) U trenutačnom geopolitičkom kontekstu ključno je da specijalizirani i operativni timovi u svakom trenutku štite povjerljivost podataka od kiberprijetnji.

Amandman 6

Prijedlog uredbe Uvodna izjava 8.d (nova)

Tekst koji je predložila Komisija

Izmjena

(8d) Prije dodjele dodatnih kadrovske resursa Komisija bi trebala provesti analizu potreba, uzimajući pritom u obzir dugoročnu perspektivu.

Amandman 7

Prijedlog uredbe Uvodna izjava 10.a (nova)

Tekst koji je predložila Komisija

Izmjena

(10a) Međuinstitucijska suradnja i povjerenje ključni su za učinkovitu i djelotvornu zaštitu informacijskog okruženja Unije, a time i njezina demokratskog glasa. Svi predmetni dionici trebali bi uvijek imati na umu povećanje sinergije, smanjenje administrativnog opterećenja i izbjegavanje udvostručavanja napora.

Obrazloženje

Nekoliko tijela i mreža radi na pripremi smjernica i prikupljanju informacija o informatičkim incidentima, odgovorima itd. Suradnja svih tih dionika ključna je kako bi se izbjeglo udvostručavanje napora, pronašle sinergije i osigurali brzi i učinkoviti komunikacijski tokovi među njima.

Amandman 8

Prijedlog uredbe Uvodna izjava 10.b (nova)

Tekst koji je predložila Komisija

Izmjena

(10b) Radi dosljednosti s politikom koju Unija promiče prema državama članicama, institucije, tijela, uredi i agencije Unije trebali bi se odreći upotrebe i razvoja softvera, kao što je Pegasus, kojim bi se moglo povrijediti pravo na privatnost i pravni poretkom Unije.

Obrazloženje

U svojem izvješću od 15. veljače 2022. naslovljenom „Uvodne napomene o modernim računalnim programima za špijuniranje“ Europski nadzornik za zaštitu podataka pozvao je države članice da se odreknu upotrebe i razvoja softvera kao što je Pegasus na europskom tlu, koji bi mogli utjecati na pravo na privatnost, demokraciju i vladavinu prava te bi stoga mogli biti nespojivi s demokratskim vrijednostima i pravnim poretkom Unije;

Amandman 9

Prijedlog uredbe Uvodna izjava 11.

Tekst koji je predložila Komisija

Izmjena

(11) U svibnju 2011. glavni tajnici institucija i tijela Unije odlučili su osnovati pretkonfiguracijski tim za hitne računalne intervencije europskih institucija, tijela i agencija (CERT-EU) pod nadzorom međuinstitucijskog upravljačkog odbora. U srpnju 2012. glavni tajnici potvrđili su praktične aranžmane i dogovorili se da će zadržati CERT-EU u obliku trajnog subjekta radi dalnjeg doprinosa poboljšanju ukupne razine sigurnosti informacijskih tehnologija u institucijama, tijelima i agencijama Unije kao primjer vidljive međuinstitucijske suradnje u

(11) U svibnju 2011. glavni tajnici institucija i tijela Unije odlučili su osnovati pretkonfiguracijski tim za hitne računalne intervencije europskih institucija, tijela i agencija (CERT-EU) pod nadzorom međuinstitucijskog upravljačkog odbora. U srpnju 2012. glavni tajnici potvrđili su praktične aranžmane i dogovorili se da će zadržati CERT-EU u obliku trajnog subjekta radi dalnjeg doprinosa poboljšanju ukupne razine sigurnosti informacijskih tehnologija u institucijama, tijelima i agencijama Unije kao primjer vidljive međuinstitucijske suradnje u

području kibersigurnosti. U rujnu 2012. osnovan je CERT-EU kao radna skupina Europske komisije s međuinstitucijskim ovlastima. U prosincu 2017. institucije i tijela Unije sklopili su međuinstitucijski dogovor o organizaciji i djelovanju CERT-EU-a. Taj bi dogovor trebalo kontinuirano prilagođavati radi pružanja potpore provedbi ove Uredbe.

području kibersigurnosti. U rujnu 2012. osnovan je CERT-EU kao **stalna** radna skupina Europske komisije s međuinstitucijskim ovlastima. U prosincu 2017. institucije i tijela Unije sklopili su međuinstitucijski dogovor o organizaciji i djelovanju CERT-EU-a. Taj bi **međuinstitucijski** dogovor trebalo kontinuirano prilagođavati radi pružanja potpore provedbi ove Uredbe *i osiguravanja sukladnosti s njom.*

³ SL C 12, 13.1.2018., str. 1.–11.

³ SL C 12, 13.1.2018., str. 1.–11.

Obrazloženje

U skladu s uvodnom izjavom 11. CERT-EU je osnovan kao trajni subjekt. Međuinstitucijski sporazum iz 2018. trebalo bi revidirati kako bi se uzela u obzir raspodjela radnih mjesta iz Priloga II.a (novi).

Amandman 10

Prijedlog uredbe Uvodna izjava 14.

Tekst koji je predložila Komisija

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

Izmjena

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

Obrazloženje

Važno je osigurati poštovanje načela rodne ravnoteže u novoosnovanom IICB-u.

Amandman 11

Prijedlog uredbe Uvodna izjava 24.

Tekst koji je predložila Komisija

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

Izmjena

(24) Budući da su usluge i zadaće CERT-EU-a u interesu svih institucija, tijela i agencija Unije, sve institucije, tijela i agencije Unije s rashodima za informacijsku tehnologiju trebali bi razmjerno pridonositi tim uslugama i zadaćama, *bilo u obliku radnih mesta, finansijskih doprinosa ili oboje, ovisno o veličini institucija, tijela i agencija te pruženim uslugama i zadaćama*. Ti doprinosi ne dovode u pitanje proračunsku autonomiju institucija, tijela i agencija Unije.

Obrazloženje

Ovisno o veličini institucija, tijela i agencija Unije, doprinosi CERT-EU-u mogli bi biti u obliku dodjele radnih mesta i finansijskih doprinosa.

Amandman 12

Prijedlog uredbe Uvodna izjava 24.a (nova)

Tekst koji je predložila Komisija

Izmjena

(24a) Sve institucije, tijela i agencije Unije trebali bi primjenjivati načela rodne ravnopravnosti i rodne ravnoteže pri imenovanju u CERT-EU, kao i pri raspodjeli svojih ljudskih resursa kada je riječ o sektoru informacijske tehnologije i kibersigurnosti. Ciljano osposobljavanje i odgovarajući resursi trebali bi biti namijenjeni za promicanje zapošljavanja žena u području kibersigurnosti u svim institucijama, tijelima i agencijama Unije

kako bi se premostio digitalni jaz među spolovima.

Obrazloženje

Važno je u Uredbu uključiti načela rodne ravnopravnosti i rodne ravnoteže.

Amandman 13

Prijedlog uredbe

Uvodna izjava 25.a (nova)

Tekst koji je predložila Komisija

Izmjena

(25a) U svojim zaključcima od 23. svibnja 2022. o razvoju položaja Europske unije u pogledu kiberprostora Vijeće je pozvalo relevantna tijela i Komisiju da ojačaju otpornost komunikacijskih mreža i infrastruktura u Europskoj uniji. Stoga je važno ojačati suverenost i otpornost infrastrukture te kontrolu veza, uključujući infrastrukture institucija, agencija i tijela Unije.

Obrazloženje

U Zaključcima Vijeća o razvoju položaja Europske unije u pogledu kiberprostora od 23. svibnja 2022. Vijeće poziva na jačanje kiberotpornosti EU-a i njegove sposobnosti za zaštitu od kibernapada.

Amandman 14

Prijedlog uredbe

Članak 4. – stavak 4.

Tekst koji je predložila Komisija

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

Izmjena

4. Sve institucije, tijela i agencije Unije dužne su imati uspostavljene učinkovite mehanizme kojima se osigurava da se *odgovarajuća sredstva iz proračuna za informacijsku tehnologiju troše na kbersigurnost, imajući na umu minimalni postotak* proračuna za informacijsku tehnologiju *koji treba potrošiti* na kbersigurnost *u skladu s*

industrijskim standardima kako bi se učinkovito zaštitilo njihovo informacijsko okruženje. Institucije, tijela i agencije Unije namjenjuju sredstva za CERT-EU-u u svojim proračunima u svrhu veće transparentnosti.

Obrazloženje

Uprijedlogu Komisije nije jasno što se misli pod „učinkoviti mehanizmi“ i „odgovarajući postotci“. Barem jedan kriterij za procjenu odgovarajućeg postotka su industrijski standardi. Namjenjivanjem sredstava iz proračuna institucija, tijela, ureda i agencija Unije povećala bi se transparentnost za ulaganja u kibersigurnost te bi se utvrdili mogući finansijski nedostaci i razmijenile najbolje prakse.

Amandman 15

Prijedlog uredbe

Članak 4. – stavak 4.a (novi)

Tekst koji je predložila Komisija

Izmjena

4.a Svaka institucija, tijelo i agencija Unije pri imenovanju u CERT-EU i dodjeli ljudskih resursa za kibersigurnost primjenjuje načela rodne ravnopravnosti i rodne ravnoteže. Ciljano osposobljavanje i odgovarajući resursi namjenjuju se za promicanje zapošljavanja žena u području kibersigurnosti u svim institucijama, tijelima i agencijama Unije kako bi se premostio digitalni jaz među spolovima.

Obrazloženje

Važno je u Uredbu uključiti načela rodne ravnopravnosti i rodne ravnoteže.

Amandman 16

Prijedlog uredbe

Članak 9. – stavak 3. – podstavak 1.a (novi)

Tekst koji je predložila Komisija

Izmjena

Članovi se imenuju uz poštovanje načela rodne ravnoteže.

Obrazloženje

Važno je u Uredbu uključiti načela rodne ravnopravnosti i rodne ravnoteže.

Amandman 17

Prijedlog uredbe

Članak 12. – stavak 7.a (novi)

Tekst koji je predložila Komisija

Izmjena

7.a Ako je potražnja za uslugama uz naknadu veća od dostupnih resursa CERT-EU-a za pružanje tih usluga, CERT-EU prednost daje zahtjevima na temelju analize rizika u kojoj se uzima u obzir upravljanje kibersigurnosnim rizicima institucija, tijela i agencija Unije koji su podnijeli zahtjev i na koje utječe relativna veličina njihovih financijskih i ljudskih resursa.

Obrazloženje

Institucijama, tijelima i agencijama Unije trebalo bi dati prednost na temelju njihova profila rizičnosti i uzimajući u obzir relativnu veličinu njihovih financijskih i ljudskih resursa.

Amandman 18

Prijedlog uredbe

Članak 14.

Tekst koji je predložila Komisija

Izmjena

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

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

Obrazloženje

Cilj je ovog amandmana pojasniti da bi izvješće o izvršenju proračuna trebalo uključivati stanje radnih mjesta i vanjskog osoblja u CERT-EU-u.

Amandman 19

Prijedlog uredbe

Članak 15. – stavak 2.

Tekst koji je predložila Komisija

Izmjena

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

Briše se.

Amandman 20

Prijedlog uredbe

Članak 15. – stavak 3.

Tekst koji je predložila Komisija

Izmjena

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

3. Zadaće i aktivnosti CERT-EU-a, uključujući usluge koje CERT-EU u skladu s člankom 12. stavcima 2., 3., 4. i 6. te člankom 13. stavkom 1. pruža institucijama, tijelima i agencijama Unije finansiranima iz naslova višegodišnjeg financijskog okvira namijenjenog europskoj javnoj upravi financiraju se iz posebne proračunske linije proračuna Komisije. Radna mjesta namijenjena CERT-EU-u detaljno se navode u bilješci uz plan radnih mjesta Komisije. ***Radna mjesta koja su privremeno popunjena zadržavaju se u planu radnih mjesta institucije posuditeljice tijekom privremenog raspoređivanja, na što se upućuje bilješkom. Taj plan radnih mjesta preispituje se svake dvije i pol godine.***

Amandman 21

Prijedlog uredbe

Članak 15. – stavak 3.a (novi)

Tekst koji je predložila Komisija

Izmjena

3.a Prijenosom od ukupno 42 radna mesta od strane relevantnih institucija, tijela i agencija Unije kako je utvrđeno u Prilogu II.a (novi), bez djelomične nadoknade zbog smanjenja broja ugovornog osoblja u CERT-EU-u, ne doveđe se u pitanje ovlasti proračunskog tijela Unije. Doprinosi predstavljaju pravedan udio koji je razmjeran odgovarajućem udjelu stalnih radnih mesta razreda AD u organizaciji i provodi se uzimajući u obzir načelo rodne ravnoteže.

Obrazloženje

Potrebno je dodijeliti 42 dodatna stalna radna mjesta CERT-EU-u. Razdiobu radnih mesta među relevantnim institucijama, agencijama i tijelima Unije trebala bi dogovoriti dva proračunska tijela tijekom međuinsticujskih pregovora o ovom prijedlogu, podložno ovlastima proračunskog tijela Unije. Važno je osigurati da se u Uredbi poštuje načelo rodne ravnoteže.

Amandman 22

Prijedlog uredbe

Članak 23. – stavak 1.

Tekst koji je predložila Komisija

Izmjena

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

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

Obrazloženje

Raspodjela radnih mesta za CERT-EU detaljno je opisana u Prilogu II.a (novi).

Amandman 23

Prijedlog uredbe Prilog II.a (novi)

Tekst koji je predložila Komisija

Izmjena

Prilog II.a (novi)

Institucija, tijelo, ured ili agencija Unije / godina	Ukupno zaposlenik a	Radna mjesta dodijeljen a CERT- EU-u u godini N	Radna mjesta dodijeljen a CERT- EU-u u godini N + 1	Radna mjesta dodijeljen a CERT- EU-u u godini N + 2	Radna mjesta dodijeljen a CERT- EU-u u godini N + 3	Radna mjesta trajno dodijelje na CERT- EU-u
<i>Od prethodne godine CERT-EU</i>		<i>nije dostupno</i>	48	42	42	
<i>Europski parlament</i>	6 773	48	-14	-14	-14	6
<i>Europska komisija</i>	23 474	0	8	9	6	23
<i>Decentralizirane agencije</i>	7 717	0	0	3	4	7
<i>Vijeće</i>	3 029	0	0	2	1	3
<i>Sud</i>	2 110	0	0	0	2	2
<i>ESVD</i>	1 753	0	0	0	1	1
<i>Revizorski sud</i>	873	0	0	0	0	0
<i>Izvršne agencije</i>	840	0	0	0	0	0
<i>EGSO</i>	669	0	0	0	0	0
<i>Zajednička poduzeća + zajedničke tehnološke inicijative + Europski institut za inovacije i tehnologiju</i>	556	0	0	0	0	0
<i>Odbor regija</i>	496	0	0	0	0	0
<i>Europski nadzornik za zaštitu podataka</i>	84	0	0	0	0	0

<i>Europski ombudsman</i>	73	0	0	0	0	0
<i>Ukupno novih zaposlenika</i>		48	42	42	42	42

Obrazloženje

Raščlamba 42 radna mesta koja će se dodijeliti CERT-EU-u kako bi se osiguralo njegovo pravilno i stabilno funkcioniranje.

POSTUPAK U ODBORU KOJI DAJE MIŠLJENJE

Naslov	Uspostava mjera za visoku zajedničku razinu kibersigurnosti u institucijama, tijelima, uredima i agencijama Unije	
Referentni dokumenti	COM(2022)0122 – C9-0122/2022 – 2022/0085(COD)	
Nadležni odbor Datum objave na plenarnoj sjednici	ITRE 4.4.2022	
Odbori koji su dali mišljenje Datum objave na plenarnoj sjednici	BUDG 4.4.2022	
Izvjestitelj(ica) za mišljenje Datum imenovanja	Nils Ušakovs 22.4.2022	
Razmatranje u odboru	20.6.2022	21.6.2022
Datum usvajanja	12.7.2022	
Rezultat konačnog glasovanja	+: -: 0:	28 0 4
Zastupnici nazočni na konačnom glasovanju	Rasmus Andresen, Anna Bonfrisco, Olivier Chastel, Lefteris Christoforou, Andor Deli, José Manuel Fernandes, Eider Gardiazabal Rubial, Vlad Gheorghe, Francisco Guerreiro, Valérie Hayer, Eero Heinäluoma, Niclas Herbst, Monika Hohlmeier, Moritz Körner, Joachim Kuhs, Zbigniew Kuźmiuk, Janusz Lewandowski, Margarida Marques, Siegfried Mureşan, Victor Negrescu, Dimitrios Papadimoulis, Bogdan Rzońca, Nicolae Ţăfărau, Nils Torvalds, Nils Ušakovs, Johan Van Overtveldt, Rainer Wieland	
Zamjenici nazočni na konačnom glasovanju	Damian Boeselager, Jan Olbrycht	
Zamjenici nazočni na konačnom glasovanju prema čl. 209. st. 7.	Alexander Bernhuber, Helmut Scholz, Birgit Sippel	

POIMENIČNO KONAČNO GLASOVANJE U ODBORU KOJI DAJE MIŠLJENJE

28	+
ID	Anna Bonfrisco
NI	Andor Deli
PPE	Alexander Bernhuber, Lefteris Christoforou, José Manuel Fernandes, Niclas Herbst, Monika Hohlmeier, Janusz Lewandowski, Siegfried Mureşan, Jan Olbrycht, Rainer Wieland
Renew	Olivier Chastel, Vlad Gheorghe, Valérie Hayer, Moritz Körner, Nils Torvalds, Nicolae řtefanuš
S&D	Eider Gardiazabal Rubial, Eero Heinäluoma, Margarida Marques, Victor Negrescu, Birgit Sippel, Nils Ušakovs
The Left	Dimitrios Papadimoulis, Helmut Scholz
Verts/ALE	Rasmus Andresen, Damian Boeselager, Francisco Guerreiro

0	-

4	0
ECR	Zbigniew Kuźmiuk, Bogdan Rzońca, Johan Van Overtveldt
ID	Joachim Kuhs

Korišteni znakovi:

+ : za
- : protiv
0 : suzdržani
31.1.2023

MIŠLJENJE ODBORA ZA USTAVNA PITANJA

upućeno Odboru za industriju, istraživanje i energetiku

o Prijedlogu uredbe Europskog parlamenta i Vijeća o mjerama za visoku zajedničku razinu kibersigurnosti u institucijama, tijelima, uredima i agencijama Unije (COM(2022)0122 – C9-0122/2022 – 2022/0085(COD))

Izvjestiteljica za mišljenje: Markéta Gregorová

KRATKO OBRAZLOŽENJE

Institucije, tijela i agencije Europske unije posljednjih godina djeluju u sve digitaliziranim kontekstu stalnog tehnološkog razvoja i posljedičnih rastućih razina kibersigurnosnih prijetnji. Tu je situaciju pogoršala zdravstvena kriza uzrokovana bolešću COVID-19 i, među ostalim, povećana praksa rada na daljinu, te je broj sofisticiranih napada iz niza izvora nastavio rasti.

Trenutačno se okruženje kibersigurnosti, uključujući upravljanje, kiberhigijenu, sveukupne kapacitete i razvijenost, znatno razlikuje među institucijama, tijelima i agencijama Unije, što stvara dodatnu prepreku otvorenoj, učinkovitoj i neovisnoj europskoj upravi.

Stoga se izvjestiteljica slaže s time da je pristup osnovnog okvira za institucije, tijela i agencije Unije za uspostavu zajedničkih sustava i zahtjeva u pogledu kibersigurnosti potreban kako bi se osiguralo da se kibersigurnost razvija u istom smjeru, čime će se doprinijeti učinkovitosti i neovisnosti europske uprave.

Izvjestiteljica nadalje smatra da je čvrst i dosljedan sigurnosni okvir iznimno važan za zaštitu svog osoblja, podataka, komunikacijskih mreža, informacijskih sustava i postupaka donošenja odluka EU-a, čime se također doprinosi demokratskom funkcioniranju Europske unije. Unaprjeđenom kulturom sigurnosti institucija, tijela i agencija Unije Europu će se isto tako pripremiti za digitalno doba te će se izgraditi gospodarstvo u službi građana otporno na promjene koje nosi budućnost.

AMANDMANI

Odbor za ustavna pitanja poziva Odbor za industriju, istraživanje i energetiku da kao nadležni odbor uzme u obzir sljedeće amandmane:

Amandman 1

Prijedlog uredbe Uvodna izjava 1.

Tekst koji je predložila Komisija

(1) U digitalnom dobu informacijska i komunikacijska tehnologija okosnica je otvorene, učinkovite i neovisne uprave u Uniji. Zbog napretka tehnologije te povećane složenosti i međusobne povezanosti digitalnih sustava kibersigurnosni rizici sve su veći, a uprava Unije osjetljivija je na kiberprijetnje i incidente, što u konačnici predstavlja prijetnju poslovnom kontinuitetu i

Izmjena

(1) U digitalnom dobu informacijska i komunikacijska tehnologija okosnica je otvorene, učinkovite i neovisne uprave u Uniji. Zbog napretka tehnologije te povećane složenosti i međusobne povezanosti digitalnih sustava kibersigurnosni rizici sve su veći, a uprava Unije osjetljivija je na kiberprijetnje i incidente, što u konačnici predstavlja prijetnju poslovnom kontinuitetu i

sposobnosti uprave da zaštiti svoje podatke. Iako su povećana upotreba usluga u oblaku, sveprisutna upotreba informacijske tehnologije, visok stupanj digitalizacije, rad na daljinu te napredak tehnologije i povezanosti danas osnovne značajke svih aktivnosti upravnih tijela Unije, digitalna otpornost još nije dovoljno ukorijenjena u njihov rad.

sposobnosti uprave da zaštiti svoje podatke. Iako su povećana upotreba usluga u oblaku, sveprisutna upotreba informacijske *i komunikacijske* tehnologije (IKT), visok stupanj digitalizacije, rad na daljinu te napredak tehnologije i povezanosti danas osnovne značajke svih aktivnosti upravnih tijela Unije, digitalna otpornost još nije dovoljno ukorijenjena u njihov rad.

Obrazloženje

U prijedlogu Komisije spominje se „informacijska tehnologija“ gdje bi se umjesto toga trebala upotrebljavati „informacijska i komunikacijska tehnologija“, što je standardni pojam koji se upotrebljava u Direktivi NIS2 i Aktu EU-a o kibersigurnosti.

Amandman 2

Prijedlog uredbe Uvodna izjava 2.

Tekst koji je predložila Komisija

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

Izmjena

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

Amandman 3

Prijedlog uredbe Uvodna izjava 3.

Tekst koji je predložila Komisija

Izmjena

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

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

Amandman 4 Prijedlog uredbe Uvodna izjava 4.

Tekst koji je predložila Komisija

(4) Institucije, tijela i agencije Unije privlačne su mete koje se suočavaju s vrlo vještim i dobro opremljenim prijetećim akterima i drugim prijetnjama. Istodobno, razina i razvijenost kiberotpornosti te sposobnost otkrivanja zlonamjernih kiberaktivnosti i odgovora na njih znatno se razlikuju od subjekta do subjekta. Kako bi europska uprava funkcionalala, institucije, tijela i agencije Unije stoga moraju ostvariti visoku zajedničku razinu kibersigurnosti putem osnovnog okvira za kibersigurnost (skupa minimalnih pravila za kibersigurnost s kojima mrežni i informacijski sustavi te njihovi operateri i korisnici moraju biti usklađeni kako bi se kibersigurnosni rizici ***sveli na najmanju mjeru***), kao i putem razmjene informacija i suradnje.

Izmjena

(4) Institucije, tijela, ***uredi*** i agencije Unije privlačne su mete koje se suočavaju s vrlo vještim i dobro opremljenim prijetećim akterima i drugim prijetnjama. Istodobno, razina i razvijenost kiberotpornosti te sposobnost otkrivanja zlonamjernih kiberaktivnosti i odgovora na njih znatno se razlikuju od subjekta do subjekta. Kako bi europska uprava funkcionalala, institucije, tijela, ***uredi*** i agencije Unije stoga moraju ostvariti visoku zajedničku razinu kibersigurnosti putem osnovnog okvira za kibersigurnost (skupa ***zajedničkih***, minimalnih pravila za kibersigurnost s kojima mrežni i informacijski sustavi te njihovi operateri i korisnici moraju biti usklađeni kako bi se ***ograničili*** kibersigurnosni rizici), kao i putem ***redovne i učinkovite*** razmjene informacija i suradnje ***te osposobljavanja u***

području kibersigurnosti.

Amandman 5

Prijedlog uredbe Uvodna izjava 7.

Tekst koji je predložila Komisija

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

Izmjena

(7) Zbog razlika među institucijama, tijelima, **uredima** i agencijama Unije pri provedbi je potrebna fleksibilnost jer ne postoji univerzalno rješenje. Mjere za visoku zajedničku razinu kibersigurnosti trebale **bi podupirati zadaće** institucija, tijela, **ureda** i agencija Unije **te uzeti u obzir** njihovu institucijsku autonomiju. Stoga bi institucije, tijela, **uredi** i agencije trebali uspostaviti vlastite okvire za upravljanje, opće upravljanje i kontrolu kibersigurnosnih rizika te donijeti vlastite osnovne okvire i planove za kibersigurnost, **uzimajući u obzir usklađenost i interoperabilnost svojih okvira na temelju zajedničkog okvira utvrđenog ovom Uredbom.**

Amandman 6

Prijedlog uredbe Uvodna izjava 8.

Tekst koji je predložila Komisija

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

Izmjena

(8) Da bi se izbjeglo nerazmjerne financijsko i administrativno opterećenje za institucije, tijela, **urede** i agencije Unije, zahtjevi za upravljanje kibersigurnosnim rizikom trebali bi **odgovarati** riziku kojem je izložen predmetni mrežni i informacijski sustav, uzimajući u obzir suvremenost mjera. Sve institucije, tijela, **uredi** i agencije Unije trebali bi nastojati odrediti **barem 10 %** svojeg proračuna za informacijske **i komunikacijske** tehnologije za poboljšanje svoje razine kibersigurnosti **srednjoročno i** dugoročno

ako je potrebno.

Amandman 7

Prijedlog uredbe Uvodna izjava 9.

Tekst koji je predložila Komisija

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

Izmjena

(9) Kako bi se postigla visoka zajednička razina kibersigurnosti, ona mora biti pod nadzorom **zajedničkog odbora EU-a s najvišom rukovodećom razinom** svake institucije, tijela, **ureda** i agencije Unije, **koji** bi **trebao** odobriti osnovni okvir za kibersigurnost kojim bi se trebali otklanjati rizici utvrđeni u skladu s unutarnjim okvirom koji svaka institucija, tijelo, **ured** i agencija mora uspostaviti. Bavljenje kulturom kibersigurnosti, tj. svakodnevna primjena kibersigurnosti, **trebalo bi postati** sastavni dio osnovnog okvira za kibersigurnost u svim institucijama, tijelima, **uredima** i agencijama Unije.

Amandman 8

Prijedlog uredbe Uvodna izjava 10.

Tekst koji je predložila Komisija

(10) Institucije, tijela i agencije Unije trebali bi procijeniti rizike povezane s odnosima s dobavljačima i pružateljima usluga, uključujući pružatelje usluga pohrane i obrade podataka ili upravljanih sigurnosnih usluga, te poduzeti odgovarajuće mjere za njihovo otklanjanje. Te mjere trebale bi biti dio osnovnog okvira za kibersigurnost i trebalo bi ih pobliže definirati u smjernicama ili preporukama koje izdaje CERT-EU. Pri definiranju mera i smjernica moraju se uzeti u obzir relevantno zakonodavstvo i

Izmjena

(10) Institucije, tijela, **uredi** i agencije Unije trebali bi procijeniti rizike povezane s odnosima s dobavljačima i pružateljima usluga, uključujući pružatelje usluga pohrane i obrade podataka ili upravljanih sigurnosnih usluga, te poduzeti odgovarajuće mjere za njihovo otklanjanje. **Te bi dobavljače i pružatelje usluga trebalo temeljito provjeriti, uzimajući u obzir cijeli lanac opskrbe te gospodarsko i političko okruženje u kojem djeluju. Ako odnosi s takvim dobavljačima i pružateljima usluga predstavljaju rizik za**

politike EU-a, uključujući procjene rizika i preporuke koje je izdala Skupina za suradnju u području sigurnosti mrežnih i informacijskih sustava, kao što su usklađena procjena rizika na razini EU-a i paket instrumenata EU-a za kibersigurnost 5G mreža. Osim toga, **moglo bi se** zahtijevati certificiranje relevantnih IKT proizvoda, usluga i procesa u okviru posebnih programa kibersigurnosne certifikacije EU-a donesenih na temelju članka 49. Uredbe (EU) 2019/881.

integritet demokratskih procesa u Uniji, trebalo bi ih prekinuti bez nepotrebne odgode. Te mjere trebale bi biti dio osnovnog okvira za kibersigurnost i trebalo bi ih pobliže definirati u smjernicama ili preporukama koje izdaje CERT-EU. Pri definiranju mjera i smjernica moraju se uzeti u obzir relevantno zakonodavstvo i politike EU-a, uključujući procjene rizika i preporuke koje je izdala Skupina za suradnju u području sigurnosti mrežnih i informacijskih sustava, kao što su usklađena procjena rizika na razini EU-a i paket instrumenata EU-a za kibersigurnost 5G mreža. Osim toga, **s obzirom na prijetnje i važnost jačanja otpornosti, trebalo bi** zahtijevati certificiranje relevantnih IKT proizvoda, usluga i procesa **koji se koriste u institucijama, tijelima, uredima i agencijama Unije** u okviru posebnih programa kibersigurnosne certifikacije EU-a donesenih na temelju članka 49. Uredbe (EU) 2019/881.

Amandman 9

Prijedlog uredbe Uvodna izjava 13.

Tekst koji je predložila Komisija

(13) Mnogi kibernapadi dio su širih kampanja usmjerenih na skupine institucija, tijela i agencija Unije ili interesnih zajednica koje uključuju institucije, tijela i agencije Unije. Kako bi omogućili proaktivne mjere za otkrivanje, odgovor na incidente ili ublažavanje, institucije, tijela i agencije Unije trebali bi obavijestiti CERT-EU o ozbiljnim kiberprijetnjama, znatnim ranjivostima i ozbiljnim incidentima te podijeliti odgovarajuće tehničke pojedinosti koje omogućuju otkrivanje ili ublažavanje sličnih kiberprijetnji, ranjivosti i incidenata u drugim institucijama, tijelima i agencijama Unije, kao i odgovor na njih.

Izmjena

(13) Mnogi kibernapadi dio su širih kampanja usmjerenih na skupine institucija, tijela, **ureda** i agencija Unije ili interesnih zajednica koje uključuju institucije, tijela, **urede** i agencije Unije. Kako bi omogućili proaktivne mjere za otkrivanje, odgovor na incidente ili ublažavanje, institucije, tijela, **uredi** i agencije Unije trebali bi obavijestiti CERT-EU o ozbiljnim kiberprijetnjama, znatnim ranjivostima i ozbiljnim incidentima te podijeliti odgovarajuće tehničke pojedinosti koje omogućuju otkrivanje ili ublažavanje sličnih kiberprijetnji, ranjivosti i incidenata u drugim institucijama, tijelima, **uredima** i agencijama Unije, kao i

Na temelju istog pristupa kao što je onaj predviđen Direktivom [prijeđlog NIS 2], ako subjekti dobiju informaciju o ozbilnjnom incidentu, trebali bi biti dužni u roku od 24 sata dostaviti ***prvu obavijest*** CERT-EU-u. Ta razmjena informacija trebala bi omogućiti CERT-EU-u da te informacije proslijedi drugim institucijama, tijelima i agencijama Unije, kao i odgovarajućim partnerima, kako bi se pomoglo zaštititi sva ***informatička*** okruženja Unije i partnera Unije od sličnih incidenata, prijetnji i ranjivosti.

odgovor na njih. Na temelju istog pristupa kao što je onaj predviđen Direktivom [prijeđlog NIS 2], ako subjekti dobiju informaciju o ozbilnjom incidentu, trebali bi biti dužni ***bez nepotrebne odgode, a u svakom slučaju najkasnije*** u roku od 24 sata dostaviti ***rano upozorenje*** CERT-EU-u. ***Institucijama, tijelima, uredima i agencijama Unije trebalo bi dodijeliti dostatna sredstva za brzo i učinkovito ispunjavanje obveza izvješćivanja kako bi se osiguralo ispravno funkciranje osmišljenog sustava.*** Ta razmjena informacija trebala bi omogućiti CERT-EU-u da te informacije proslijedi drugim institucijama, tijelima, ***uredima*** i agencijama Unije, kao i odgovarajućim partnerima, kako bi se pomoglo zaštititi sva ***informacijska i komunikacijska*** okruženja Unije i partnera Unije od sličnih incidenata, prijetnji i ranjivosti.

Amandman 10

Prijedlog uredbe Uvodna izjava 14.

Tekst koji je predložila Komisija

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

Izmjena

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

Amandman 11

Prijedlog uredbe Uvodna izjava 16.

Tekst koji je predložila Komisija

(16) IICB bi trebao nadzirati usklađenost s ovom Uredbom te pratiti smjernice, preporuke i pozive na djelovanje koje izdaje CERT-EU. IICB bi u tehničkim pitanjima **trebalo** imati potporu tehničkih savjetodavnih skupina *čiji sastav IICB određuje prema vlastitu nahodenju te* koje bi **prema potrebi** trebale blisko surađivati s CERT-EU-om, institucijama, tijelima i agencijama Unije te drugim dionicima. Prema potrebi, IICB bi trebao izdavati **neobvezujuća** upozorenja i **preporučivati** revizije.

Izmjena

(16) IICB bi trebao nadzirati usklađenost s ovom Uredbom te pratiti smjernice, preporuke i pozive na djelovanje koje izdaje CERT-EU. IICB bi u tehničkim pitanjima **trebao** imati potporu tehničkih savjetodavnih skupina koje bi trebale blisko surađivati s CERT-EU-om, institucijama, tijelima, **uredima** i agencijama Unije te drugim dionicima, **kako je primjereno**. Prema potrebi, IICB bi trebao izdavati upozorenja i **preporuke za** revizije.

Amandman 12

Prijedlog uredbe Uvodna izjava 17.

Tekst koji je predložila Komisija

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

Izmjena

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

Amandman 13

Prijedlog uredbe Uvodna izjava 18.

Tekst koji je predložila Komisija

Izmjena

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

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

Amandman 14

Prijedlog uredbe Uvodna izjava 19.a (nova)

Tekst koji je predložila Komisija

Izmjena

(19.a) Kako bi se osigurala bolja provedba kibersigurnosnih mjera i smjernica za institucije, tijela, urede i agencije Unije te konsolidirala kultura kibersigurnosti u njima, CERT-EU bi također trebao poboljšati suradnju s Europskom mrežom i centrom za stručnost u području kibersigurnosti.

Amandman 15

Prijedlog uredbe Uvodna izjava 20.

Tekst koji je predložila Komisija

Izmjena

(20) Pri pružanju potpore operativnoj kibersigurnosti CERT-EU trebao bi

(20) Pri pružanju potpore operativnoj kibersigurnosti CERT-EU trebao bi

koristiti raspoloživo stručno znanje Agencije Europske unije za kibersigurnost u okviru strukturirane suradnje kako je predviđeno Uredbom (EU) 2019/881 Europskog parlamenta i Vijeća⁵. **Prema potrebi** bi **trebalo** definirati namjenske aranžmane između ta dva subjekta kako bi se utvrdila praktična provedba takve suradnje i izbjeglo udvostručivanje aktivnosti. CERT-EU trebao bi surađivati s Agencijom Europske unije za kibersigurnost na analizi prijetnji i redovito izvješćivati Agenciju o stanju kiberprijetnji.

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

Amandman 16 Prijedlog uredbe Uvodna izjava 24.

Tekst koji je predložila Komisija

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

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

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

Izmjena

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

Amandman 17

Prijedlog uredbe Uvodna izjava 25.

Tekst koji je predložila Komisija

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

Izmjena

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

Amandman 18

Prijedlog uredbe Članak 1. – stavak 1. – točka a

Tekst koji je predložila Komisija

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

Izmjena

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

Amandman 19

Prijedlog uredbe Članak 1. – stavak 1. – točka c

Tekst koji je predložila Komisija

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

Izmjena

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

Amandman 20

Prijedlog uredbe

Članak 2.a (novi)

Tekst koji je predložila Komisija

Izmjena

Članak 2.a

Obrada osobnih podataka

Obrada osobnih podataka koju na temelju ove Uredbe provode CERT-EU, IICB i sve institucije, tijela, uredi i agencije Unije provodi se u skladu s Uredbom (EU) 2018/1725 Europskog parlamenta i Vijeća.

Amandman 21

Prijedlog uredbe

Članak 3. – stavak 1. – točka 2.

Tekst koji je predložila Komisija

Izmjena

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

(2) „mrežni i informacijski sustav” znači mrežni i informacijski sustav *kako je definiran u članku 6. točki 1. Direktive [prijeđlog NIS 2];*

Amandman 22

Prijedlog uredbe

Članak 3. – stavak 1. – točka 4.

Tekst koji je predložila Komisija

Izmjena

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

(4) „kibersigurnost” znači kibersigurnost *kako je definirana u članku 2. točki 1. Uredbe (EZ) br. 2019/881 Europskog parlamenta i Vijeća^{1a}*

^{1a} Uredba (EU) 2019/881 Europskog parlamenta i Vijeća od 17. travnja 2019. o ENISA-i (Agencija Europske unije za kibersigurnost) te o kibersigurnosnoj certifikaciji u području informacijske i komunikacijske tehnologije i stavljanju izvan snage Uredbe (EU) br. 526/2013

(Akt o kibersigurnosti) (SL L 151,
7.6.2019., str. 15.).

Amandman 23

Prijedlog uredbe

Članak 3. – stavak 1. – točka 5.

Tekst koji je predložila Komisija

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

Izmjena

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

Amandman 24

Prijedlog uredbe

Članak 3. – stavak 1. – točka 7.

Tekst koji je predložila Komisija

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

Izmjena

(7) „ozbiljan incident” znači svaki incident *koji je uzrokovao ili može uzrokovati ozbiljne poremećaje u funkcioniranju subjekta Unije ili finansijski gubitak za dotični subjekt iz Unije ili koji je utjecao ili može utjecati na druge fizičke ili pravne osobe uzrokujući znatnu materijalnu ili nematerijalnu štetu*;

Amandman 25

Prijedlog uredbe

Članak 3. – stavak 1. – točka 11.

Tekst koji je predložila Komisija

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

Izmjena

(11) „ozbiljna kiberprijetnja” znači kiberprijetnja *kako je definirana u članku 6. točki 11. Direktive [prijedlog NIS 2]*;

Amandman 26

Prijedlog uredbe

Članak 3. – stavak 1. – točka 14.

Tekst koji je predložila Komisija

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

Izmjena

(14) „*rizik*” znači *svaki rizik kako je definiran u članku 6. točki 9. Direktive [prijeđlog NIS 2];*

Amandman 27

Prijedlog uredbe

Članak 3. – stavak 1. – točka 14.a (nova)

Tekst koji je predložila Komisija

Izmjena

(14.a) „*IKT okruženje*” znači *svaki lokalni ili virtualni IKT proizvod, IKT usluga i IKT proces kako su definirani u članku 2. točkama 12., 13. i 14. Uredbe (EU) 2019/881 i svaki mrežni i informacijski sustav bez obzira na to jesu li u vlasništvu institucije, tijela, ureda ili agencije Unije i upravlja li njima institucija, tijelo, ured ili agencija Unije ili su smješteni na poslužitelju i njima upravlja treća strana, uključujući mobilne uređaje, korporativne mreže i poslovne mreže koje nisu povezane s internetom te sve uređaje povezane s IKT okruženjem;*

Obrazloženje

Pojam je premješten iz članka 4. stavka 2. ovog Prijedloga u članak s definicijama s obzirom na to da se taj pojam dosljedno upotrebljava u cijelom tekstu. Predložena definicija tog pojma temelji se na definicijama njegovih sastavnih dijelova iz članka 2. Uredbe (EU) 2019/881 o Aktu o kibersigurnosti.

Amandman 28

Prijedlog uredbe

Članak 3. – stavak 1. – točka 15.

Tekst koji je predložila Komisija

Izmjena

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

Briše se.

Amandman 29

Prijedlog uredbe

Članak 4. – stavak 1.

Tekst koji je predložila Komisija

Izmjena

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

1. *Na temelju sveobuhvatne sigurnosne revizije*, sve institucije, tijela, uredi i agencije Unije uspostavljaju unutarnji okvir za upravljanje, opće upravljanje i kontrolu kibersigurnosnih rizika („okvir”) kojim se podupiru zadaće subjekta, pri čemu primjenjuju svoju institucijsku autonomiju, *uzimajući u obzir i uskladenost i interoperabilnost svojeg okvira s okvirima drugih relevantnih institucija, tijela, ureda i agencija*. Provedbu nadzire najviša rukovodeća razina predmetnog subjekta, *koja je odgovorna za osiguravanje učinkovitog i razboritog upravljanja* svim kibersigurnosnim rizicima. Okvir se mora uspostaviti najkasnije do [15 mjeseci *nakon datuma* stupanja na snagu ove Uredbe].

Amandman 30

Prijedlog uredbe

Članak 4. – stavak 2.

Tekst koji je predložila Komisija

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

Izmjena

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

Amandman 31

Prijedlog uredbe

Članak 4. – stavak 4.

Tekst koji je predložila Komisija

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

Izmjena

4. Sve institucije, tijela, **uredi** i agencije Unije dužne su imati uspostavljene učinkovite mehanizme kojima se osigurava da se **srednjoročno najmanje 10% ukupnog** proračuna za informacijsku **i komunikacijsku** tehnologiju troši na kibersigurnost.

Amandman 32

Prijedlog uredbe

Članak 4. – stavak 5.a (novi)

Tekst koji je predložila Komisija

Izmjena

5.a Lokalni službenik za kibersigurnost surađuje sa službenikom za zaštitu podataka iz članka 43. Uredbe (EU) 2018/1725 kada je riječ o

aktivnostima koje se preklapaju kojima se tehnička i integrirana zaštita podataka primjenjuje na kibersigurnosne mjere i kada odabiru kibersigurnosne mjere koje uključuju zaštitu osobnih podataka, integrirano upravljanje rizicima i integrirano rješavanje sigurnosnih incidenta.

Amandman 33

Prijedlog uredbe Članak 5. – stavak 1.

Tekst koji je predložila Komisija

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

Izmjena

1. Najviša rukovodeća razina svake institucije, tijela, **ureda** i agencije Unije odobrava osnovni okvir za kibersigurnost svoje organizacije radi otklanjanja rizika utvrđenih u unutarnjem okviru iz članka 4. stavka 1. Time se podupiru zadaće organizacije i primjenjuje njezina institucijska autonomija, **uz potpuno poštovanje zahtjeva iz ove Uredbe te uzimajući u obzir usklađenost i interoperabilnost svojeg okvira s okvirom drugih relevantnih institucija, tijela, ureda i agencija, kao i smjernice i preporuke koje je donio IICB na prijedlog CERT-EU-a i primjenjive programe kibersigurnosne certifikacije EU-a.** Osnovni okvir za kibersigurnost se mora uspostaviti najkasnije do [18 mjeseci **nakon datuma** stupanja na snagu ove Uredbe] i odnosi se na područja navedena u Prilogu I. i mjere navedene u Prilogu II.

Amandman 34

Prijedlog uredbe Članak 5. – stavak 2.

Tekst koji je predložila Komisija

2. Više rukovodstvo svih institucija,

Izmjena

2. Više rukovodstvo svih institucija,

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

tijela, *ureda* i agencija Unije redovito sudjeluje u posebnim osposobljavanjima kako bi steklo dovoljno znanja i vještina da shvati i procijeni kibersigurnosne rizike i prakse upravljanja kibersigurnošću te njihov utjecaj na poslovanje organizacije *uz odgovarajuće resurse. Osim takvih posebnih osposobljavanja i u svrhu izgradnje i konsolidacije kulture kibersigurnosti, u plan za kibersigurnost uključuje se redovito osposobljavanje članova osoblja u području kibersigurnosti i ažurira se najmanje svake dvije godine. Osiguravaju se dostatna sredstva za kvalitetno osposobljavanje.*

Amandman 35

Prijedlog uredbe Članak 6. – stavak 1.

Tekst koji je predložila Komisija

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

Izmjena

Sve institucije, tijela, *uredi* i agencije Unije **provode procjenu razvijenosti kibersigurnosti do ... [6 mjeseci nakon stupanja na snagu ove Uredbe] i najmanje svake dvije godine nakon toga, uključujući** sve elemente njihovih **informacijskih i komunikacijskih** okruženja kako je opisano u članku 4., pri čemu uzimaju u obzir relevantne smjernice i preporuke donesene u skladu s člankom 13. **Procjena razvijenosti temelji se na neovisnim revizijama kibersigurnosti koje provode provjereni pružatelji.**

Amandman 36

Prijedlog uredbe Članak 7. – stavak 1.

Tekst koji je predložila Komisija

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

Izmjena

1. Na temelju zaključaka izvedenih iz procjene razvijenosti i s obzirom na sredstva i rizike utvrđene u skladu s člankom 4., najviša rukovodeća razina svih institucija, tijela, **ureda** i agencija Unije bez nepotrebne odgode odobrava plan za kibersigurnost nakon uspostave okvira za upravljanje, opće upravljanje i kontrolu rizika te osnovnog okvira za kibersigurnost. Planom se nastoji povećati ukupna kibersigurnost predmetnog subjekta i time pridonijeti postizanju ili poboljšanju visoke zajedničke razine kibersigurnosti u svim institucijama, tijelima, **uredima** i agencijama Unije. Kako bi se pružila potpora zadaćama subjekta na temelju njegove institucijske autonomije, plan obuhvaća barem područja navedena u Prilogu I., mjere navedene u Prilogu II. te mjere povezane s pripravnošću i odgovorom na incidente i oporavkom od njih, kao što su **sigurnosna procjena dobavljača i usluga**, nadzor i vođenje evidencije. Plan se revidira najmanje svake **dvije** godine na temelju procjena razvijenosti provedenih u skladu s člankom 6.

Amandman 37

Prijedlog uredbe

Članak 7. – stavak 2.

Tekst koji je predložila Komisija

2. Plan za kibersigurnost sadržava dužnosti i zadaće članova osoblja koje se odnose na njegovu provedbu.

Izmjena

2. Plan za kibersigurnost sadržava dužnosti, **pripravnost** i zadaće članova osoblja koje se odnose na njegovu provedbu.

Amandman 38

**Prijedlog uredbe
Članak 7. – stavak 3.**

Tekst koji je predložila Komisija

3. U planu za kibersigurnost ***u obzir se uzimaju sve primjenjive smjernice i preporuke*** koje je izdao CERT-EU.

Izmjena

3. U planu za kibersigurnost ***uključene su sve predložene mjere sadržane u primjenjivim smjernicama i preporukama*** koje je izdao CERT-EU.

Amandman 39

**Prijedlog uredbe
Članak 7. – stavak 3.a (novi)**

Tekst koji je predložila Komisija

Izmjena

3.a Institucije, tijela, uredi i agencije Unije podnose svoje planove za kibersigurnost IICB-u. Ti se planovi dijele u mjeri u kojoj je to moguće bez rizika od otkrivanja ili otkrivanja osjetljivih ili povjerljivih informacija o određenim tehničkim kibersigurnosnim aranžmanima i sposobnostima subjekta iz Unije neovlaštenim trećim stranama.

Amandman 40

**Prijedlog uredbe
Članak 9. – stavak 2. – točka a**

Tekst koji je predložila Komisija

(a) praćenje provedbe ove Uredbe u institucijama, tijelima i agencijama Unije;

Izmjena

(a) praćenje provedbe ove Uredbe u institucijama, tijelima, ***uredima*** i agencijama Unije ***te izdavanje preporuka za postizanje zajedničke visoke razine kibersigurnosti;***

Amandman 41

**Prijedlog uredbe
Članak 9. – stavak 3. – podstavak 1. – uvodni dio**

Tekst koji je predložila Komisija

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

Izmjena

IICB se sastoji od tri predstavnika koje Mreža agencija Unije (EUAN) imenuje na prijedlog svojeg savjetodavnog odbora za IKT (ICTAC) da zastupaju interes **ureda**, agencija i tijela koja sama upravljaju svojim **informacijskim i komunikacijskim** okruženjem i po jednog predstavnika kojeg imenuje svako od sljedećih tijela:

Amandman 42

Prijedlog uredbe

Članak 9. – stavak 3. – podstavak 1. – točka ka (nova)

Tekst koji je predložila Komisija

Izmjena

(ka) Europski nadzornik za zaštitu podataka.

Amandman 43

Prijedlog uredbe

Članak 10. – stavak 1. – točka aa (nova)

Tekst koji je predložila Komisija

Izmjena

(aa) na temelju prijedloga voditelja CERT-EU-a odobrava preporuke za postizanje zajedničke visoke razine kibersigurnosti, namijenjene jednoj ili svim institucijama, tijelima, uredima i agencijama Unije;

Amandman 44

Prijedlog uredbe

Članak 11. – stavak 1. – točka a

Tekst koji je predložila Komisija

Izmjena

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

(a) izdati upozorenje; prema potrebi, pristup upozorenju na odgovarajući se način ograničava **zajednički dogovorenom metodologijom** ako postoji uvjerljiv

kibersigurnosni rizik;

kibersigurnosni rizik;

Amandman 45

Prijedlog uredbe

Članak 11. – stavak 1. – točka b

Tekst koji je predložila Komisija

(b) *preporučiti* mjerodavnoj revizorskoj službi da provede reviziju.

Izmjena

(b) *naložiti* mjerodavnoj revizorskoj službi da provede reviziju.

Amandman 46

Prijedlog uredbe

Članak 12. – stavak 1.

Tekst koji je predložila Komisija

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

Izmjena

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

Amandman 47

Prijedlog uredbe

Članak 12. – stavak 2. – točka d

Tekst koji je predložila Komisija

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

Izmjena

(d) skreće pozornost IICB-a na sva pitanja koja se odnose na provedbu ove Uredbe i provedbu smjernica, preporuka i poziva na djelovanje *te daje prijedloge za*

pravnu zaštitu;

Amandman 48

Prijedlog uredbe Članak 12. – stavak 4.

Tekst koji je predložila Komisija

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

Izmjena

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

Amandman 49

Prijedlog uredbe Članak 12. – stavak 5. – uvodni dio

Tekst koji je predložila Komisija

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

Izmjena

5. CERT-EU može *institucijama, tijelima, uredima i agencijama Unije* pružati sljedeće usluge koje nisu opisane u njegovu katalogu usluga („usluge uz naknadu”):

Amandman 50

Prijedlog uredbe Članak 12. – stavak 5. – točka a

Tekst koji je predložila Komisija

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

Izmjena

(a) usluge kojima se podupire kibersigurnost *informacijskog i komunikacijskog* okruženja institucija, tijela, ureda i agencija Unije, osim onih iz stavka 2., na temelju sporazumâ o razini

resursima;

usluga i ovisno o dostupnim resursima;

Amandman 51

Prijedlog uredbe

Članak 12. – stavak 5. – točka b

Tekst koji je predložila Komisija

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

Izmjena

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

Amandman 52

Prijedlog uredbe

Članak 12. – stavak 5. – točka c

Tekst koji je predložila Komisija

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

Izmjena

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

Amandman 53

Prijedlog uredbe

Članak 12. – stavak 6.

Tekst koji je predložila Komisija

6. CERT-EU može organizirati vježbe u području kibersigurnosti ili preporučiti

Izmjena

6. CERT-EU može organizirati vježbe u području kibersigurnosti ili preporučiti

sudjelovanje u postojećim vježbama, u bliskoj suradnji s Agencijom Europske unije za kibersigurnost kad je to primjenjivo, kako bi se *ispitala* razina kibersigurnosti institucija, tijela i agencija Unije.

sudjelovanje u postojećim vježbama, u bliskoj suradnji s Agencijom Europske unije za kibersigurnost kad je to primjenjivo, kako bi se *redovito ispitivala* razina kibersigurnosti institucija, tijela, *ureda* i agencija Unije. *Nadalje, pojačanom suradnjom i zajedničkim programima s Europskom mrežom i centrom za stručnost u području kibersigurnosti (ECCC), CERT-EU može podupirati istraživanja i inovacije te pomoći u jačanju kibersigurnosnih sposobnosti institucija, tijela, ureda i agencija Unije.*

Amandman 54

Prijedlog uredbe Članak 12. – stavak 7.

Tekst koji je predložila Komisija

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

Izmjena

7. CERT-EU *pruža* pomoć institucijama, tijelima, *uredima* i agencijama Unije u pogledu incidenata u povjerljivim *informacijskim i komunikacijskim* okruženjima ako *predmetne institucije, tijela, uredi ili agencije Unije* to izričito *zatraže i ako CERT-EU ima potrebna sredstva za to ili prima takva sredstva od dotičnog subjekta.*

Amandman 55

Prijedlog uredbe Članak 14. – stavak 1.

Tekst koji je predložila Komisija

Voditelj CERT-EU-a redovito podnosi izvješća IICB-u i predsjedniku IICB-a o uspješnosti CERT-EU-a, financijskom planiranju, prihodima, izvršenju proračuna, sklopljenim sporazumima o razini usluga i pisanim sporazumima, suradnji s ugovornim stranama i partnerima te

Izmjena

Voditelj CERT-EU-a redovito, *barem jednom godišnje*, podnosi izvješća IICB-u i predsjedniku IICB-a o uspješnosti CERT-EU-a, financijskom planiranju, prihodima, izvršenju proračuna, sklopljenim sporazumima o razini usluga i pisanim sporazumima, suradnji s ugovornim

službenim putovanjima osoblja,
uključujući izvješća iz članka 10. stavka 1.

stranama i partnerima te službenim
putovanjima osoblja, uključujući izvješća
iz članka 10. stavka 1.

Amandman 56

Prijedlog uredbe Članak 16. – stavak 1.

Tekst koji je predložila Komisija

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

Izmjena

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

Amandman 57

Prijedlog uredbe Članak 16. – stavak 2.

Tekst koji je predložila Komisija

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

Izmjena

2. CERT-EU može s nacionalnim partnerima u državama članicama razmjenjivati informacije o određenim incidentima bez suglasnosti **pogodenih institucija, tijela, ureda ili agencija Unije, pod uvjetom da je obrada osobnih podataka u skladu s primjenjivim odredbama Uredbe (EU) 2018/1725**, kako bi se olakšalo otkrivanje sličnih kiberprijetnji ili incidenata. Informacije o određenim incidentima kojima se otkriva identitet mete kiberincidenta CERT-EU može razmjenjivati samo uz suglasnost **pogodenih institucija, tijela, ureda ili**

agencija Unije.

Amandman 58

Prijedlog uredbe

Članak 17. – stavak 1.

Tekst koji je predložila Komisija

1. CERT-EU može s partnerima iz trećih zemalja, uključujući partnere iz određenih industrijskih sektora, surađivati na pitanjima alata i metoda, kao što su tehnike, taktike, postupci i najbolja praksa, te na pitanjima kiberprijetnji i ranjivosti. Za suradnju s takvim partnerima, među ostalim u okvirima u kojima partneri koji nisu iz EU-a surađuju s nacionalnim partnerima iz država članica, CERT-EU mora zatražiti prethodno odobrenje IICB-a.

Izmjena

1. CERT-EU može s partnerima iz trećih zemalja, uključujući partnere iz određenih industrijskih sektora, surađivati na pitanjima alata i metoda, kao što su tehnike, taktike, postupci i najbolja praksa, te na pitanjima kiberprijetnji i ranjivosti. Za suradnju s takvim partnerima, među ostalim u okvirima u kojima partneri koji nisu iz EU-a surađuju s nacionalnim partnerima iz država članica, CERT-EU mora zatražiti prethodno odobrenje IICB-a.
Svakom takvom suradnjom poštuje se demokratski integritet EU-a.

Amandman 59

Prijedlog uredbe

Članak 17. – stavak 2.

Tekst koji je predložila Komisija

2. CERT-EU može surađivati s drugim partnerima, kao što su komercijalni subjekti, međunarodne organizacije, nacionalni subjekti izvan Europske unije ili pojedinačni stručnjaci, kako bi prikupio informacije o općim i specifičnim kiberprijetnjama, ranjivostima i mogućim protumjerama. Za širu suradnju s tim partnerima CERT-EU mora zatražiti prethodno odobrenje IICB-a.

Izmjena

2. CERT-EU može surađivati s drugim partnerima, kao što su komercijalni subjekti, međunarodne organizacije, nacionalni subjekti izvan Europske unije ili pojedinačni stručnjaci, kako bi prikupio informacije o općim i specifičnim kiberprijetnjama, ranjivostima i mogućim protumjerama. Za širu suradnju s tim partnerima CERT-EU mora zatražiti prethodno odobrenje IICB-a.
Svakom takvom suradnjom poštuje se demokratski integritet EU-a.

Amandman 60

Prijedlog uredbe Članak 17. – stavak 3.

Tekst koji je predložila Komisija

3. Uz suglasnost *sastavnice pogodene* incidentom CERT-EU može informacije o incidentu podijeliti s partnerima koji mogu pridonijeti njegovoj analizi.

Izmjena

3. Uz suglasnost *institucija, tijela, ureda ili agencija Unije pogodenih* incidentom CERT-EU može informacije o incidentu podijeliti s partnerima koji mogu pridonijeti njegovoj analizi.

Amandman 61

Prijedlog uredbe Članak 19. – stavak -1. (novi)

Tekst koji je predložila Komisija

Izmjena

-1. *Institucije, tijela, uredi ili agencije Unije mogu CERT-EU-u dobrovoljno dostaviti informacije o kiberprijetnjama, incidentima, izbjegnutim incidentima i ranjivostima koji na njih utječu. CERT-EU osigurava dostupnost učinkovitih sredstava komunikacije u svrhu olakšavanja razmjene informacija sa subjektima Unije. CERT-EU može dati prednost obradi obveznih obavijesti pred obradom obavijesti na dobrovoljnoj osnovi.*

Amandman 62

Prijedlog uredbe Članak 19. – stavak 1.

Tekst koji je predložila Komisija

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

Izmjena

1. Kako bi CERT-EU mogao *obavljati svoju misiju i zadaće kako su definirani u članku 12.*, može od institucija, tijela, ureda i agencija Unije zatražiti da mu iz svojih evidencija *informacijskih i komunikacijskih* sustava dostave informacije, *uključujući informacije koje*

agencija kojoj je podnesen zahtjev bez nepotrebne odgode prenosi tražene informacije i sva njihova naknadna ažuriranja.

se odnose na kiberprijetnje, izbjegnute incidente, ranjivosti, pokazatelje ugroženosti, kibersigurnosna upozorenja i preporuke o konfiguraciji kibersigurnosnih alata za otkrivanje kiberincidenta. Subjekt kojem je podnesen zahtjev bez nepotrebne odgode prenosi tražene informacije i sva njihova naknadna ažuriranja.

Amandman 63

Prijedlog uredbe Članak 19. – stavak 2.

Tekst koji je predložila Komisija

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

Izmjena

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

Amandman 64

Prijedlog uredbe Članak 20. – naslov

Tekst koji je predložila Komisija

Obveze *obavlješćivanja*

Izmjena

Obveze *izvješćivanja*

Amandman 65

Prijedlog uredbe Članak 20. – stavak 1. – podstavak 1.

Tekst koji je predložila Komisija

Sve institucije, tijela i agencije Unije *dostavljaju prvu obavijest* CERT-EU-u o

Izmjena

Sve institucije, tijela, *uredi* i agencije Unije *pružaju rano upozorenje* CERT-EU-u o

ozbiljnim kiberprijetnjama, znatnim ranjivostima i ozbiljnim incidentima bez nepotrebne odgode, a u svakom slučaju najkasnije 24 sata od saznanja o njima.

ozbiljnim kiberprijetnjama, znatnim ranjivostima i ozbiljnim incidentima bez nepotrebne odgode, a u svakom slučaju najkasnije 24 sata od saznanja o njima. *U tom se ranom upozorenju, ako je primjenjivo, navodi je li znatan incident vjerojatno prouzročen nezakonitim ili zlonamjernim djelovanjem te ima li ili bi mogao imati prekogranični učinak.*

Amandman 66

Prijedlog uredbe

Članak 20. – stavak 1. – podstavak 2.

Tekst koji je predložila Komisija

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

Izmjena

U opravdanim slučajevima i u dogovoru s CERT-EU-om predmetna institucija, tijelo, *ured* ili agencija Unije može odstupiti od *tog roka*.

Amandman 67

Prijedlog uredbe

Članak 20. – stavak 2. – uvodni dio

Tekst koji je predložila Komisija

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

Izmjena

2. Osim toga, institucije, tijela, *uredi* i agencije Unije *dodatno šalju obavijest CERT-EU-u* bez nepotrebne odgode, *a u svakom slučaju u roku od 72 sata od primitka informacije o ozbiljnog incidentu, ažuriraju rano upozorenje i dostavljaju inicijalnu procjenu ozbiljnog incidenta, njegove ozbiljnosti i učinka, s relevantnim tehničkim pojedinostima o kiberprijetnjama, ranjivostima i incidentima a koje omogućuju poduzimanje mjera za otkrivanje, odgovor na incident ili ublažavanje. Obavijest obuhvaća, ako su dostupni:*

Amandman 68

Prijedlog uredbe

Članak 20. – stavak 2. – podstavak 1.a (novi)

Tekst koji je predložila Komisija

Izmjena

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

Amandman 69

Prijedlog uredbe

Članak 20. – stavak 2.a (novi)

Tekst koji je predložila Komisija

Izmjena

2.a Najkasnije mjesec dana nakon podnošenja obavijesti o ozbiljnem incidentu institucije, tijela, uredi i agencije Unije podnose konačno izvješće CERT-EU-u, koje uključuje barem sljedeće:

- (a) detaljan opis ozbiljnog incidenta, njegovu ozbiljnost i učinak;*
- (b) vrstu prijetnje ili temeljnog uzroka koji je vjerojatno prouzročio ozbiljan incident;*
- (c) provedene i tekuće mjere ublažavanja;*
- (d) ako je primjenjivo, prekogranični učinak ozbiljnog incidenta;*

Ako je ozbiljan incident još u tijeku u trenutku podnošenja završnog izvješća iz prvog podstavka, podnosi se izvješće o napretku u tom trenutku i završno izvješće u roku od mjesec dana nakon što je incident riješen.

Amandman 70

Prijedlog uredbe

Članak 20. – stavak 2.b (novi)

Tekst koji je predložila Komisija

Izmjena

(2.b) U opravdanim slučajevima i u dogovoru s CERT-EU-om predmetna institucija, tijelo ili agencija Unije može odstupiti od roka utvrđenog u stavku 2.a.

Amandman 71

Prijedlog uredbe Članak 20. – stavak 3.

Tekst koji je predložila Komisija

Izmjena

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

3. CERT-EU jedanput mjesečno dostavlja ENISA-i sažeto izvješće koje uključuje anonimizirane i zbirne podatke o ozbiljnim kiberprijetnjama, znatnim ranjivostima i ozbiljnim incidentima prijavljenima u skladu sa stavkom 1. **To izvješće predstavlja doprinos dvogodišnjem izvješću o stanju kibersigurnosti u Uniji u skladu s člankom 18. Direktive [prijedlog NIS 2].**

Amandman 72

Prijedlog uredbe Članak 20. – stavak 4.

Tekst koji je predložila Komisija

Izmjena

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

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

Amandman 73

**Prijedlog uredbe
Članak 20. – stavak 5.**

Tekst koji je predložila Komisija

Izmjena

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

Briše se.

Amandman 74

**Prijedlog uredbe
Članak 24. – stavak 2.**

Tekst koji je predložila Komisija

Izmjena

2. Komisija Europskom parlamentu i Vijeću podnosi izvješće o provedbi ove Uredbe najkasnije **48** mjeseci od stupanja na snagu ove Uredbe, a nakon toga svake **tri** godine.

2. Komisija Europskom parlamentu i Vijeću podnosi izvješće o provedbi ove Uredbe najkasnije **36** mjeseci od stupanja na snagu ove Uredbe, a nakon toga svake **dvije** godine.

Amandman 75

**Prijedlog uredbe
Članak 24. – stavak 3.**

Tekst koji je predložila Komisija

Izmjena

3. Komisija provodi evaluaciju ove Uredbe i podnosi izvješće Europskom parlamentu, Vijeću, Europskom gospodarskom i socijalnom odboru i Odboru regija najranije **pet godina** od stupanja na snagu ove Uredbe.

3. Komisija provodi evaluaciju ove Uredbe i podnosi izvješće Europskom parlamentu, Vijeću, Europskom gospodarskom i socijalnom odboru i Odboru regija najranije **tri godine** od stupanja na snagu ove Uredbe **s obzirom na brzi razvoj kiberprijetnji.**

Amandman 76

**Prijedlog uredbe
Prilog I. – stavak 1. – uvodni dio**

Tekst koji je predložila Komisija

Izmjena

Područja kojima se treba posvetiti u osnovnom okviru za kibersigurnost:

Barem sljedećim područjima se treba posvetiti u osnovnom okviru za kibersigurnost:

Amandman 77

Prijedlog uredbe

Prilog I. – stavak 1. – točka 1.a (nova)

Tekst koji je predložila Komisija

Izmjena

(1.a) osposobljavanje osoblja u području kibersigurnosti;

Amandman 78

Prijedlog uredbe

Prilog I.. – stavak 1. – točka 3.

Tekst koji je predložila Komisija

Izmjena

(3) upravljanje imovinom, uključujući popis **informatičke** imovine i kartografiju **informatičke** mreže;

(3) stjecanje i upravljanje imovinom, uključujući popis **informacijske i komunikacijske** imovine i kartografiju **informacijske i komunikacijske** mreže;

Amandman 79

Prijedlog uredbe

Prilog I. – stavak 1. – točka 7.

Tekst koji je predložila Komisija

Izmjena

(7) nabava, razvoj i održavanje sustava;

(7) nabava, razvoj i održavanje sustava, uključujući interni razvoj softvera otvorenog koda;

Amandman 80

Prijedlog uredbe

Prilog I. – stavak 1. – točka 7.a (nova)

Tekst koji je predložila Komisija

Izmjena

(7.a) revizije kibersigurnosti;

Amandman 81

Prijedlog uredbe

Prilog I. – stavak 1. – točka 9.

Tekst koji je predložila Komisija

Izmjena

(9) upravljanje incidentima, uključujući pristupe za poboljšanje pripravnosti, odgovora na incidente i oporavka od njih te suradnju s CERT-EU-om, primjerice održavanje nadzora nad sigurnošću i vođenje evidencije o njoj;

(9) upravljanje incidentima, uključujući pristupe za poboljšanje pripravnosti, odgovora na incidente i oporavka od njih, *poštovanje i skraćivanje rokova za obveze izvješćivanja* te suradnju s CERT-EU-om, primjerice održavanje nadzora nad sigurnošću i vođenje evidencije o njoj;

Amandman 82

Prijedlog uredbe

Prilog II. – stavak 1. – točka 3.a (nova)

Tekst koji je predložila Komisija

Izmjena

(3.a) redovitim osposobljavanjem osoblja u području kibersigurnosti;

Amandman 83

Prijedlog uredbe

Prilog II. – stavak 1. – točka 4. – podtočka a

Tekst koji je predložila Komisija

Izmjena

(a) uklanjanjem ugovornih prepreka koje pružateljima **informacičkih** usluga otežavaju razmjenu informacija o incidentima, ranjivostima i kiberprijetnjama s CERT-EU-om;

(a) uklanjanjem ugovornih prepreka koje pružateljima **informacijskih i komunikacijskih** usluga otežavaju razmjenu informacija o incidentima, ranjivostima i kiberprijetnjama s CERT-EU-om;

POSTUPAK U ODBORU KOJI DAJE MIŠLJENJE

Naslov	Uspostava mjera za visoku zajedničku razinu kibersigurnosti u institucijama, tijelima, uredima i agencijama Unije	
Referentni dokumenti	COM(2022)0122 – C9-0122/2022 – 2022/0085(COD)	
Nadležni odbor Datum objave na plenarnoj sjednici	ITRE 4.4.2022	
Odbori koji su dali mišljenje Datum objave na plenarnoj sjednici	AFCO 4.4.2022	
Izvjestitelj(ica) za mišljenje Datum imenovanja	Markéta Gregorová 20.6.2022	
Razmatranje u odboru	26.10.2022	1.12.2022
Datum usvajanja	25.1.2023	
Rezultat konačnog glasovanja	+: -: 0:	24 0 0
Zastupnici nazočni na konačnom glasovanju	Gerolf Annemans, Gabriele Bischoff, Damian Boeselager, Gwendoline Delbos-Corfield, Salvatore De Meo, Daniel Freund, Charles Goerens, Esteban González Pons, Laura Huhtasaari, Victor Negrescu, Max Orville, Domènec Ruiz Devesa, Helmut Scholz, Pedro Silva Pereira, Sven Simon, Guy Verhofstadt, Loránt Vincze, Rainer Wieland	
Zamjenici nazočni na konačnom glasovanju	Nathalie Colin-Oesterlé, Pascal Durand, Seán Kelly, Jaak Madison, Maite Pagazaurtundúa	
Zamjenici nazočni na konačnom glasovanju prema čl. 209. st. 7.	Leszek Miller	

POIMENIČNO KONAČNO GLASOVANJE U ODBORU KOJI DAJE MIŠLJENJE

24	+
ID	Gerolf Annemans, Laura Huhtasaari, Jaak Madison
PPE	Nathalie Colin-Oesterlé, Salvatore De Meo, Esteban González Pons, Seán Kelly, Sven Simon, Loránt Vincze, Rainer Wieland
Renew	Charles Goerens, Max Orville, Maite Pagazaurtundúa, Guy Verhofstadt
S&D	Gabriele Bischoff, Pascal Durand, Leszek Miller, Victor Negrescu, Domènec Ruiz Devesa, Pedro Silva Pereira
The Left	Helmut Scholz
Verts/ALE	Damian Boeselager, Gwendoline Delbos-Corfield, Daniel Freund

0	-

0	0

Objašnjenje korištenih znakova:

- + : za
- : protiv
- 0 : suzdržani

POSTUPAK U NADLEŽNOM ODBORU

Naslov	Uspostava mjera za visoku zajedničku razinu kibersigurnosti u institucijama, tijelima, uredima i agencijama Unije		
Referentni dokumenti	COM(2022)0122 – C9-0122/2022 – 2022/0085(COD)		
Datum podnošenja EP-u	22.3.2022		
Nadležni odbor Datum objave na plenarnoj sjednici	ITRE 4.4.2022		
Odbori koji daju mišljenje Datum objave na plenarnoj sjednici	BUDG 4.4.2022	LIBE 4.4.2022	AFCO 4.4.2022
Pridruženi odbori Datum objave na plenarnoj sjednici	LIBE 15.9.2022		
Izvjestitelji Datum imenovanja	Henna Virkkunen 18.5.2022		
Razmatranje u odboru	26.10.2022		
Datum usvajanja	9.3.2023		
Rezultat konačnog glasovanja	+: -: 0:	58 0 0	
Zastupnici nazočni na konačnom glasovanju	Nicola Beer, Hildegard Bentele, Tom Berendsen, Vasile Blaga, Michael Bloss, Marc Botenga, Martin Buschmann, Cristian-Silviu Bușoi, Jerzy Buzek, Ignazio Corrao, Beatrice Covassi, Ciarán Cuffe, Josianne Cutajar, Nicola Danti, Christian Ehler, Valter Flego, Niels Fuglsang, Lina Gálvez Muñoz, Claudia Gamon, Jens Geier, Nicolás González Casares, Bart Groothuis, Christophe Grudler, Henrike Hahn, Robert Hajšel, Ivo Hristov, Romana Jerković, Seán Kelly, Łukasz Kohut, Miapetra Kumpula-Natri, Marisa Matias, Dan Nica, Angelika Niebler, Ville Niinistö, Johan Nissinen, Mauri Pekkarinen, Tsvetelina Penkova, Morten Petersen, Manuela Ripa, Robert Roos, Maria Spyroki, Riho Terras, Grzegorz Tobiszowski, Patrizia Toia, Pernille Weiss		
Zamjenici nazočni na konačnom glasovanju	Andrus Ansip, Pascal Arimont, Izaskun Bilbao Barandica, Franc Bogović, Jakop G. Dalunde, Matthias Ecke, Cornelia Ernst, Jens Gieseke, Jutta Paulus, Marion Walsmann, Emma Wiesner		
Zamjenici nazočni na konačnom glasovanju prema čl. 209. st. 7.	Agnès Evren, Tilly Metz		
Datum podnošenja	10.3.2023		

POIMENIČNO KONAČNO GLASOVANJE U NADLEŽNOM ODBORU

58	+
ECR	Johan Nissinen, Robert Roos, Grzegorz Tobiszowski
NI	Martin Buschmann
PPE	Pascal Arimont, Hildegard Bentele, Tom Berendsen, Vasile Blaga, Franc Bogovič, Cristian-Silviu Bușoi, Jerzy Buzek, Christian Ehler, Agnès Evren, Jens Gieseke, Seán Kelly, Angelika Niebler, Maria Spyroki, Riho Terras, Marion Walsmann, Pernille Weiss
Renew	Andrus Ansip, Nicola Beer, Izaskun Bilbao Barandica, Nicola Danti, Valter Flego, Claudia Gamon, Bart Groothuis, Christophe Grudler, Mauri Pekkarinen, Morten Petersen, Emma Wiesner
S&D	Beatrice Covassi, Josianne Cutajar, Matthias Ecke, Niels Fuglsang, Lina Gálvez Muñoz, Jens Geier, Nicolás González Casares, Robert Hajšel, Ivo Hristov, Romana Jerković, Łukasz Kohut, Miapetra Kumpula-Natri, Dan Nica, Tsvetelina Penkova, Patrizia Toia
The Left	Marc Botenga, Cornelia Ernst, Marisa Matias
Verts/ALE	Michael Bloss, Ignazio Corrao, Ciarán Cuffe, Jakop G. Dalunde, Henrike Hahn, Tilly Metz, Ville Niinistö, Jutta Paulus, Manuela Ripa

0	-

Korišteni znakovi:

- + : za
- : protiv
- 0 : suzdržani