

Otkrivanje kibernetičkih incidenata i odgovor na njih

Ostvaruje se napredak u pogledu okvira EU-a za suradnju, ali zbog kašnjenja u provedbi i ograničene razmjene informacija taj je okvir samo djelomično djelotvoran



Sadržaj

Odlomak

01 – 23 | Glavne poruke

01 – 07 | Zašto je ovo područje važno

08 – 23 | Nalazi i preporuke Suda

24 – 01 | Detaljnije o opažanjima Suda

24 – 74 | Iako se mrežama i mehanizmima EU-a za kibernetičku sigurnost podupiru suradnja i pružanje odgovora, njihova je djelotvornost smanjena zbog ograničene razmjene informacija i nepotpune provedbe

24 – 51 | Mreže EU-a omogućuju suradnju država članica, ali njihova dodana vrijednost smanjena je zbog ograničene razmjene informacija

52 – 61 | Pričuva EU-a za kibernetičku sigurnost omogućuje brzu aktivaciju usluga odgovora na incidente

62 – 74 | Cilj je europskog sustava uzbunjivanja u području kibernetičke sigurnosti povećati kapacitete za otkrivanje prijetnji, ali on nije u funkciji

75 – 01 | Projektima financiranim iz programa Digitalna Europa nastoji se ojačati kibernetička sigurnost, ali u njima se pojavljuju izazovi u pogledu provedbe i izvješćivanja

75 – 81 | Zbog kašnjenja u uspostavi zajednice stručnjaka za kibernetičku sigurnost ta zajednica nije mogla prilagoditi program Digitalna Europa svojim potrebama

82 – 96 | Projektima financiranim sredstvima EU-a nastoje se ostvariti relevantni ciljevi, ali u mnogima od njih pojavljuju se operativni problemi

97 – 01 | Za većinu projekata financiranih sredstvima EU-a nisu utvrđeni odgovarajući okviri uspješnosti, a podatci o uspješnosti u području kibernetičke sigurnosti u sklopu programa Digitalna Europa nisu točni

Prilozi

Prilog I. – O reviziji

Prilog II. – Akteri uključeni u kibernetičku sigurnost u EU-u

Prilog III. – Odabrane mjere u području kibernetičke sigurnosti

Prilog IV. – Procjena projekata u području kibernetičke sigurnosti financiranih sredstvima EU-a koju je proveo Sud

Pokrate i skraćeni nazivi

Pojmovnik

Odgovori Komisije

Odgovori Europskog stručnog centra za industriju, tehnologiju i istraživanja u području kibersigurnosti (ECCC)

Odgovori Agencije Europske unije za kibersigurnost (ENISA)

Kronologija

Revizorski tim

01

Glavne poruke

Zašto je ovo područje važno

- 01** Sve veća digitalizacija našeg gospodarstva i svakodnevnice sa sobom nosi veći rizik od kibernetičkih napada. Kibernetička sigurnost definira se kao „aktivnosti koje su nužne za zaštitu od kiberprijetnji mrežnih i informacijskih sustava, korisnika tih sustava i drugih osoba na koje one utječu”¹. Za kibernetičku sigurnost potrebno je primijeniti holistički pristup s ciljem sprečavanja i otkrivanja kibernetičkih prijetnji te odgovor na takve prijetnje i oporavak od njih.
- 02** U područje kibernetičke sigurnosti u EU-u uključeni su brojni javni i privatni subjekti u civilnoj sferi na regionalnoj i nacionalnoj razini te na razini EU-a. Kibernetička sigurnost ujedno je jedan od ključnih elemenata nacionalne sigurnosti i obrane.
- 03** Države članice snose glavnu odgovornost za sprečavanje kibernetičkih incidenata i kriza, pripremu za njih i odgovor na krize i incidente koji ih pogađaju. Budući da takvi incidenti mogu utjecati na neometano funkcioniranje unutarnjeg tržišta, EU također ima važnu ulogu u slučaju značajnog incidenta ili krize. EU je posljednjih godina ojačao svoj regulatorni okvir za kibernetičku sigurnost koji se kontinuirano dorađuje² te je uspostavio mreže i mehanizme, kao što je prikazano na [slici 1.](#) u nastavku i u [Prilogu II.](#)

¹ Uredba (EU) 2019/881 ([Akt o kibernetičkoj sigurnosti](#)).

² Na primjer, u studenome 2025. Komisija je predložila [Digitalni omnibus](#), a u siječnju 2026. izmijenjeni [Akt EU-a o kibernetičkoj sigurnosti](#).

Slika 1. | Mreže i mehanizmi EU-a za kibernetičku sigurnost u razdoblju 2016. – 2025.



CSIRT-ovi: timovi za odgovor na računalne sigurnosne incidente

GU Connect: Glavna uprava za komunikacijske mreže, sadržaje i tehnologije

EU-CyCLONe: Europska mreža organizacija za vezu za kibernetičke krize

Direktiva NIS: Direktiva (EU) 2016/1148 o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije

Direktiva NIS 2: Direktiva (EU) 2022/2555 o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije

Izvor: Sud.

- 04** U tekucem višegodišnjem financijskom okviru za razdoblje 2021. – 2027. glavni je izvor financijskih sredstava za kibernetičku sigurnost [program Digitalna Europa \(DIGITAL\)](#). Ukupni proračun tog programa iznosi 8,1 milijardu eura, od čega je za jačanje kibernetičke sigurnosti dodijeljen iznos od 1,4 milijarde eura.

- 05** Cilj ove revizije bio je procijeniti olakšava li se mjerama EU-a na djelotvoran način otkrivanje značajnih kibernetičkih incidenata i kibernetičkih incidenata velikih razmjera i odgovor na njih. Sud je procijenio je li to vrijedilo za sljedeće:
- mreže i mehanizme na razini EU-a (tj. mrežu timova za odgovor na računalne sigurnosne incidente (mreža CSIRT-ova), Europsku mrežu organizacija za vezu za kibernetičke krize (mreža EU-CyCLONe), europski sustav uzbunjivanja u području kibernetičke sigurnosti, centar za situaciju u kibernetičkom prostoru i pričuvu EU-a za kibernetičku sigurnost);
 - mjere financirane iz programa Digitalna Europa.
- 06** Sud očekuje da će njegovi nalazi doprinijeti jačanju kibernetičke otpornosti EU-a povećanjem djelotvornosti i učinkovitosti mreža i mehanizama EU-a, kao i poboljšanjem načina na koji se odabiru i prate mjere financirane sredstvima EU-a.
- 07** Revizijom je obuhvaćeno razdoblje 2022. – 2025. i ona se temelji na pregledu dokumentacije i analizi relevantnih dokumenata, revizijskim posjetima trima državama članicama (Irskoj, Grčkoj i Italiji) te pisanim upitnicima i razgovorima s dionicima. Dodatne informacije te pojedinosti o opsegu revizije i revizijskom pristupu navedene su u [Prilogu I.](#)

Nalazi i preporuke Suda

- 08** Sud općenito zaključuje da se mjerama EU-a samo djelomično olakšava otkrivanje značajnih kibernetičkih incidenata i kibernetičkih incidenata velikih razmjera te odgovor na njih. Iako se okvir za suradnju postupno uspostavlja, rad na njegovu potpunom dovršetku i dalje je u tijeku. Zbog ograničene razmjene informacija, nedostataka u izvješćivanju i znatnih kašnjenja u provedbi nije moguće iskoristiti puni potencijal mreža i mehanizama EU-a. Projektima financiranim iz programa Digitalna Europa nastoje se ostvariti relevantni ciljevi, ali u nizu njih pojavljuju se operativni izazovi i kašnjenja te postoje nedostaci u općem okviru za praćenje uspješnosti.
- 09** Trenutačni okvir mreža i mehanizama EU-a za olakšavanje otkrivanja značajnih kibernetičkih incidenata i odgovor na njih uspostavljen je postupno. Vijeće je 2025. donijelo [Plan za kibernetičku sigurnost](#), kojim je utvrđen okvir EU-a za upravljanje kibernetičkim krizama. Sud je utvrdio da se tim planom u velikoj mjeri pojašnjavaju uloge i odgovornosti u pogledu upravljanja kibernetičkim krizama u EU-u. Neovisno o tomu, tek treba formalizirati proceduralne mehanizme u pogledu načina suradnje mreže CSIRT-ova (koja je uspostavljena 2016.) i mreže EU-CyCLONe (čija je uloga formalizirana 2023.) (odlomci [24](#) – [30](#)).

- 10** Sud je utvrdio da se informacije preko tih mreža razmjenjuju u ograničenoj mjeri. Razlog za to ponajprije leži u kašnjenjima u prenošenju [Direktive o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije](#) (Direktiva NIS 2) u nacionalno pravo, poteškoćama u utvrđivanju toga ima li određeni incident prekogranični učinak i nacionalnom zakonodavstvu o sigurnosti kojim se sprečava razmjena informacija. Dodana vrijednost tih mreža znatno se smanjuje ako države članice nisu spremne razmjenjivati pravodobne i upotrebljive informacije (odlomci [31 – 44](#)).



Preporuka 1.

Potrebno je ojačati razmjenu informacija među državama članicama

Kako bi se poboljšali otkrivanje kibernetičkih incidenata i odgovor na njih, Komisija bi, uz potporu Agencije Europske unije za kibersigurnost (ENISA), trebala učiniti sljedeće:

- (a) predložiti skupini za suradnju u području mrežne i informacijske sigurnosti da provede detaljnu analizu nacionalnih sigurnosnih ograničenja kojima se ograničava razmjena informacija i koja utječu na kibernetičku otpornost EU-a te da pronađe pravna i tehnička rješenja za povećanje razmjene informacije uz istodobno poštovanje granica nacionalne sigurnosti;
- (b) ne dovodeći u pitanje odluke suzakonodavaca, u suradnji s državama članicama zajamčiti da se jedinstvenom ulaznom točkom za prijavljivanje incidenata koja je predložena u Digitalnom omnibusu mogu otkrivati potencijalni prekogranični incidenti;
- (c) raditi na pronalasku rješenja kojima se omogućuje prijavljivanje incidenata ENISA-i u stvarnom vremenu.

Ciljni rok provedbe: 2027. za točke (a) i (b) te 2028. za točku (c)

- 11** Komisija je 2022. uspostavila interni „centar za situaciju u kibernetičkom prostoru” radi povećanja svoje informiranosti o stanju u tom području kako bi dobivala podršku u ispunjavanju svojih institucijskih odgovornosti u pogledu upravljanja krizama. Funkcioniranje tog centra u velikoj se mjeri temelji na ugovoru sklopljenom s vanjskim pružateljima usluga. Sud je utvrdio da se aktivnosti koje obavljaju vanjski pružatelji usluga dijelom preklapaju s već postojećim funkcijama Agencije Europske unije za kibersigurnost (ENISA) u području informiranosti o stanju i praćenja prijetnji. Sud smatra da se načinom na koji je taj centar uspostavljen nije u dovoljnoj mjeri iskoristio potencijal za racionalizaciju upotrebom već dostupnih informacija Komisije i ENISA-e. Nadalje, zbog nepostojanja sveobuhvatnog i detaljnog plana za budućnost nakon isteka ugovora stvara se rizik za rad centra za situaciju u kibernetičkom prostoru nakon 2026. (odlomci [45 – 51](#)).



Preporuka 2.

Potrebno je racionalizirati kapacitete EU-a za informiranost o stanju u području kibernetičke sigurnosti i optimizirati diseminaciju informacija

Radi povećanja učinkovitosti Komisija bi u suradnji s ENISA-om trebala procijeniti izvedivost zajedničkog prikupljanja i analize informacija za informiranost o stanju. Predmetne informacije i povezana izvješća o kibernetičkim prijetnjama ujedno bi trebala staviti na raspolaganje svim relevantnim službama i agencijama EU-a.

Ciljni rok provedbe: 2027.

- 12** **Aktom o kibernetičkoj solidarnosti** iz 2024. uspostavljena je pričuva EU-a za kibernetičku sigurnost, i to s ciljem pružanja potpore državama članicama u odgovoru na velike kibernetičke incidente i oporavku od njih. Pričuva obuhvaća odabrane pružatelje usluga za svaku državu članicu, koji mogu odgovoriti na incidente 24 sata dnevno. Iako se tim pristupom pomaže u ispunjavanju specifičnih zahtjeva država članica i izgradnji povjerenja, raspoloživi proračun raspodijeljen je ravnomjerno među državama članicama i njime se ne uzimaju u obzir posebne potrebe svake države članice (odlomci [52](#) – [57](#)).
- 13** Sud smatra da se dostupnošću pružatelja usluga s kojima su unaprijed sklopljeni ugovori omogućuje brza aktivacija usluga odgovora na incidente. Iako je cilj pričuve EU-a za kibernetičku sigurnost prije svega pružiti potporu odgovoru i oporavku, ako se ne upotrijebi za odgovor na incidente, može se upotrijebiti za pripravnost. Takvim fleksibilnim pristupom može se spriječiti neiskorištavanje unaprijed plaćenih usluga. Međutim, ta se pričuva uglavnom upotrebljava za pripravnost, a ne za odgovor, suprotno njezinoj predviđenoj svrsi (odlomci [58](#) – [61](#)).
- 14** Europski sustav uzbunjivanja u području kibernetičke sigurnosti mreža je nacionalnih i prekograničnih kibernetičkih centara čiji je cilj poboljšati otkrivanje i analizu kibernetičkih prijetnji te odgovor na njih. Sud je utvrdio da u vrijeme obavljanja revizije zbog znatnih kašnjenja u javnoj nabavi alata i usluga postojeća dva centra (ATHENA i ENSOC) još nisu bila počela s radom te da europski sustav uzbunjivanja u području kibernetičke sigurnosti još nije funkcionirao (odlomci [62](#) – [70](#)).

- 15** Jedan je od ključnih ciljeva europskog sustava uzbunjivanja u području kibernetičke sigurnosti poticati korisnu razmjenu informacija među klasterima država članica. Iako se time mogu riješiti neki od problema povezanih s razmjenom informacija, integracija prekograničnih centara u već složeno okruženje u području kibernetičke sigurnosti ujedno je vrlo zahtjevan zadatak. Sud je utvrdio da još nisu postojali potrebni sporazumi o suradnji, zajednička taksonomija i standardi interoperabilnosti potrebni za potpuno funkcioniranje europskog sustava uzbunjivanja u području kibernetičke sigurnosti (odlomci [71](#) – [74](#)).



Preporuka 3.

Potrebno je integrirati europski sustav uzbunjivanja u području kibernetičke sigurnosti u okruženje EU-a u tom području

Komisija bi u suradnji s ENISA-om i državama članicama trebala zajamčiti da postoje mehanizmi za suradnju i standardi interoperabilnosti kako bi se olakšala razmjena informacija među prekograničnim centrima koji su dio europskog sustava uzbunjivanja u području kibernetičke sigurnosti, mreže CSIRT-ova i mreže EU-CyCLONe.

Ciljni rok provedbe: 2028.

- 16** Komisija je 2018. predložila uspostavu Europskog stručnog centra za industriju, tehnologiju i istraživanja u području kibersigurnosti (Europski stručni centar u području kibernetičke sigurnosti ili ECCC) radi upravljanja komponentom kibernetičke sigurnosti u sklopu programa Digitalna Europa od 2021. U [Uredbi o ECCC-u](#) pozvalo se na uspostavu zajednice stručnjaka za kibernetičku sigurnost sastavljene od predstavnika relevantnih sektora, akademske zajednice i istraživačkih organizacija. Odabrani članovi iz te zajednice činili bi stratešku savjetodavnu skupinu (odlomci [75](#) i [76](#)).
- 17** Sud je utvrdio da je došlo do kašnjenja u postizanju financijske neovisnosti ECCC-a, kao i u uspostavi zajednice stručnjaka za kibernetičku sigurnosti i strateške savjetodavne skupine. Zbog toga predmetna zajednica i skupina nisu mogle pružiti svoj doprinos oblikovanju programa rada u sklopu programa Digitalna Europa. Sud smatra da je riječ o propuštenoj prilici (odlomci [77](#) – [81](#)).
- 18** Sud je za sve projekte koje je ispitao utvrdio da se njima nastoje ostvariti relevantni ciljevi kojima se doprinosi postizanju ciljeva programa Digitalna Europa u vezi s kibernetičkom sigurnošću. Međutim, utvrdio je slučajeve u kojima kvaliteta ili postignuti rezultati nisu bili zadovoljavajući, uglavnom zbog kašnjenja u provedbi (odlomci [82](#) – [87](#)).

- 19** Uredbom o programu Digitalna Europa predviđeno je da se zbog sigurnosnih razloga pružanje financijskih sredstava za kibernetičku sigurnost može ograničiti na subjekte koji imaju poslovni nastan u državama članicama i koji su pod kontrolom država članica ili državljana država članica. Središnja služba za potvrde u sklopu [Europske izvršne agencije za istraživanje](#) provodi tu procjenu vlasničke i kontrolne strukture u ime ECCC-a (odlomci [88](#) – [91](#)).
- 20** U slučaju pružanja financijske potpore trećim stranama odgovornost za provedbu procjene vlasničke i kontrolne strukture snose korisnici potpore u sklopu projekata, i to na temelju vlastitog pristupa i metodologije. Sud je utvrdio da ECCC ne potvrđuje njihovu metodologiju i ne obavlja provjere kojima bi se zajamčilo da su odabrane treće strane u vlasništvu i pod kontrolom subjekata iz EU-a. Sud smatra da postoji znatan rizik od toga da korisnici ne raspolažu kapacitetima za odgovarajuću provedbu tih procjena. Predmetni rizik nije odgovarajuće ublažen i mogao bi dovesti do ugrožavanja osjetljive infrastrukture, operativnih podataka i tehnologija ključnih za sigurnost (odlomci [92](#) – [96](#)).



Preporuka 4.

Potrebno je zajamčiti pouzdanu procjenu vlasničke i kontrolne strukture subjekata koji primaju financijska sredstva EU-a iz programa Digitalna Europa

Europski stručni centar u području kibernetičke sigurnosti trebao bi:

- (a) dobiti razumno jamstvo da korisnici odgovorni za pružanje financijske potpore trećim stranama raspolažu administrativnim i tehničkim kapacitetima potrebnim za obavljanje odgovarajućih procjena vlasničke i kontrolne strukture na temelju postojeće metodologije dostupne korisnicima koji pružaju financijsku potporu trećim stranama; i
- (b) na temelju uzorka provjeriti jesu li financijska sredstva EU-a primili isključivo prihvatljivi subjekti.

Ciljni rok provedbe: 2026. za točku (a) i 2027. za točku (b)

- 21** Korisnici koji upravljaju projektima financiranim sredstvima EU-a moraju izvješćivati ECCC o svojem napretku i rezultatima na temelju ključnih etapa i postignuća. Ključne etape i postignuća imaju ključnu ulogu u praćenju projekata te ih je potrebno pravilno utvrditi. Sud je utvrdio da se gotovo ni u jednom projektu iz njegova uzorka nisu primjenjivale upute za utvrđivanje ključnih etapa i postignuća te da mnoge ključne etape i postignuća nisu bili korisni za praćenje napretka (odlomci [97 – 99](#)).
- 22** Sud je utvrdio da mnogi pokazatelji uspješnosti koje su korisnici upotrebljavali nisu relevantni ni mjerljivi te da za njih nisu utvrđene ciljne i polazne vrijednosti. Nadalje, izvješćivanje o tim pokazateljima nije bilo odgovarajuće te stoga ne može poslužiti kao osnova za procjenu uspješnosti projekata (odlomci [100 – 102](#)).
- 23** Kako bi se pratilo ono što je postignuto programom Digitalna Europa u cjelini, za sve projekte potrebno je izvješćivati o specifičnim programskim pokazateljima koji se upotrebljavaju pri izradi Komisijinih godišnjih [izvješća o uspješnosti programa](#). ECCC je odgovoran za prikupljanje i provjeru podataka dostavljenih u vezi s tim pokazateljima. Sud je utvrdio niz problema u načinu na koji se podatci prikupljaju i u njihovoj ukupnoj kvaliteti. Nije pronašao dokaze koji bi potvrdili da je ECCC provjerio točnost dostavljenih podataka. Sud na temelju provjera obavljenih na svojem uzorku smatra da dostavljani podatci ne pružaju točan odraz postignutih rezultata (odlomci [103 – 106](#)).



Preporuka 5.

Potrebno je ojačati okvir za praćenje uspješnosti komponente kibernetičke sigurnosti u sklopu programa Digitalna Europa

Kako bi se omogućilo odgovarajuće praćenje napretka i uspješnosti, Europski stručni centar u području kibernetičke sigurnosti trebao bi:

- (a) prije sklapanja ugovora o dodjeli bespovratnih sredstava zajamčiti da su za sve projekte utvrđene ključne etape, postignuća i pokazatelji uspješnosti koji su u skladu s uputama navedenim u obrascu zahtjeva za bespovratna sredstva;
- (b) osmisлити i primijeniti pouzdan sustav za prikupljanje, sljedivost, provjeru i objedinjavanje podataka za pokazatelje uspješnosti komponente kibernetičke sigurnosti u sklopu programa Digitalna Europa kako bi se zajamčilo da se u pokazateljima točno odražavaju postignuti rezultati.

Ciljni rok provedbe: 2027.

Detaljnije o opažanjima Suda

Iako se mrežama i mehanizmima EU-a za kibernetičku sigurnost podupiru suradnja i pružanje odgovora, njihova je djelotvornost smanjena zbog ograničene razmjene informacija i nepotpune provedbe

Mreže EU-a omogućuju suradnju država članica, ali njihova dodana vrijednost smanjena je zbog ograničene razmjene informacija

- 24** Trenutačni okvir mreža i mehanizama na razini EU-a za olakšavanje otkrivanja značajnih kibernetičkih incidenata i odgovor na njih uspostavljen je postupno, počevši s [Direktivom o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije](#)³ (Direktiva NIS), koja je stupila na snagu u kolovozu 2016. Akteri koji su trenutačno uključeni u kibernetičku sigurnost u EU-u prikazani su u [Prilogu II.](#)

³ Direktiva (EU) 2016/1148.

Mreže EU-a omogućuju suradnju država članica na tehničkoj i operativnoj razini

- 25** Direktivom NIS uspostavljena je mreža CSIRT-ova koja okuplja službu CERT-EU (Služba za kibernetičku sigurnost institucija, tijela, ureda i agencija Unije) i CSIRT-ove koje su imenovala države članice. Cilj je te mreže izgraditi povjerenje i pouzdanje među nacionalnim CSIRT-ovima te promicati brzu i djelotvornu operativnu suradnju među državama članicama.
- 26** Mreža EU-CyCLONe uspostavljena je 2020. kao neslužbena mreža za suradnju nacionalnih tijela zaduženih za upravljanje kibernetičkim krizama. Ima ulogu poveznice između tehničke razine na kojoj djeluje mreža CSIRT-ova i političke razine Vijeća Europske unije i njegovih aranžmana za integrirani politički odgovor na krizu. Stupanjem na snagu Direktive NIS 2 2023. formalizirana je uloga mreže EU-CyCLONe te su joj povjerene jasne ovlasti.
- 27** Sud je procijenio jesu li uloge i odgovornosti tih mreža na razini EU-a dobro definirane i omogućuju li one suradnju država članica.
- 28** ENISA djeluje kao tajništvo mreže CSIRT-ova i mreže EU-CyCLONe te im stavlja na raspolaganje resurse, stručno znanje, infrastrukturu i IT alate potrebne za suradnju i sigurnu komunikaciju za razmjenu informacija. U anketi o zadovoljstvu dionika⁴ provedenoj početkom 2025. ENISA je dobila dobre ocjene za svoju uspješnost u ulozi tajništva tih mreža. Te pozitivne povratne informacije potvrđene su i tijekom revizijskih posjeta koje je Sud obavio, tijekom kojih su nacionalna tijela za kibernetičku sigurnost navela da cijene njezin rad.
- 29** Vijeće je 2025. donijelo Plan za kibernetičku sigurnost, u kojem su utvrđene uloge i odgovornosti ključnih aktera (uključujući mrežu CSIRT-ova i mrežu EU-CyCLONe) i mehanizmi uključeni tijekom kibernetičkih incidenata ili kriza velikih razmjera. Sud je utvrdio da se tim planom u velikoj mjeri pojašnjavaju uloge i odgovornosti u pogledu upravljanja kibernetičkim krizama u EU-u i da se u njemu uzimaju u obzir promjene u predmetnom okružju od donošenja prvog plana 2017. Njime su utvrđene tri razine suradnje: tehnička, operativna i politička. U tom se planu navode pojedinosti o novim mrežama i strukturama uspostavljenim od 2017., kao što su mreža EU-CyCLONe, timovi EU-a za brz odgovor na hibridne prijetnje i europski sustav uzbunjivanja u području kibernetičke sigurnosti, te se opisuje način na koji bi se upravljanje kibernetičkim krizama trebalo integrirati u širi okvir EU-a za odgovor na krize.

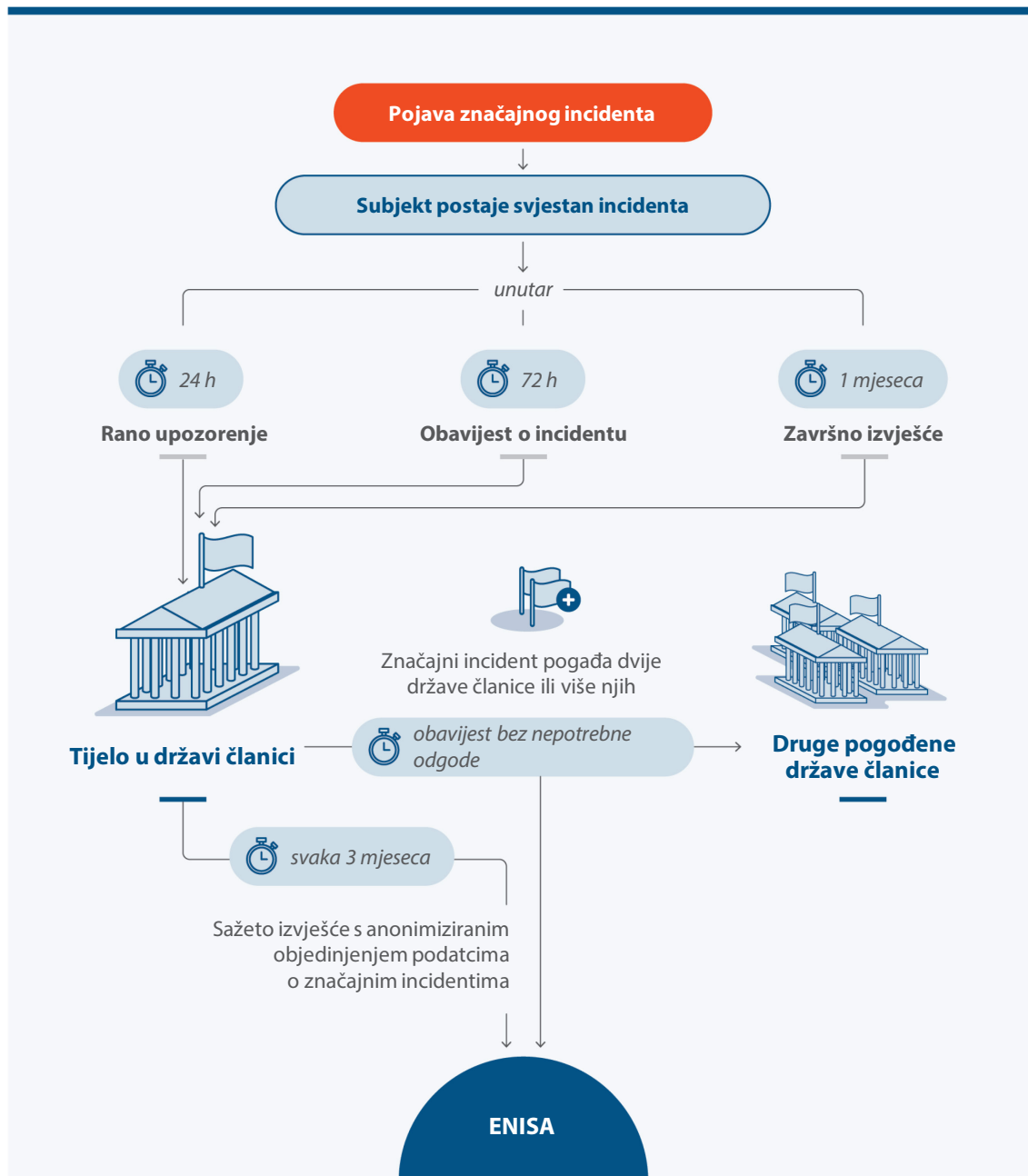
⁴ ENISA, konsolidirano godišnje izvješće o radu za 2024., str. 33. i 36.

- 30** Međutim, iako je mreža CSIRT-ova službeno uspostavljena 2016., a mreža EU-CyCLONe 2023., te dvije mreže tek trebaju formalizirati proceduralne mehanizme za međusobnu suradnju. Isto tako, još nisu dogovorile kriterije na temelju kojih bi mreža CSIRT-ova trebala obavještavati mrežu EU-CyCLONe o tome da uočeni kibernetički incident čini potencijalan ili aktualan kibernetički incident velikih razmjera. Predmetne dvije mreže moraju dogovoriti i zajedničku taksonomiju za razine ozbiljnosti i ključne koncepte – kao što su „prijetnja”, „akter prijetnje”, „incident” ili „učinak” – što je nužno za omogućavanje automatizirane razmjene informacija. Trenutačno ima prostora za slobodno tumačenje toga kad se određeni incident može smatrati značajnim incidentom ili incidentom velikih razmjera. U svim trima državama članicama koje je Sud posjetio tijela za kibernetičku sigurnost spomenula su nepostojanje zajedničke taksonomije.

Zbog ograničene razmjene informacija i nedostatnog izvješćivanja znatno se smanjuje dodana vrijednost uspostavljenih mreža

- 31** Geografske granice ne sprečavaju pojavu i širenje kibernetičkih incidenata i kibernetičkih napada. Razmjena informacija među državama članicama o, na primjer, taktikama i tehnikama koje upotrebljavaju akteri prijetnji te o digitalnim znakovima prodora u određenu mrežu ili informacijski sustav („pokazatelji ugroženosti”) mogu znatno doprinijeti povećanju kibernetičke sigurnosti.
- 32** Sud je utvrdio da su se informacije razmjenjivale u ograničenoj mjeri, zbog čega je znatno smanjenja dodana vrijednost uspostavljenih mreža. Ograničenja koja je Sud utvrdio uglavnom se odnose na kašnjenja u prenošenju Direktive NIS 2 u nacionalno pravo, probleme s utvrđivanjem toga ima li određeni incident prekogranični učinak, nacionalno zakonodavstvo o sigurnosti kojim se ograničava razmjena informacija i nedostatak povjerenja. Direktivom NIS 2 uveden je niz zahtjeva u pogledu izvješćivanja za subjekte obuhvaćene njezinim područjem primjene i za tijela u državama članicama, kako je prikazano na [slici 2](#).

Slika 2. | Vremenski okvir za izvješćivanje o incidentima u skladu s Direktivom o mjerama za visoku zajedničku razinu kibernetičke sigurnosti širom EU-a (Direktiva NIS 2)



Izvor: Sud, na temelju podataka ENISA-e.

- 33** Države članice morale su [prenijeti Direktivu NIS 2](#) u nacionalno pravo do listopada 2024., ali samo su je dvije države članice prenijele u tom roku. Kašnjenja u prenošenju znatno utječu na razmjenu informacija jer subjekti obuhvaćeni Direktivom NIS 2 u međuvremenu nisu zakonski obvezni prijavljivati incidente. Komisija je procijenila⁵ da je Direktivom NIS bilo obuhvaćeno 15 500 subjekata, dok je područjem primjene Direktive NIS 2 obuhvaćeno više od 110 000 subjekata. Na primjer, sektor javne uprave – koji je prema [izvješću ENISA-e o prijetnjama](#) iz 2025. najčešća meta – nije bio obvezan prijavljivati incidente u skladu s Direktivom NIS.
- 34** Izvješćivanjem ENISA-e o podacima o incidentima svaka tri mjeseca (tj. dugo nakon što već dođe do određenog incidenta) ograničava se njegova dodana vrijednost. Ti podatci uglavnom služe u statističke svrhe i za izvješćivanje o povijesnim trendovima, a ne za poboljšanje otkrivanja i odgovora. ENISA državama članicama stavlja na raspolaganje [internetski alat](#) za podnošenje izvješća. Obrazac za izvješćivanje sadržava minimalni skup podataka koje je potrebno dostaviti, kao što su vrsta incidenta i pogođeni sektor. Osim toga, ENISA predlaže da države članice pruže dodatne informacije kako bi se omogućila detaljnija analiza podataka, na primjer povezivanjem incidenata s određenim slabim točkama. Međutim, te informacije ne pružaju sve države članice, čime se znatno smanjuje kvaliteta i dodana vrijednost prikupljenih podataka.
- 35** ENISA je u svojem [izvješću iz 2024. o stanju u području kibernetičke sigurnosti u EU-u](#) navela da se vjerojatno prijavljuje manji broj incidenata od stvarnog jer se broj prijavljenih incidenata čini niskim. U razdoblju 2018. – 2021. države članice prijavljivale su ENISA-i godišnje između 100 i 500 incidenata. Broj incidenata postupno se povećavao te je 2024. dosegnuo 1276⁶.

⁵ Europska komisija, [izvješće o procjeni učinka](#) iz 2020.

⁶ Podatci za 2024. iz sustava [CIRAS](#).

- 36** U svojem [izvješću o prijetnjama](#) iz 2025., kojim je obuhvaćeno razdoblje od lipnja 2024. do lipnja 2025., ENISA je na temelju obavještajnih podataka otvorenog koda, kao što su novinski članci, utvrdila da je zabilježeno približno 4800 kibernetičkih incidenata⁷. Pritom nije u svakom slučaju bilo riječ o incidentu koji bi bilo potrebno prijaviti u skladu s Direktivom NIS 2 jer ENISA pri prikupljanju podataka obuhvaća širi spektar incidenata. S druge strane, o mnogim se značajnim incidentima ne izvješćuje u obavještajnim podacima otvorenog koda. Budući da su podatci koje države članice dostavljaju anonimizirani, ENISA ne može povezati incidente koje utvrdi s incidentima koje su prijavile države članice. Stoga nije moguće točno utvrditi u kojoj je mjeri broj prijavljenih incidenata manji od stvarnog, ali Sud smatra da razlika između broja incidenata koje su prijavile države članice i broja incidenata u izvješću o prijetnjama pokazuje da nisu prijavljeni svi značajni incidenti.
- 37** Još je jedan pokazatelj da se prijavljuje manji broj incidenata od stvarnog broj obavijesti o značajnim prekograničnim incidentima poslan drugim pogođenim državama članicama i ENISA-i. Sličan zahtjev postojao je u Direktivi NIS, ali smatrao se nedjelotvornim jer je Komisija 2020. zaključila⁸ da se obavijesti rijetko šalju unatoč obvezi njihova slanja. Izostanak obavješćivanja pripisala je činjenici da nije jasno navedeno na koji bi se način informacije trebale dijeliti i nepostojanju zajedničkih ciljeva kojima bi se poticala razmjena.
- 38** Obveza obavješćivanja drugih država članica ključna je za izbjegavanje učinka „prelijevanja” incidenata i neobavješćivanje negativno utječe na kibernetičku sigurnost EU-a. Tijekom 2025. prijavljeno je samo 14 značajnih prekograničnih incidenata, a prijavilo ih je sedam država članica. Države članice podnijele su dva izvješća o incidentima 2024., nijedno 2023. i tri 2022. s mogućim prekograničnim učinkom. To pokazuje da se prijavljuje vrlo malen broj značajnih prekograničnih incidenata i da se u povezanim podacima ne odražava stvarni razmjer takvih napada. Za usporedbu, ENISA je u svojem [izvješću o prijetnjama iz 2024.](#) utvrdila 322 incidenta koji su posebno bili usmjereni na dvije države članice ili više njih. Incident koji je pogodio poduzeće Collins Aerospace (vidjeti [okvir 1.](#)) primjer je slučaja u kojem države članice nisu prijavile incident unatoč njegovu značajnom prekograničnom učinku.

⁷ ENISA, [izvješće o prijetnjama iz 2025.](#)

⁸ Europska komisija, [izvješće o procjeni učinka iz 2020.](#)

Okvir 1.

Kibernetički incident koji je poremetio rad zračnih luka

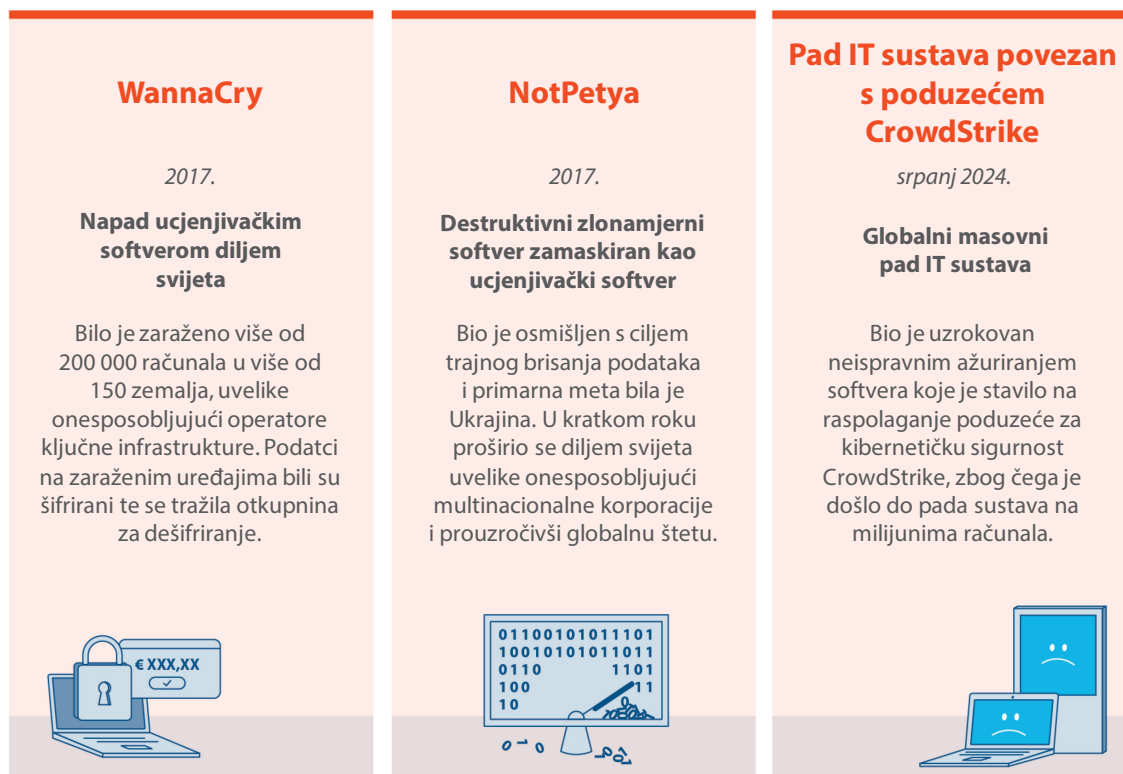
U rujnu 2025. poduzeće Collins Aerospace, veliki pružatelj tehnoloških rješenja u zrakoplovnoj industriji, pretrpjelo je značajan napad ucjenjivačkim softverom čiji je cilj bio njegov softver za obradu podataka o putnicima. Taj je napad prisilio velike europske zračne luke da se vrate ručnoj obradi, zbog čega je došlo do znatnih kašnjenja i otkazivanja letova. Poremećaji su bili najveći u zračnoj luci London Heathrow, zračnoj luci Bruxelles, zračnoj luci Berlin Brandenburg i zračnoj luci Dublin.

U skladu s Direktivom NIS 2 incident se smatra „značajnim” ako, među ostalim, uzrokuje ozbiljne poremećaje u funkcioniranju usluga ili financijske gubitke za predmetni subjekt. Unatoč tomu, nijedna država članica nije postupila s tim incidentom kao sa značajnim incidentom ili prekograničnim incidentom velikih razmjera. Stoga nijedna od pogođenih država članica nije službeno obavijestila ENISA-u ili druge države članice o tom incidentu. Mreža CSIRT-ova nije obavijestila mrežu EU-CyCLONE, koja zbog toga nije pružila podršku koordiniranom upravljanju incidentom.

Izvor: analiza koju je proveo Sud na temelju razgovora s osobljem ENISA-e.

- 39** Još je jedan razlog za ograničeno prijavljivanje prekograničnih incidenata taj što tijela u državama članicama imaju slobodu u odlučivanju o tome ima li prijavljeni incident prekogranični učinak i utvrđivanju drugih pogođenih država članica. Subjekt zadužen za prijavljivanje ili relevantno tijelo u državi članici možda neće biti svjesno prekogranične prirode određenih napada na temelju dostupnih informacija. Trenutačno ne postoji platforma na razini EU-a u sklopu koje bi se primala izvješća o incidentima u stvarnom vremenu od svih država članica i koja bi mogla povezivati informacije o sektorima ili pokazateljima ugroženosti kako bi se otkrili prekogranični incidenti. Stoga postoji znatan rizik od toga da se određeni prekogranični incidenti ne utvrde i ne prijave.
- 40** Od 2016. nijedna država članica nije smatrala određeni kibernetički incident „incidentom velikih razmjera”. U načelu, definicijom takvih incidenata obuhvaćen je svaki incident koji značajno utječe na najmanje dvije države članice. Međutim, čak ni kibernetički incidenti koji su uzrokovali globalne prekide rada i znatnu štetu, kao što su oni prikazani na [slici 3.](#), nisu se smatrali incidentima velikih razmjera. Slijedom toga, eskalacijski postupak mreže EU-CyCLONE nije nijednom aktiviran u potpunosti zbog kibernetičkog incidenta velikih razmjera.

Slika 3. | Primjeri velikih kibernetičkih incidenata



Izvor: Sud, prilagođeno na temelju podataka društva [Cloudflare](#), [ENISA-e](#) i [Europola](#), internetskih stranica časopisa [Wired](#) te podataka poduzeća [IBM](#) i [CrowdStrike](#).

- 41** Uz primjenu obveze izvješćivanja na relevantne subjekte i na države članice, uspostavljena je mreža CSIRT-ova kako bi se olakšala razmjena informacija. Rad te mreže zasniva se na povjerenju među državama članica te se u okviru nje informacije razmjenjuju na dobrovoljnoj osnovi. Njezina dodana vrijednost znatno se smanjuje ako države članice nisu spremne razmjenjivati pravodobne i upotrebljive informacije.
- 42** Razmjena informacija na razini EU-a ograničena je nacionalnim zakonodavstvom o sigurnosti u svakoj državi članici. Ako država članica smatra da su informacije o određenom ključnom subjektu povezane s kibernetičkim napadom klasificirane ili da bi izvješćivanje o određenom incidentu štetilo njezinoj nacionalnoj sigurnosti, nije obvezna podijeliti te informacije. Tijekom posjeta Suda državama članicama predstavnici mreže CSIRT-ova i mreže EU-CyCLONe naveli su da se informacije mogu razmjenjivati samo unutar granica nacionalnog zakonodavstva o sigurnosti. Na razini EU-a nije provedena analiza nacionalnih pravnih okvira država članica i njihova učinka na razmjenu informacija.

- 43** Mreža CSIRT-ova sastojala se 2016. od 28 nacionalnih CSIRT-ova, s po dva predstavnika iz svake države članice. Nedostatna razmjena informacija stalan je problem te je u [Komisijinoj evaluaciji](#) Direktive NIS potvrđeno da „države članice ne razmjenjuju sustavno informacije jedna s drugom”, što djelomično utječe na djelotvornost mjera u području kibernetičke sigurnosti i razinu zajedničke informiranosti o stanju na razni EU-a. Na temelju Direktive NIS 2 mnoge države članice imenovala su povrh nacionalnog CSIRT-a sektorske CSIRT-ove, čime se ta mreža znatno proširila. U vrijeme obavljanja revizije sastojala se od 42 CSIRT-a i više od 700 pojedinačnih sudionika. Time izgradnja povjerenja postaje još zahtjevnija jer je teško održavati bliske veze među svim članovima.
- 44** Mreža CSIRT-ova svjesna je problema s razmjenom informacija i razmatra razne mjere za povećanje povjerenja u sve široj mreži. Uspostava manjih klastera država članica koji bi imali ulogu prekograničnih centara, kako je detaljno opisano u odlomcima [62 – 74](#), alternativan je pristup radu mreže na razini EU-a koji bi mogao pomoći u savladavanju tog izazova.

Usluge koje se pružaju na temelju ugovora koji je sklopio centar za situaciju u kibernetičkom prostoru dijelom se preklapaju s već postojećim funkcijama, a njegov rad u budućnosti nije jasan

- 45** U skladu s Direktivom NIS 2 u slučajevima u kojima potencijalan ili aktualan kibernetički incident velikih razmjera ima ili će vjerojatno imati znatan učinak Komisija postaje članica mreže EU-CyCLONe⁹. Zbog te nove uloge i promjena u području kibernetičkih prijetnji Komisija je 2022. u sklopu GU-a Connect uspostavila radnu skupinu za koordinaciju u području kibernetičke sigurnosti. Ta radna skupina uključuje centar za situaciju u kibernetičkom prostoru, koji bi Komisiji trebao pomoći da poveća svoju informiranost o stanju i time joj pružiti podršku u ispunjavanju njezinih institucijskih odgovornosti u pogledu upravljanja krizama. Ujedno bi trebao pomagati GU-u Connect u pružanju savjeta na političkoj razini.

⁹ Članak 16. stavak 2. [Direktive NIS](#).

- 46** Komisiji u uspostavi centra za situaciju u kibernetičkom prostoru u velikoj mjeri pružaju potporu vanjski pružatelji usluga s kojima je u prosincu 2022. [sklopljen ugovor](#) u vrijednosti od gotovo 18 milijuna eura za razdoblje od četiriju godina. Sud je procijenio uspostavu tog centra, njegova ostvarenja i Komisijine planove za njegovo buduće funkcioniranje.
- 47** U sklopu pruženih usluga ugovaratelji su izradili preglednik koji se temelji na komercijalnim obavještajnim podacima o kibernetičkim prijetnjama kako bi se prikazivale i dijelile informacije o prijetnjama. Izrađuju i razna izvješća s obavještajnim podacima o kibernetičkim prijetnjama, uključujući dnevna i tjedna izvješća te tematska izvješća o pojedinačnim zemljama ili gospodarskim sektorima. Centar za situaciju u kibernetičkom prostoru fizički je smješten u jednoj od zgrada Komisije i sastoji od prostorije opremljene radnim stanicama koje su daljinski povezane s preglednikom kojim upravljaju ugovaratelji. U vrijeme obavljanja revizije taj se centar sastojao od malog broja članova osoblja Komisije, a potporu u njegovu radu pružali su brojni analitičari koje su stavili na raspolaganje ugovaratelji, kao i stručnjaci iz ENISA-e.
- 48** Sud je utvrdio da se aktivnosti koje obavljaju vanjski pružatelji usluga dijelom preklapaju s već postojećim funkcijama ENISA-e. ENISA ima stalne kapacitete za informiranost o stanju i praćenje prijetnji. Redovito objavljuje izvješća o kibernetičkim prijetnjama, uključujući kratka izvješća o specifičnim incidentima, kao i tjedna izvješća s pregledom prijetnji. Ta se izvješća temelje na obavještajnim podacima otvorenog koda i slična su izvješćima koja izrađuju ugovaratelji. Osim toga, ENISA izrađuje sažetke na visokoj razini za oblikovatelje politika tijekom kriznih razdoblja ili doprinosi izradi takvih sažetaka, koji su također usporedivi s dokumentima koje izrađuje centar za situaciju u kibernetičkom prostoru.
- 49** Nadalje, podaci koje centar za situaciju u kibernetičkom prostoru upotrebljava za izradu tih izvješća temelje se na komercijalnim obavještajnim podacima o kibernetičkim prijetnjama i slični su podacima koje upotrebljavaju druge službe Komisije, kao što su Glavna uprava za digitalne usluge i služba CERT-EU. Sud smatra da se načinom na koji je taj centar uspostavljen nije u dovoljnoj mjeri iskoristio potencijal za racionalizaciju upotrebom već dostupnih informacija Komisije i ENISA-e.
- 50** Sklopljeni ugovor istječe u prosincu 2026., nakon čega ugovaratelji više neće pružati usluge za centar za situaciju u kibernetičkom prostoru. Te usluge uključuju stavljanje na raspolaganje podataka dostupnih u pregledniku i izradu izvješća o prijetnjama, kao i stavljanje centru na raspolaganje većine osoblja potrebnog za njegov rad. Preglednik će biti predan Komisiji, ali ako se ne bude redovito ažurirao obavještajnim podacima o kibernetičkim prijetnjama, izgubit će svoju dodanu vrijednost.

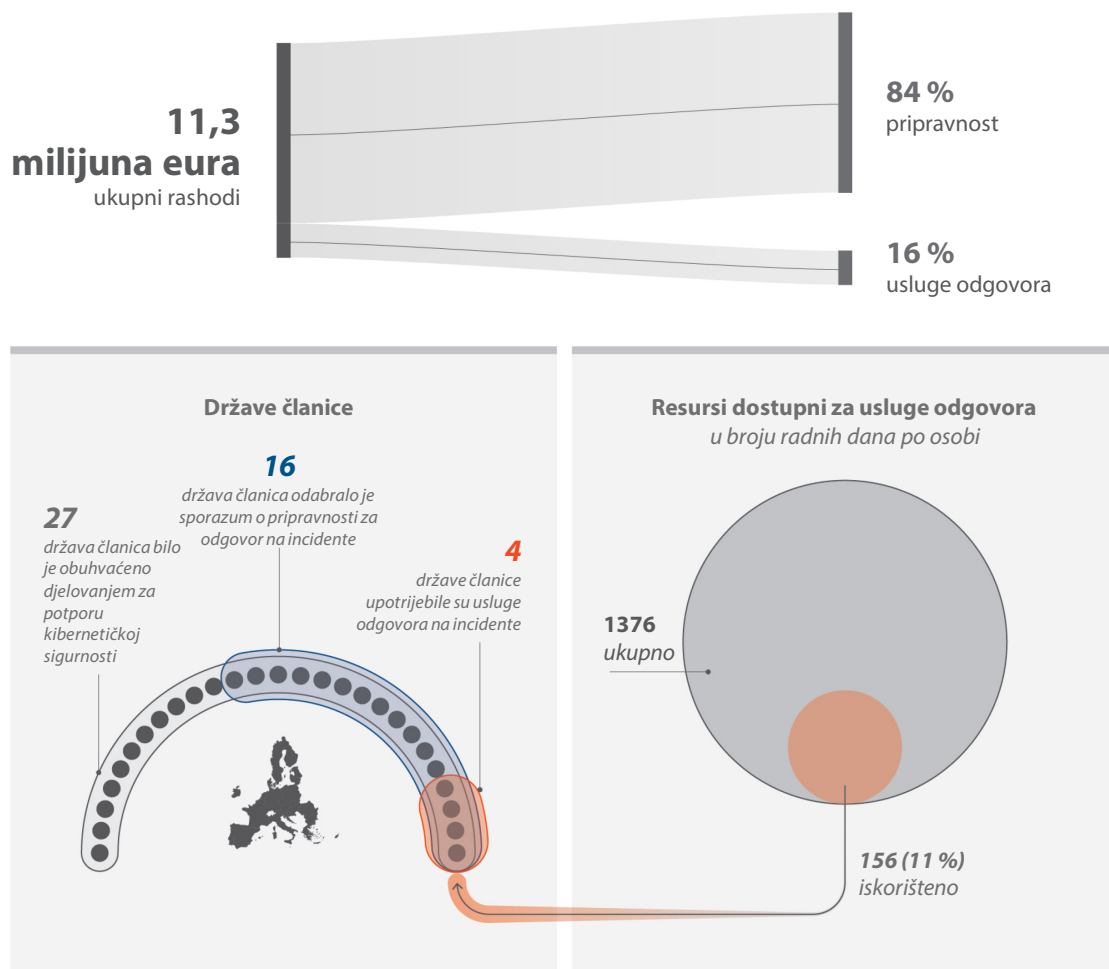
- 51** U vrijeme obavljanja revizije Komisija nije imala nikakve planove u pogledu potpore koju vanjski pružatelji usluga pružaju u radu predmetnog centra za razdoblje nakon isteka ugovora. Sud smatra da se zbog nepostojanja sveobuhvatnog i detaljnog plana za budućnost nakon isteka ugovora stvara rizik za rad centra za situaciju u kibernetičkom prostoru nakon 2026.

Pričuva EU-a za kibernetičku sigurnost omogućuje brzu aktivaciju usluga odgovora na incidente

- 52** Neposredno nakon ruske vojne agresije na Ukrajinu i uzimajući u obzir sve veću učestalost kibernetičkih napada velikih razmjera Komisija je 2022. ENISA-i stavila na raspolaganje izvanredna financijska sredstva u iznosu od 15 milijuna eura za provedbu pilot-programa [djelovanja za potporu kibernetičkoj sigurnosti](#), koji je pokrenut 2023. Komisija je 2023. stavila na raspolaganje dodatna financijska sredstva (otprilike 20 milijuna eura) kako bi se provedba tog programa produljila do kraja 2026.
- 53** Radi pripreme za suočavanje s kibernetičkim incidentima velikih razmjera Komisija je predložila i [Akt o kibernetičkoj solidarnosti](#), koji je donesen u prosincu 2024. Tim je aktom uspostavljena pričuva EU-a za kibernetičku sigurnost kojom su obuhvaćene usluge odgovora na incidente koje pružaju pouzdani pružatelji usluga. Ta se pričuva počela postupno upotrebljavati 2025., s proračunom od 36 milijuna eura za razdoblje 2025. – 2027.
- 54** Sud je procijenio način na koji je organiziran program djelovanja za potporu kibernetičkoj sigurnosti jer on čini temelj za pričuvu EU-a za kibernetičku sigurnost. Provjerio je i jesu li pri osmišljavanju te pričuve uzeta u obzir iskustva stečena od 2022.
- 55** ENISA je osmislila djelovanje za potporu kibernetičkoj sigurnosti kao mehanizam za podupiranje pripravnosti i odgovora država članica na kibernetičke incidente ili krize velikih razmjera. ENISA unaprijed sklapa ugovore za sve usluge, što znači da pružatelji usluga mogu započeti s aktivnostima čim države članice to od njih zatraže. Razlog za to leži i u načinu na koji je ENISA ustrojena, kojim se jamči da je 24 sata dnevno dostupan službenik koji obrađuje zahtjeve država članica.

- 56** ENISA je odlučila ravnomjerno raspodijeliti dostupan proračun među državama članicama. U praksi, ENISA je raspisala otvoreni natječajni postupak podijeljen u 27 grupa, jednu po svakoj državi članici, kako bi se odabrala do tri privatna pružatelja sigurnosnih usluga koji će pružati usluge do kraja 2026. Osim toga, ENISA je odabrala dio pružatelja usluga u sklopu paneuropske grupe za pružanje usluga zemljama izvan EU-a koje ispunjavaju uvjete za to, kao i institucijama, tijelima i agencijama EU-a, ili za potporu odgovoru na prekogranične incidente.
- 57** Taj je pristup omogućio ENISA-i da uzme u obzir specifične nacionalne zahtjeve, uključujući jezik, nacionalne sigurnosne provjere ili potvrđenu prisutnost u državama članicama. S druge strane, budući da pružatelji usluga nisu odabrani kako bi mogli pružati usluge u cijelom EU-u, velik je nedostatak tog pristupa taj da ako određena država članica ne iskoristi unaprijed ugovorene usluge, proračun rezerviran za takve usluge za određenu državu članicu ne može se upotrijebiti za pomoć drugoj državi članici.
- 58** U okviru djelovanja za potporu kibernetičkoj sigurnosti države članice mogle su odabrati usluge pripravnosti ili usluge odgovora ili kombinaciju obiju vrsta usluga. Države članice u prvom su redu odabrale da će raspoloživa financijska sredstva upotrijebiti za poboljšanje svoje pripravnosti (84 % rashoda 2023.). Države članice koje su se odlučile na sporazum o pripravnosti za odgovor na incidente (tj. unaprijed utvrđen sporazum s određenim pružateljem usluga kojim se jamči da država članica može dobiti njegove usluge na zahtjev radi brzog odgovora na kibernetičke incidente) upotrebljavale su te usluge u umjerenoj mjeri, kao što je prikazano na [slici 4](#). U trima posjećenim državama članicama relevantna tijela navela su da cijene način na koji ENISA upravlja djelovanjem za potporu kibernetičkoj sigurnosti.

Slika 4. | ENISA: djelovanje za potporu kibernetičkoj sigurnosti do 2023.



Izvor: Sud, na temelju podataka ENISA-e.

- 59** Za razdoblje 2024. – 2026. samo je devet država članica zatražilo sporazum o pripravnosti za odgovor na incidente. U razgovorima koje je Sud obavio s osobljem ENISA-e i relevantnih tijela u trima državama članicama potvrđeno je da se prednost uvelike davala aktivnostima u području pripravnosti.
- 60** Iako je cilj pričuve EU-a za kibernetičku sigurnost prije svega pružiti potporu odgovoru na velike kibernetičke incidente i oporavku od njih, unaprijed naručene usluge financirane iz pričuve EU-a za kibernetičku sigurnost koje nisu upotrijebljene za odgovor na incidente mogu se umjesto toga upotrijebiti kao usluge u području pripravnosti. Takvim fleksibilnim pristupom može se spriječiti neiskorištavanje unaprijed plaćenih usluga.
- 61** Sud smatra da se u modelu odabranom za pričuvu EU-a za kibernetičku sigurnost uzimaju u obzir iskustva stečena u okviru programa djelovanja za potporu kibernetičkoj sigurnosti. Međutim, podatci o upotrebi tog programa upućuju na to da postoji rizik od toga da se pričuva EU-a za kibernetičku sigurnost u prvom redu upotrebljava za pripravnost, a ne za odgovor, što je suprotno njezinoj svrsi utvrđenoj u Aktu o kibernetičkoj solidarnosti.

Cilj je europskog sustava uzbunjivanja u području kibernetičke sigurnosti povećati kapacitete za otkrivanje prijetnji, ali on nije u funkciji

- 62** Jedan je od ključnih ciljeva europskog sustava uzbunjivanja u području kibernetičke sigurnosti poticati korisnu razmjenu informacija kako bi se poboljšali otkrivanje i analiza kibernetičkih prijetnji te odgovor na njih. Sudjelovanje u tom sustavu temelji se na dobrovoljnoj osnovi, ali države članice koje odluče pridružiti se jednom od prekograničnih kibernetičkih centara moraju se obvezati na razmjenu relevantnih informacija s drugim članovima. Suradnjom u klasterima u pouzdanom i sigurnom okružju države članice mogu izbjeći neke od problema povezanih s razmjenom informacija koji su navedeni u odlomcima [31](#) – [44](#).
- 63** U vrijeme obavljanja revizije 13 država članica bilo je odlučilo sudjelovati u europskom sustavu uzbunjivanja u području kibernetičke sigurnosti, uspostavivši dva prekogranična centra: ATHENA i ENSOC. Tijekom 2026. dodijeljena su sredstva za uspostavu trećeg prekograničnog kibernetičkog centra, NBCC-a, čime se broj zemalja koje su članice te mreže povećava na ukupno 20 (18 država članica te Island i Norveška¹⁰), kao što je prikazano na [slici 5](#).

¹⁰ Pridružene zemlje koje nisu članice EU-a u skladu s člankom 10. stavkom 1. točkom (a) Uredbe (EU) 2021/694.

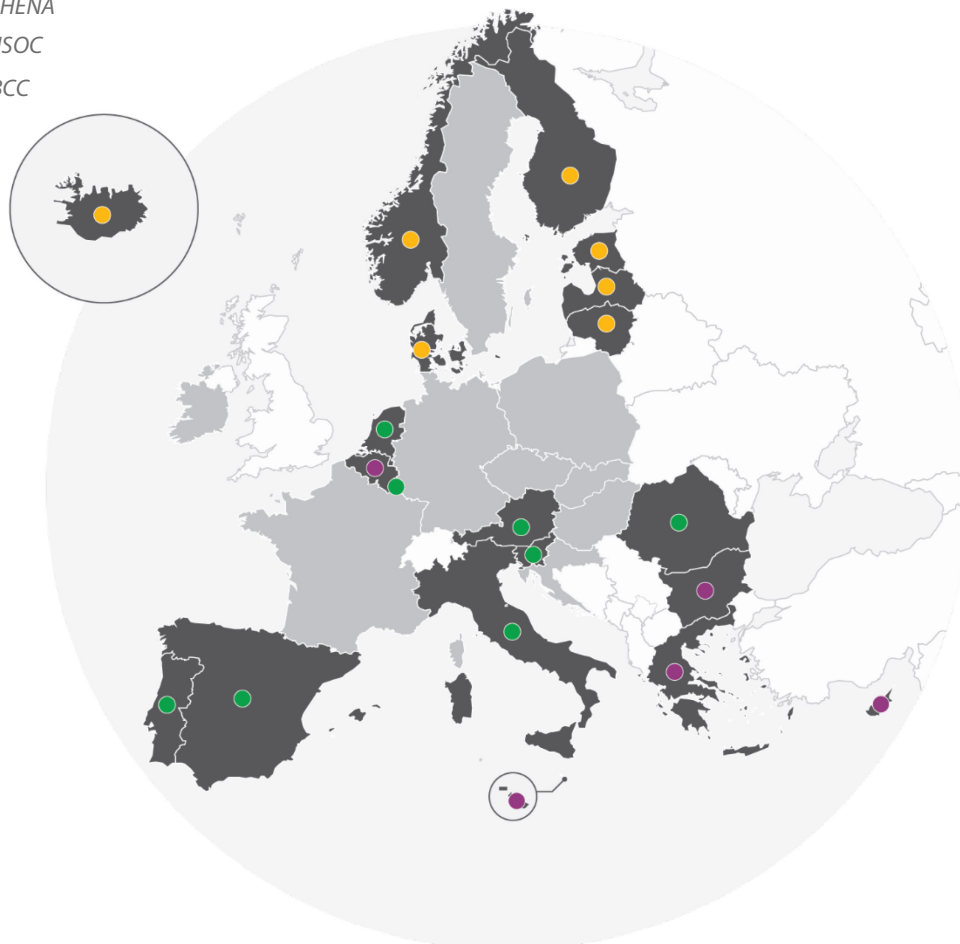
Slika 5. | Zemlje uključene u europski sustav uzbunjivanja u području kibernetičke sigurnosti

■ Zemlje uključene u europski sustav uzbunjivanja u području kibernetičke sigurnosti

● ATHENA

● ENSOC

● NBCC



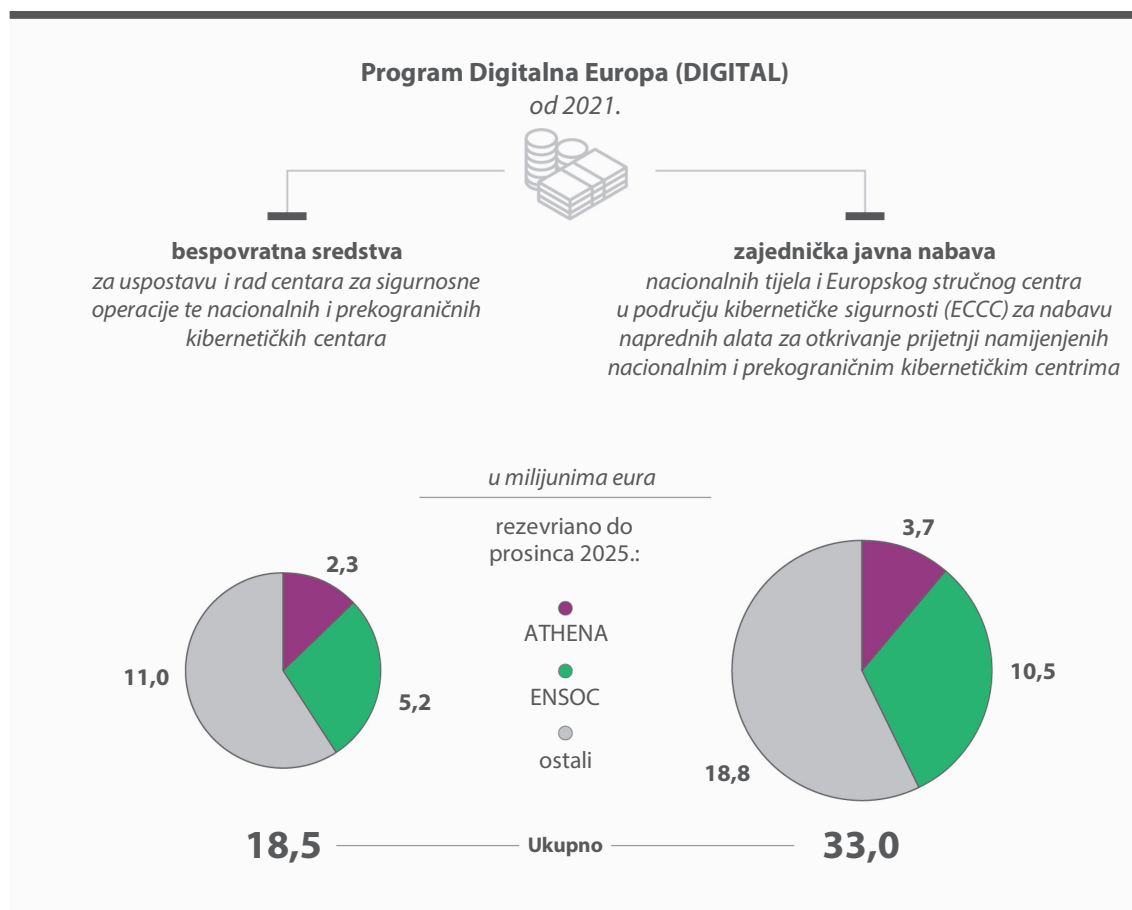
Izvor: Sud.

- 64** Sud je procijenio način na koji su uspostavljena prva dva prekogranična kibernetička centra, kao i njihov napredak u ostvarivanju ciljeva europskog sustava uzbunjivanja u području kibernetičke sigurnosti. Ispitao je i kako se uspostava tih centara uklapa u šire kibernetičko okruženje, kao i njihovo međudjelovanje s postojećim mrežama i strukturama.

Dosad nisu postignuti konkretni rezultati zbog znatnih kašnjenja u javnoj nabavi

- 65** Financijska sredstva za potporu uspostavi nacionalnih i prekograničnih kibernetičkih centara dostupna su u okviru programa Digitalna Europa od 2021. Ta se sredstva pružaju na temelju složenog postupka preko dvaju usporednih tokova sredstava: tradicionalna bespovratna sredstva za potporu uspostavi i radu centara te zajednička javna nabava radi pribavljanja naprednih alata za otkrivanje prijetnji, kao što je prikazano na [slici 6](#). Nakon raspisivanja poziva na podnošenje prijedloga u studenome 2022. ATHENA i ENSOC započeli su s radom u siječnju 2024.

Slika 6. | Financijska sredstva iz programa Digitalna Europa namijenjena kibernetičkim centrima



Izvor: Sud, na temelju podataka ECCC-a

- 66** Povezane ograničene postupke javne nabave u dvije faze¹¹ organizirali su članovi centara ATHENA i ENSOC, kao i GU Connect (prva faza) i novoosnovani ECCC (druga faza). Cilj je pristupa u dvije faze ograničiti protok osjetljivih informacija na način da se detaljne tehničke specifikacije pruže samo kandidatima odabranim u prvoj fazi.
- 67** Prva faza pokrenuta je u svibnju 2024. za ENSOC i u srpnju 2024. za ATHENA-u. Zainteresirana poduzeća mogla su se prijaviti u roku od mjesec dana. Međutim, kandidati koji su bili uspješni obaviješteni su o tome tek u travnju 2025., gotovo godinu dana nakon pokretanja postupka.
- 68** Osim toga, ni postupak javne nabave koji je provodio ENSOC ni onaj koji je provodila ATHENA nisu mogli prijeći u drugu fazu u to vrijeme jer članovi centara i ECCC poduzećima koja su ušla u uži izbor nisu mogli dostaviti tehničke specifikacije koje su tim poduzećima bile potrebne za podnošenje ponude jer su još radili na njihovu dovršetku.
- 69** Druga faza postupaka javne nabave počela je tek u kolovozu 2025. za određene grupe ENSOC-a, a za ATHENA-u je bila planirana za početak 2026. U vrijeme obavljanja revizije, 18 mjeseci nakon pokretanja postupka javne nabave, nije bio sklopljen ugovor ni za jednu od grupa. Sud smatra da su izostanak odgovarajuće pripreme i složenost postupaka javne nabave negativno utjecali na njihov pravodoban dovršetak.
- 70** Stoga je utvrdio da prekogranični centri nisu na dobrom putu da ostvare svoje ciljeve. Bez alata za otkrivanje prijetnji i razmjenu informacija ti centri ne mogu obavljati svoje aktivnosti te europski sustav uzbunjivanja u području kibernetičke sigurnosti još ne funkcionira, čime se odgađa djelotvoran razvoj naprednih kapaciteta za otkrivanje i sprečavanje kibernetičkih prijetnji i incidenata. Kako bi se uzela u obzir dosadašnja kašnjenja u postupcima javne nabave (15 mjeseci za ATHENA-u i 18 mjeseci za ENSOC), potpisane su izmjene sporazuma o dodjeli bespovratnih sredstava radi produljenja njegova trajanja.

¹¹ Poziv ENSOC-a na podnošenje ponuda i poziva ATHENA-e na podnošenje ponuda.

Prekograničnim kibernetičkim centrima stvaraju se dodatni komunikacijski kanali kojima se još više povećava složenost

- 71** Jedna je od ključnih zadaća prekograničnih kibernetičkih centara razmjenjivati relevantne informacije kako bi se poboljšalo otkrivanje prijetnji i odgovor na njih. To uključuje informacije o kibernetičkim prijetnjama, slabim točkama, pokazateljima ugroženosti i akterima prijetnji. Zadaće prekograničnih kibernetičkih centara djelomično se preklapaju sa zadaćama nacionalnih CSIRT-ova i mreže CSIRT-ova, posebno u pogledu razmjene informacija o kibernetičkim prijetnjama i slabim točkama. Ne postoji jasno razgraničenje između uloga prekograničnih kibernetičkih centara i CSIRT-ova. U skladu s Planom za kibernetičku sigurnost iz 2025. (odlomak [29](#)) prekogranični kibernetički centri trebali bi djelovati i na tehničkoj razini (kao i nacionalni CSIRT-ovi i mreža CSIRT-ova) i na operativnoj razini (kao i mreža EU-CyCLONe).
- 72** U skladu s Aktom o kibernetičkoj solidarnosti prekogranični kibernetički centri trebaju međusobno sklopiti sporazume o suradnji kako bi se olakšala razmjena informacija. ENISA je u skladu s tim aktom do veljače 2026. trebala pružiti smjernice za interoperabilnost među prekograničnim kibernetičkim centrima. U međuvremenu je ECCC u prosincu 2025. dodijelio bespovratna sredstva jednom konzorciju (uključujući određene članove ENSOC-a i ATHENA-e) kako bi se utvrdio tehnički okvir za interoperabilnost među prekograničnim kibernetičkim centrima. Međutim, predmetne smjernice i okvir dovršit će se tek nakon što prekogranični kibernetički centri počnu s radom. Kao što je Sud istaknuo u mišljenju o Prijedlogu akta o kibernetičkoj solidarnosti iz 2023. ¹², postoji rizik od toga da se bez brzog dogovora osmisle sustavi koji su međusobno nekompatibilni, što bi dovelo do većih troškova.
- 73** Od prekograničnih kibernetičkih centara traži se i da bez nepotrebne odgode prosljede relevantne informacije o kibernetičkim incidentima velikih razmjera mreži EU-CyCLONe i CSIRT-ovima. Na razini država članica uspostava nacionalnih kibernetičkih centara i sudjelovanje u prekograničnim kibernetičkim centrima doveli su do stvaranja dodatnih komunikacijskih slojeva. Složenost povećava i koordinacija s državama članicama izvan EU-a ¹³, koje nisu članice mreže CSIRT-ova ili mreže EU-CyCLONe.

¹² [Mišljenje 02/2023](#) o Prijedlogu uredbe Europskog parlamenta i Vijeća o utvrđivanju mjera za povećanje solidarnosti i kapaciteta u Uniji za otkrivanje kibersigurnosnih prijetnji i incidenata, pripremu za njih i odgovor na njih, odlomak 26.

¹³ Island i Norveška.

- 74** Potrebni su jasni sporazumi o suradnji kako bi se dogovorili zajednička taksonomija i način razmjene informacija te kako bi se zajamčila interoperabilnost. Iskustva stečena u okviru mreže CSIRT-ova pokazuju da je riječ o znatnom izazovu. Sud je utvrdio da u vrijeme obavljanja revizije nisu bili dogovoreni nikakvi proceduralni mehanizmi za suradnju i razmjenu informacija. Sud smatra da bi se uspostavom nacionalnih i prekograničnih kibernetičkih centara mogla promicati djelotvornija razmjena informacija. Međutim, integracija prekograničnih centara u već složeno okruženje u području kibernetičke sigurnosti bit će zahtjevan zadatak i sa sobom nosi potrebu za dodatnim komunikacijskim kanalima i mehanizmima za suradnju.

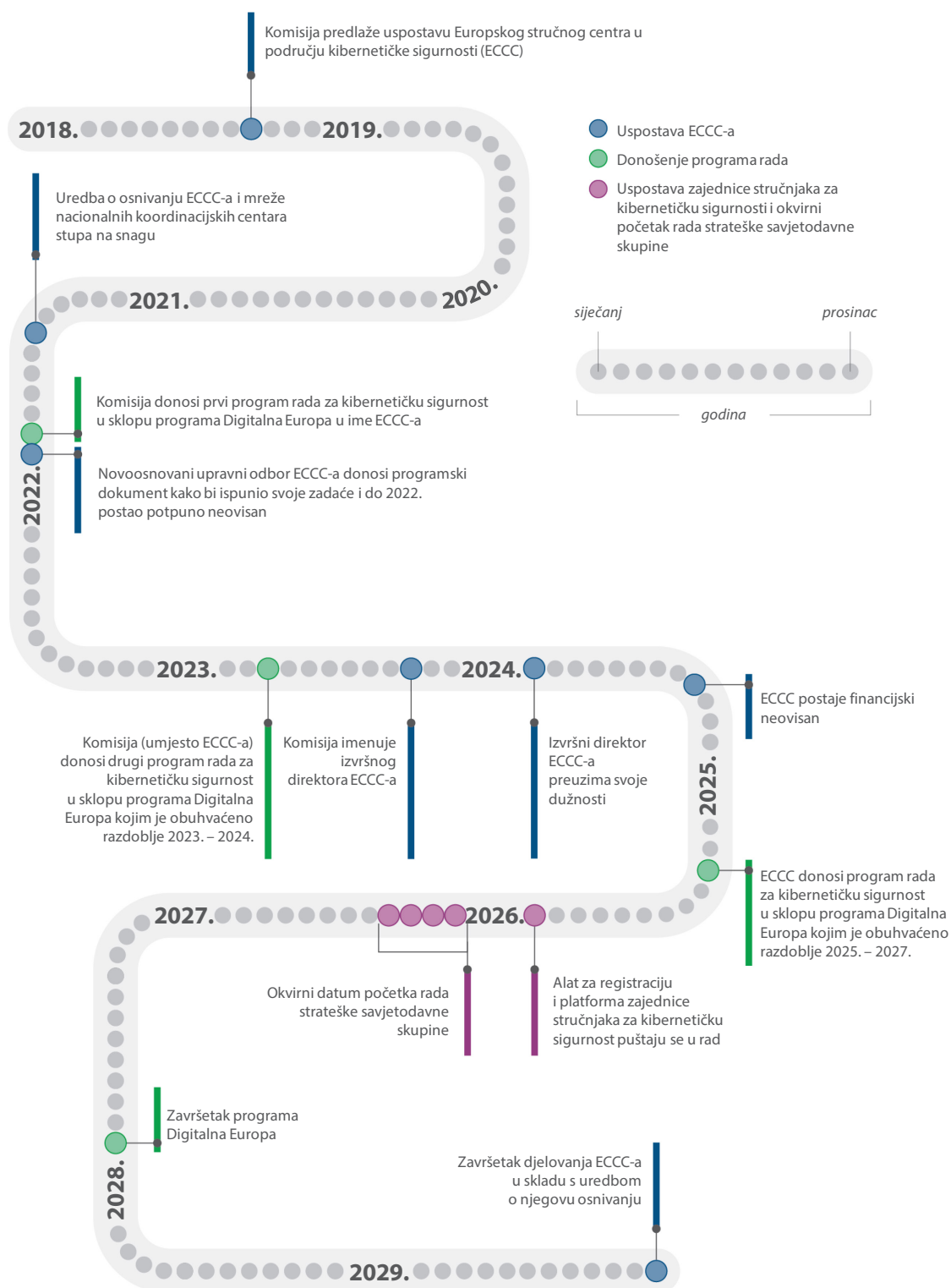
Projektima financiranim iz programa Digitalna Europa nastoji se ojačati kibernetička sigurnost, ali u njima se pojavljuju izazovi u pogledu provedbe i izvješćivanja

Zbog kašnjenja u uspostavi zajednice stručnjaka za kibernetičku sigurnost ta zajednica nije mogla prilagoditi program Digitalna Europa svojim potrebama

- 75** Komisija je u svrhu upravljanja komponentom kibernetičke sigurnosti u sklopu programa Digitalna Europa 2018. predložila uspostavu Europskog stručnog centra u području kibernetičke sigurnosti (ECCC). Uredbom o ECCC-u planirano je da tom centru potporu u njegovu radu pruža mreža sastavljena od 29 nacionalnih koordinacijskih centara, po jednog iz svake države članice, kao Islanda i Norveške. U toj se uredbi pozvalo i na osnivanje zajednice stručnjaka za kibernetičku sigurnost, sastavljene od predstavnika relevantnih sektora, akademske zajednice i istraživačkih organizacija, kao i drugih relevantnih udruženja civilnog društva.

- 76** Do 20 članova te zajednice imenovala bi strateška savjetodavna skupina, koja čini jednu od triju sastavnica strukture ECCC-a. Jedna je od glavnih zadaća te skupine organizirati javna savjetovanja radi prikupljanja informacija za program rada ECCC-a i programe rada u sklopu programa Digitalna Europa.
- 77** Sud je procijenio jesu li program Digitalna Europa i povezani programi rada doneseni na temelju pouzdane analize potreba, kao i način na koji ECCC, mreža nacionalnih koordinacijskih centara, zajednica stručnjaka za kibernetičku sigurnost i strateška savjetodavna skupina doprinose tim programima rada. U praksi su ECCC, mreža nacionalnih koordinacijskih centara, zajednica stručnjaka za kibernetičku sigurnost i strateška savjetodavna skupina uspostavljeni postupno tijekom nekoliko godina (vidjeti [sliku 7.](#)).

Slika 7. | Kronološki prikaz uspostave Europskog stručnog centra u području kibernetičke sigurnosti, mreže nacionalnih koordinacijskih centara, zajednice stručnjaka za kibernetičku sigurnost i strateške savjetodavne skupine



Izvor: Sud.

- 78** Budući da je ECCC započeo s radom u potpunosti tek u rujnu 2024., Komisija je u ime ECCC-a donijela programe rada za razdoblja 2021. – 2022. i 2023. – 2024. U okviru tih dvaju programa rada koje je donijela Komisija nije bilo moguće uzeti u obzir informacije zajednice stručnjaka za kibernetičku sigurnost.
- 79** U međuvremenu su države članice započele s uspostavom svojih nacionalnih koordinacijskih centara, koji djeluju kao kontaktne točke na nacionalnoj razini za navedenu zajednicu. Njihova uspostava i rad sufinancirani su iz programa Digitalna Europa, pri čemu je u vrijeme obavljanja revizije odobreno više od 90 milijuna eura, uključujući otprilike 44 milijuna eura koji će se dodatno raspodijeliti pružanjem financijske potpore trećim stranama. Proračunom je predviđeno dodatnih 38 milijuna eura do 2027. za potporu nacionalnim koordinacijskim centrima.
- 80** Sud je utvrdio da u prosincu 2025., četiri godine nakon uspostave ECCC-a i mreže nacionalnih koordinacijskih centara, zajednica stručnjaka za kibernetičku sigurnost još nije bila uspostavljena, a savjetodavna stručna skupina još nije bila imenovana. ECCC je posljednji programa rada za kibernetičku sigurnost u sklopu programa Digitalna Europa donio 14. ožujka 2025. te je njime obuhvaćeno razdoblje 2025. – 2027. ECCC je svoj program rada pripremio i donio nakon opsežnog savjetovanja s državama članicama i mrežom nacionalnih koordinacijskih centara, ali nije mogao iskoristiti informacije i savjete zajednice stručnjaka za kibernetičku sigurnost i stručne savjetodavne skupine. To je u suprotnosti s odredbama uredbe o osnivanju ECCC-a te Sud smatra da je riječ o propuštenoj prilici.
- 81** Provedba programa Digitalna Europa trebala bi završiti 2027. ako se razdoblje njegove provedbe ne produlji, a ECCC bi trebao prestati s radom 2029. Stoga bi potpora mreže nacionalnih koordinacijskih centara, zajednice stručnjaka za kibernetičku sigurnost i stručne savjetodavne skupine, nakon što se uspostave, mogla biti relevantna samo tijekom kratkog razdoblja.

Projektima financiranim sredstvima EU-a nastoje se ostvariti relevantni ciljevi, ali u mnogima od njih pojavljuju se operativni problemi

82 Sud je sastavio uzorak od 11 projekata relevantnih za otkrivanje kibernetičkih incidenata i odgovor na njih koji su financirani iz programa Digitalna Europa u razdoblju 2022. – 2025. (vidjeti [sliku 5.](#) u [Prilogu I.](#) i [Prilog III.](#)). Sud je procijenio sljedeće:

- jesu li ciljevi tih projekata bili u skladu s očekivanim ishodima navedenim u pozivima na podnošenje prijedloga i s očekivanim ishodima programa Digitalna Europa općenito;
- jesu li projektima dosad postignuta planirana ostvarenja i rezultati;
- jesu li ostvarenja projekata postignuta na vrijeme.

Sud iznosi rezultate te procjene u [Prilogu IV.](#)

U nekim projektima vidljivi su rani rezultati, ali u mnogima se pojavljuju operativni izazovi i kašnjenja

83 Sud je utvrdio da se svim projektima nastoje ostvariti ciljevi kojima se doprinosi postizanju ciljeva programa Digitalna Europa u vezi s kibernetičkom sigurnošću¹⁴ te da je u njima uzeta u obzir većina ciljeva iz povezanih poziva na podnošenje prijedloga¹⁵.

84 Od 11 projekata iz uzorka Suda dva projekta bila su u ranoj fazi provedbe te Sud stoga nije mogao donijeti zaključak o njihovoj uspješnosti. Od preostalih projekata Sud je procijenio da su njih četiri bila na zadovoljavajućoj razini u smislu postizanja njihovih planiranih ostvarenja i rezultata. Sud je smatrao da su u dvama projektima vidljivi određeni nedostaci, a tri projekta procijenio je nezadovoljavajućim (vidjeti [Prilog IV.](#)).

85 Jedan je od izričitih ciljeva programa Digitalna Europa povećati razinu kibernetičke sigurnosti u malim i srednjim poduzećima (MSP-ovi). U tom su pogledu u sklopu nekoliko projekata ponuđena konkretna rješenja za MSP-ove (vidjeti [okvir 2.](#)).

¹⁴ Članak 6. [Uredbe \(EU\) 2021/694](#) o uspostavi programa Digitalna Europa.

¹⁵ Pozivi na podnošenje prijedloga: [izgradnja kapaciteta centara za sigurnosne operacije](#); [uvođenje mreže nacionalnih koordinacijskih centara s državama članicama](#); [potpora za pripravnost i uzajamna pomoć](#); [te nove primjene umjetne inteligencije i drugih razvojnih tehnologija za centre za sigurnosne operacije](#).

Okvir 2.

Primjeri projekata kojima su ostvareni konkretni rezultati za MSP-ove

Cilj je projekta **GR-SME-SOC** (projekt br. 6 u **Prilogu III.**) MSP-ovima u Grčkoj staviti na raspolaganje alate i usluge u području kibernetičke sigurnosti uspostavom centra za sigurnosne operacije prilagođenog njihovim potrebama. S provedbom tog projekta započelo se u siječnju 2024. te ga provodi konzorcij sastavljen od pet grčkih organizacija. Plan je nuditi besplatne usluge u području kibernetičke sigurnosti za 120 MSP-ova tijekom jedne godine, nakon čega će te usluge postati komercijalno dostupne. Tim se projektom MSP-ovima nude napredne usluge kao što je praćenje u stvarnom vremenu, otkrivanje prijetnji na temelju umjetne inteligencije i brz odgovor na incidente.

U sklopu projekta **NCC-IE** (projekt br. 3 u **Prilogu III.**) koordinator tog projekta osigurao je bespovratna sredstva u iznosu od otprilike 1,8 milijuna eura za više od 50 irskih MSP-ova radi poboljšanja njihove kibernetičke sigurnosti. Predmetni program bespovratnih sredstava mogla su iskoristiti poduzeća koja zapošljavaju od 2 do otprilike 200 djelatnika, uključujući obiteljska poduzeća, *start-up* poduzeća i globalne izvoznike u različitim sektorima. Bespovratna sredstva dodjeljivala su se isključivo poduzećima za koja je obavljena prethodna provjera kibernetičke sigurnosti kojom je upravljala državna agencija Enterprise Ireland. Bespovratnim sredstvima pokrivalo se 80 % troškova (do 60 000 eura) za provedbu preporuka iznesenih na temelju te provjere.

Izvor: Sud.

- 86** U mnogim projektima iz uzorka Suda pojavljuju se poteškoće s poštovanjem rokova ili operativni izazovi (vidjeti **Prilog IV.**). Sud je utvrdio da u četirima projektima dolazi do znatnih kašnjenja. To uključuje centre ENSOC i ATHENA, kao što je detaljno objašnjeno u odlomcima **65 – 70**. Dodatni primjeri navedeni su u **okviru 3**.

Okvir 3.

Primjeri projekata u kojima se pojavljuju operativni izazovi i kašnjenja

U Irskoj je jedini korisnik bespovratnih sredstava za projekt **ILG-SOC** (projekt br. 8 u *Prilogu III.*) tamošnja Agencija za upravljačku potporu lokalnoj upravi. Cilj je projekta uspostaviti središnji centar za sigurnosne operacije za 31 lokalno tijelo radi upotrebe naprednih alata za otkrivanje prijetnji i odgovor na njih. S provedbom projekta započelo se u listopadu 2023. na razdoblje od tri godine. U sklopu provjere obavljene u sredini razdoblja provedbe sva su ostvarena postignuća odbijena. Predmetni projekt uključuje nekoliko postupaka javne nabave koji su bili neuspješni ili u kojima je došlo do kašnjenja. Razdoblje provedbe projekta bit će produženo (bez dodatnih financijskih sredstava), čime bi se moglo dobiti dovoljno vremena za uspješan dovršetak projekta.

Cilj je projekta **EL-SOC** u Grčkoj (projekt br. 5 u *Prilogu III.*) uspostaviti konsolidirani centar za sigurnosne operacije na nacionalnoj razini, u sklopu kojeg bi se objedinjavale informacije iz sektorskih centara za sigurnosne operacije. Time bi se pružio sveobuhvatan pregled stanja u području kibernetičke sigurnosti u stvarnom vremenu. Predmetni projekt provodi se od siječnja 2024. do prosinca 2026. Planirana javna nabava hardvera i usluga odgođena je zbog problema s dovršavanjem i objavom tehničkih specifikacija za poziv na podnošenje prijedloga. Koordinator projekta naveo je kao razloge za kašnjenje i probleme povezane s osiguravanjem nacionalnih sredstava za sufinanciranje i ograničenu raspoloživost osoblja zaduženog za javnu nabavu.

Izvor: Sud.

- 87** U dvama drugim projektima iz uzorka Suda došlo je do umjerenih kašnjenja, a u trima projektima ostvarenja se postižu na vrijeme. Naposljetku, dva su projekta u ranoj fazi provedbe te Sud stoga ne može o njima donijeti zaključak.

Zbog sigurnosnih ograničenja pojavili su se operativni izazovi, a u slučajevima u kojima provjere provode korisnici postoje znatni rizici

- 88** Uredbom o programu Digitalna Europa predviđeno je da se zbog sigurnosnih razloga pružanje financijskih sredstava za kibernetičku sigurnost može ograničiti na subjekte koji imaju poslovni nastan u EU-u i koji su pod kontrolom država članica ili građana EU-a. Cilj je tog ograničenja ublažiti rizik od uplitanja ili utjecaja zemalja izvan EU-a i spriječiti razmjenu osjetljivih sigurnosnih informacija s tijelima u zemljama izvan EU-a.
- 89** Obveza da vlasništvo i kontrola moraju ostati unutar EU-a primjenjuje se ne samo na korisnike bespovratnih sredstava već i na njihove podugovaratelje i sve primatelje financijske potpore trećim stranama. Osim za potonju kategoriju (vidjeti odlomke [92 – 96](#)) procjenu obavlja središnja služba za potvrde u sklopu [Europske izvršne agencije za istraživanje](#). Međutim, konačnu odluku o prihvatljivosti za sudjelovanje u ograničenim pozivima na podnošenje prijedloga i dalje donosi tijelo koje dodjeljuje bespovratna sredstva, tj. GU Connect ili ECCC.
- 90** Tijekom revizijskih aktivnosti Suda korisnici su u više navrata spomenuli praktične izazove koje sa sobom nose procjene vlasničke i kontrolne strukture. Procjena toga jesu li vlasništvo i kontrola u rukama subjekta iz EU-a može biti složen i dugotrajan proces. Za takvu procjenu potrebno je analizirati cjelokupnu vlasničku strukturu i lanac kontrole u svakoj organizaciji, uključujući sve razine vlasništva do krajnjih vlasnika. Središnja služba za potvrde od svakog subjekta traži da dostavi opsežnu [dokumentaciju s dokazima](#) o svojoj vlasničkoj strukturi i posebnim pravima, korporativnom upravljanju i svim komercijalnim, financijskim ili drugim vezama kojima se prenosi kontrola.
- 91** U trima projektima financiranim sredstvima EU-a iz uzorka Suda najmanje je jedan korisnik u sklopu jednog konzorcija naknadno isključen jer se smatralo da je u vlasništvu ili pod kontrolom subjekta izvan EU-a. Isključivanje članova konzorcija pokazuje da postoje sudionici u programu Digitalna Europa koji ne razumiju u potpunosti koncept zadržavanja vlasništva i kontrole unutar EU-a. Cjelokupno gledajući, prema podacima središnje službe za potvrde 7 % svih podnositelja zahtjeva za bespovratna sredstva za kibernetičku sigurnost iz programa Digitalna Europa ili podugovaratelja nije uspješno prošlo procjenu vlasničke i kontrolne strukture u razdoblju 2022. – 2025. Zbog slučajeva u kojima se neprihvatljivi sudionici prijavljuju na pozive na podnošenje prijedloga dolazi do kašnjenja, kao što je opisano u [okviru 4](#).

Okvir 4.

Primjer slučaja u kojem su korisnici isključeni nakon što nisu prošli sigurnosnu provjeru

Dva člana konzorcija u sklopu projekta NG-SOC (projekt br. 7 u [Prilogu III.](#)) nisu uspješno prošla procjenu vlasničke i kontrolne strukture. Ishod procjene najavljen je otprilike mjesec dana prije roka za sklapanje sporazuma o dodjeli bespovratnih sredstava. Koordinator projekta morao je pristati preuzeti poslove koji su bili dodijeljeni dvama isključenim članovima jer nije bilo vremena za pronalazak novog partnera. Jedan od isključenih članova djelovao je u specifičnom sektoru, u kojem se razvijeno rješenje trebalo primijeniti u pilot-fazi. Stoga se znatan dio projekta, koji se odnosio na testiranje rješenja u praksi, nije mogao provesti kako je bilo predviđeno. Situacija je kasnije ispravljena izmjenom sporazuma o dodjeli bespovratnih sredstava kako bi se uključili novi članovi.

Izvor: Sud.

- 92** U okviru dvaju projekata koje je Sud pregledao (NCC-IE i CYberSynchrony) pruža se financijska potpora trećim stranama. Tim se mehanizmom financiranja korisnicima bespovratnih sredstava omogućuje da dio tih sredstava iskoriste za financiranje drugih subjekata na temelju otvorenih poziva na podnošenje prijedloga. Pružanjem financijske potpore trećim stranama može se olakšati pristup financijskim sredstvima EU-a. U tom slučaju korisnici snose isključivu odgovornost za provedbu procjena vlasničke i kontrolne strukture, a središnja služba za potvrde nije uključena.
- 93** Komisija je 2021. objavila opće javne smjernice za prijavitelje koji sudjeluju u ograničenim pozivima na podnošenje prijedloga, koje su ažurirane 2026. Iako je za pozive na podnošenje prijedloga u sklopu programa Digitalna Europa mogućnost pružanja financijske potpore trećim stranama dostupna od 2021., ni Komisija ni ECCC korisnicima nisu stavili na raspolaganje detaljnu metodologiju za obavljanje procjene vlasničke i kontrolne strukture pri provjeri trećih strana kojima pružaju financijsku potporu. U srpnju 2025. ECCC je stavio na raspolaganje neobvezujuće smjernice, kojima je mreži nacionalnih koordinacijskih centara omogućena primjena strukturiranog pristupa procjenama vlasničke i kontrolne strukture. Dokument sa smjernicama sadržava opća načela i korake koji bi se mogli poduzeti. Međutim, u smjernicama se ne navodi na koji bi se način trebale provoditi predmetne provjere, zbog čega su korisnici odgovorni za osmišljavanje vlastitog pristupa.
- 94** Sud je utvrdio da ECCC ne potvrđuje metodologiju koju korisnici usvoje i ne obavlja provjere na temelju uzorka kako bi se zajamčilo da je ta metodologija dovoljno pouzdana i da su odabrani primatelji financijske potpore uistinu u vlasništvu i pod kontrolom subjekata iz EU-a.

- 95** Sud je u [godišnjem izvješću za 2024.](#) utvrdio da korisnici kojima je Komisija povjerila upravljanje financijskom potporom trećim stranim (u području istraživanja) nisu bili dužni dokazati djelotvornost svojih provjera u svrhu jamčenja pravilnosti rashoda EU-a. Slično tomu, ECCC ne obavlja procjenu administrativnih i tehničkih kapaciteta korisnika za odgovarajuće upravljanje procjenama vlasničke i kontrolne strukture. Kao što je detaljno opisano u odlomku [90](#), ta procjena može biti složena i na razini EU-a provodi je posebna služba sa specijaliziranim stručnim znanjem.
- 96** U tom kontekstu Sud smatra da postoji znatan rizik od toga da korisnici, koji su odgovorni za provedbu procjena vlasničke i kontrolne strukture, ne raspolažu kapacitetima za njihovu odgovarajuću provedbu. S obzirom na prirodu financiranih aktivnosti, tim bi se nedostatkom mogli ugroziti osjetljiva infrastruktura, operativni podatci i tehnologije ključne za sigurnost.

Za većinu projekata financiranih sredstvima EU-a nisu utvrđeni odgovarajući okviri uspješnosti, a podatci o uspješnosti u području kibernetičke sigurnosti u sklopu programa Digitalna Europa nisu točni

Za većinu projekata financiranih sredstvima EU-a nisu utvrđeni odgovarajući okviri uspješnosti

- 97** Korisnici koji upravljaju projektima financiranim sredstvima EU-a moraju izvješćivati ECCC o svojem napretku i rezultatima na temelju ključnih etapa, postignuća i pokazatelja, kao što je prikazano na [slici 8](#). Sud je procijenio omogućuje li se ključnim etapama i postignućima predviđenim za svaki projekt na odgovarajući način praćenje projekata. Procijenio je i jesu li njihovi pokazatelji uspješnosti relevantni i mjerljivi te jesu li za njih utvrđene polazne i ciljne vrijednosti.

Slika 8. | Ključne etape, postignuća koja je potrebno ostvariti i pokazatelji uspješnosti u projektima u sklopu programa Digitalna Europa

	 Ključne etape	 Postignuća	 Pokazatelji uspješnosti
Što su	kontrolne točke tijekom cijelog projekta koje pomažu u utvrđivanju napretka	podnesena ostvarenja projekta kako bi se pokazao napredak	upotrebljavaju se za mjerenje rezultata
Kako se utvrđuju	povezani su samo s glavnim ostvarenjima (ograničen broj)	samo glavna ostvarenja (maksimalno od 10 do 15 po projektu)	trebaju biti specifični, mjerljivi, dostižni, relevantni i vremenski ograničeni
Primjeri	“pokretanje pilot-faze platforme”	“priručnik za korisnike platforme”	“smanjenje vremena potrebnog za odgovor na incidente za 30 %”
	Strukturirani pristup, dio internetskog sustava za upravljanje bespovratnim sredstvima		Nestrukturirani pristup

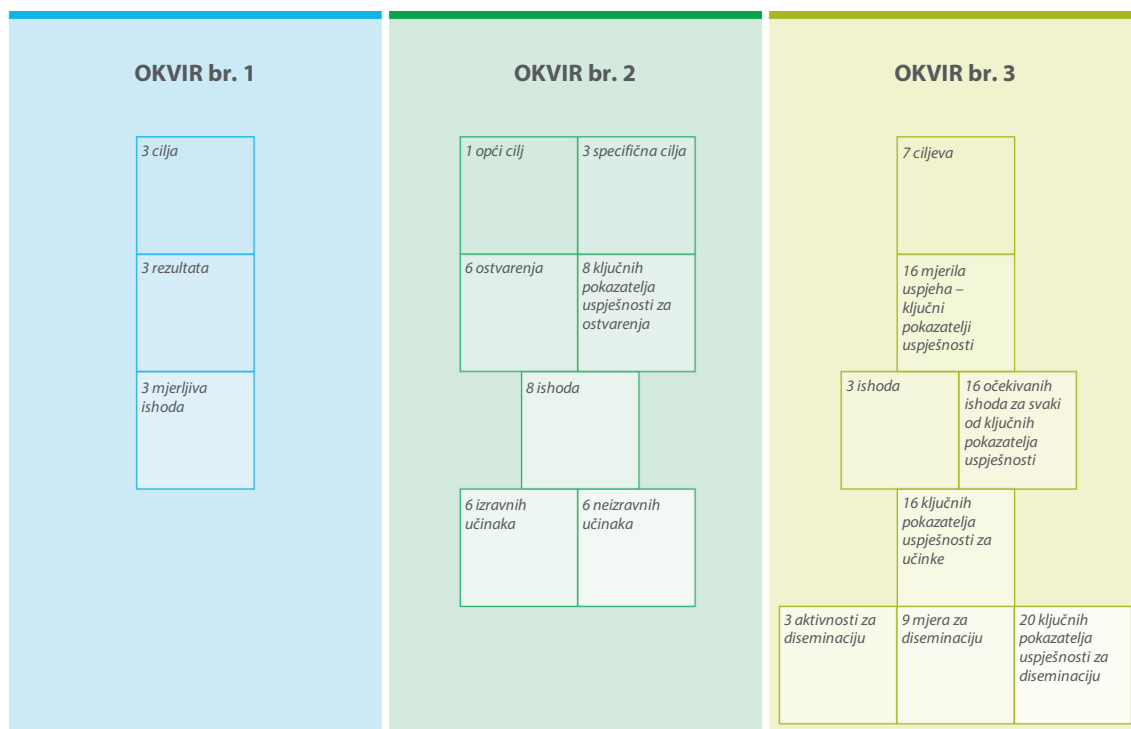
Izvor: Sud, na temelju [zahtjeva za bespovratna sredstva](#).

- 98** Korisnici u svojim projektnim prijedlozima moraju utvrditi niz ključnih etapa i postignuća koja je potrebno ostvariti na temelju strukturiranog pristupa pojašnjenog u uputama za prijavitelje. Sve ključne etape i postignuća navedeni su u internetskom sustavu za upravljanje bespovratnim sredstvima kako bi se olakšalo njihovo praćenje. ECCC trenutačno provjerava svaki projekt dvaput: jednom u sredini njegove provedbe i jednom nakon njegova dovršetka. Tijekom tih provjera vanjski stručnjaci utvrđuju jesu li dostignute ključne etape i ostvarena postignuća, a ECCC ih potvrđuje. Ključne etape i postignuća stoga imaju ključnu ulogu u praćenju projekata te ih je potrebno pravilno utvrditi.

99 Sud je utvrdio da se u gotovo nijednom od projekata iz njegova uzorka nisu primjenjivale upute u pogledu broja ključnih etapa i postignuća: broj ključnih etapa po projektu kreće se između 8 i 39, a broj postignuća između 8 i 45. U mnogim ključnim etapama i postignućima nisu uzete u obzir upute o tome kako bi ih trebalo utvrditi te oni stoga nisu korisni za praćenje napretka (na primjer, „sastanak radi pokretanja izrade poziva na podnošenje prijedloga za istraživanje” ili „službeni zapisnici sa sastanaka o projektu”). U slučaju triju projekata odbor za evaluaciju utvrdio je te probleme prije sklapanja sporazuma o dodjeli bespovratnih sredstava. U dvama slučajevima korisnici su predložili tek manje izmjene (npr. u pogledu rokova) bez rješavanja ključnih problema, dok u trećem nisu uvedene nikakve izmjene. Za šest drugih projekata iz uzorka analiza koju je Sud proveo pokazuje da ključne etape ili postignuća nisu u skladu s uputama i da nisu uvijek prikladni. Sud smatra da se neodgovarajuće utvrđenim postignućima ili ključnim etapama ili njihovim prevelikim brojem otežava praćenje napretka.

100 Za razliku od ključnih etapa i postignuća na pokazatelje uspješnosti ne primjenjuje se strukturirani pristup te oni nisu objedinjeni u tablici u sustavu za upravljanje bespovratnim sredstvima, već se umjesto toga mogu pronaći u različitim odjeljcima prijedloga. Taj je pristup doveo do toga da su korisnici predložili mnoštvo različitih okvira uspješnosti. Dok su neki utvrdili samo ciljeve projekata povezane s pokazateljima uspješnosti, drugi su utvrdili mnogo složenije okvire uspješnosti. Sud navodi nekoliko primjera na [slici 9.](#) u nastavku.

Slika 9. | Primjer različitih okvira uspješnosti osmišljenih za projekte



Izvor: Sud.

- 101** Zaključak je analize koju je Sud proveo da mnogi pokazatelji uspješnosti koji se upotrebljavaju u projektima nisu relevantni ni mjerljivi te da za njih nisu utvrđene ciljne i polazne vrijednosti (vidjeti [okvir 5.](#)). Nadalje, u sedam projekata utvrđeno je 20 ili više pokazatelja, pri čemu su za jedan projekt utvrđena 52 pokazatelja. Sud iznosi rezultate te procjene u [Prilogu IV.](#)

Okvir 5.

Primjeri neodgovarajućih pokazatelja uspješnosti

Pokazatelji koji nisu mjerljivi:

- „Pokazateljem ugroženosti i drugim pruženim uslugama jačaju se kapaciteti MSP-ova u području kibernetičke sigurnosti”;
- „Stavljanje na raspolaganje alata i metoda za odgovor na incidente kojima se omogućuje integracija s komunikacijskim kanalima mreže EU-CyCLONe”.

Pokazatelji za koje nisu utvrđene polazne ili ciljne vrijednosti:

- „≥ 20 % bolja pripravnost osoblja”;
- „≥ 20 % manje napora potrebnih za usklađivanje s relevantnim inicijativama EU-a za kibernetičku sigurnost”.

Pokazatelji koji nisu povezani s uspješnošću:

- „Završno izvješće o projektu na kraju faze financiranja”;
- „Broj polaznika koji će sudjelovati u svim tečajevima osposobljavanja”.

Izvor: Sud, na temelju projektne dokumentacije.

- 102** Cjelokupno gledajući, Sud smatra da se zbog mnoštva različitih okvira uspješnosti, neodgovarajućeg utvrđivanja pokazatelja i njihova prekomjernog broja znatno otežava praćenje uspješnosti. Stoga nije moguće odgovarajuće procijeniti uspješnost projekata. Složenost se dodatno povećava time što obrazac za izvješćivanje ne sadržava poseban odjeljak o pokazateljima uspješnosti projekata, zbog čega se u sklopu većine projekata iz uzorka Suda nije izvješćivalo o tim pokazateljima.

Podatci o uspješnosti komponente kibernetičke sigurnosti u sklopu programa Digitalna Europa nisu točni

- 103** Kako bi se pratila postignuća u okviru programa Digitalna Europa, relevantnom uredbom predviđeni su programski pokazatelji o kojima je potrebno izvješćivati za sve projekte, kao što je detaljno opisano u [okviru 6](#).

Okvir 6.

Pokazatelji za kibernetičku sigurnost u sklopu Digitalna Europa

1.a Količina infrastruktura i/ili alata za kibernetičku sigurnost nabavljenih zajedničkom javnom nabavom, među ostalim u okviru europskog sustava uzbunjivanja u području kibernetičke sigurnosti

1.b Količina infrastruktura i/ili alata za kibernetičku sigurnost koji su uvedeni

2. Broj korisnika i zajednica korisnika s pristupom europskim kapacitetima za kibernetičku sigurnost

3. Broj djelovanja kojima se podupire pripravnost i odgovor na kibernetičke sigurnosne incidente u okviru mehanizma za izvanredne kibernetičke sigurnosne situacije

Izvor: Prilog II. [Uredbi \(EU\) 2021/694](#) o uspostavi programa Digitalna Europa; okvir za praćenje i evaluaciju programa Digitalna Europa ([SWD\(2024\) 37](#)).

- 104** Sud je procijenio jesu li se za projekte iz njegova uzorka dostavljali podatci o tim pokazateljima te je ispitao način na koji ECCC prikuplja i provjerava te podatke.
- 105** Podatci o pokazateljima za program Digitalna Europa moraju se dostaviti za sve projekte prije njihovih provjera u sredini razdoblja provedbe i konačnih provjera u sustavu za upravljanje bespovratnim sredstvima. Sud je utvrdio da su od sedam projekata koji su u vrijeme obavljanja revizije bili na polovici razdoblja provedbe i za koje su stoga trebali biti dostavljeni podatci za navedene pokazatelje ti podatci dostavljeni samo za njih tri. Od tih triju projekata za njih dva dostavljene su netočne informacije: u slučaju jednog dostavljeni su podatci za pogrešne pokazatelje, a u slučaju drugog dostavljene su ciljne vrijednosti umjesto postignutih rezultata.

106 Komisija izvješćuje svake godine o tim pokazateljima u svojim [izvješćima o uspješnosti programa](#). Time se dionicima omogućuje da procjene ostvaruju li se predmetnim programom njegovi ciljevi. Prema izvješćima o uspješnosti programa za 2024. ostvaruje se zadovoljavajući napredak u pogledu pokazatelja za kibernetičku sigurnost u sklopu programa Digitalna Europa. ECCC je objasnio Sudu da je upotrijebio niz anketa upućenih korisnicima potpore u sklopu projekata kako bi prikupio podatke za te pokazatelje umjesto da upotrijebi podatke iz sustava za upravljanje bespovratnim sredstvima. Sud je pregledao raščlanjene podatke koje mu je ECCC stavio na raspolaganje i utvrdio niz problema u načinu na koji su oni prikupljeni i u njihovoj ukupnoj kvaliteti. Utvrdio je da prikupljeni podatci ne odgovaraju vrijednostima navedenim u izvješću o uspješnosti programa te stoga nije jasno na koji su način izračunane prikazane vrijednosti. Sud nije pronašao dokaze koji bi potvrdili da je ECCC provjerio točnost dostavljenih podataka. Sud na temelju provjera projekata iz uzorka koji je sastavio, za koje većina vrijednosti nedostaje ili nije točna, smatra da se u dostavljenim podacima ne odražavaju na odgovarajući način postignuti rezultati.

Ovo je izvješće usvojilo III. revizijsko vijeće, kojim predsjedava član Revizorskog suda George-Marius Hyzler, na sastanku održanom u Luxembourg 16. lipnja 2026.

Za Revizorski sud

Tony Murphy
predsjednik

Prilozi

Prilog I. – O reviziji

- 01** Kibernetička sigurnost ili kibernetsigurnost definira se kao „aktivnosti koje su nužne za zaštitu od kiberprijetnji mrežnih i informacijskih sustava, korisnika tih sustava i drugih osoba na koje one utječu”¹. Kibernetička prijetnja ili kiberprijetnja znači „svaka moguća okolnost, događaj ili djelovanje koji bi mogli oštetiti, poremetiti ili na drugi način negativno utjecati na mrežne i informacijske sustave, korisnike tih sustava i druge osobe”². Za kibernetičku sigurnost potreban je holistički pristup, koji se sastoji od niza međusobno povezanih aktivnosti za sprečavanje i otkrivanje kibernetičkih prijetnji te odgovor na takve prijetnje i oporavak od njih, kao što je prikazano na [slici 1.](#) u nastavku.

¹ Uredba (EU) 2019/881 ([Akt o kibernetičkoj sigurnosti](#)).

² Članak 2. [Akta o kibernetičkoj sigurnosti](#).

Slika 1. | Primjeri aktivnosti u području kibernetičke sigurnosti

Sprečavanje 	Smanjivanje rizika od kibernetičkih incidenata i svođenje njihovih potencijalnih učinaka na najmanju moguću mjeru <i>Primjeri: antivirusni softver, vatrozidovi, enkripcija, dvofaktorska autentifikacija, upravljanje ažuriranjem softvera, osposobljavanje osoblja radi podizanja razine osviještenosti o sigurnosti</i>
Otkrivanje 	Otkrivanje zlonamjernih aktivnosti <i>Primjeri: praćenje mreže, informiranost o stanju</i>
Odgovor 	Upravljanje kibernetičkim incidentom i njegovo ublažavanje ograničavanjem prijetnje i sprečavanjem daljnje štete <i>Primjeri: uklanjanje prijetnji, ograničavanje prijetnje izoliranjem poslužitelja, deaktivacija kompromitiranih korisničkih računa i ponovno postavljanje lozinki</i>
Oporavak 	Vraćanje pogođenih sustava, podataka i usluga u sigurno i operativno stanje <i>Primjeri: ponovna instalacija operativnih sustava na pogođenim poslužiteljima, vraćanje podataka iz sigurnosnih kopija, izvlačenje pouka, ažuriranje politika</i>

Izvor: Sud, na temelju uvodne izjave 78. Direktive (EU) 2022/2555 o mjerama za visoku zajedničku razinu kibersigurnosti (Direktiva NIS 2).

02 Agencija Europske unije za kibersigurnost (ENISA) smatra da je razina kibernetičke prijetnje visoka, napominjući da su takve prijetnje postale znatno složenije i da se taj trend nastavlja³. Takvim prijetnjama naglašava se ključna važnost kibernetičke sigurnosti u sve digitalnijim gospodarstvima i društvima. U [izvješću o prijetnjama](#) iz 2025. ENISA je utvrdila da su ucjenjivački programi najkritičnija prijetnja u EU-u. Na [slici 2.](#) prikazani su ciljani sektori.

³ Izvješće ENISA-e iz 2024. o stanju u području kibernetičke sigurnosti u Uniji.

Slika 2. | Sektori koji su meta kibernetičkih napada



Izvor: Sud, na temelju podataka [ENISA-e](#).

Značajni kibernetički incidenti i kibernetički incidenti velikih razmjera

03 Kibernetički incidenti, koji uključuju kibernetičke prijetnje i nenamjerne događaje (kao što su oni navedeni na [slici 3.](#) i u odlomku [40](#)), „mogu ometati pružanje javnih usluga [i] obavljanje gospodarskih djelatnosti, [...] uzrokovati znatne financijske gubitke, narušiti povjerenje korisnika, nanijeti veliku štetu gospodarstvu i demokratskim sustavima Unije te čak imati zdravstvene ili po život opasne posljedice”⁴. Kibernetički incident smatra se⁵:

- **značajnim** ako je uzrokovao ili bi mogao uzrokovati ozbiljne poremećaje u funkcioniranju usluga ili financijske gubitke za predmetni subjekt ili ako je utjecao ili bi mogao utjecati na druge fizičke ili pravne osobe uzrokovanjem znatne materijalne ili nematerijalne štete;
- **velikih razmjera** ako je uzrokovao razinu poremećaja koja premašuje sposobnost države članice da na njega odgovori ili koji ima znatan učinak na najmanje dvije države članice.

04 Kibernetički incident velikih razmjera može se proširiti i pretvoriti u pravu **kibernetičku krizu EU-a** ako sprečava pravilno funkcioniranje unutarnjeg tržišta ili stvara ozbiljne rizike za javnu sigurnost i zaštitu za subjekte ili građane u nekoliko država članica ili Uniji u cjelini⁶.

⁴ Uvodna izjava 2. Uredbe (EU) 2025/38 ([Akt o kibernetičkoj solidarnosti](#))).

⁵ Članci 6. i 23. [Direktive NIS 2](#), dodatno utvrđeno u [Provedbenoj uredbi Komisije \(EU\) 2024/2690](#) za niz pružatelja usluga u sektoru digitalne infrastrukture.

⁶ Uvodna izjava 69. [Direktive NIS 2](#).

Okvir politike EU-a

- 05** Kibernetički ekosustav EU-a složen je i višeslojan te prožima niz područja unutarnje politike, kao što su pravosuđe i unutarnji poslovi, jedinstveno digitalno tržište i politike istraživanja⁷. U vanjskoj politici, kibernetička sigurnost čini važan element diplomacije i zauzima sve veći dio u obrambenoj politici EU-a koja je u nastajanju⁸.
- 06** Posljednjih je godina EU ojačao svoj regulatorni okvir za kibernetičku sigurnost. Na [slici 3.](#) u nastavku prikazani su najrelevantniji zakonodavni akti i instrumenti politike na razini EU-a. U skladu s opsegom ove revizije (vidjeti odlomke [13](#) – [14](#)) Sud se usredotočio na instrumente koji su povezani s otkrivanjem značajnih kibernetičkih incidenata i kibernetičkih incidenata velikih razmjera te odgovorom na njih.

⁷ Informativni dokument Suda o izazovima u pogledu djelotvornosti kibersigurnosne politike EU-a, str. 12.

⁸ Na primjer, [položaj Europske unije u pogledu kiberprostora \(2022.\)](#), [okvir za koordinirani odgovor EU-a na hibridne kampanje \(2022.\)](#), [politika kiberobrane EU-a \(2023.\)](#) i [izmijenjeni paket instrumenata za kibernetičku diplomaciju \(2023.\)](#).

Slika 3. | Relevantni zakonodavni akti i instrumenti politike na razini EU-a

- Donošenje zakonodavnih akata i instrumenata politike
- Uspostava mreža i struktura



Izvor: Sud.

Uloge i odgovornosti

- 07** U područje kibernetičke sigurnosti u EU-u uključeni su brojni privatni i javni subjekti u civilnoj sferi na regionalnoj i nacionalnoj razini te na razini EU-a, među ostalim tijela zadužena za izvršavanje zakonodavstva. Kibernetička sigurnost ujedno je jedan od ključnih elemenata nacionalne sigurnosti i obrane⁹. U *Prilogu II.* prikazani su akteri koji su trenutačno uključeni u kibernetičku sigurnost u EU-u.
- 08** Države članice snose glavnu odgovornost za sprečavanje bilo kakvih kibernetičkih incidenata i kriza, pripremu za njih i odgovor na krize i incidente koji ih pogađaju. U skladu s *člankom 4. stavkom 2. Ugovora o Europskoj uniji* nacionalna sigurnost ostaje isključiva odgovornost svake države članice. Budući da bi kibernetički incidenti mogli poremetiti i oštetiti ključnu informacijsku infrastrukturu, o kojoj ovisi neometano funkcioniranje unutarnjeg tržišta, EU također ima važnu ulogu u slučaju značajnog incidenta ili krize¹⁰. Glavni subjekti na razini EU-a prikazani su na *slici 4.* u nastavku.

⁹ Mišljenje 02/2023 o Prijedlogu akta o kibernetičkoj solidarnosti.

¹⁰ Plan EU-a za upravljanje kibernetičkim krizama.

Slika 4. | Tijela na razini EU-a koja imaju ključnu ulogu u kibernetičkoj sigurnosti

Sud je ispitao

- **pravni okvir** koji se primjenjuje za otkrivanje značajnih kibernetičkih incidenata i kibernetičkih incidenata velikih razmjera te za odgovor na njih
- **uloge i odgovornosti** mreža i struktura uspostavljenih na razini EU-a

Sud je analizirao

- dokumente o funkcioniranju **mreže CSIRT-ova** i **mreže EU-CyCLONe**
- dokumentaciju o **okviru za izradu programa i praćenje uspješnosti u sklopu programa Digitalna Europa**
- dokumentaciju o **13 odabranih mjera financiranih sredstvima EU-a** (11 dodjela bespovratnih sredstava i dva ugovora – vidjeti detaljan popis u Prilogu III.)

* Sud je odabrao mjere financirane sredstvima EU-a u trima zemljama (Irskoj, Grčkoj i Italiji) u slučaju kojih su relevantna financijska sredstva iz programa Digitalna Europa dosegla značajniji iznos. Navedenih 11 dodjela bespovratnih sredstava odabrano je s popisa 137 projekata financiranih sredstvima EU-a koji su relevantni za otkrivanje prijetnji i odgovor na njih, pri čemu je cilj bio obuhvatiti raznoliku kombinaciju projekata.

Sud je obavio razgovore s

- korisnicima **bespovratnih sredstava EU-a u okviru 11 dodjela obuhvaćenih uzorkom**
- predstavnicima nacionalnih tijela za kibernetičku sigurnost u **trima državama članicama** (Irskoj, Grčkoj i Italiji)
- predstavnicima Europske komisije (**GU-a Connect**), **ENISA-e** i **ECCC-a**

Izvor: Sud.

Financijska sredstva EU-a

- 09** U tekućem višegodišnjem financijskom okviru za razdoblje 2021. – 2027. glavni je izvor financijskih sredstava za kibernetičku sigurnost [program Digitalna Europa \(DIGITAL\)](#). Uveden je 2021. i riječ je o prvom programu EU-a koji je posebno usmjeren na poticanje digitalne transformacije EU-a, s ukupnim proračunom od 8,1 milijarde eura¹¹.
- 10** Mjere u području kibernetičke sigurnosti financiraju se iz tog programa u sklopu njegova specifičnog cilja 3 – kibernetička sigurnost i povjerenje. Konkretnije, riječ je o proračunu od 1,4 milijarde eura koji je predviđen za sljedeće:
- jačanje koordinacije u području kibernetičke sigurnosti između instrumentima i podatkovnom infrastrukturu država članica;
 - podupiranje širokog uvođenja rješenja za kibernetičku sigurnost u cijelom gospodarstvu.
- 11** Većina financijskih sredstava za kibernetičku sigurnost u okviru programa Digitalna Europa pruža se na temelju poziva na podnošenje prijedloga, pri čemu je od studenoga 2021. do prosinca 2025. raspisano 12 takvih poziva. Financijska sredstva EU-a raspoloživa za te pozive iznose 825 milijuna eura. Planiraju se novi pozivi za 2026. i 2027. na temelju kojih bi se trebala dodijeliti dodatna bespovratna sredstva u iznosu od 212 milijuna eura.
- 12** Još je jedan važan program EU-a za potporu kibernetičkoj sigurnosti program [Obzor Europa](#). Projekti kibernetičke sigurnosti uglavnom se financiraju u okviru [klastera 3 – civilna sigurnost za društvo](#) – te su obično u ranoj fazi spremnosti za provedbu zbog usmjerenosti programa Obzor Europa na istraživanje i inovacije. Financijska sredstva za mjere u području kibernetičke sigurnosti pružaju se i iz [Mehanizma za oporavak i otpornost](#).

¹¹ [Program Digitalna Europa](#).

Opseg revizije i revizijski pristup

13 Sve češće kibernetičke prijetnje i njihov mogući učinak istaknuli su potrebu za jačanjem naše kolektivne kibernetičke otpornosti. Cilj ove revizije bio je procijeniti olakšava li se mjerama EU-a na djelotvoran način otkrivanje značajnih kibernetičkih incidenata i kibernetičkih incidenata velikih razmjera te odgovor na takve incidente. Sud je posebno procijenio je li to vrijedilo za sljedeće:

- mreže i mehanizme na razini EU-a (konkretno, mrežu CSIRT-ova, mrežu EU-CyCLONe, europski sustav uzbunjivanja u području kibernetičke sigurnosti, centar za situaciju u kibernetičkom prostoru i pričuvu EU-a za kibernetičku sigurnost);
- mjere financirane iz programa Digitalna Europa.

Sud revizijom nije obuhvatio suradnju u području izvršavanja zakonodavstva na razini EU-a, kao ni radnje za odvrćanje od kibernetičkih napada poduzete na razini EU-a u obliku diplomatskih mjera ili obrambenih aktivnosti.

14 Revizijom je obuhvaćeno razdoblje 2022. – 2025. i ona se temelji na pregledu dokumentacije i analizi relevantnih dokumenata, revizijskim posjetima trima državama članicama (Irskoj, Grčkoj i Italiji) te pisanim upitnicima i razgovorima s dionicima. Na [slici 5.](#) prikazan je način na koji je Sud prikupio dokaze za svoja opažanja.

Slika 5. | Provedene revizijske aktivnosti

Sud je ispitao

- **pravni okvir** koji se primjenjuje za otkrivanje značajnih kibernetičkih incidenata i kibernetičkih incidenata velikih razmjera te za odgovor na njih
- **uloge i odgovornosti** mreža i struktura uspostavljenih na razini EU-a

Sud je analizirao

- dokumente o funkcioniranju **mreže CSIRT-ova** i **mreže EU-CyCLONe**
- dokumentaciju o **okviru za izradu programa i praćenje uspješnosti u sklopu programa Digitalna Europa**
- dokumentaciju o **13 odabranih mjera financiranih sredstvima EU-a** (11 dodjela bespovratnih sredstava i dva ugovora – vidjeti detaljan popis u Prilogu III.)

* Sud je odabrao mjere financirane sredstvima EU-a u trima zemljama (Irskoj, Grčkoj i Italiji) u slučaju kojih su relevantna financijska sredstva iz programa Digitalna Europa dosegala značajniji iznos. Navedenih 11 dodjela bespovratnih sredstava odabrano je s popisa 137 projekata financiranih sredstvima EU-a koji su relevantni za otkrivanje prijetnji i odgovor na njih, pri čemu je cilj bio obuhvatiti raznoliku kombinaciju projekata.

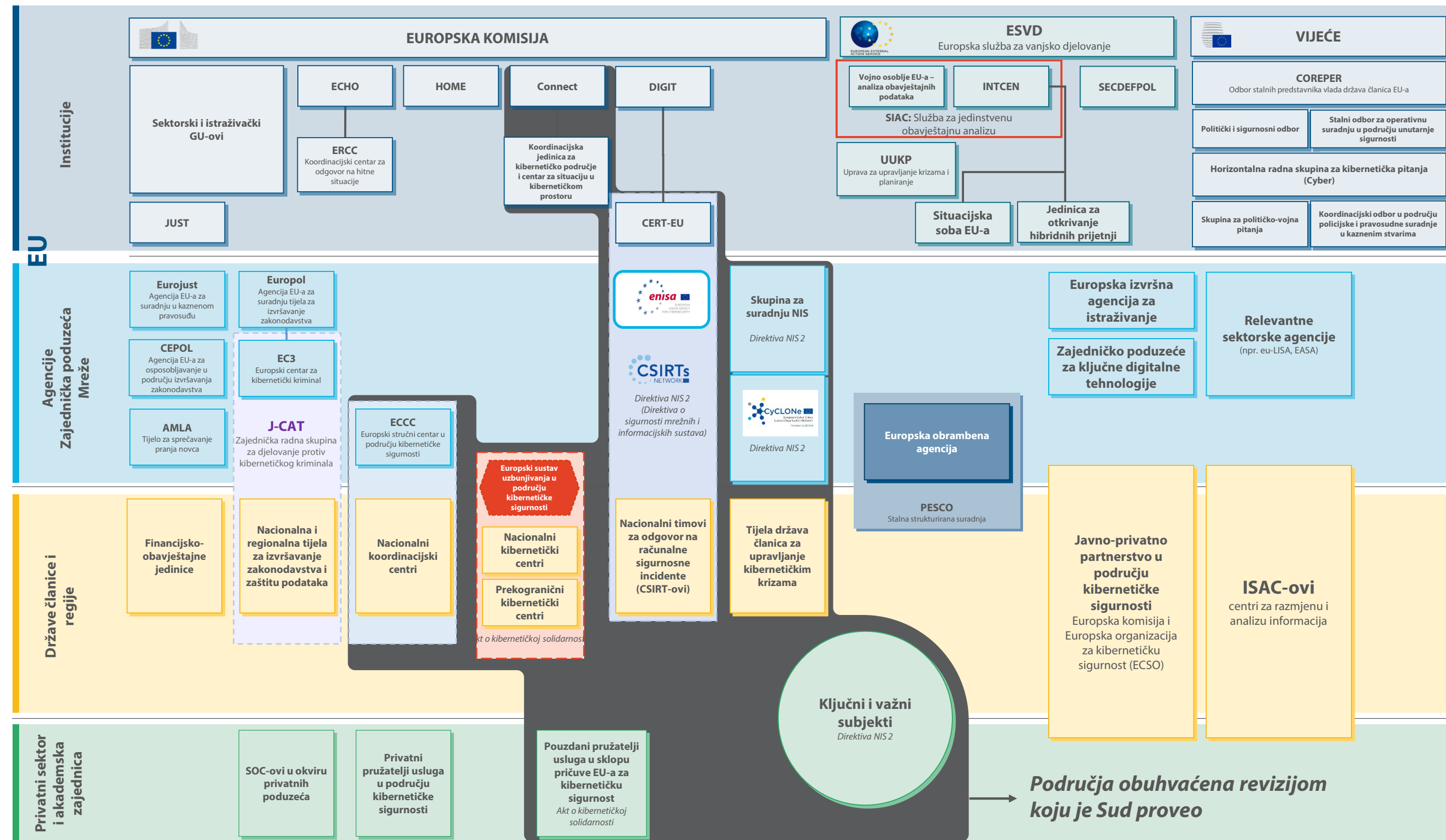
Sud je obavio razgovore s

- korisnicima **bespovratnih sredstava EU-a u okviru 11 dodjela obuhvaćenih uzorkom**
- predstavnicima nacionalnih tijela za kibernetičku sigurnost u **trima državama članicama** (Irskoj, Grčkoj i Italiji)
- predstavnicima Europske komisije (**GU-a Connect**), **ENISA-e** i **ECCC-a**

Izvor: Sud.

- 15** Sud očekuje da će njegovi nalazi doprinijeti povećanju djelotvornosti i učinkovitosti otkrivanja značajnih kibernetičkih incidenata i kibernetičkih incidenata velikih razmjera te odgovora na njih na razini EU-a, kao i poboljšanju načina na koji se odabiru i prate mjere financirane sredstvima EU-a. [Revizijska metodologija](#) Suda u skladu je s međunarodnim revizijskim standardima koje je objavila [Međunarodna organizacija vrhovnih revizijskih institucija \(INTOSAI\)](#).

Prilog II. – Akteri uključeni u kibernetičku sigurnost u EU-u



GU Connect: Glavna uprava za komunikacijske mreže, sadržaje i tehnologije
GU ECHO: Glavna uprava za europsku civilnu zaštitu i europske operacije humanitarne pomoći

GU HOME: Glavna uprava za migracije i unutarnje poslove
GU JUST: Glavna uprava za pravosuđe i zaštitu potrošača
DIGIT: Glavna uprava za digitalne usluge
EASA: Agencija Europske unije za sigurnost zračnog prometa

EU-CyCLONE: Europska mreža organizacija za vezu za kibernetičke krize
eu-LISA: Agencija Europske unije za operativno upravljanje opsežnim informacijskim sustavima u području slobode, sigurnosti i pravde
INTJEN: Obavještajni i situacijski centar Europske unije

SECDEFPOL: sigurnosna i obrambena politika
SOC: centar za sigurnosne operacije

Prilog III. – Odabrane mjere u području kibernetičke sigurnosti

Br.	Naziv	Zemlje	Datum početka	Datum završetka	Ukupni troškovi (u milijunima eura) i doprinos EU-a (u %)	Poveznica na portal EU-a za financiranje i natječaje
Bespovratna sredstva za prekogranične kibernetičke centre koji su dio europskog sustava uzbunjivanja u području kibernetičke sigurnosti						
1	Uspostava prekograničnih centara za sigurnosne operacije (ATHENA)	Bugarska, Grčka, Cipar, Malta	1.1.2024.	31.3.2028.	4,7 (50 %)	
2	PREKOGRANIČNA PLATFORMA ENSOC-a (ENSOC)	Španjolska, Italija, Luksemburg, Nizozemska, Austrija, Portugal, Rumunjska	1.1.2024.	30.6.2028.	10,4 (50 %)	
Bespovratna sredstva za uvođenje mreže nacionalnih koordinacijskih centara u državama članicama						
3	Osmišljavanje i uvođenje nacionalnog centra za koordinaciju i razvoj u području kibernetičke sigurnosti za Irsku (NCC-IE)	Irski	2.10.2023.	1.10.2026.	4,2 (47 %)	
4	Talijanski nacionalni koordinacijski centar (NCC-IT)	Italija	1.11.2023.	31.10.2025.	2,0 (50 %)	
Bespovratna sredstva za izgradnju kapaciteta centara za sigurnosne operacije, promicanje novih primjena umjetne inteligencije i drugih razvojnih tehnologija za centre za sigurnosne operacije te pružanje potpore i uzajamne pomoći u području pripravnosti						
5	Jačanje kapaciteta grčkog konsolidiranog centra za sigurnosne operacije (EL-SOC)	Grčka, Cipar	1.1.2024.	31.12.2026.	9,7 (50 %)	
6	Grčki centar za sigurnosne operacije za mala i srednja poduzeća (GR-SME-SOC)	Grčka	1.1.2024.	31.12.2026.	12,1 (50 %)	

Br.	Naziv	Zemlje	Datum početka	Datum završetka	Ukupni troškovi (u milijunima eura) i doprinos EU-a (u %)	Poveznica na portal EU-a za financiranje i natječaje
7	Centri za sigurnosne operacije sljedeće generacije (NG-SOC)	Grčka, Španjolska, Cipar, Luksemburg, Slovenija, Norveška	1.1.2024.	31.12.2026.	4,8 (50 %)	
8	Irski centar za sigurnosne operacije lokalne uprave (ILG-SOC)	Irska	1.10.2023.	30.9.2026.	8,3 (50 %)	
9	Međusobno povezani ekosustav mreža za koordinaciju i odgovor u području kibernetičke sigurnosti (mreža Cyber-CORE)	Irska	1.1.2024.	31.12.2026.	3,6 (50 %)	
10	Usklađivanje ljudskih resursa, procesa i tehnologije za otpornu kibernetičku sigurnost (CYberSynchrony)	Belgija, Grčka, Italija, Cipar, Nizozemska	1.6.2024.	31.5.2027.	7,0 (100 %)	
11	Napredni suradnički centri za sigurnosne operacije (ACSOC)	Grčka, Italija, Rumunjska	1.1.2025.	31.12.2027.	3,0 (50 %)	
Okvirni ugovor za ENISA-ino djelovanje za potporu kibernetičkoj sigurnosti						
12	Potpora ENISA-i za pružanje usluga u okviru djelovanja za potporu kibernetičkoj sigurnosti (28 grupa)	27 grupa za države članice 1 paneuropska grupa	1.12.2022. ¹	31.12.2025.	28,3 (100 %)	
Ugovor o uslugama za centar za situaciju u kibernetičkom prostoru u sklopu GU-a Connect						
13	Prilagođene usluge za potporu centru za situaciju i analizu u kibernetičkom prostoru za Europsku komisiju	—	30.12.2022.	30.12.2026.	18,0 (100 %)	

Izvor: Sud.

¹ Niz ugovora sklopljen je tijekom prosinca 2022.

Prilog IV. – Procjena projekata u području kibernetičke sigurnosti financiranih sredstvima EU-a koju je proveo Sud

		Projektom se uzima u obzir većina potreba utvrđenih u pozivu na podnošenje prijedloga	Projektom su dosad postignuta planirana ostvarenja i rezultati	Ostvarenja projekta postignuta su u zadanom roku	Pokazatelji uspješnosti projekata relevantni su i mjerljivi te su za njih utvrđene polazne i ciljne vrijednosti
Zadovoljavajuće Nezadovoljavajuće Određeni nedostaci Nije moguće donijeti zaključak (prerano za ocjenu)					
Br.	Projekt				
1	Uspostava prekograničnih centara za sigurnosne operacije (ATHENA)				
2	PREKOGRAFIČNA PLATFORMA ENSOC-a (ENSOC)				
3	Osmišljavanje i uvođenje nacionalnog centra za koordinaciju i razvoj u području kibernetičke sigurnosti za Irsku (NCC-IE)				
4	Talijanski nacionalni koordinacijski centar (NCC-IT)				
5	Jačanje kapaciteta grčkog konsolidiranog centra za sigurnosne operacije (EL-SOC)				
6	Grčki centar za sigurnosne operacije za mala i srednja poduzeća (GR-SME-SOC)				
7	Centri za sigurnosne operacije sljedeće generacije (NG-SOC)				
8	Irski centar za sigurnosne operacije lokalne uprave (ILG-SOC)				
9	Međusobno povezani ekosustav mreža za koordinaciju i odgovor u području kibernetičke sigurnosti (mreža Cyber-CORE)				
10	Usklađivanje ljudskih resursa, procesa i tehnologije za otpornu kibernetičku sigurnost (CYberSynchrony)				
11	Napredni suradnički centri za sigurnosne operacije (ACSOC)				

Pokrate i skraćeni nazivi

Pokrata ili skraćeni naziv	Definicija/objašnjenje
CSIRT	Tim za odgovor na računalne sigurnosne incidente
DIGITAL	Program Digitalna Europa
ECCC	Europski stručni centar u području kibernetičke sigurnosti
ENISA	Agencija Europske unije za kibersigurnost
EU-CyCLONe	Europska mreža organizacija za vezu za kibernetičke krize
GU Connect	Glavna uprava za komunikacijske mreže, sadržaje i tehnologije
MSP	Mala i srednja poduzeća
NIS	Mrežna i informacijska sigurnost
SOC	Centar za sigurnosne operacije

Pojmovnik

Pojam	Definicija/objašnjenje
Akter prijetnje	Pojedinac ili skupina koja namjerno uzrokuje štetu, ometa usluge ili krađe podatke iskorištavanjem slabih točaka u IT sustavima, mrežama i uređajima.
Centar za sigurnosne operacije	Organizacijska jedinica koja radi na sprečavanju kibernetičkih prijetnji i kibernetičkih incidenata te prikuplja povezane obavještajne podatke.
Kibernetička prijetnja (kiberprijetnja)	Potencijalna upotreba kibernetičkog prostora kako bi se ugrozili dostupnost, autentičnost, integritet ili povjerljivost podatkovnih ili informacijskih sustava.
Kibernetički centar	Središnja platforma koja objedinjuje razne usluge, alate i stručnjake u području IT-a radi poboljšanja praćenja, otkrivanja i analiziranja kibernetičkih prijetnji, sprečavanja kibernetičkih incidenata i pružanja potpore izradi obavještajnih podataka o kibernetičkim prijetnjama.
Kibernetički incident	Događaj kojim se ugrožava dostupnost, autentičnost, integritet ili povjerljivost podatkovnih ili informacijskih sustava.
Kibernetički incident velikih razmjera	Kibernetički incident koji je toliko razoran da ga jedna država članica ne može razriješiti sama ili koji ima znatan učinak na najmanje dvije države članice.
Taksonomija	U kontekstu kibernetičke sigurnosti klasifikacijski sustav koji se upotrebljava za organizaciju, kategorizaciju i strukturiranje znanja o ključnim konceptima kao što su prijetnje i incidenti.
Ucjenjivački program (engl. ransomware)	Zlonamjerni program koji žrtvama onemogućuje pristup računalnom sustavu ili koji šifrira datoteke kako se ne bi mogle otvarati te obično prisiljava žrtve da plate otkupninu za ponovno stjecanje pristupa.
Značajan kibernetički incident	Kibernetički incident zbog kojeg je došlo ili može doći do ozbiljnog poremećaja ili financijskog gubitka za određenu organizaciju ili znatne štete za druge subjekte ili pojedince.

Odgovori Komisije

<https://www.eca.europa.eu/hr/publications/SR-2026-19>

Odgovori Europskog stručnog centra za industriju, tehnologiju i istraživanja u području kibersigurnosti (ECCC)

<https://www.eca.europa.eu/hr/publications/SR-2026-19>

Odgovori Agencije Europske unije za kibersigurnost (ENISA)

<https://www.eca.europa.eu/hr/publications/SR-2026-19>

Kronologija

<https://www.eca.europa.eu/hr/publications/SR-2026-19>

Revizorski tim

U tematskim izvješćima Suda iznose se rezultati revizija koje su provedene za politike i programe EU-a ili teme povezane s upravljanjem u posebnim proračunskim područjima. U odabiru i oblikovanju takvih revizijskih zadataka Sud nastoji postići što veći učinak uzimajući u obzir rizike za uspješnost ili usklađenost, vrijednost predmetnih prihoda ili rashoda, predstojeće razvojne promjene te politički i javni interes.

Ovu reviziju uspješnosti provelo je III. revizijsko vijeće, kojim predsjedava član Suda George-Marius Hyzler i koje je specijalizirano za rashodovna područja vanjskog djelovanja, sigurnosti i pravosuđa. Reviziju je predvodio član Suda George-Marius Hyzler, a potporu su mu pružali voditelj njegova ureda Romuald Kayibanda, ataše u njegovu uredu Annette Farrugia, rukovoditelj Cyril Messein, voditelj radnog zadatka Frédéric Soblet te revizori Jurgen Manjé i Flavia Di Marco. Jezičnu podršku pružala je Zoe Amador Martínez. Grafičku podršku pružala je Dunja Weibel.



Slijeva nadesno: Frédéric Soblet, Romuald Kayibanda, George-Marius Hyzler, Jurgen Manjé, Cyril Messein.

AUTORSKA PRAVA

© Europska unija, 2026.

Politika Europskog revizorskog suda (Sud) o ponovnoj uporabi sadržaja utvrđena je u [Odluci Suda br. 6-2019](#) o politici otvorenih podataka i ponovnoj uporabi dokumenata.

Osim ako je drukčije navedeno (npr. u pojedinačnim napomenama o autorskim pravima), sadržaj Suda koji je u vlasništvu EU-a ima dozvolu [Creative Commons Attribution 4.0 International \(CC BY 4.0\)](#). Stoga je opće pravilo da je ponovna uporaba dopuštena pod uvjetom da se na odgovarajući način navede izvor i naznače eventualne promjene. Osoba koja ponovno upotrebljava sadržaj Suda ne smije izmijeniti izvorno značenje ili poruku. Sud ne snosi odgovornost za posljedice ponovne uporabe.

Ako određeni sadržaj prikazuje osobe čiji je identitet moguće utvrditi, npr. u slučaju fotografija koje prikazuju osoblje Suda, ili ako uključuje djela trećih strana, potrebno je zatražiti dodatno dopuštenje.

U slučaju dobivanja takvog dopuštenja njime se poništava i zamjenjuje prethodno opisano opće dopuštenje i jasno se navode sva ograničenja koja se primjenjuju na uporabu tog sadržaja.

Za uporabu ili reprodukciju sadržaja koji nije u vlasništvu EU-a dopuštenje se po potrebi mora zatražiti izravno od nositelja autorskih prava.

Fotografija na naslovnoj stranici: © 4AXY – stock.adobe.com.

Ikone na slici 6. i slici 8.: izrađeno s pomoću alata dostupnih na stranici [Flaticon.com](#).

© Freepik Company S.L. Sva prava pridržana.

Zemljovid na slici 5.: [Eurostat](#).

Softver ili dokumenti na koje se primjenjuju prava industrijskog vlasništva, kao što su patenti, žigovi, registrirani dizajn, logotipi i nazivi, nisu obuhvaćeni politikom Suda o ponovnoj uporabi sadržaja.

Na internetskim stranicama institucija Europske unije unutar domene europa.eu dostupne su poveznice na internetske stranice trećih strana. Sud nema nikakvu kontrolu nad njihovim sadržajem te je stoga preporučljivo da provjerite njihove politike zaštite osobnih podataka i autorskih prava.

Upotreba logotipa Suda

Logotip Suda ne smije se upotrebljavati bez prethodne suglasnosti Suda.

HTML	ISBN 978-92-849-7871-7	ISSN 2315-2230	doi:10.2865/8756828	QJ-01-26-032-HR-Q
PDF	ISBN 978-92-849-7872-4	ISSN 2315-2230	doi:10.2865/5605188	QJ-01-26-032-HR-N

KAKO UPUĆIVATI

Europski revizorski sud, [tematsko izvješće 19/2026](#) „Otkrivanje kibernetičkih incidenata i odgovor na njih – Ostvaruje se napredak u pogledu okvira EU-a za suradnju, ali zbog kašnjenja u provedbi i ograničene razmjene informacija taj je okvir samo djelomično djelotvoran”, Ured za publikacije Europske unije, 2026.

EU je posljednjih godina ojačao svoj regulatorni okvir za kibernetičku sigurnost te je uspostavio mreže i mehanizme za odgovor na kibernetičke incidente. Projekti u području kibernetičke sigurnosti financiraju se i sredstvima EU-a iz programa Digitalna Europa.

Sud zaključuje da se mjerama EU-a samo djelomično olakšava otkrivanje značajnih kibernetičkih incidenata i kibernetičkih incidenata velikih razmjera te odgovor na njih. Iako se okvir za suradnju postupno uspostavlja, rad na njegovu potpunom dovršetku i dalje je u tijeku. Zbog ograničene razmjene informacija, nedostataka u izvješćivanju i znatnih kašnjenja u provedbi nije moguće iskoristiti puni potencijal mreža i mehanizama EU-a. Projektima se nastoje ostvariti relevantni ciljevi, ali u nizu njih pojavljuju se operativni izazovi i kašnjenja. Osim toga, postoje nedostaci u općem okviru za praćenje uspješnosti. Sud iznosi preporuke za uklanjanje tih nedostataka.

Tematsko izvješće Suda u skladu s člankom 287. stavkom 4. drugim podstavkom UFEU-a.



EUROPSKI
REVIZORSKI
SUD



Ured za publikacije
Europske unije

EUROPSKI REVIZORSKI SUD
12, rue Alcide De Gasperi
1615 Luxembourg
LUKSEMBURG

Tel.: +352 4398-1

Upiti: eca.europa.eu/hr/contact
Internetske stranice: eca.europa.eu
Društvene mreže: @EUauditors