SL 2022 05

Posebno poročilo

Kibernetska varnost institucij, organov in agencij EU

Raven pripravljenosti na splošno ni sorazmerna z grožnjami

EVROPSKO RAČUNSKO SODIŠČE

Vsebina

Povzetek

I V uredbi EU o kibernetski varnosti je kibernetska varnost opredeljena kot „dejavnosti, ki so potrebne za zaščito omrežij in informacijskih sistemov, uporabnikov takih sistemov in drugih oseb, na katere vplivajo kibernetske grožnje”. Institucije, organi in agencije EU so zaradi občutljivih informacij, ki jih obdelujejo, privlačne tarče morebitnih napadalcev, zlasti skupin, ki so sposobne izvajati visoko izpopolnjene prikrite napade za namene kibernetskega vohunjenja in druge namene. Institucije, organi in agencije EU so kljub svoji institucionalni neodvisnosti in upravni avtonomiji med sabo tesno povezani. Zato bi bili lahko zaradi slabosti v posamezni instituciji, organu ali agenciji EU varnostnim grožnjam izpostavljeni tudi drugi.

II Ker število kibernetskih napadov na institucije, organe in agencije EU močno narašča, je bil cilj te revizije ugotoviti, ali so institucije, organi in agencije EU kot celota vzpostavili ustrezne ureditve, da bi se zaščitili pred kibernetskimi grožnjami. Sodišče je prišlo do zaključka, da skupnost institucij, organov in agencij EU ni dosegla takšne ravni pripravljenosti na področju kibernetske varnosti, ki bi bila sorazmerna z grožnjami.

III Sodišče ugotavlja, da se ključne dobre prakse na področju kibernetske varnosti, vključno z nekaterimi bistvenimi kontrolami, niso vedno izvajale in da je več institucij, organov in agencij EU očitno namenilo premalo sredstev za kibernetsko varnost. Poleg tega v nekaterih institucijah, organih in agencijah EU še ni vzpostavljeno dobro upravljanje kibernetske varnosti: pogosto primanjkuje strategij za varnost IT ali pa teh ne potrdi višje vodstvo, varnostne politike niso vedno formalizirane, ocene tveganja pa ne zajemajo celotnega okolja IT. Vse institucije, organi in agencije EU ne pridobijo redno neodvisnega zagotovila za kibernetsko varnost.

IV Usposabljanje na področju kibernetske varnosti ni vedno sistematično. Nekaj več kot polovica institucij, organov in agencij EU zagotavlja stalno usposabljanje na področju kibernetske varnosti za osebje za IT in strokovnjake za varnost IT. Malo institucij, organov in agencij EU zagotavlja obvezno usposabljanje na področju kibernetske varnosti za vodilne uslužbence, odgovorne za sisteme IT, ki vsebujejo občutljive informacije. Vaje z uporabo lažnega predstavlja so pomembno orodje za usposabljanje osebja in ozaveščanje, vendar jih vse institucije, organi in agencije EU ne uporabljajo sistematično.

V Institucije, organi in agencije EU so sicer vzpostavili strukture za sodelovanje in izmenjavo informacij o kibernetski varnosti, vendar je Sodišče ugotovilo, da potencialne sinergije niso v celoti izkoriščene. Institucije, organi in agencije EU si ne izmenjujejo sistematično informacij o projektih, povezanih s kibernetsko varnostjo, ocenah varnosti in pogodbah o storitvah. Poleg tega osnovna komunikacijska orodja, kot sta šifrirana elektronska pošta ali videokonferenca, niso popolnoma interoperabilna. Zaradi tega lahko pride do manj varne izmenjave informacij, podvajanja prizadevanj in višjih stroškov.

VI Skupina za odzivanje na računalniške grožnje za evropske institucije, organe in agencije (CERT-EU) in Agencija Evropske unije za kibernetsko varnost (ENISA) sta glavna subjekta, zadolžena za podpiranje institucij, organov in agencij EU na področju kibernetske varnosti. Ker pa so njuni viri omejeni in ker se prednost daje drugim področjem, institucijam, organom in agencijam EU nista mogla zagotoviti vse potrebne podpore, zlasti v zvezi s krepitvijo zmogljivosti tistih, ki so manj zrele. Institucije, organi in agencije EU sicer zelo cenijo skupino CERT-EU, vendar na njeno uspešnost vplivajo vse večja delovna obremenitev, nestabilno financiranje in zaposlovanje ter nezadostno sodelovanje nekaterih institucij, organov in agencij EU, ki ne posredujejo vedno pravočasno informacij o šibkih točkah in pomembnih kibernetskih incidentih, ki so vplivali nanje ali bi lahko vplivali na druge.

VII Sodišče na podlagi teh zaključkov priporoča:

- naj Komisija izboljša kibernetsko pripravljenost institucij, organov in agencij EU, in sicer z zakonodajnim predlogom za uvedbo skupnih zavezujočih pravil o kibernetski varnosti za vse institucije, organe in agencije EU ter povečanje virov za skupino CERT-EU,

- naj Komisija v okviru medinstitucionalnega odbora za digitalno preobrazbo spodbuja nadaljnje sinergije med institucijami, organi in agencijami EU na izbranih področjih,

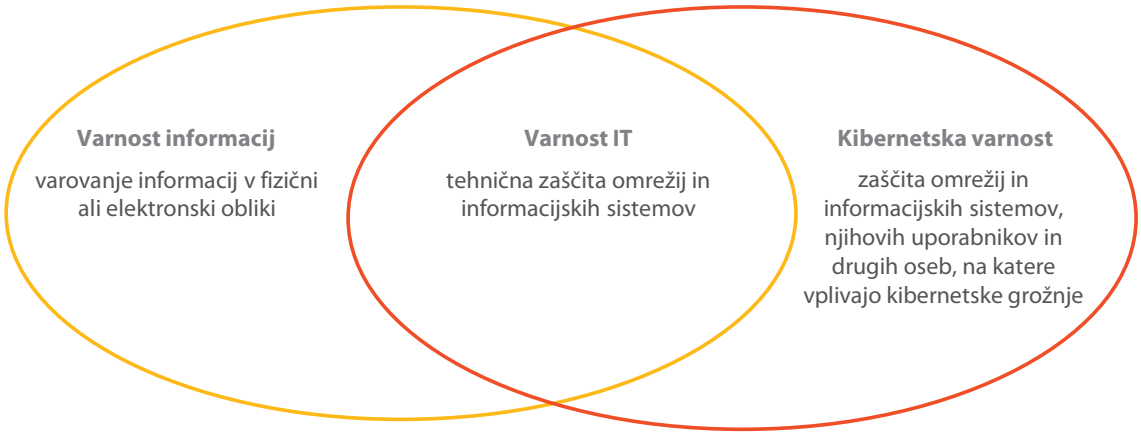
- naj se skupina CERT-EU in agencija ENISA bolj osredotočita na institucije, organe in agencije EU, ki so manj zrele na področju kibernetske varnosti,

Uvod

Kaj je kibernetska varnost?

01 V uredbi o kibernetski varnosti[1] je kibernetska varnost opredeljena kot „dejavnosti, ki so potrebne za zaščito omrežij in informacijskih sistemov, uporabnikov takih sistemov in drugih oseb, na katere vplivajo kibernetske grožnje”. Kibernetska varnost temelji na varnosti informacij, tj. ohranjanju zaupnosti, celovitosti in razpoložljivosti informacij[2] v fizični ali elektronski obliki. Zaščita omrežij in informacijskih sistemov, v katerih se take informacije hranijo, se imenuje varnost informacijske tehnologije (IT) (glej ***sliko 1***).

Slika 1 – Kibernetska varnost je povezana z varnostjo informacij in IT



Vir: Evropsko računsko sodišče

02 Kibernetska varnost kot disciplina obsega opredeljevanje, preprečevanje in odkrivanje kibernetskih incidentov ter odzivanje nanje in ponovno vzpostavitev prejšnjega stanja. Incidenti lahko zajemajo vse od na primer nenamernega razkritja informacij do napadov, katerih cilj je ogroziti kritično infrastrukturo, in kraje identitete in osebnih podatkov[3].

---

[1] Uredba (EU) 2019/881.

[2] ISO/IEC 27000:2018.

[3] Sodišče, Pregled št. 2/2019: Izzivi za uspešno politiko EU za kibernetsko varnost (informativni dokument).

03 Okvir za kibernetsko varnost zajema številne elemente, vključno z zahtevami in tehničnimi kontrolami za varnost omrežij in informacijskih sistemov ter ustreznimi ureditvami upravljanja in programi ozaveščanja o kibernetski varnosti za uslužbence.

Kibernetska varnost institucij, organov in agencij EU

04 Institucije, organi in agencije EU so zaradi občutljivih informacij, ki jih obdelujejo, privlačne tarče morebitnih napadalcev, zlasti skupin, ki so sposobne izvajati visoko izpopolnjene prikrite napade („napredne trajne grožnje”) za namene kibernetskega vohunjenja in druge namene[4]. Uspešni kibernetski napadi na institucije, organe in agencije EU imajo lahko znatne politične posledice ter lahko škodujejo splošnemu ugledu EU in spodkopavajo zaupanje v njene institucije.

05 Zaradi pandemije COVID-19 so morali institucije, organi in agencije EU tako kot druge organizacije po vsem svetu nenadoma pospešiti digitalno preobrazbo in preiti na delo na daljavo. To je znatno povečalo število možnih točk dostopa za napadalce („napadno površino”), saj se je obseg vsake organizacije razširil na domove in mobilne naprave, povezane z internetom, z novimi šibkimi točkami, ki jih je mogoče izkoristiti. Storitve dostopa na daljavo so ena od najpogostejših poti, prek katerih skupine, katerih cilj so institucije, organi in agencije EU, z naprednimi trajnimi grožnjami pridobijo začetni dostop do omrežij teh organizacij[5].

06 Število kibernetskih incidentov narašča. Posebej zaskrbljujoč trend je drastično povečanje števila pomembnih incidentov, ki vplivajo na institucije, organe in agencije EU[6], zaradi česar je bilo leto 2021 rekordno. Pomembni incidenti so incidenti, ki niso niti ponavljajoči se niti osnovni. Običajno vključujejo uporabo novih metod in tehnologij in lahko traja več tednov, če ne več mesecev, da se raziščejo in da se ponovno vzpostavi prejšnje stanje. Med letoma 2018 in 2021 se je število pomembnih incidentov povečalo za več kot desetkrat[7]. Samo v zadnjih dveh letih so bili pomembni incidenti zaznani pri vsaj 22 posameznih institucijah, organih in agencijah EU. Nedaven

---

[4] CERT-EU, *Threat Landscape Report*, junij 2021.

[5] Prav tam.

[6] Prav tam.

[7] Prav tam.

primer je kibernetski napad na Evropsko agencijo za zdravila, pri katerem so bili občutljivi podatki razkriti in manipulirani tako, da bi spodkopali zaupanje v cepiva[8].

07 Institucije in agencije EU ter številni različni organi EU so zelo heterogena skupina. Sedem institucij EU je bilo ustanovljenih s Pogodbama. Decentralizirane agencije in drugi organi EU pa so ustanovljeni z akti sekundarne zakonodaje. Vsak od njih je ločen pravni subjekt. Obstajajo različne pravne oblike agencij: šest izvajalskih agencij Komisije in 37 decentraliziranih agencij EU[9]. Institucije, organi in agencije EU zajemajo tudi urade, diplomatski zbor (Evropska služba za zunanje delovanje), skupna podjetja in druge organe EU. Institucije, organi in agencije EU so sami odgovorni za opredelitev lastnih zahtev glede kibernetske varnosti in izvajanje lastnih varnostnih ukrepov.

08 Komisija je za okrepitev kibernetske varnosti institucij, organov in agencij EU leta 2012 ustanovila skupino za odzivanje na računalniške grožnje za evropske institucije, organe in agencije (CERT-EU) kot stalno projektno skupino. Skupina CERT-EU deluje kot koordinacijsko središče za izmenjavo informacij o kibernetski varnosti in za odzivanje na incidente, namenjeno institucijam, organom in agencijam EU, ter sodeluje z drugimi skupinami za odzivanje na incidente na področju računalniške varnosti (CSIRT) v državah članicah in specializiranimi podjetji za varnost IT. Organizacija in delovanje skupine CERT-EU sta trenutno določena v medinstitucionalnem dogovoru iz leta 2018[10], sklenjenem med institucijami, organi in agencijami EU, ki jim skupina CERT-EU zagotavlja storitve in so imenovani tudi „udeleženci”. Trenutno je 87 udeležencev.

09 Drug ključni akter, ki podpira institucije, organe in agencije EU, je Agencija Evropske unije za kibernetsko varnost (ENISA), ki si prizadeva doseči visoko skupno raven kibernetske varnosti po vsej EU. Naloga agencije ENISA, ki je bila ustanovljena leta 2004, je povečati verodostojnost izdelkov, procesov in storitev informacijske in komunikacijske tehnologije (IKT) s certifikacijskimi shemami za kibernetsko varnost, sodelovati z institucijami, organi in agencijami EU in državami članicami ter jim pomagati pri tem, da se pripravijo na kibernetske grožnje. Agencija ENISA pomaga institucijam, organom in agencijam EU pri krepitvi zmogljivosti in operativnem sodelovanju.

---

[8] *Cyberattack on EMA – update 6*, 25. januar 2021.

[9] Posebno poročilo Sodišča št. 22/2020 – Prihodnost agencij EU: potencial za več fleksibilnosti in sodelovanja, odstavek 01.

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

10 Ti so kljub svoji institucionalni neodvisnosti med seboj močno povezani. Vsak dan si izmenjujejo informacije, delijo pa si tudi več skupnih sistemov in omrežij. Zaradi slabosti v posameznih institucijah, organih in agencijah EU bi bili lahko tudi drugi izpostavljeni varnostnim grožnjam, saj je pri številnih kibernetskih napadih za dosego cilja ali končnega cilja potreben več kot en korak[11]. Uspešen napad na šibkejšo institucijo, organ ali agencijo EU se lahko uporabi kot odskočna deska za napad na druge. Institucije, organi in agencije EU so povezani tudi z javnimi in zasebnimi organizacijami v državah članicah in jih lahko zaradi svoje nezadostne kibernetske pripravljenosti prav tako izpostavijo kibernetskim grožnjam.

11 Trenutno ni pravnega okvira za informacijsko in kibernetsko varnost v institucijah, organih in agencijah EU. Zanje namreč ne velja najširša zakonodaja EU o kibernetski varnosti, tj. niti direktiva o varnosti omrežij in informacij[12] iz leta 2016 niti predlog za njeno spremembo, tj. revidirana direktiva o varnosti omrežij in informacij[13]. Prav tako ni izčrpnih informacij o sredstvih, ki so jih institucije, organi in agencije EU porabili za kibernetsko varnost.

12 Komisija je julija 2020 objavila sporočilo o strategiji EU za varnostno unijo[14] za obdobje 2020–2025. Njeni ključni ukrepi vključujejo „skupna pravila o informacijski in kibernetski varnosti za vse institucije, organe in agencije EU”. Namen tega novega okvira je podpreti močno in učinkovito operativno sodelovanje s poudarkom na vlogi skupine CERT-EU. Komisija se je v strategiji EU za kibernetsko varnost v digitalnem desetletju[15], objavljeni decembra 2020, zavezala, da bo predlagala uredbo o skupnih pravilih o kibernetski varnosti za vse institucije, organe in agencije EU. Predlagala je tudi vzpostavitev nove pravne podlage za okrepitev pooblastil in financiranja skupine CERT-EU.

---

[11] ENISA, *Threat Landscape 2020*, *Sectoral/thematic threat analysis*.

[12] Direktiva (EU) 2016/1148 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji.

[13] Predlog direktive o ukrepih za visoko skupno raven kibernetske varnosti v Uniji.

[14] COM(2020) 605 final.

[15] JOIN(2020) 18 final.

Obseg revizije in revizijski pristop

13 Ker število kibernetskih napadov močno narašča in ker so lahko zaradi slabosti v eni instituciji, organu ali agenciji EU varnostnim grožnjam izpostavljeni tudi drugi, je bil cilj te revizije ugotoviti, ali so te organizacije kot celota vzpostavile ustrezne ureditve, da bi se zaščitile pred kibernetskimi grožnjami. Da bi lahko Sodišče odgovorilo na to glavno revizijsko vprašanje, je obravnavalo tri podvprašanja:

(1) Ali so vse institucije, organi in agencije EU sprejeli ključne prakse na področju kibernetske varnosti?

(2) Ali institucije, organi in agencije EU učinkovito sodelujejo med seboj na področju kibernetske varnosti?

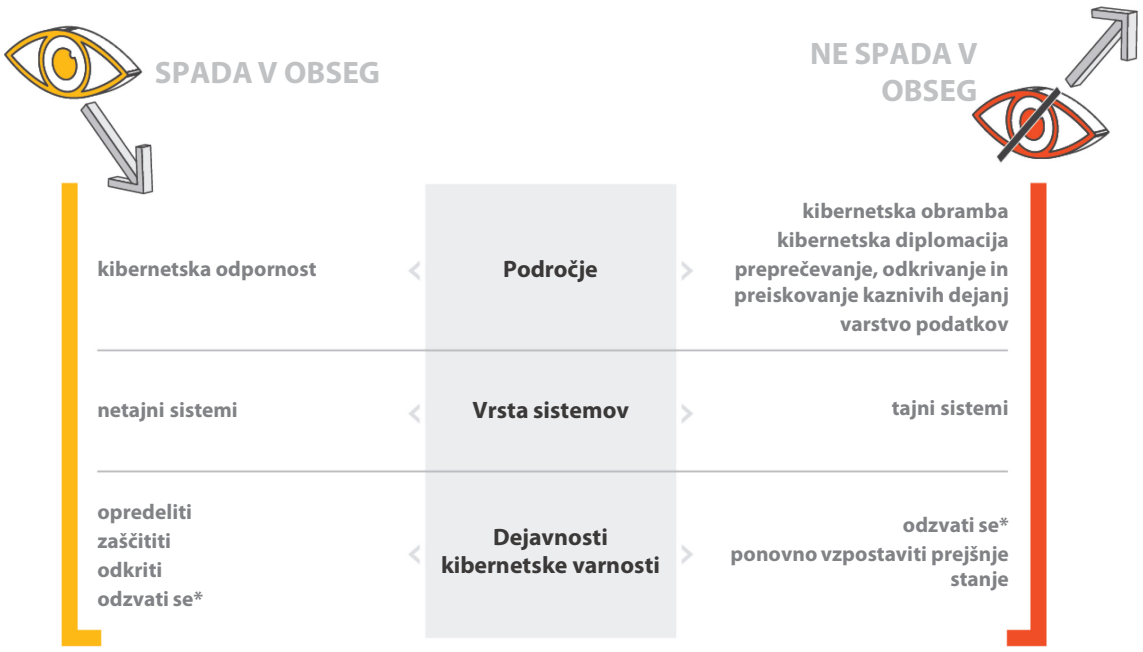
(3) Ali agencija ENISA in skupina CERT-EU institucijam, organom in agencijam EU zagotavljata ustrezno podporo na področju kibernetske varnosti?

14 Časovni razpored revizije je usklajen s strategijo EU za varnostno unijo. Sodišče želi z oceno sedanjih ureditev institucij, organov in agencij EU na področju kibernetske varnosti opredeliti področja, na katerih so potrebne izboljšave in ki jih lahko Komisija upošteva pri pripravi zakonodajnega predloga za skupna zavezujoča pravila o kibernetski varnosti za vse institucije, organe in agencije EU.

15 Revizija je zajela razvoj dogodkov in pobude na področju kibernetske varnosti od januarja 2018 (ko je bil sklenjen medinstitucionalni dogovor skupine CERT-EU) do oktobra 2021.

16 Sodišče je obseg revizije omejilo na kibernetsko odpornost in netajne sisteme. Osredotočilo se je na vidike pripravljenosti (dejavnosti, ki ustrezajo pojmom „opredeliti, zaščititi, odkriti”). Dejavnosti, ki ustrezajo pojmoma „odzvati se” in „ponovno vzpostaviti prejšnje stanje”, niso bile zajete v obseg revizije, vendar pa je Sodišče preučilo nekatere organizacijske elemente odzivanja na incidente. Obseg revizije prav tako ni zajemal vidikov varstva podatkov, preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, kibernetske obrambe in kibernetske diplomacije (glej ***sliko 2***).

Slika 2 – Obseg revizije



** Sodišče je preučilo le nekatere organizacijske vidike odzivanja na incidente. Drugi vidiki niso spadali v obseg revizije.*

Vir: Evropsko računsko sodišče

17 Revizijske ugotovitve Sodišča temeljijo na obsežni analizi razpoložljive dokumentacije, dopolnjeni z razgovori. Sodišče je izvedlo anketo v obliki samoocene, v katero je vključilo 65 institucij, organov in agencij EU, da bi zbralo informacije o njihovih ureditvah na področju kibernetske varnosti in njihova mnenja o medinstitucionalnem sodelovanju. Anketiralo je vse institucije, organe in agencije EU, ki spadajo v obseg njegovih revizijskih pravic in upravljajo lastno infrastrukturo IT, pa tudi samo Sodišče. Med njimi so bili institucije, decentralizirane agencije, skupna podjetja in organi. Sodišče je anketiralo tudi civilne misije, ki so začasni avtonomni subjekti, ki se financirajo iz proračuna EU in so neodvisni z vidika IT. V ***Prilogi I*** je celoten seznam anketiranih institucij, organov in agencij EU. Evropski varuh človekovih pravic in Evropski nadzornik za varstvo podatkov nista bila vključena v obseg te revizije.

18 Anketa je imela 100-odstotno stopnjo odziva in je bila izhodišče za nadaljnjo analizo. Poleg tega je Sodišče izbralo vzorec sedmih institucij, organov in agencij EU, ki je reprezentativen za njihovo heterogenost, ter na podlagi njihovih odgovorov opravilo še razgovore in zahtevalo dokumentacijo. Merila za izbor, ki jih je upoštevalo, so vključevala pravno podlago, velikost (v smislu uslužbencev in proračuna) in sektor. Vzorec institucij, organov in agencij EU so sestavljali Evropska komisija, Evropski parlament, Agencija EU za kibernetsko varnost (ENISA), Evropski bančni organ (EBA), Evropska agencija za pomorsko varnost (EMSA), svetovalna misija EU v Ukrajini (EUAM Ukraine) in Skupno podjetje za pobudo za inovativna zdravila (Skupno podjetje IMI).

19 Sodišče je organiziralo tudi videokonference s skupino CERT-EU, svetovalnim odborom mreže agencij za informacijsko in komunikacijsko tehnologijo (ICTAC), medinstitucionalnim odborom za digitalno preobrazbo (ICDT) in drugimi ustreznimi deležniki.

Opažanja

Institucije, organi in agencije EU imajo zelo različne ravni zrelosti na področju kibernetske varnosti in ne upoštevajo vedno dobre prakse

20 V tem delu so preučeni posamezne ureditve in okviri institucij, organov in agencij EU na področju kibernetske varnosti. Sodišče je ocenilo, ali je njihov pristop do kibernetske varnosti dosleden in ustrezen, in sicer glede upravljanja varnosti IT, obvladovanja tveganja, dodeljevanja virov, usposabljanja za ozaveščanje, kontrol in neodvisnega zagotovila.

Upravljanje varnosti IT v institucijah, organih in agencijah EU pogosto ni dobro razvito, ocene tveganja pa niso celovite

V več institucijah, organih in agencijah EU obstajajo vrzeli v upravljanju varnosti IT

21 Dobro upravljanje ima pomembno vlogo v uspešnem okviru za varnost informacij in sistemov IT. Z določanjem prioritet in sprejemanjem odločitev se namreč opredeljujejo cilji in usmeritev organizacije. Po mnenju Združenja za revizijo in kontrolo informacijskih sistemov (ISACA)[16] bi moral okvir za upravljanje varnosti IT na splošno vključevati več elementov:

- celovito varnostno strategijo, ki je neločljivo povezana s poslovnimi cilji,
- upravljanje varnostnih politik, ki obravnavajo vsak vidik strategije, nadzora in ureditve,
- celoten sklop standardov za vsako politiko, ki opisuje operativne korake, potrebne za uskladitev s politiko,
- institucionalizirane postopke spremljanja za zagotovitev izpolnjevanja zahtev in povratnih informacij o uspešnosti,
- uspešno organizacijsko strukturo brez navzkrižja interesov.

[16] ISACA, *Certified Information System Auditor Review Manual*, 2019.

22 Sodišče je v več institucijah, organih in agencijah EU odkrilo pomanjkljivosti v upravljanju varnosti IT. Samo 58 % institucij, organov in agencij EU (38 od 65) je pripravilo strategijo ali vsaj načrt za varnost IT, odobren na ravni upravnega odbora / višjega vodstva. Razčlenitev po vrsti institucij, organov in agencij EU kaže, da je delež najnižji pri civilnih misijah in decentraliziranih agencijah (ki skupaj pomenijo 71 % anketiranih institucij, organov in agencij EU) (glej ***tabelo 1***). Brez na ravni višjega vodstva odobrene strategije ali načrta za varnost IT obstaja tveganje, da najvišje vodstvo ne ve za težave v zvezi z varnostjo IT ali da teh ne obravnava dovolj prednostno.

Tabela 1 – Delež (v odstotkih) institucij, organov in agencij EU s strategijo ali načrtom za varnost IT, ki ga je odobrilo višje vodstvo

Razvrstitev po številu uslužbencev

< 100 uslužbencev (22 institucij, organov in agencij EU)	100 do 249 uslužbencev (17 institucij, organov in agencij EU)	250 do 1 000 uslužbencev (16 institucij, organov in agencij EU)	> 1 000 uslužbencev (10 institucij, organov in agencij EU)
45 %	53 %	69 %	80 %

Razčlenitev po vrstah institucij, organov in agencij EU

Decentralizirane agencije (35 institucij, organov in agencij EU)	Civilne misije (11 institucij, organov in agencij EU)	Organi (4 institucije, organi in agencije EU)	Institucije (6 institucij, organov in agencij EU)	Skupna podjetja (9 institucij, organov in agencij EU)
45 %	56 %	75 %	83 %	89 %

Vir: anketa Evropskega računskega sodišča

23 Sodišče je preučilo strategije/načrte za varnost IT, ki jih je predložilo sedem institucij, organov in agencij EU v vzorcu (glej odstavek ***18***). Ugotovilo je, da so strategije institucij, organov in agencij EU razmeroma dobro povezane z njihovimi poslovnimi cilji. Strategija Komisije za varnost IT na primer zajema razsežnost varnosti IT iz digitalne strategije Evropske komisije[17] ter je zasnovana tako, da podpira njen časovni načrt in cilje. Vendar so samo tri institucije, organi in agencije EU v vzorcu Sodišča v svoje strategije/načrte za varnost IT vključili konkretne cilje in časovni okvir za njihovo uresničitev.

[17] Sporočilo Komisiji, digitalna strategija Evropske komisije: *A digitally transformed, user-focused and data-driven Commission*, C(2018) 7118 final, 21.11.2018.

24 V varnostnih politikah so določeni pravila in postopki, ki jih morajo upoštevati posamezniki, ki uporabljajo ali upravljajo informacije in vire IT. Pripomorejo k zmanjševanju tveganj za kibernetsko varnost in obveščanju o tem, kaj storiti v primeru incidentov. Sodišče je ugotovilo, da ima 78 % institucij, organov in agencij EU formalno politiko za varnost informacij, le 60 % pa jih ima formalne politike za varnost IT (za opredelitev varnosti informacij in IT glej ***sliko 1***). Ugotovilo je tudi, da imajo štiri od sedmih institucij, organov in agencij EU v vzorcu varnostne politike, skladne z njihovimi strategijami za varnost IT. Vendar so v treh od teh štirih politike za varnost IT le delno dopolnjene s posodobljenimi podrobnimi varnostnimi standardi, ki opisujejo operativne korake, potrebne za izvajanje politik. Neobstoj formalnih varnostnih standardov povečuje tveganje, da se težave v zvezi z varnostjo IT znotraj iste institucije, organa ali agencije EU ne obravnavajo ustrezno in dosledno. Poleg tega otežuje merjenje tega, koliko organizacija izpolnjuje zahteve svoje politike varnosti IT. Od sedmih institucij, organov in agencij EU v vzorcu ima samo Komisija strukturirane postopke za spremljanje izpolnjevanja zahtev svojih politik in standardov za varnost IT, čeprav jih uporablja le omejeno število generalnih direktoratov (GD) (glej ***okvir 1***).

Okvir 1

Izpolnjevanje zahtev na področju varnosti IT v Komisiji

V skladu z decentraliziranim upravljanjem IT v Komisiji je vodja vsakega generalnega direktorata lastnik storitve, ki je odgovoren za to, da sistemi izpolnjujejo standarde varnosti IT. Generalni direktorat za informatiko (GD DIGIT) in Generalni direktorat za človeške vire in varnost (GD HR) spremljata in omogočata lažje izvajanje praks upravljanja izpolnjevanja zahtev. GD DIGIT je vzpostavil orodje (t. i. GRC), ki generalnim direktoratom omogoča merjenje izpolnjevanja zahtev v zvezi s kontrolami politike varnosti IT in poročanje o njih.

580 kontrol je razdeljenih v tri skupine: splošne kontrole (večinoma kontrole upravljanja), kontrole, značilne za posamezne generalne direktorate, in kontrole, značilne za posamezne sisteme. Orodje deluje, vendar ga je doslej uporabljalo le pet generalnih direktoratov. GD DIGIT zato nima pregleda o izpolnjevanju zahtev v Komisiji kot celoti. Vendar lahko Odbor Komisije za informacijsko tehnologijo in kibernetsko varnost (ITCB) zahteva, da GD DIGIT preuči izpolnjevanje specifičnega standarda (npr. večfaktorska avtentikacija leta 2021), ter izda nezavezujoča mnenja in priporočila ali, v primeru kritičnih tveganj, tudi formalne zahteve.

25 Drug pomemben element dobrega upravljanja kibernetske varnosti je imenovanje pooblaščene osebe za varnost informacij (CISO). V skupini standardov ISO 27000[18] to sicer ni izrecno določeno, vendar je imenovanje pooblaščene osebe za varnost informacij ali osebe z enakovredno vlogo postala razširjena praksa v organizacijah in je del smernic ISACA. Pooblaščena oseba za varnost informacij je običajno splošno odgovorna za programe za varnost informacij in IT v organizaciji. V izogib navzkrižju interesov bi morala biti ta oseba v določeni meri neodvisna od funkcije/službe za IT[19].

26 Anketa Sodišča je pokazala, da 60 % institucij, organov in agencij EU ni imenovalo neodvisne pooblaščene osebe za varnost informacij ali osebe z enakovredno vlogo. Tudi v primerih, ko je bila pooblaščena oseba za varnost informacij (ali oseba z enakovredno vlogo) imenovana, se je vloga teh oseb med institucijami, organi in agencijami EU zelo razlikovala in so se njihove funkcije različno razlagale. Zlasti v majhnih in srednjih institucijah, organih in agencijah EU so se pooblaščene osebe za varnost informacij običajno povezovale z bolj operativnimi vlogami, ki niso funkcionalno neodvisne od službe za IT.
Zaradi tega bi lahko bila omejena samostojnost pooblaščenih oseb za varnost informacij pri izvajanju njihovih prioritet na področju varnosti. Agencija ENISA trenutno pripravlja okvir EU za znanja in spretnosti na področju kibernetske varnosti, katerega cilj je med drugim zagotoviti skupno razumevanje vlog, pristojnosti ter znanj in spretnosti.

KLJUČNI PODATKI: **upravljanje varnosti IT v institucijah, organih in agencijah EU**

58 %
institucij, organov in agencij EU ima strategijo ali načrt za varnost IT, **ki ga je potrdilo višje vodstvo**

78 %
institucij, organov in agencij EU ima formalno **politiko za varnost informacij**

60 %
institucij, organov in agencij EU ima formalne politike in standarde za **varnost IT**

40 %
institucij, organov in agencij EU je imenovalo **neodvisno pooblaščeno osebo za varnost informacij**

[18] *ISO/IEC standard 27000:2018*, poglavje 5.

[19] *COBIT 5 for Information Security*, oddelek 4.2.

Ocene tveganja za varnost IT, ki jih izvajajo institucije, organi in agencije EU, večinoma ne zajemajo njihovega celotnega okolja IT

27 Vsi mednarodni standardi za varnost IT poudarjajo pomen vzpostavitve ustrezne metode za ocenjevanje in obvladovanje varnostnih tveganj, ki vplivajo na sisteme IT in podatke, ki jih ti vsebujejo. Ocene tveganja bi bilo treba izvajati redno, da se obravnavajo spremembe zahtev organizacije glede varnosti informacij in spremembe tveganj, s katerimi se spoprijema[20]. Ocenam bi moral slediti načrt za zmanjšanje tveganj (ali načrt za varnost IT).

28 Večina anketiranih institucij, organov in agencij EU (58 od 65) je navedla, da upošteva okvir ali metodologijo za izvajanje ocen tveganja za svoje sisteme IT. Vendar pa ni skupne metodologije, ki bi se uporabljala v vseh institucijah, organih in agencijah EU. Vsaj 26 institucij, organov in agencij EU delno ali v celoti uporablja metodologije, ki jih je razvila Komisija. Zlasti jih je 31 % uporabljalo metodologijo za obvladovanje tveganja za varnost IT iz leta 2018 (ITSRM2). Druge institucije, organi in agencije EU uporabljajo metodologije, ki temeljijo na znanih industrijskih standardih (kot so ISO27001, ISO27005, okvir za kibernetsko varnost ameriškega nacionalnega inštituta za standarde in tehnologijo (NIST-CSF) ali kontrole organizacije Center for Internet Security (CIS)), ali druge interne metodologije.

29 Od sedmih institucij, organov in agencij EU v vzorcu samo dva izvajata celovite ocene tveganja, ki zajemajo njihovo celotno okolje IT (tj. vse njihove sisteme IT). Večina jih izvaja posamezne ocene tveganja samo za njihove najpomembnejše sisteme IT. Sodišče je odkrilo več primerov ocen tveganja, izvedenih pred uvedbo novih sistemov. Ni pa našlo dokazov o nadaljnjih ocenah tveganja, povezanih na primer z naknadnimi spremembami njihovih sistemov/infrastrukture.

Institucije, organi in agencije EU ne obravnavajo dosledno kibernetske varnosti, bistvene kontrole pa niso vedno vzpostavljene

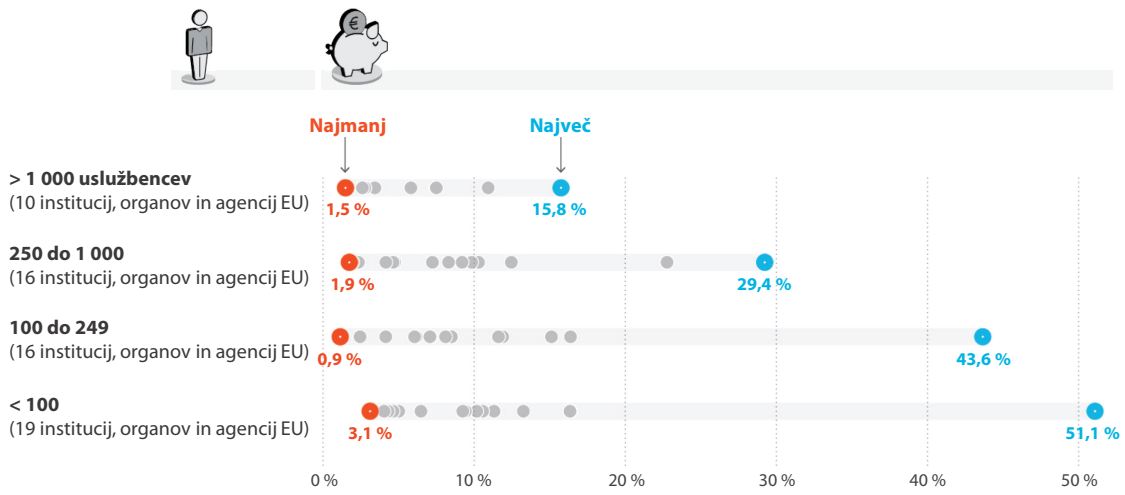
Dodelitev virov za kibernetsko varnost se med institucijami, organi in agencijami EU zelo razlikuje

30 Sodišče je v anketi zaprosilo institucije, organe in agencije EU, naj predložijo svoje skupne odhodke za IT v letu 2020 in oceno zneska, porabljenega za kibernetsko varnost. Podatki Sodišča kažejo znatne razlike v odstotku odhodkov za IT, ki so jih posamezne institucije, organi ali agencije EU dodelili za kibernetsko varnost. To velja

[20] Glej na primer *ISO/IEC 27000:2018*, oddelek 4.5.

tudi za institucije, organe ali agencije EU podobne velikosti, kar zadeva število uslužbencev. Kot je prikazano na ***sliki 3***, so razlike med institucijami, organi in agencijami EU z manj uslužbenci običajno še posebej velike.

Slika 3 – Odhodki za kibernetsko varnost kot delež (v odstotkih) skupnih odhodkov za IT (institucije, organi in agencije EU so razvrščeni po številu uslužbencev)



Opomba: Štiri institucije, organi in agencije EU niso predložili podatkov o odhodkih za kibernetsko varnost.

Vir: anketa Evropskega računskega sodišča

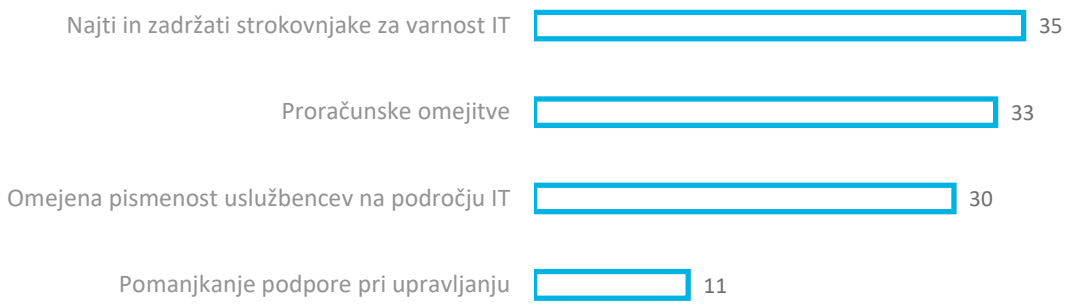
31 Optimalno raven porabe za kibernetsko varnost je težko oceniti v absolutnih vrednosti. Odvisna je od številnih dejavnikov, kot so napadna površina organizacije, občutljivost podatkov, ki jih obravnava, njen profil tveganja in pripravljenost za tveganje ter sektorske pravne/regulativne zahteve. Vendar podatki Sodišča jasno kažejo, da so razlike bistvene in da razlogi za to niso vedno očitni. Nekatere institucije, organi in agencije EU za kibernetsko varnost porabijo precej manj kot podobne organizacije podobne velikosti, kar lahko kaže na premajhno porabo, če so izpostavljeni podobnim grožnjam in tveganjem.

32 Večina institucij, organov in agencij EU je majhnih ali srednjih v smislu uslužbencev in odhodkov za IT, pri čemer jih imata dve tretjini manj kot 350 uslužbencev. Najmanjši od institucij, organov in agencij EU ima le 15 uslužbencev. Upravljanje kibernetske varnosti je za manjše institucije, organe in agencije EU zahtevnejše in zahteva več virov. Večinoma ne morejo izkoristiti ekonomije obsega in nimajo zadostnega notranjega strokovnega znanja. Glede na anketo in razgovore, ki jih je opravilo Sodišče, imajo največje institucije, kot sta Komisija in Evropski parlament, skupine strokovnjakov, ki svoj celotni delovni čas namenijo upravljanju kibernetske varnosti. V najmanjših institucijah, organih in agencijah EU, v katerih so uslužbenci in

viri še posebej omejeni, sploh ni takih strokovnjakov, upravljanju kibernetske varnosti pa del svojega delovnega časa namenijo uslužbenci z izkušnjami na področju IT. Ker so institucije, organi in agencije EU med seboj tesno povezani, to pomeni povečano tveganje (glej tudi odstavek ***10***).

33 Sodišče je v anketi vprašalo institucije, organe in agencije EU, kateri so glavni izzivi pri izvajanju uspešnih politik kibernetske varnosti v njihovih organizacijah (glej ***sliko 4)***. Največji izziv je, da je strokovnjakov za kibernetsko varnost malo ter da jih številne institucije, organi in agencije EU zaradi konkurence zasebnega sektorja ter drugih institucij, organov in agencij EU težko privabijo. Med težavami, ki so bile večkrat navedene, so tudi dolgotrajni postopki zaposlovanja, nekonkurenčni pogodbeni pogoji in pomanjkanje privlačnih poklicnih možnosti. Pomanjkanje strokovnjakov pomeni veliko tveganje za uspešno obravnavanje kibernetske varnosti.

Slika 4 – Izzivi pri izvajanju uspešnih politik kibernetske varnosti v institucijah, organih in agencijah EU (izbran je bil lahko več kot en dejavnik)



Vir: anketa Evropskega računskega sodišča

Večina institucij, organov in agencij EU ponuja neko obliko usposabljanja za ozaveščanje o kibernetski varnosti, vendar to ni sistematično ali dobro usmerjeno

34 Izkoriščanje šibkih točk sistemov in naprav ni edini način, na katerega lahko potencialni napadalci povzročijo škodo. Uporabnike lahko tudi spodbudijo k temu, da razkrijejo občutljive informacije ali prenesejo zlonamerno programsko opremo, na primer z lažnim predstavljanjem ali socialnim inženiringom. Uslužbenci so del prve obrambne linije vsake organizacije. Zato so programi ozaveščanja in usposabljanja o kibernetski varnosti pomemben element uspešnega okvira za kibernetsko varnost.

35 Velika večina anketiranih institucij, organov in agencij EU (95 %) zagotavlja neko obliko splošnega usposabljanja o kibernetski ozaveščenosti za vse uslužbence, tri pa tega ne zagotavljajo. Vendar le 41 % institucij, organov in agencij EU organizira specifično usposabljanje ali tečaje ozaveščanja za vodilne uslužbence, le 29 % pa jih zagotavlja obvezno usposabljanje na področju kibernetske varnosti za vodilne uslužbence, odgovorne za sisteme IT, ki vsebujejo občutljive informacije. Ozaveščenost in zavezanost vodstva sta ključna za uspešno upravljanje kibernetske varnosti. Od 11 institucij, organov in agencij EU, ki so navedli pomanjkanje podpore vodstva kot enega od izzivov za uspešno kibernetsko varnost, so le tri zagotovili nekaj usposabljanja za ozaveščanje, ki je bilo namenjeno vodstvu. Stalno usposabljanje na področju kibernetske varnosti za osebje za IT in strokovnjake za varnost IT zagotavlja 58 % oziroma 51 % institucij, organov in agencij EU.

36 Vse institucije, organi in agencije EU nimajo mehanizmov za spremljanje udeležbe uslužbencev pri usposabljanju na področju kibernetske varnosti ter posledične spremembe njihove ozaveščenosti in vedenja. Zlasti v manjših organizacijah se lahko organizirajo sestanki za kibernetsko ozaveščenost, in sicer v okviru neformalnih sestankov uslužbencev. Glavni način, na katerega organizacije merijo ozaveščenost uslužbencev, je, da redno preizkušajo njihovo vedenje, tudi z anketami o zrelosti ali z vajami z uporabo lažnega predstavljanja. V zadnjih petih letih je 55 % institucij, organov in agencij EU organiziralo eno ali več simuliranih kampanj lažnega predstavljanja (ali podobne vaje). Ker je lažno predstavljanje ena ključnih groženj, s katerimi se srečujejo uslužbenci v javni upravi[21], so te vaje pomembno orodje za usposabljanje uslužbencev in ozaveščanje. Sodišče je ugotovilo, da so ukrepi Komisije za kibernetsko ozaveščanje dobra praksa in da so na voljo drugim zainteresiranim institucijam, organom in agencijam EU (glej ***okvir 2***).

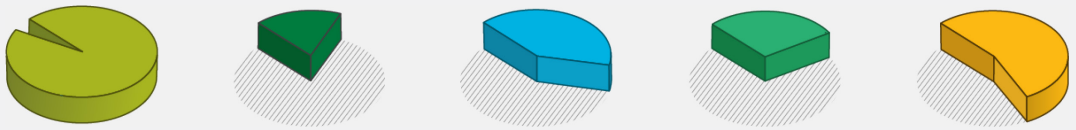
[21] ENISA, *Threat Landscape 2020*, *Sectoral/thematic threat analysis*.

Okvir 2

Usposabljanje o kibernetski ozaveščenosti v Komisiji

Komisija ima posebno skupino za kibernetsko ozaveščanje (*Cyber Aware*), ki deluje znotraj GD DIGIT in vodi njen program ozaveščanja o kibernetski varnosti. Program se upravlja in izvaja skupaj z GD HR, Generalnim sekretariatom, Generalnim direktoratom za komunikacijska omrežja, vsebine in tehnologijo (GD CNECT) in skupino CERT-EU. Usposabljanje je visokokakovostno in ima pogosto medinstitucionalni doseg. Usposabljanja se oglašujejo prek biltena učenja (*Learning Bulletin*), ki dosega približno 65 000 uslužbencev EU. Komisija je prek platforme *Cyber Aware* v zadnjih petih letih organizirala 15 vaj z uporabo lažnega predstavljanja, pred kratkim pa tudi prvo vajo na ravni celotne Komisije.

KLJUČNI PODATKI: **usposabljanje za ozaveščanje o kibernetski varnosti v institucijah, organih in agencijah EU**



95 %
jih zagotavlja neko obliko **splošnega usposabljanja za ozaveščanje** za uslužbence

19 %
jih sistematično **ne obvešča/ usposablja** novih uslužbencev

41 %
jih ima specifično **usposabljanje za vodstvene delavce**

29 %
jih ima **obvezno usposabljanje** za vodilne uslužbence, odgovorne za sisteme IT, ki vsebujejo občutljive informacije

55 %
jih je med uslužbenci opravilo test z **lažnim predstavljanjem**

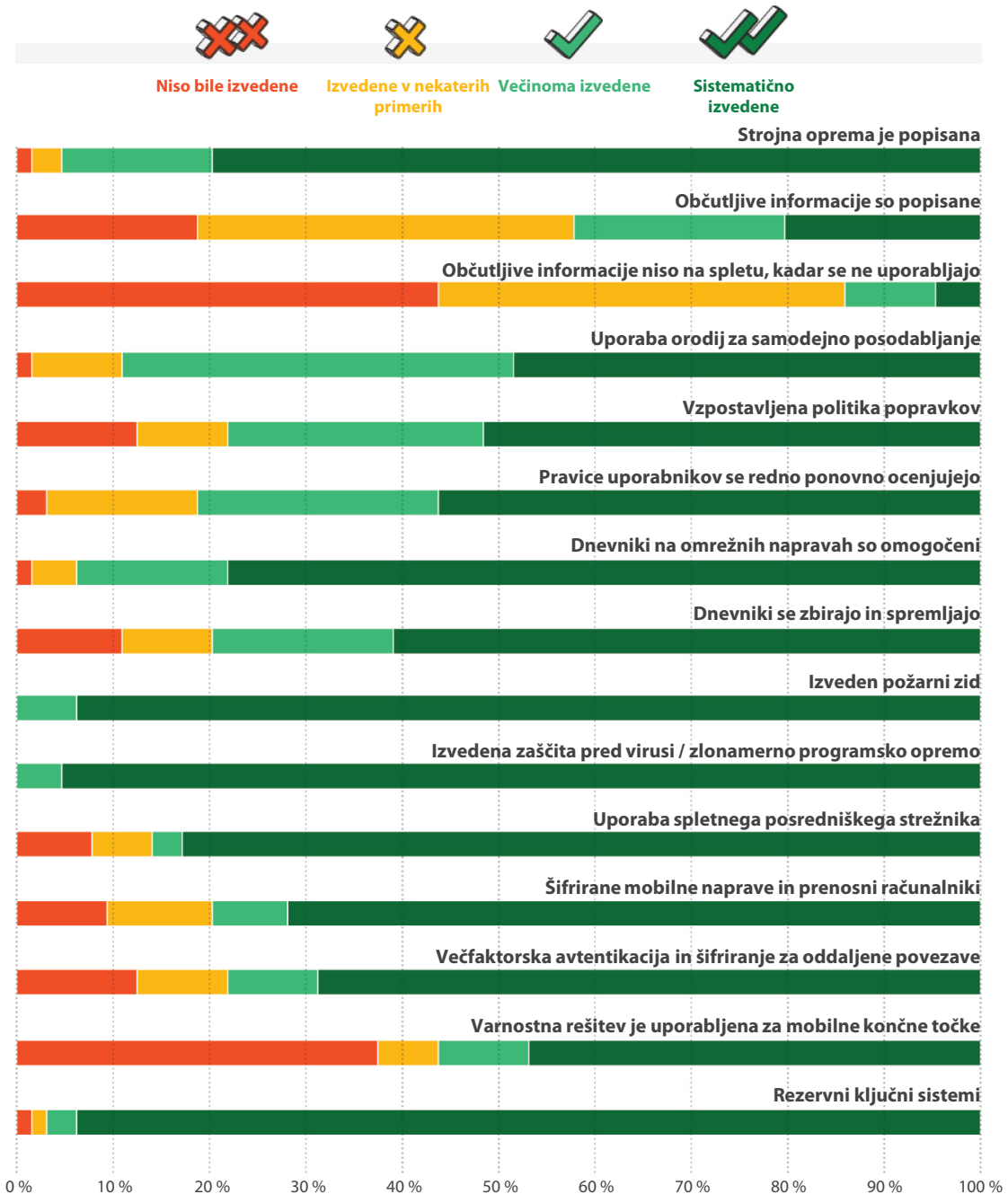
Bistvene kontrole se ne izvajajo vedno ali pa niso formalizirane v standarde

37 Sodišče je institucije, organe in agencije EU prosilo, naj samoocenijo izvajanje izbranih bistvenih kontrol[22]. Izbralo je sklop najboljših praks, ki bi jih lahko ustrezno izvajale tudi manjše organizacije[23]. Rezultati so povzeti v ***tabeli 5***. Večina anketiranih institucij, organov in agencij EU je sprejela izbrane bistvene kontrole. Vendar se zdi, da so pri vsaj 20 % institucij, organov in agencij EU kontrole na nekaterih področjih pomanjkljive ali omejene.

[22] Sklop kontrol, ki izhajajo iz kontrol CIS 7.1, tj. okvira najboljših praks, ki jih je oblikovala organizacija Centre for Internet Security.

[23] Izvedbena skupina 1 (IG1) kontrol CIS.

Slika 5 – Izvajanje bistvenih kontrol v institucijah, organih in agencijah EU (rezultati samoocenjevanja)



Vir: anketa Evropskega računskega sodišča

38 Sodišče je za sedem institucij, organov in agencij EU v vzorcu zahtevalo dokazila in ustrezne standarde/politike za vsako kontrolo, za katero so navedli, da je bila izvedena. Te dokumente je pridobilo za 62 % kontrol. Kot je bilo pojasnjeno med razgovori, so bile tehnične kontrole v več primerih vzpostavljene, vendar niso bile formalizirane v posodobljene standarde ali politike, kar povečuje tveganje, da se težave v zvezi z varnostjo IT ne obravnavajo dosledno znotraj določene institucije, organa ali agencije EU (glej tudi odstavek ***24***).

Več institucij, organov in agencij EU ne pridobi redno neodvisnega zagotovila za njihove ureditve v zvezi s kibernetsko varnostjo

39 Po mnenju Združenja za revizijo in kontrolo informacijskih sistemov (ISACA)[24] je notranja revizija ena od treh bistvenih obrambnih linij organizacije, pri čemer sta drugi dve upravljanje in obvladovanje tveganja. Notranje revizije prispevajo k izboljšanju upravljanja varnosti informacij in IT. Sodišče je preučilo, kako pogosto institucije, organi in agencije EU z notranjimi ali zunanjimi revizijami in proaktivnim preizkušanjem svoje kibernetske obrambe pridobijo neodvisno zagotovilo o svojem okviru za varnost IT.

40 Služba Komisije za notranjo revizijo (IAS) je med drugim odgovorna za izvajanje revizij v zvezi z IT v Komisiji, decentraliziranih agencijah, skupnih podjetjih in Evropski službi za zunanje delovanje (ESZD). Pristojna je za 46 (70 %) od 65 institucij, organov in agencij EU, ki jih je anketiralo Sodišče, v zadnjih petih letih pa je izvedla revizije v zvezi z varnostjo IT v šestih različnih institucijah, organih in agencijah EU. Poleg tega je GD HR pristojen za izvajanje inšpekcijskih pregledov v zvezi z varnostjo IT, ki zajemajo tehnične vidike varnosti informacij[25]. Od preostalih institucij, organov in agencij EU jih je sedem poročalo, da imajo lastno funkcijo notranje revizije, ki zajema vidike IT, za 12 institucij, organov in agencij EU pa iz odgovorov na anketo Sodišča ni bilo mogoče ugotoviti, ali imajo take zmogljivosti za notranjo revizijo.

---

[24] ISACA, *Auditing Cyber Security: Evaluating Risk and Auditing Controls*, 2017.

[25] Sklep 2017/46 o varnosti komunikacijskih in informacijskih sistemov v Evropski komisiji.

41 Še eden od načinov za pridobitev neodvisnega zagotovila so zunanje revizije varnosti IT, ki jih izvajajo neodvisni subjekti. Kljub hitro spreminjajočemu se kibernetskemu okolju med začetkom leta 2015 in prvim četrtletjem leta 2021 v 34 % institucij, organov in agencij EU niso bile opravljene notranje ali zunanje revizije varnosti IT. Razčlenitev tega deleža po vrsti institucij, organov in agencij EU kaže, da v 75 % organov EU, 66 % skupnih podjetij in 45 % civilnih misij od leta 2015 ni bila opravljena notranja ali zunanja revizija varnosti IT.

42 Poleg notranjih in zunanjih revizij lahko organizacije pridobijo zagotovilo o svojem okviru za varnost IT tudi s proaktivnim preizkušanjem kibernetske obrambe za odkrivanje šibkih točk. Eden od načinov za to so penetracijski testi (imenovani tudi etični vdori v informacijske sisteme), ki jih sestavljajo dovoljeni simulirani kibernetski napadi na posamezne računalniške sisteme. V odgovorih na anketo Sodišča je 69 % institucij, organov in agencij EU navedlo, da so v zadnjih petih letih opravili vsaj en penetracijski test. V 45 % primerov je te teste opravila skupina CERT-EU.

43 Vaje z „rdečo ekipo” so še en način preskušanja kibernetske obrambe s simuliranimi napadi z uporabo tehnik, ki so se nedavno uporabljale v napadih v resničnem svetu. So kompleksnejše in celovitejše kot penetracijski preizkusi, saj vključujejo več sistemov in možnih načinov napada. Institucije, organi in agencije EU jih redkeje izvajajo: 46 % institucij, organov in agencij EU je v zadnjih petih letih poročalo o vsaj eni vaji z rdečo ekipo. Skupina CERT-EU je opravila 75 % teh vaj. Priprava in izvedba vaj z rdečo ekipo vključuje veliko dela, skupina CERT-EU pa ima trenutno zmogljivosti za izvedbo največ pet do šest vaj na leto.

44 Razen dveh nedavno ustanovljenih 16 (25 %) anketiranih institucij, organov in agencij EU v zadnjih petih letih ni izvedlo penetracijskih testov ali vaj z rdečo ekipo. Na splošno sedem institucij, organov in agencij EU (10 %) ni skušalo pridobiti nobene vrste neodvisnega zagotovila o svoji ureditvi varnosti IT: eno skupno podjetje, ena decentralizirana agencija in pet civilnih misij.

KLJUČNI PODATKI: **neodvisno zagotovilo o varnosti IT v institucijah, organih in agencijah EU v zadnjih petih letih**

66 %
jih je **izvedlo** vsaj **eno notranjo ali zunanjo revizijo** v zvezi z varnostjo IT

69 %
jih je **izvedlo** vsaj **penetracijski test**

46 %
jih je **izvedlo** vsaj **vajo z rdečo ekipo**

10 %
jih **ni izvedlo** nobene oblike **neodvisne revizije ali preizkušanja** varnosti IT

Institucije, organi in agencije EU so vzpostavili mehanizme za sodelovanje, vendar obstajajo pomanjkljivosti

45 V tem delu se obravnavajo akterji in odbori, ustanovljeni za spodbujanje sodelovanja med institucijami, organi in agencijami EU na področju kibernetske varnosti, ter medinstitucionalne ureditve upravljanja in usklajevanja. Natančneje povedano, Sodišče je preučilo dva medinstitucionalna akterja, tj. agencijo ENISA in skupino CERT-EU, ter dva medinstitucionalna odbora, tj. medinstitucionalni odbor za digitalno preobrazbo (ICDT), zlasti njegovo podskupino za kibernetsko varnost (CSSG), in svetovalni odbor za informacijsko in komunikacijsko tehnologijo (ICTAC). Poleg tega je ocenilo obseg sinergij, ki so jih ti ustvarili za okrepitev pripravljenosti institucij, organov in agencij EU na področju kibernetske varnosti.

Za institucije, organe in agencije EU obstaja formalizirana struktura za usklajevanje njihovih dejavnosti, čeprav z nekaterimi težavami pri upravljanju

46 Medinstitucionalni odbor za digitalno preobrazbo in svetovalni odbor za informacijsko in komunikacijsko tehnologijo sta glavna odbora, ki spodbujata sodelovanje na področju IT med institucijami, organi in agencijami EU. Medinstitucionalni odbor za digitalno preobrazbo, ki ga sestavljajo vodilni uslužbenci institucij in organov EU na področju IT, je forum za spodbujanje izmenjave informacij in sodelovanja. Ima podskupino za kibernetsko varnost (ICDT CSSG), ki poroča medinstitucionalnemu odboru za digitalno preobrazbo in lahko priporoči sprejetje odločitev o specifičnih vprašanjih. Svetovalni odbor za informacijsko in komunikacijsko tehnologijo pa je podskupina mreže agencij EU, neformalne mreže, ki so jo vzpostavili vodje agencij EU in je osredotočena na sodelovanje med agencijami in skupnimi podjetji. Medinstitucionalni odbor za digitalno preobrazbo in svetovalni odbor za informacijsko in komunikacijsko tehnologijo imata jasno opredeljene, komplementarne

vloge: Svetovalni odbor za informacijsko in komunikacijsko tehnologijo pokriva decentralizirane agencije in skupna podjetja, medinstitucionalni odbor za digitalno preobrazbo pa institucije in organe. Medinstitucionalni odbor za digitalno preobrazbo in svetovalni odbor za informacijsko in komunikacijsko tehnologijo sta po naravi bolj neformalni svetovalni skupini ter foruma za izmenjavo informacij in najboljših praks. Več informacij o teh medinstitucionalnih odborih je v ***Prilogi II***.

Zastopanost institucij, organov in agencij EU v ustreznih forumih ni vedno ustrezna

47 Čeprav so strukture za zastopanje jasne, pa vse institucije, organi in agencije EU ne menijo, da je njihova dejanska zastopanost ustrezna. Sodišče je v anketi vprašalo za mnenje o trditvi „Moje potrebe so dovolj upoštevane na ustreznih medinstitucionalnih forumih, moja institucija, organ oziroma agencija EU pa je ustrezno zastopana v odborih odločanja", pri čemer se 42 % institucij, organov in agencij EU s trditvijo ni strinjalo. Nekateri najmanjši so menili, da nimajo dovolj virov, da bi dejavno sodelovali v medinstitucionalnih forumih.

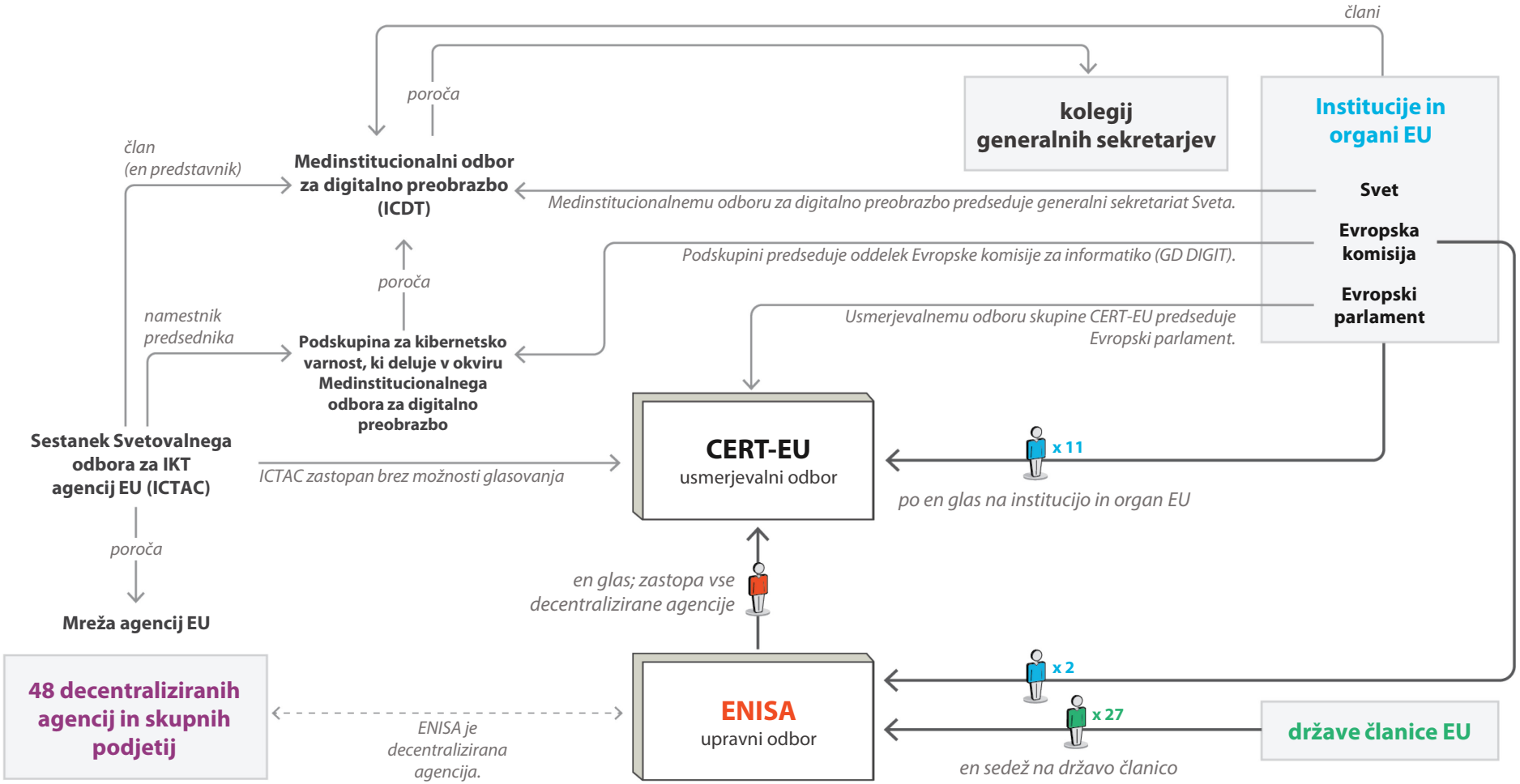
48 V usmerjevalnem odboru skupine CERT-EU, ki je njen glavni organ odločanja, tudi niso reprezentativno zastopani vsi njeni udeleženci. Skupina CERT-EU zagotavlja storitve 87 institucijam, organom in agencijam EU ter trem drugim organizacijam. Vendar pa usmerjevalni odbor vključuje le predstavnike 11 podpisnikov medinstitucionalnega dogovora (sedem institucij EU ter ESZD, Ekonomsko-socialni odbor, Odbor regij in Evropsko investicijsko banko) in predstavnika agencije ENISA, ki imajo vsak po en glas[26].

49 Več kot polovica udeležencev skupine CERT-EU so decentralizirane agencije in skupna podjetja EU, ki imajo skupaj približno 12 000 uslužbencev. Njihove interese v usmerjevalnem odboru skupine CERT-EU formalno zastopa agencija ENISA, vendar so njena pooblastila za zastopanje agencij in skupnih podjetij EU šibka, saj je ti za to niso neposredno imenovali ali izvolili. V praksi stališča decentraliziranih agencij in skupnih podjetij na sejah usmerjevalnega odbora izrazi predstavnik svetovalnega odbora za informacijsko in komunikacijsko tehnologijo, ki se teh sej lahko udeleži in tako pomaga agenciji ENISA pri njeni vlogi zastopanja agencij. Čeprav ta predstavnik izraža stališča in interese 48 institucij, organov in agencij EU, trenutno nima uradnega sedeža ali glasu v usmerjevalnem odboru. Svetovalni odbor za informacijsko in komunikacijsko tehnologijo je aprila 2021 predsedniku usmerjevalnega odbora skupine CERT-EU poslal uradno zahtevo za glasovalne pravice v odboru. Med pripravo tega poročila ta zahteva

[26] Člen 7 medinstitucionalnega dogovora, podpisanega 20. decembra 2017.

še ni bila odobrena. Pregled zastopanosti institucij, organov in agencij EU v odborih odločanja je na ***sliki 6***.

Slika 6 – Pregled upravljanja na področju kibernetske varnosti in zastopanosti v odborih odločanja



Vir: Evropsko računsko sodišče

50 Medinstitucionalno upravljanje na področju kibernetske varnosti v institucijah, organih in agencijah EU je razdrobljeno in trenutno noben posamezen subjekt nima celovitega pregleda nad zrelostjo teh organizacij na področju kibernetske varnosti, pooblastila za prevzem vodilne vloge ali uveljavljanje skupnih zavezujočih pravil. Agencija ENISA in skupina CERT-EU lahko institucije, organe in agencije EU le „podpirata" in jim „pomagata". Relevantna odbora nimata pristojnosti odločanja in lahko institucijam, organom in agencijam EU le dajeta priporočila. Poleg tega za petino anketiranih institucij, organov in agencij EU tudi ni jasno, na koga se lahko obrnejo za določeno storitev, orodje ali rešitev.

Med ključnimi akterji obstajata memoranduma o soglasju, ki pa doslej nista prinesla konkretnih rezultatov

51 Maja 2018 je bil podpisan memorandum o soglasju med agencijo ENISA, skupino CERT-EU, Evropskim centrom Europola za boj proti kibernetski kriminaliteti (EC3) in Evropsko obrambno agencijo (EDA). Osredotočen je na pet področij sodelovanja: izmenjavo informacij, izobraževanje in usposabljanje, vaje iz kibernetske varnosti, tehnično sodelovanje ter strateške in upravne zadeve. Memorandum o soglasju bi sicer s skupnim delovnim programom lahko pripomogel k izogibanju podvajanja, vendar Sodišče ni odkrilo dokazov, da je prinesel konkretne rezultate in skupne ukrepe.

52 V uredbi o kibernetski varnosti, ki je začela veljati junija 2019, je bil predviden podpis novega in posebnega dogovora o sodelovanju med skupino CERT-EU in agencijo ENISA. Omeniti je treba, da je bilo za podpis memoranduma o soglasju februarja 2021 potrebno več kot leto in pol. Namen tega memoranduma o soglasju je vzpostaviti strukturirano sodelovanje med skupino CERT-EU in agencijo ENISA. V njem so opredeljena njuna področja sodelovanja (krepitev zmogljivosti, operativno sodelovanje ter znanje in informacije), okvirno pa je določena tudi delitev vlog med njima: skupina CERT-EU bo prevzela vodilno vlogo pri zagotavljanju pomoči institucijam, organom in agencijam EU, agencija ENISA pa bo prispevala k tem prizadevanjem. V memorandumu o soglasju niso opredeljene praktične ureditve, ki so določene v letnem načrtu sodelovanja. Upravni odbor agencije ENISA je prvi letni načrt sodelovanja za leto 2021 sprejel julija 2021, usmerjevalni odbor skupine CERT-EU pa septembra 2021. Zato je še prezgodaj, da bi se z revizijo Sodišča ocenilo, ali je ta načrt prinesel oprijemljive rezultate.

53 Ker imata oba memoranduma o soglasju iz odstavkov ***51*** in ***52*** skupne cilje in področja sodelovanja, kot so usposabljanje, vaje ali izmenjava informacij, obstaja tveganje prekrivanja in odvečnih nalog.

Potencialne sinergije v okviru sodelovanja še niso v celoti izkoriščene

Sprejeti so bili pozitivni ukrepi za doseganje sinergij

54 V delovnih programih svetovalnega odbora za informacijsko in komunikacijsko tehnologijo ter odbora podskupine za kibernetsko varnost, ki deluje v okviru medinstitucionalnega odbora za digitalno preobrazbo, so opredeljene relevantne teme, pri katerih je mogoče s sodelovanjem doseči večjo učinkovitost. Praktični primeri pobud, ki so institucijam, organom in agencijam EU omogočile, da izkoristijo sinergije, so:

- medinstitucionalne okvirne pogodbe,
- skupni center za ponovno vzpostavitev delovanja po nesreči, ki ga od leta 2019 gosti Urad Evropske unije za intelektualno lastnino (EUIPO) ter je namenjen decentraliziranim agencijam in omogoča vsaj 20-odstotni prihranek stroškov v primerjavi s tržnimi cenami (devet agencij je sprejelo to rešitev za ponovno vzpostavitev delovanja po nesreči),
- sporazumi med šestimi skupnimi podjetji s sedežem v isti stavbi o delitvi skupne infrastrukture in skupnega okvira za varnost IT (od leta 2014).

55 Drug pomemben primer je sistem „GovSec”, ki je institucijam, organom in agencijam EU v pomoč pri izvajanju ocen tveganja v zvezi s sprejetjem rešitev v oblaku. Glede na anketo, ki jo je opravilo Sodišče, 75 % institucij, organov in agencij EU že uporablja nekatere javne platforme v oblaku, več tistih, ki jih še ne, pa namerava migrirati v oblak. Komisija od leta 2019 uporablja pristop *cloud-first* (prednost računalništvu v oblaku), ki predvideva varno ponudbo storitev v hibridnih/več oblakih[27]. Komisija deluje tudi kot posrednik ponudbe računalništva v oblaku za vse institucije, organe in agencije EU, in sicer v kontekstu okvirne pogodbe *Cloud II*. Za obvladovanje varnostnih tveganj in tveganj za varstvo podatkov na platformah v oblaku so potrebni nova znanja in spretnosti ter drugačen pristop kot pri tradicionalni infrastrukturi IT na kraju samem. Uspešno obvladovanje tveganja na področju varnosti informacij v oblaku je skupni izziv za institucije, organe in agencije EU, sistem GovSec pa je primer rešitve, ki bi lahko izpolnil potrebe več, če ne vseh, teh organizacij.

[27] Evropska komisija, *The European Commission Cloud Strategy*, 2019.

Sodelovanje in izmenjava praks med institucijami, organi in agencijami EU še vedno nista optimalna

56 Obstoj medinstitucionalnih odborov ne pomeni, da bo samodejno prišlo do sinergij, institucije, organi in agencije EU pa si vedno ne izmenjujejo najboljših praks, strokovnega znanja, metodologij in pridobljenih izkušenj. Poleg tega se institucije, organi in agencije EU same odločajo o tem, v kakšnem obsegu bodo sodelovale pri delu podskupine za kibernetsko varnost, ki deluje v okviru Medinstitucionalnega odbora za digitalno preobrazbo. Člani te podskupine lahko kljub udeležbi na sestankih prispevajo le toliko, kolikor jim omogočajo njihove redne naloge v institucijah, organih in agencijah EU, kar je že upočasnilo napredek pri izvajanju ukrepov, o katerih so se dogovorile nekatere projektne skupine.

57 Sodišče je odkrilo specifična področja, na katerih za institucije, organe in agencije EU ni ureditev za izmenjavo izkušenj in pobud. V okviru okvirne pogodbe o zmogljivosti za obrambo omrežja lahko na primer institucije, organi in agencije EU zaprosijo za izvedbo študije za konsolidacijo zahtev glede kibernetske varnosti in iskanje rešitev. Ker pa repozitorija takih študij, ki so jih izvedli druge institucije, organi in agencije EU ali zaprosili za njihovo izvedbo, ni, lahko institucije, organi in agencije EU večkrat zahtevajo izvedbo iste študije. Poleg tega institucije, organi in agencije EU drug drugemu sistematično ne razkrivajo svojih pogodbenih razmerij z določenimi dobavitelji ali svoje uporabe posebnih programskih rešitev. Ta vrzel v znanju lahko povzroči dodatne stroške in zamujene sinergije.

58 Prav tako si institucije, organi in agencije EU ne izmenjujejo sistematično informacij o projektih kibernetske varnosti, ki jih izvajajo, čeprav bi ti lahko imeli medinstitucionalni učinek. Pooblastila podskupine za kibernetsko varnost, ki deluje v okviru medinstitucionalnega odbora za digitalno preobrazbo, vključujejo določbo, da si institucije, organi in agencije EU izmenjujejo informacije o novih projektih, ki bi lahko vplivali na kibernetsko varnost drugih institucij, organov in agencij EU in/ali varstvo informacij, ki izvirajo iz njih. Vendar pa podskupina za kibernetsko varnost, ki deluje v okviru medinstitucionalnega odbora za digitalno preobrazbo, o takih projektih ni obveščena.

59 Novoustanovljene agencije morajo svojo infrastrukturo IT in okvir za varnost IT vzpostaviti na novo. Za nove agencije ni nobenega kataloga storitev, zbirke orodij ali jasnih smernic/zahtev. Posledično imajo institucije, organi in agencije EU precej različna okolja IT, saj lahko vsaka organizacija sama neodvisno nabavlja lastno programsko in strojno opremo, infrastrukturo in storitve. Enako je z okvirom za varnost IT, saj ni skupnih zahtev in standardov. Zaradi tega prihaja do morebitnega podvajanja

prizadevanj in neučinkovite porabe sredstev EU, pa tudi do večje kompleksnosti, ki skupini CERT-EU otežuje podporo, ki jo mora zagotavljati.

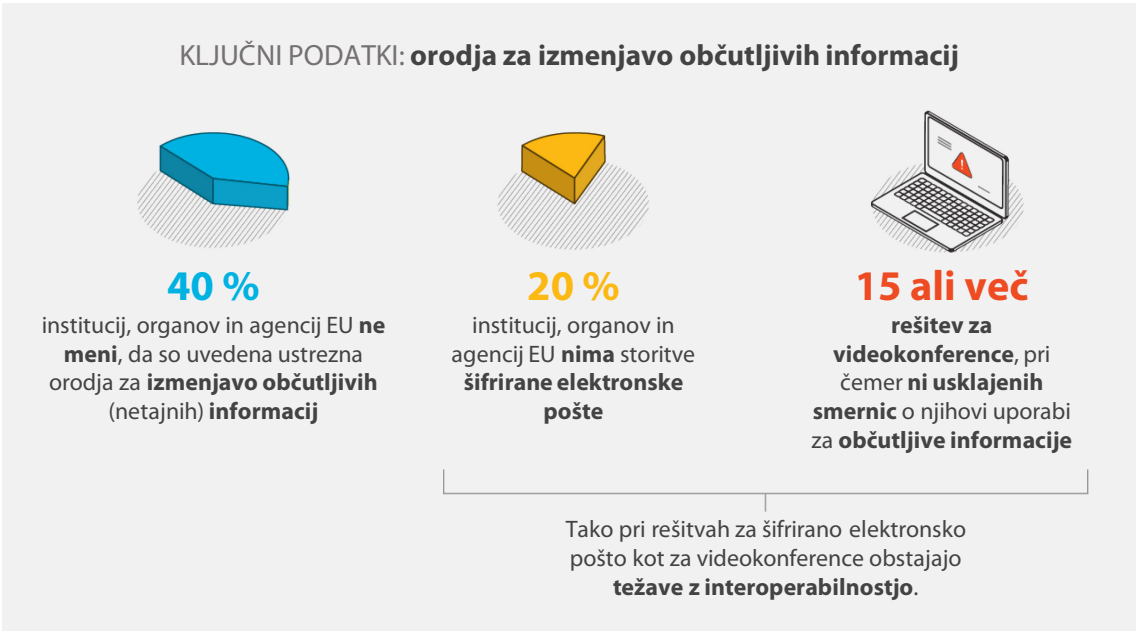
Pri izmenjavi občutljivih informacij obstajajo praktične pomanjkljivosti

60 Nekatere institucije, organi in agencije EU še vedno nimajo ustreznih rešitev za izmenjavo občutljivih netajnih informacij. Tisti, ki jih imajo, pa so na splošno sprejeli svoje različne izdelke in sisteme, kar pomeni, da je interoperabilnost težava. Skupne varne platforme obstajajo le za posebne namene. To so na primer platforme, ki jih skupina CERT-EU ponuja vsem udeležencem za izmenjavo občutljivih informacij o incidentih, grožnjah in šibkih točkah.

61 Več kot 20 % institucij, organov in agencij EU na primer nima storitve šifrirane elektronske pošte. Tisti, ki jo imajo, imajo pogosto težave z interoperabilnostjo, certifikati pa niso vzajemno priznani. Svetovalni odbor za informacijsko in komunikacijsko tehnologijo in medinstitucionalni odbor za digitalno preobrazbo že več let razpravljata o možnostih za nadgradljivo in interoperabilno rešitev, leta 2018 pa je bil izveden pilotni projekt. Vendar ta težava še ni rešena.

62 Druga težava je to, da ni skupnih oznak za občutljive netajne podatke. Oznake so kategorizacije, na podlagi katerih imetniki informacij vedo, katere specifične varnostne zahteve so za te informacije potrebne. Med institucijami, organi in agencijami EU se razlikujejo, kar otežuje izmenjavo in pravilno obravnavanje informacij.

63 Leta 2020 so morali institucije, organi in agencije EU zaradi pandemije COVID-19 v velikem obsegu sprejeti komunikacijska in videokonferenčna orodja, da bi zagotovili neprekinjeno poslovanje. Sodišče je odkrilo vsaj 15 različnih programskih rešitev za videokonference, ki se uporabljajo v institucijah, organih in agencijah EU. Tudi kadar različne institucije, organi in agencije EU uporabljajo isto rešitev/platformo, ta pogosto ni interoperabilna, tudi če vse strani uporabljajo isto programsko rešitev. Poleg tega so se smernice o tem, katere informacije (v smislu občutljivosti) bi se lahko izmenjevale ali obravnavale na določeni platformi, med institucijami, organi in agencijami EU razlikovale. Takšne težave privedejo do gospodarske in operativne neučinkovitosti ter lahko povzročijo morebitne varnostne težave.



Agencija ENISA in skupina CERT-EU institucijam, organom in agencijam EU še nista zagotovili vse potrebne podpore

64 Sodišče je za ta del preučilo dva glavna subjekta, katerih naloga je podpirati institucije, organe in agencije EU na področju kibernetske varnosti: agencijo ENISA in skupino CERT-EU. Sodišče ocenjuje, ali je podpora, ki sta jo zagotovila ta dva subjekta, dosegla institucije, organe in agencije EU ter ali se z njo obravnavajo njihove potrebe, pri čemer Sodišče poudarja razloge za ugotovljene pomanjkljivosti.

Agencija ENISA je eden ključnih akterjev na področju kibernetske varnosti EU, vendar je njena podpora doslej dosegla zelo malo institucij, organov in agencij EU

65 Junija 2019 je začela veljati uredba o kibernetski varnosti[28], s katero je bila nadomeščena prejšnja pravna podlaga[29] agencije ENISA. Agencija je tako dobila večja pooblastila. Natančneje povedano, v uredbi je določeno, da bi morala agencija ENISA dejavno podpirati države članice ter tudi institucije, organe in agencije EU pri izboljšanju njihove kibernetske varnosti, in sicer s krepitvijo zmogljivosti, povečanjem operativnega sodelovanja in vzpostavitvijo sinergij. Na področju krepitve zmogljivosti ima agencija ENISA zdaj pooblastila, da pomaga institucijam, organom in agencijam EU

[28] Naloge agencije ENISA so navedene v poglavju II (členi 5–12) Uredbe (EU) 2019/881.

[29] Uredba (EU) št. 526/2013 Evropskega parlamenta in Sveta; za naloge agencije ENISA na podlagi te uredbe glej člen 3.

„pri njihovih prizadevanjih za izboljšanje preprečevanja, odkrivanja in analiziranja kibernetskih groženj in incidentov […], zlasti z ustrezno podporo skupini CERT-EU”[30]. Agencija ENISA bi morala tudi pomagati institucijam EU pri pripravi in pregledu strategij EU za kibernetsko varnost, pri čemer bi spodbujala njihovo razširjanje in spremljala napredek pri njihovem izvajanju.

66 V uredbi o kibernetski varnosti je sicer jasno navedeno, da bi morala agencija ENISA podpirati institucije, organe in agencije EU pri izboljšanju njihove kibernetske varnosti, vendar agencija ENISA še ni dokončala akcijskih načrtov v zvezi s svojim ciljem, v okviru katerega naj bi pomagala pri krepitvi zmogljivosti teh organizacij (za podrobnosti glej ***okvir 3***).

[30] Člen 6 Uredbe (EU) 2019/881.

Okvir 3

Nezadostna usklajenost ciljev in izložkov agencije ENISA v zvezi z institucijami, organi in agencijami EU

Med triletnimi prioritetami agencije ENISA, navedenimi v večletnem delovnem programu za obdobje 2018–2020 pod ciljem 3.2 – pomoč institucijam EU pri krepitvi zmogljivosti, sta:

- ponujati proaktivno svetovanje institucijam Unije o krepitvi njihove varnosti omrežij in informacij (opredeliti prioritete agencij in organov EU z največjimi potrebami po krepitvi zmogljivosti na področju varnosti omrežij in informacij z vzpostavitvijo rednih stikov z njimi (npr. letne delavnice) in se osredotočiti na te prioritete),
- prizadevati si za zagotavljanje pomoči institucijam EU v zvezi s pristopi k varnosti omrežij in informacij in za olajšanje teh pristopov (vzpostaviti partnerstva s skupino CERT-EU in institucijami z močnimi zmogljivostmi na področju varnosti omrežij in informacij ter jih s tem podpirati pri izvajanju ukrepov v okviru tega cilja).

V delovnih programih agencije ENISA za leta 2018, 2019 in 2020 sta pod ciljem 3.2 le dva operativna cilja (izložka):

- sodelovanje v usmerjevalnem odboru skupine CERT-EU in zastopanje agencij EU, ki uporabljajo storitve skupine CERT-EU,
- sodelovanje z ustreznimi organi EU pri pobudah, ki zajemajo razsežnost varnosti omrežij in informacij, ki je povezana z njihovimi nalogami (vključno z EASA, skupino CERT-EU, EDA, EC3).

Operativni cilji ne vključujejo nobene dejavnosti, povezane s proaktivnim svetovanjem. Poleg tega cilj opredelitve prioritet za agencije z največjimi potrebami ni bil prenesen v operativne izložke, saj je bil nadomeščen s ciljem povezovanja z agencijami, da bi se zastopale njihove potrebe v usmerjevalnem odboru skupine CERT-EU.

67 Glavni organ odločanja agencije ENISA je njen upravni odbor, ki ga sestavljajo po en član, ki ga imenuje vsaka od 27 držav članic, in dva člana, ki ju imenuje Komisija[31] (glej ***sliko 6***). Vsak član ima en glas, odločitve pa se sprejemajo z večino glasov[32]. Zato imajo lahko ukrepi, ki se nanašajo na države članice, večjo prednost kot tisti za institucije, organe in agencije EU. Na primer, v delovnem programu agencije ENISA za

[31] Člen 14 uredbe o kibernetski varnosti.

[32] Člen 18 uredbe o kibernetski varnosti.

leto 2018 se je upravni odbor zaradi nezadostnih virov odločil, da bo nekatere dejavnosti obravnaval prednostno, tri, med katerimi je bila tudi podpora za oceno obstoječih politik/postopkov/praks na področju varnosti omrežij in informacij v institucijah EU, pa odstranil. Namen te dejavnosti je bil agenciji ENISA omogočiti, da pripravi pregled praks institucij, organov in agencij EU in njihove okvirne zrelosti na področju kibernetske varnosti kot podlago za prihodnje ciljno usmerjene ukrepe.

68 Zato se ambicija agencije ENISA zagotavljati proaktivno pomoč institucijam, organom in agencijam EU, kot je izražena v njenih strateških ciljih, ni uresničila v operativnih ciljih ali konkretnih ukrepih. Podpora na področjih krepitve zmogljivosti in operativnega sodelovanja je bila doslej omejena (izvajala se je na zahtevo) na nekatere specifične institucije, organe in agencije EU.

69 V uredbi o kibernetski varnosti je določeno tudi, da bi morala agencija ENISA za to, da bi institucijam, organom in agencijam EU pomagala pri krepitvi zmogljivosti, zagotavljati ustrezno podporo skupini CERT-EU. V času revizije je bila ta podpora omejena na nekaj specifičnih ukrepov. Agencija ENISA je na primer leta 2019 izvedla medsebojni strokovni pregled skupine CERT-EU, in sicer v okviru svojega članstva v mreži skupine CSIRT v EU (vzpostavljeni na podlagi direktive o varnosti omrežij in informacij).

70 Glede na odgovore iz ankete Sodišča agencija ENISA objavlja visokokakovostna poročila in smernice o kibernetski varnosti, od katerih nekatere uporabljajo institucije, organi in agencije EU. Vendar ni specifičnih smernic, ki bi bile pripravljene posebej za institucije, organe in agencije EU ter njihovo okolje in potrebe. Institucije, organi in agencije EU, zlasti tisti, ki so manj napredni na področju kibernetske varnosti, potrebujejo praktične smernice ne le o tem, kaj storiti, temveč tudi, kako to storiti. Agencija ENISA in skupina CERT-EU sta doslej zagotavljali takšno podporo v omejenem in nesistematičnem obsegu.

71 Agencija ENISA je organizirala več tečajev usposabljanja o kibernetski varnosti, ki so bili namenjeni predvsem organom držav članic, vendar se jih je udeležilo tudi omejeno število udeležencev iz institucij, organov in agencij EU. Zagotovila je le dva tečaja za samoučenje, ki sta bila posebej namenjena institucijam, organom in agencijam EU. Na svojem spletišču ponuja tudi spletno gradivo za usposabljanje, ki je dostopno institucijam, organom in agencijam EU, vendar so bili do zdaj to večinoma tečaji za tehnične strokovnjake skupine CSIRT in kot taki za večino teh organizacij niso bili koristni.

72 Poleg usposabljanja lahko agencija ENISA institucije, organe in agencije EU podpira tudi z vajami na področju kibernetske varnosti. Oktobra 2020 je v sodelovanju s skupino CERT-EU pomagala izvesti vajo iz kibernetske varnosti za svetovalni odbor za informacijsko in komunikacijsko tehnologijo, ki je edina vaja, ki jo je agencija ENISA organizirala posebej za udeležence iz institucij, organov in agencij EU. Poleg tega je pomagala organizirati številne vaje na zahtevo nekaterih institucij, organov in agencij EU (npr. EU-LISA, EMSA, Evropskega parlamenta in Europola), in sicer predvsem za njihove deležnike v organih držav članic, pri čemer je sodelovalo tudi nekaj uslužbencev institucij, organov in agencij EU.

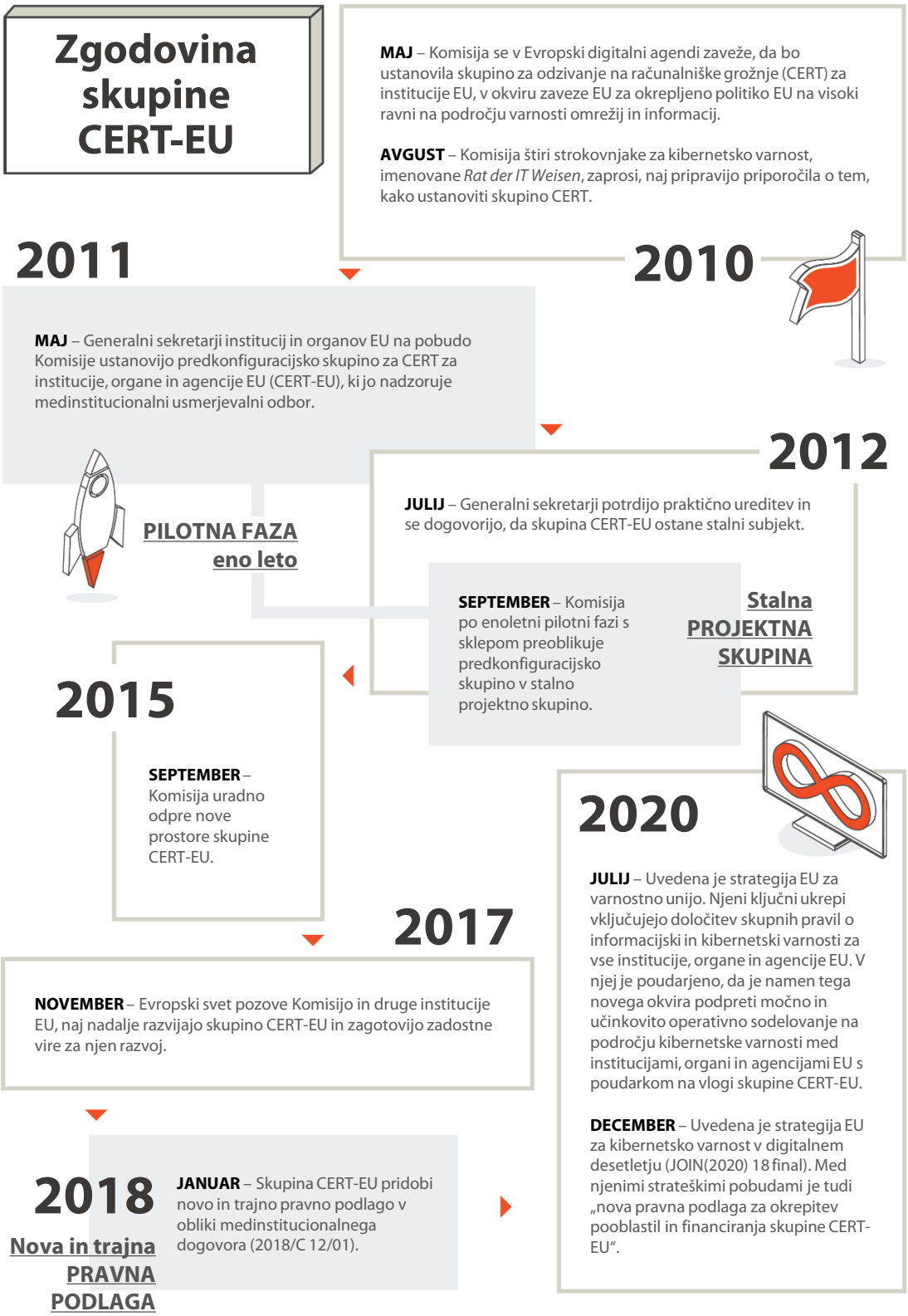
73 Z uredbo o kibernetski varnosti je bila uvedena tudi nova vloga agencije ENISA, in sicer pomagati institucijam, organom in agencijam EU pri njihovih politikah razkrivanja šibkih točk, ki je na prostovoljni osnovi. Vendar agencija ENISA še vedno nima pregleda nad politikami posameznih institucij, organov in agencij EU glede razkrivanja šibkih točk ter jim ne zagotavlja podpore pri vzpostavitvi in izvajanju teh politik.

Skupino CERT-EU njeni udeleženci zelo cenijo, vendar njena sredstva niso sorazmerna s sedanjimi izzivi na področju kibernetske varnosti

74 Na podlagi vrste pobud (glej ***sliko 7***) je bila septembra 2012 s sklepom Komisije[33] ustanovljena skupina za odzivanje na računalniške grožnje za evropske institucije, organe in agencije (CERT-EU) kot stalna projektna skupina za institucije, organe in agencije EU (glej odstavek ***08***).

[33] Sporočilo za medije Evropske komisije: Po uspešnem poskusnem projektu okrepljena kibernetska varnost v institucijah EU.

Slika 7 – Zgodovina skupine CERT-EU



Vir: Evropsko računsko sodišče

75 Skupina CERT-EU je sicer pri svojem delovanju neodvisna, vendar je še vedno projektna skupina, ki ni pravna oseba. Upravno deluje znotraj Evropske komisije (GD DIGIT), ki ji zagotavlja logistično in upravno podporo. Cilj skupine CERT-EU je povečati varnost infrastrukture institucij, organov in agencij EU na področju IKT s povečanjem njihove zmogljivosti za obvladovanje kibernetskih groženj in ranljivosti ter za preprečevanje in odkrivanje kibernetskih napadov ter odzivanje nanje. Skupina CERT-EU ima približno 40 uslužbencev, organiziranih v skupine strokovnjakov, ki se osredotočajo na primer na obveščevalne podatke o kibernetskih grožnjah, digitalno forenziko in odzivanje na incidente.

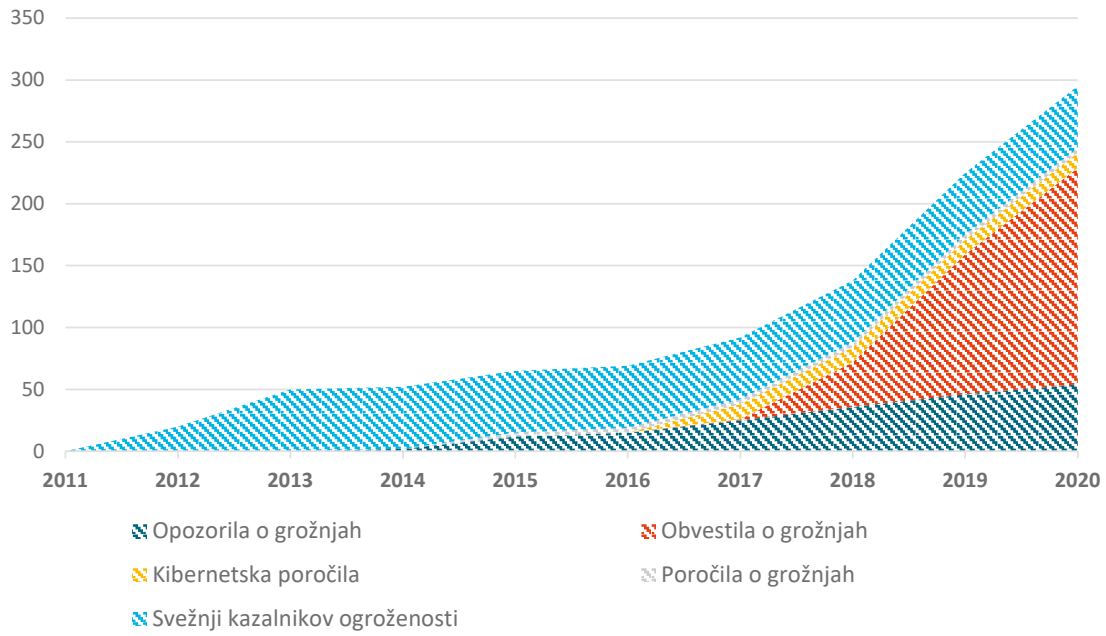
Skupina CERT-EU je cenjen partner z vse večjo delovno obremenitvijo

76 Skupina CERT-EU na četrtletnih delavnicah in letnih dvostranskih srečanjih ter z anketami o zadovoljstvu pridobi povratne informacije in predloge svojih udeležencev. Ankete o zadovoljstvu in anketa Sodišča kažejo, da so udeleženci večinoma zadovoljni s storitvami, ki jih zagotavlja skupina CERT-EU. Razvoj kataloga storitev skupine CERT-EU potrjuje njena prizadevanja za prilagoditev potrebam institucij, organov in agencij EU.

77 Medtem ko velike institucije, organi in agencije EU z velikimi internimi zmogljivostmi običajno uporabljajo skupino CERT-EU predvsem kot središče za izmenjavo informacij in vir obveščevalnih podatkov o grožnjah, pa se manjše institucije, organi in agencije EU opirajo na skupino CERT-EU za širšo paleto storitev, kot so dnevniki spremljanja, penetracijski testi, vaje z rdečo ekipo in podpora pri odzivanju na incidente. Storitve skupine CERT-EU so še posebej dragocene za manjše institucije, organe in agencije EU, in sicer zaradi njihovega omejenega internega strokovnega znanja in pomanjkanja ekonomije obsega (glej odstavka ***31*** in ***33***).

78 Skupina CERT-EU je v zadnjih letih zaradi drastičnega povečanja groženj in incidentov okrepila svoje zmogljivosti in postopke. Število informacijskih izdelkov skupine CERT-EU, zlasti opozoril in obvestil o grožnjah, stalno narašča (***slika 8***). Leta 2020 je skupina CERT-EU izdala 171 obvestil o grožnjah in 53 opozoril o grožnjah (kar je precej več kot 80 obvestil in 40 opozoril, kolikor jih je prvotno pričakovala).

Slika 8 – Povečanje izdelkov z obveščevalnimi podatki o grožnjah



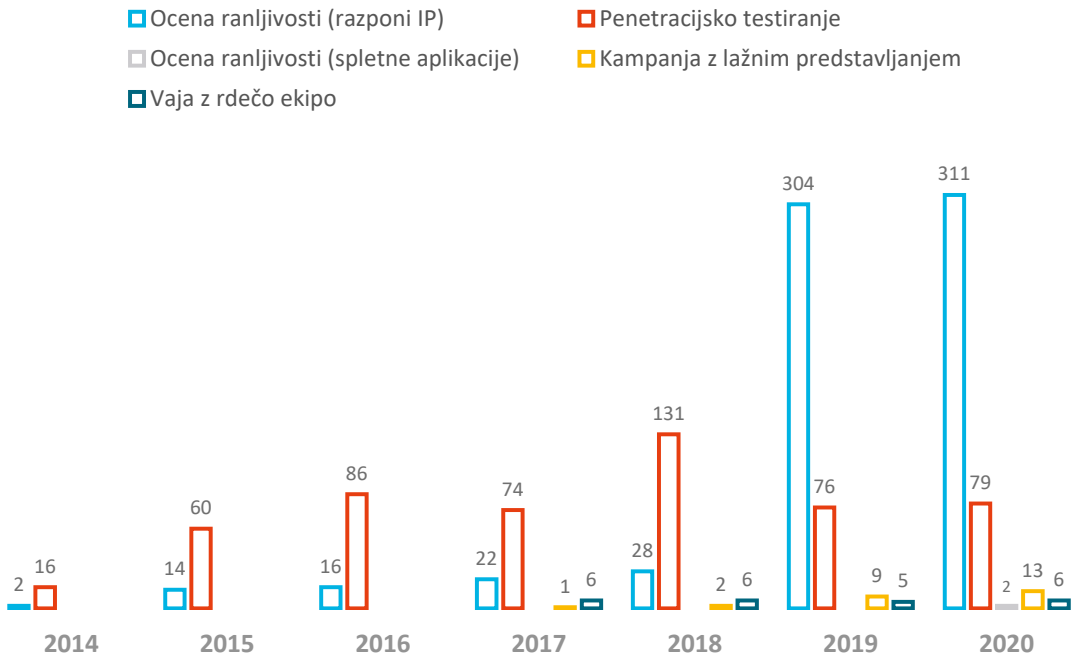
Vir: Evropsko računsko sodišče na podlagi podatkov skupine CERT-EU

79 Skupina CERT-EU prav tako podpira institucije, organe in agencije EU pri obvladovanju kibernetskih incidentov. 52 % institucij, organov in agencij EU ima interne skupine za odzivanje ali vsaj koordinatorje incidentov, preostalih 48 % pa se jih v primeru incidenta opira na skupino CERT-EU in/ali druge zunanje ponudnike. Pri obvladovanju zapletenih incidentov pa lahko za podporo skupine CERT-EU zaprosijo tudi velike institucije, organi in agencije EU, ki imajo interne zmogljivosti odzivanja.

80 Skupno število incidentov, ki jih je obravnavala skupina CERT-EU, se je povečalo s 561 leta 2019 na 884 leta 2020. Zlasti pomembni incidenti so se povečali s samo enega leta 2018 na 13 leta 2020. Leta 2021 je bilo pomembnih incidentov 17, medtem ko jih je bilo v letu 2020, ki je bilo do takrat rekordno, 13. Ti pomembni incidenti so na splošno rezultat zelo izpopolnjenih groženj. Vplivajo lahko na več institucij, organov in agencij EU, vključujejo stike z organi, prizadete strani in skupina CERT-EU pa običajno potrebujejo tedne ali mesece, da jih raziščejo in izkoreninijo.

81 Skupina CERT-EU je tudi glavni ponudnik proaktivnih ocen in preizkusov kibernetske obrambe institucij, organov in agencij EU. Povzetek dejavnosti skupine CERT-EU na tem področju je prikazan na ***sliki 9***. Poleg tega skupina CERT-EU od leta 2020 izvaja tudi zunanje preglede omrežij (*external network scans*).

Slika 9 – Preizkusi in ocene, ki jih je opravila skupina CERT-EU



Vir: Evropsko računsko sodišče na podlagi podatkov skupine CERT-EU

Udeleženci ne izmenjujejo pravočasno relevantnih informacij s skupino CERT-EU

82 V medinstitucionalnem dogovoru[34] je navedeno, da bi morali udeleženci skupino CERT-EU obvestiti o pomembnih kibernetskih incidentih, toda v praksi se to vedno ne zgodi. Medinstitucionalni dogovor ne zagotavlja mehanizma za izvrševanje obveznega in pravočasnega poročanja udeležencev skupine CERT-EU o „pomembnih" incidentih. Na podlagi splošne opredelitve „pomembnih incidentov" v medinstitucionalnem dogovoru se lahko institucije, organi in agencije EU sami odločijo, ali bodo incident prijavili. Po navedbah vodstva skupine CERT-EU nekateri udeleženci niso pravočasno izmenjevali informacij o pomembnih incidentih, kar ovira vlogo skupine CERT-EU kot koordinacijskega središča za izmenjavo informacij o kibernetski varnosti in za odzivanje na incidente za vse institucije, organe in agencije EU. Eden od udeležencev, ki se je spopadal z zelo izpopolnjeno grožnjo, na primer ni obvestil skupine CERT-EU ali prosil za njeno podporo. Skupina CERT-EU zato ni mogla zbirati obveščevalnih podatkov o kibernetskih grožnjah, ki bi bili koristni za podporo drugim udeležencem, ki se spoprijemajo z enako grožnjo. Ta napad je vplival na vsaj šest institucij, organov in agencij EU.

[34] Člen 3.3 medinstitucionalnega dogovora, podpisanega 20. decembra 2017.

83 Prav tako udeleženci s skupino CERT-EU niso dejavno pravočasno izmenjevali informacij o kibernetskih grožnjah in šibkih točkah, ki vplivajo nanje, čeprav bi na podlagi medinstitucionalnega dogovora[35] to morali početi. Skupina za digitalno forenziko in odzivanje na incidente v okviru skupine CERT-EU ni prejela obvestil o šibkih točkah ali pomanjkljivostih pri nadzoru, odkritih zunaj konteksta incidentov, ki jih aktivno preiskuje. Udeleženci ne izmenjujejo proaktivno relevantnih ugotovitev internih ali zunanjih revizij v zvezi z varnostjo.

84 Poleg tega v medinstitucionalnem sporazumu ni določeno, da morajo institucije, organi in agencije EU skupini CERT-EU poročati o pomembnih spremembah svojega okolja IT, zato udeleženci skupine CERT-EU niso sistematično obveščali o zadevnih spremembah. Institucije, organi in agencije EU na primer skupine CERT-EU ne obvestijo vedno o vsakršni spremembi svojih razponov IP (tj. seznama internetnih naslovov svoje infrastrukture). Skupina CERT-EU potrebuje posodobljen razpon IP, da lahko na primer izvede preglede (*scans*), ko se odkrijejo večje šibke točke. Če institucije, organi in agencije EU skupine CERT-EU ne obveščajo o takih spremembah, jim ta težje zagotavlja podporo in težje spremlja sisteme, posledično pa to pomeni tudi več dela pri popravljanju netočnih podatkov v orodjih za spremljanje. Po navedbah vodstva skupine CERT-EU ta pri obravnavi incidenta včasih odkrije prej neznano infrastrukturo IT. Poleg tega razen specifičnih primerov trenutno nima celovitega pregleda nad sistemi in omrežji IT skupnosti institucij, organov in agencij EU.

85 Dokler se v medinstitucionalnem dogovoru ne določi mehanizem izvrševanja, bodo obvestila, ki jih institucije, organi in agencije EU pošiljajo skupini CERT-EU in so bistven element pri oblikovanju skupnosti institucij, organov in agencij EU za kibernetsko pripravljenost s skupino CERT-EU kot osrednjo točko, še naprej nesistematična.

[35] Člen 3.2 medinstitucionalnega dogovora.

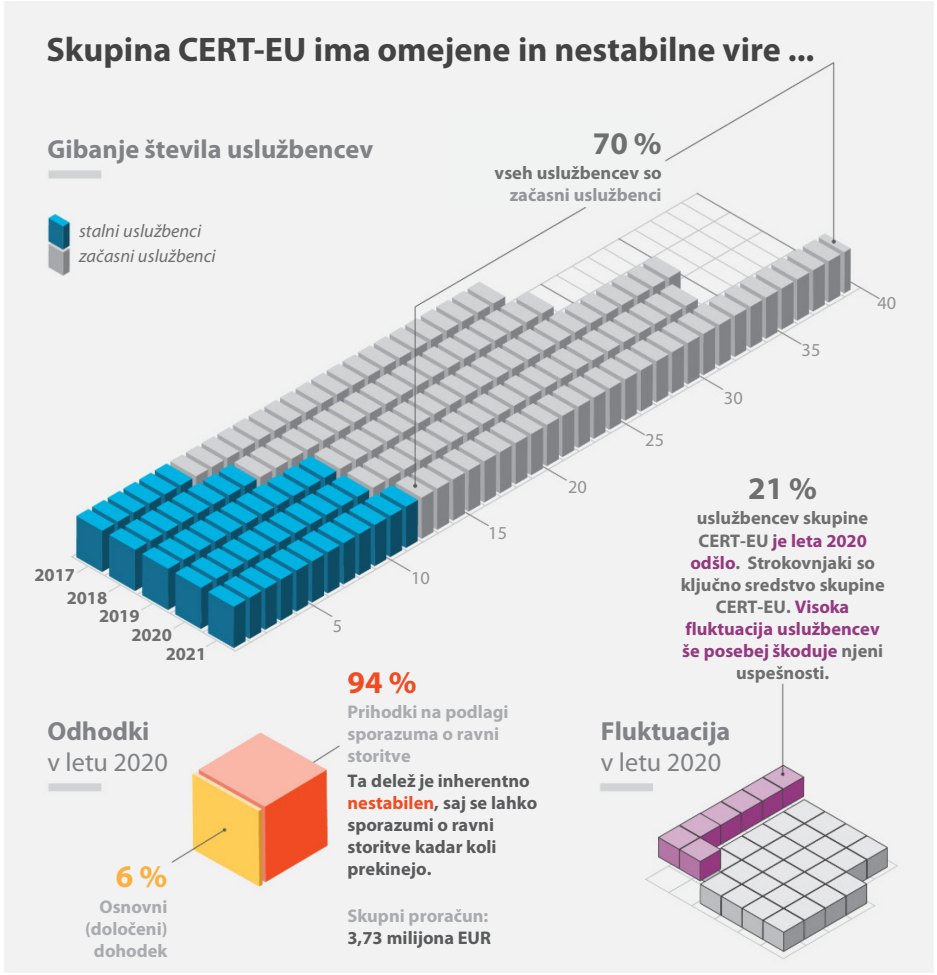
Zagotavljanje virov skupini CERT-EU je nestabilno in ni sorazmerno s trenutno stopnjo ogroženosti

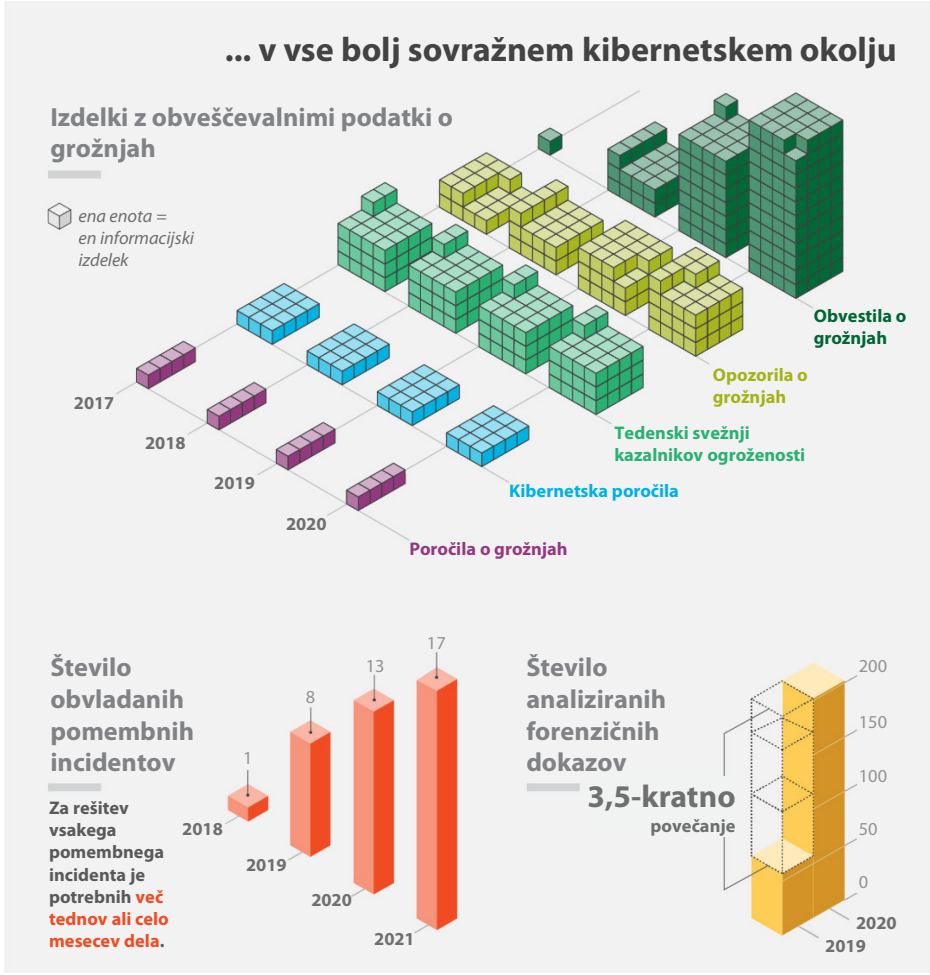
86 V medinstitucionalnem dogovoru[36] je navedeno, da „je treba [skupini CERT-EU] zagotoviti vzdržno financiranje in osebje, obenem pa zagotoviti stroškovno učinkovitost in ustrezno jedro stalnega osebja”. Najpomembnejše sredstvo skupine CERT-EU so visoko usposobljeni in specializirani uslužbenci. Na ***sliki 10*** je ponazorjeno gibanje števila uslužbencev v skupini CERT-EU od njene ustanovitve leta 2011 do danes.

87 Več kot dve tretjini uslužbencev skupine CERT-EU so pogodbeni uslužbenci. Njihova plača ni zelo konkurenčna na trgu strokovnjakov za kibernetsko varnost, po mnenju vodstva skupine CERT-EU pa jih je tudi vse težje najeti in obdržati. Če plače niso dovolj privlačne za kandidate z več izkušnjami, je skupina CERT-EU primorana k temu, da zaposli kandidate z manj izkušnjami ter nato vlaga čas v njihovo usposabljanje. Poleg tega se pogodbe sklenejo za največ šest let, kar pomeni, da skupina CERT-EU nima druge možnosti, kot da se od pogodbenih uslužbencev poslovi na vrhuncu njihovega strokovnega razvoja. Fluktuacija zaposlenih je bila še posebej velika leta 2020. Skupino CERT-EU je namreč zapustilo 21 % uslužbencev, vseh pa ni bilo mogoče nadomestiti. Kar zadeva prejšnji dve leti, je leta 2019 skupino zapustilo 9 % uslužbencev, leta 2018 pa 13 %.

[36] Uvodna izjava 7 medinstitucionalnega dogovora.

Slika 10 – Viri in izzivi skupine CERT-EU





Vir: Evropsko računsko sodišče na podlagi podatkov skupine CERT-EU

88 Vodstvo skupine CERT-EU je poudarilo, da je skupina za digitalno forenziko in odzivanje na incidente pogosto preobremenjena, druge skupine pa ne morejo slediti povpraševanju. Skupina CERT-EU je bila zato prisiljena zmanjšati obseg dejavnosti. Zaradi pomanjkanja virov na primer trenutno ne izvaja ocen zrelosti svojih udeležencev. Tudi njena storitev „opozorila o sumljivi dejavnosti" se je začela uporabljati pozneje, kot je bilo pričakovano, prav tako zaradi pomanjkanja virov. Poleg tega je več udeležencev, s katerimi je Sodišče opravilo razgovore, izrazilo pripombe glede časa, potrebnega za dostop do storitev skupine CERT-EU.

89 Zaradi omejenih virov se je morala skupina CERT-EU doslej osredotočati zlasti na zaščito konvencionalne infrastrukture IT „na kraju samem" pred velikimi grožnjami skupin (ki jih običajno podpirajo države), ki pomenijo napredne trajne grožnje. Toda po navedbah njenega vodstva je treba zaradi razširjenega obsega IT institucij, organov in agencij EU (ki zdaj vključuje oblak, mobilne naprave in orodja za delo na daljavo) okrepiti spremljanje in zaščito, poleg tega pa je treba nameniti več pozornosti tudi grožnjam nižje stopnje (kot sta kibernetska kriminaliteta in izsiljevalsko programje).

90 V medinstitucionalnem dogovoru niso določene operativne zmogljivosti skupine CERT-EU 24 ur na dan, sedem dni v tednu. Skupina CERT-EU trenutno nima virov ali ustreznega okvira za človeške vire, da bi stalno in strukturirano delovala zunaj delovnega časa, čeprav se kibernetski napadi dogajajo tudi takrat. Kar zadeva institucije, organe in agencije EU, pa jih ima le 35 od 65 anketiranih uslužbenca za IT, ki je dosegljiv zunaj delovnega časa.

91 Usmerjevalni odbor je leta 2012 za financiranje operacij skupine CERT-EU odobril model sporazuma o ravni storitve. Osnovne storitve se vsem udeležencem zagotavljajo brezplačno, za razširjene storitve, ki so plačljive, pa se lahko sklene sporazum o ravni storitve. Proračun skupine CERT-EU za leto 2020 je znašal 3 745 000 EUR, od tega je bilo 6 % financiranih iz proračuna EU in 94 % iz sporazumov o ravni storitve. Vendar pa so udeleženci zelo različni: nekateri imajo zrele zahteve glede varnosti IT, drugi pa skromne proračune za IT in zelo nizko stopnjo zrelosti na področju kibernetske varnosti. Zato je rezultat razprav o sporazumu o ravni storitve kombinacija visokih varnostnih zahtev nekaterih institucij, organov in agencij EU ter relativnega pomanjkanja pripravljenosti ali sposobnosti drugih, da k temu prispevajo.

92 Poleg tega je treba vsak sporazum o ravni storitve vsako leto podaljšati, kar ni le upravno breme, ampak povzroča tudi težave z denarnim tokom, saj skupina CERT-EU ne dobi istočasno sredstev na podlagi vseh sporazumov o ravni storitve. Agencije lahko sporazum o ravni storitve kadar koli prekinejo. To pomeni tveganje, da bo nastal začarani krog in bo morala skupina CERT-EU zaradi izgube prihodkov zmanjšati obseg svojih storitev in ne bo mogla slediti povpraševanju, kar bo spodbudilo druge institucije, organe in agencije EU, da prekinejo svoje sporazume o ravni storitve in se obrnejo na zasebne ponudnike. Glede na navedeno sedanji model financiranja ni idealen za zagotavljanje stabilne in optimalne ravni storitev.

93 Usmerjevalni odbor skupine CERT-EU je zaradi hitro spreminjajočih se kibernetskih groženj (glej odstavka ***06*** in ***80***) na seji 19. februarja 2020 potrdil strateški predlog za razširitev storitev skupine CERT-EU na področju kibernetske varnosti in razvoj polne operativne zmogljivosti. Predlogu je bila priložena analiza kadrovskih in finančnih potreb skupine CERT-EU. V njej je bilo ugotovljeno, da bi skupina CERT-EU potrebovala 14 dodatnih stalnih delovnih mest upravnih uslužbencev, ki bi se postopoma dodajala v obdobju 2021–2023. Skupina CERT-EU bi nato od leta 2023 naprej delovala s polno zmogljivostjo. Kar zadeva financiranje, bi morala v skladu s tem predlogom povečati svoj proračun za 7,6 milijona EUR v obdobju 2021–2023, da bi ta do leta 2024 dosegel 11,3 milijona EUR.

94 Kljub potrditvi strateškega predloga o zagotavljanju dodatnih virov za skupino CERT-EU pa institucije, organi in agencije EU še niso dosegli dogovora o praktičnih podrobnostih, in sicer za vmesno obdobje 2021–2023 in dolgoročno za obdobje po začetku veljavnosti prihodnje uredbe o kibernetski varnosti (glej odstavek ***12***).

Zaključki in priporočila

95 Sodišče ugotavlja, da skupnost institucij, organov in agencij EU ni dosegla ravni kibernetske pripravljenosti, ki bi bila sorazmerna z grožnjami. Delo Sodišča kaže, da imajo institucije, organi in agencije EU različne stopnje zrelosti na področju kibernetske varnosti; ker so pogosto povezani med sabo ter z drugimi javnimi in zasebnimi organizacijami v državah članicah, so lahko zaradi slabosti v enem od njih kibernetskim grožnjam izpostavljeni tudi drugi.

96 Sodišče je ugotovilo, da se ključne dobre prakse na področju kibernetske varnosti, vključno z nekaterimi bistvenimi kontrolami, niso vedno izvajale. Dobro upravljanje kibernetske varnosti je bistveno za varnost informacij in sistemov IT, vendar v nekaterih institucijah, organih in agencijah EU še ni vzpostavljeno: pogosto primanjkuje strategij in načrtov za varnost IT ali pa teh ne potrdi višje vodstvo, varnostne politike niso vedno formalizirane, ocene tveganja pa ne zajemajo celotnega okolja IT. Poraba za kibernetsko varnost je neenakomerna, saj nekatere institucije, organi in agencije EU temu očitno namenijo premalo sredstev v primerjavi s podobnimi organizacijami podobne velikosti (glej odstavke ***21***–***33*** ter ***37*** in ***38***).

97 Programi ozaveščanja in usposabljanja o kibernetski varnosti so pomemben element uspešnega okvira za kibernetsko varnost. Vendar le 29 % institucij, organov in agencij EU zagotavlja obvezno usposabljanje na področju kibernetske varnosti za vodilne uslužbence, odgovorne za sisteme IT, ki vsebujejo občutljive informacije, pri čemer je usposabljanje pogosto neformalno. V zadnjih petih letih je 55 % institucij, organov in agencij EU organiziralo eno ali več simuliranih kampanj lažnega predstavljanja (ali podobne vaje). Te vaje so pomembno orodje za usposabljanje osebja in ozaveščanje, vendar jih vse institucije, organi in agencije EU ne uporabljajo sistematično (glej odstavke ***34***–***36***). Poleg tega vse institucije, organi in agencije EU ne pridobijo redno neodvisnega zagotovila za kibernetsko varnost (glej odstavke ***39***–***44***).

98 Skupina CERT-EU je med institucijami, organi in agencijami EU, ki uporabljajo njene storitve, zelo cenjena, vendar so njene zmogljivosti preobremenjene. Njena delovna obremenitev na področju obveščevalnih podatkov o grožnjah in obvladovanjae incidentov se od leta 2018 hitro povečuje. Število pomembnih kibernetskih incidentov se je povečalo za več kot desetkrat. Hkrati institucije, organi in agencije EU vedno ne posredujejo pravočasno informacij o pomembnih incidentih, šibkih točkah in pomembnih spremembah v njihovi infrastrukturi IT. To ovira uspešnost skupine CERT-EU, ki tako ne more opozoriti institucij, organov in agencij EU, na katere bi to lahko vplivalo, lahko pa tudi povzroči, da pomembni incidenti ostanejo neodkriti.

Poleg tega so viri skupine CERT-EU nestabilni in niso sorazmerni s trenutnimi stopnjami ogroženosti ali potrebami institucij, organov in agencij EU. Usmerjevalni odbor skupine CERT-EU je leta 2020 potrdil strateški predlog o zagotavljanju dodatnih virov, ki jih skupina potrebuje, vendar udeleženci še niso dosegli dogovora o praktičnih podrobnostih zagotavljanja teh virov. Zato skupina CERT-EU ne more slediti povpraševanju in je prisiljena zmanjšati obseg dejavnosti (glej odstavke ***74***–***93***).

Priporočilo 1 – Izboljšati pripravljenost vseh institucij, organov in agencij EU na področju kibernetske varnosti s skupnimi zavezujočimi pravili in povečanjem virov za skupino CERT-EU

Komisija naj v svoj prihodnji predlog uredbe o ukrepih za visoko skupno stopnjo kibernetske varnosti vseh institucij, organov in agencij EU vključi naslednja načela:

(a) višje vodstvo bi moralo biti odgovorno za upravljanje kibernetske varnosti, in sicer s potrditvijo strategij za kibernetsko varnost in ključnih varnostnih politik ter imenovanjem neodvisne pooblaščene osebe za varnost informacij (ali osebe z enakovredno vlogo);

(b) institucije, organi in agencije EU bi morali imeti okvir za obvladovanje tveganja na področju varnosti IT, ki bi pokrival njihovo celotno infrastrukturo IT, in izvajati redne ocene tveganja;

(c) institucije, organi in agencije EU bi morali zagotoviti sistematično usposabljanje za ozaveščanje za vse uslužbence, vključno z vodstvom;

(d) institucije, organi in agencije EU bi morali zagotoviti redne revizije in preizkuse kibernetske obrambe. Revizije bi morale vključevati tudi ustreznost virov, namenjenih kibernetski varnosti;

(e) institucije, organi in agencije EU bi morali skupini CERT-EU nemudoma poročati o pomembnih kibernetskih incidentih ter relevantnih spremembah in šibkih točkah v zvezi z njihovo infrastrukturo IT;

(f) institucije, organi in agencije EU bi morali povečati in v proračunu dodeliti sredstva za skupino CERT-EU v skladu s potrebami, opredeljenimi v strateškem predlogu, ki ga potrdi njen usmerjevalni odbor;

(g) uredba bi morala vključevati določbe o imenovanju subjekta, ki bi bil predstavnik vseh institucij, organov in agencij EU ter bi imel ustrezna pooblastila in sredstva za spremljanje skladnosti vseh institucij, organov in agencij EU s skupnimi pravili o kibernetski varnosti ter za izdajanje smernic, priporočil in pozivov k ukrepanju.

Ciljni rok za izvedbo: prvo četrtletje leta 2023.

99 Institucije, organi in agencije EU so vzpostavili mehanizme za sodelovanje na področju kibernetske varnosti, vendar je Sodišče ugotovilo, da potencialne sinergije niso v celoti izkoriščene. Obstaja formalizirana struktura za izmenjavo informacij, v kateri imajo akterji in odbori komplementarne vloge. Vendar na sodelovanje manjših

institucij, organov in agencij EU v medinstitucionalnih forumih vplivajo omejeni viri, zastopanost decentraliziranih agencij in skupnih podjetij v usmerjevalnem odboru skupine CERT-EU pa ni optimalna. Sodišče je ugotovilo tudi, da si institucije, organi in agencije EU med seboj ne izmenjujejo sistematično informacij o projektih, povezanih s kibernetsko varnostjo, ocenah varnosti in drugih pogodbah o storitvah. Zaradi tega lahko pride do podvajanja prizadevanj in višjih stroškov. Sodišče je opazilo operativne težave pri izmenjavi občutljivih netajnih informacij prek šifrirane elektronske pošte ali videokonference, ki so posledica tega, da rešitve IT niso interoperabilne, nedoslednih smernic o njihovi dovoljeni uporabi ter pomanjkanja skupnih oznak za informacije in pravil o njihovem obravnavanju (glej odstavke ***45***–***63***).

Priporočilo 2 – Zavzemati se za nadaljnje sinergije na izbranih področjih med institucijami, organi in agencijami EU

Komisija naj v okviru medinstitucionalnega odbora za digitalno preobrazbo spodbuja naslednje ukrepe med institucijami, organi in agencijami EU:

(a) sprejeti rešitve za interoperabilnost varnih komunikacijskih kanalov (od šifrirane elektronske pošte do videokonferenc) ter zavzemati se za dogovor o skupnih oznakah in skupnih pravilih za obravnavanje občutljivih netajnih informacij;

(b) sistematično izmenjevati informacije o projektih, povezanih s kibernetsko varnostjo, ki bi lahko imeli medinstitucionalni učinek, o varnostnih ocenah, opravljenih o programski opremi, in veljavnih pogodbah z zunanjimi ponudniki;

(c) opredeliti specifikacije za skupno javno naročanje in okvirne pogodbe za storitve na področju kibernetske varnosti, v katerih lahko sodelujejo vse institucije, organi in agencije EU, da se spodbudi ekonomija obsega.

Ciljni rok za izvedbo: četrto četrtletje leta 2023.

100 Agencija Evropske unije za kibernetsko varnost (ENISA) in skupina CERT-EU sta glavna subjekta, zadolžena za podpiranje institucij, organov in agencij EU na področju kibernetske varnosti. Ker pa so njuni viri omejeni in ker se prednost daje drugim področjem, institucijam, organom in agencijam EU nista mogla zagotoviti vse potrebne podpore, zlasti v zvezi s krepitvijo zmogljivosti teh organizacij z nižjo stopnjo zrelosti na področju kibernetske varnosti (glej odstavke ***64***–***93***).

Priporočilo 3 – Povečati osredotočenost skupine CERT-EU in agencije ENISA na institucije, organe in agencije EU z nižjo stopnjo zrelosti

Skupina CERT-EU in agencija ENISA naj:

(a) opredelita prednostna področja, na katerih institucije, organi in agencije EU najbolj potrebujejo podporo, na primer z ocenami zrelosti;

(b) izvajata ukrepe za krepitev zmogljivosti v skladu z memorandumom o soglasju.

Ciljni rok za izvedbo: četrto četrtletje leta 2022.

To poročilo je sprejel senat III, ki ga vodi članica Evropskega računskega sodišča Bettina Jakobsen, v Luxembourgu na zasedanju 22. februarja 2022.

Za Evropsko računsko sodišče

Klaus-Heiner Lehne
predsednik

Prilogi

Priloga I – Seznam anketiranih institucij, organov in agencij EU

Ime institucije, organa ali agencije EU	Vrsta
Evropski parlament	institucija (člen 13(1) PEU)
Svet Evropske unije in Evropski svet	institucija (člen 13(1) PEU)
Evropska komisija	institucija (člen 13(1) PEU)
Sodišče Evropske unije	institucija (člen 13(1) PEU)
Evropska centralna banka (ECB)	institucija (člen 13(1) PEU)
Evropsko računsko sodišče	institucija (člen 13(1) PEU)
Evropska služba za zunanje delovanje (ESZD)	organ (člen 27(3) PEU)
Evropski ekonomsko-socialni odbor (EESO) in Evropski odbor regij (OR)[37]	organa (člen 13(4) PEU)
Evropska investicijska banka (EIB)	organ (člen 308 PDEU)
Evropski organ za delo (ELA)	decentralizirana agencija
Agencija Evropske unije za sodelovanje energetskih regulatorjev (ACER)	decentralizirana agencija
Urad Organa evropskih regulatorjev za elektronske komunikacije (Urad BEREC)	decentralizirana agencija
Urad Skupnosti za rastlinske sorte (CPVO)	decentralizirana agencija
Evropska agencija za varnost in zdravje pri delu (EU-OSHA)	decentralizirana agencija
Evropska agencija za mejno in obalno stražo (Frontex)	decentralizirana agencija
Agencija Evropske unije za operativno upravljanje obsežnih informacijskih sistemov s področja svobode, varnosti in pravice (eu-LISA)	decentralizirana agencija
Agencija Evropske unije za azil (EUAA)	decentralizirana agencija
Agencija Evropske unije za varnost v letalstvu (EASA)	decentralizirana agencija
Evropski bančni organ (EBA)	decentralizirana agencija
Evropski center za preprečevanje in obvladovanje bolezni (ECDC)	decentralizirana agencija
Evropski center za razvoj poklicnega usposabljanja (Cedefop)	decentralizirana agencija
Evropska agencija za kemikalije (ECHA)	decentralizirana agencija
Evropska agencija za okolje (EEA)	decentralizirana agencija
Evropska agencija za nadzor ribištva (EFCA)	decentralizirana agencija
Evropska agencija za varnost hrane (EFSA)	decentralizirana agencija

[37] EESO in OR se štejeta za eno samo institucijo, organ ali agencijo EU.

Ime institucije, organa ali agencije EU	Vrsta
Evropska fundacija za izboljšanje življenjskih in delovnih razmer (Eurofound)	decentralizirana agencija
Agencija Evropske unije za vesoljski program [nekdanja: Agencija za evropski GNSS – GSA] (EUSPA)	decentralizirana agencija
Evropski inštitut za enakost spolov (EIGE)	decentralizirana agencija
Evropski organ za zavarovanja in poklicne pokojnine (EIOPA)	decentralizirana agencija
Evropska agencija za pomorsko varnost (EMSA)	decentralizirana agencija
Evropska agencija za zdravila (EMA)	decentralizirana agencija
Evropski center za spremljanje drog in zasvojenosti z drogami (EMCDDA)	decentralizirana agencija
Agencija Evropske unije za kibernetsko varnost (ENISA)	decentralizirana agencija
Agencija Evropske unije za usposabljanje na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj (CEPOL)	decentralizirana agencija
Agencija Evropske unije za sodelovanje na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj (Europol)	decentralizirana agencija
Agencija Evropske unije za železnice (ERA)	decentralizirana agencija
Evropski organ za vrednostne papirje in trge (ESMA)	decentralizirana agencija
Evropska fundacija za usposabljanje (ETF)	decentralizirana agencija
Agencija Evropske unije za temeljne pravice (FRA)	decentralizirana agencija
Urad Evropske unije za intelektualno lastnino [do 23. marca 2016 imenovan OHIM] (EUIPO)	decentralizirana agencija
Enotni odbor za reševanje (SRB)	decentralizirana agencija
Agencija Evropske unije za pravosodno sodelovanje v kazenskih zadevah (Eurojust)	decentralizirana agencija
Prevajalski center za organe Evropske unije (CdT)	decentralizirana agencija
Evropsko javno tožilstvo (EJT)	decentralizirana agencija
Evropski inštitut za inovacije in tehnologijo (EIT)	organ, ustanovljen v okviru raziskav in inovacij
Skupno podjetje za raziskave o upravljanju zračnega prometa enotnega evropskega neba (SESAR)	skupno podjetje, ustanovljeno na podlagi PDEU
Skupno podjetje Elektronske komponente in sistemi za evropski vodilni položaj (ECSEL)	skupno podjetje, ustanovljeno na podlagi PDEU
Skupno podjetje za gorivne celice in vodik 2 (GCV 2)	skupno podjetje, ustanovljeno na podlagi PDEU
Skupno podjetje za pobudo za inovativna zdravila 2 (IMI2)	skupno podjetje, ustanovljeno na podlagi PDEU
Skupno podjetje Čisto nebo 2 (Čisto nebo 2)	skupno podjetje, ustanovljeno na podlagi PDEU

Ime institucije, organa ali agencije EU	Vrsta
Skupno podjetje (za skupno tehnološko pobudo) za industrijske panoge, ki temeljijo na rabi biomase (BBI)	skupno podjetje, ustanovljeno na podlagi PDEU
Skupno podjetje (za skupno tehnološko pobudo) Shift2Rail (S2R)	skupno podjetje, ustanovljeno na podlagi PDEU
Skupno podjetje za evropsko visokozmogljivostno računalništvo (EuroHPC)	skupno podjetje, ustanovljeno na podlagi PDEU
Evropsko skupno podjetje za ITER – Fuzija za energijo (F4E)	skupno podjetje, ustanovljeno na podlagi PDEU
svetovalna misija Evropske unije v Ukrajini (EUAM Ukraine)	civilna misija (SVOP)
svetovalna misija EU za meje v Libiji (EUBAM Libya)	civilna misija (SVOP)
misija EU za krepitev zmogljivosti v Nigru (EUCAP Sahel Niger)	civilna misija (SVOP)
nadzorna misija EU v Gruziji (EUMM Georgia)	civilna misija (SVOP)
koordinacijski urad EU za podporo palestinski policiji (EUPOL COPPS)	civilna misija (SVOP)
svetovalna misija EU v Srednjeafriški republiki (EUMAM RCA)	civilna misija (SVOP)
svetovalna misija EU v Iraku (EUAM Iraq)	civilna misija (SVOP)
misija pomoči EU za mejni prehod Rafa (EUBAM Rafah)	civilna misija (SVOP)
misija EU za krepitev zmogljivosti v Maliju (EUCAP Sahel Mali)	civilna misija (SVOP)
misija EU za krepitev zmogljivosti v Somaliji (EUCAP Somalia)	civilna misija (SVOP)
misija EU za krepitev pravne države na Kosovu (EULEX KOSOVO)	civilna misija (SVOP)

Priloga II – Dodatne informacije o ključnih medinstitucionalnih odborih

Medinstitucionalni odbor za digitalno preobrazbo (ICDT)

Medinstitucionalni odbor za digitalno preobrazbo je forum za izmenjavo informacij in spodbujanje sodelovanja na področju IT. Ustanovljen je bila maja 2020 in je nadomestil nekdanji *Comité Interinstitutionnel de l'Informatique* (CII). Sestavljajo ga vodilni uslužbenci iz oddelkov IT v institucijah, organih in agencijah EU. Ima podskupino za kibernetsko varnost (ICDT CSSG), katere naloga je spodbujati sodelovanje na področju kibernetske varnosti med institucijami, organi in agencijami EU ter ki deluje kot forum za izmenjavo informacij.

Pristojnost odločanja medinstitucionalnega odbora za digitalno preobrazbo je omejena na vprašanja, ki ne vplivajo na način, kako institucije uresničujejo svoje poslanstvo, in na upravljanje znotraj posameznih institucij. Za odločitve, ki presegajo njegove pristojnosti, lahko medinstitucionalni odbor za digitalno preobrazbo daje priporočila kolegiju generalnih sekretarjev institucij in organov EU.

V skladu z mandatom medinstitucionalnega odbora za digitalno preobrazbo so njegovi člani predstavniki vsake od institucij in organov EU ter en predstavnik, ki ga imenujejo agencije EU (svetovalni odbor za informacijsko in komunikacijsko tehnologijo – ICTAC). Trenutno mu predseduje generalni sekretariat Sveta.

Podskupina za kibernetsko varnost, ki deluje v okviru medinstitucionalnega odbora za digitalno preobrazbo (ICDT CSSG)

Podskupina za kibernetsko varnost, ki deluje v okviru medinstitucionalnega odbora za digitalno preobrazbo, je bila v sedanji sestavi ustanovljena septembra 2020 in je nadomestila stalno varnostno podskupino nekdanje CII. V primerjavi s svojo predhodnico ima podskupina bolj strukturiran, ambiciozen in v rezultate usmerjen pristop. Njene dejavnosti izvajajo projektne skupine, ki se redno sestajajo in se osredotočajo na ključna skupna vprašanja:

- projekta skupina 1: skupni standardi, primerjalna analiza in zrelost,
- projekta skupina 2: platforma za izmenjavo metod in orodij ter pogodb,
- projekta skupina 3: varnost oblakov,
- projekta skupina 4: razvoj talentov na področju kibernetskih znanj in spretnosti,
- projekta skupina 5: kibernetska ozaveščenost,

- projekta skupina 6: varnost videokonferenc.

Sekretariat podskupine je v skladu z njenimi pooblastili odgovoren za redno spremljanje napredka pri dejavnostih projektnih skupin in poročanje o njem. Redno pripravlja poročila predsedniku in namestniku predsednika podskupine, pri čemer redno zbira prispevke koordinatorjev projektnih skupin. Ob koncu vsakega leta mora podskupina predložiti tudi zbirno poročilo o dejavnostih.

Podskupini trenutno predseduje Komisija, namestnik predsednika pa je predstavnik svetovalnega odbora za informacijsko in komunikacijsko tehnologijo. Podskupina sicer nima pristojnosti odločanja, vendar lahko medinstitucionalnemu odboru za digitalno preobrazbo daje priporočila glede odločitev o pomembnih vprašanjih.

Mreža agencij

Mreža agencij EU je neformalna mreža, ki so jo leta 2012 ustanovili vodje agencij EU. Trenutno zajema 48 decentraliziranih agencij in skupnih podjetij EU. Njen cilj je članom mreže zagotoviti platformo za izmenjavo in sodelovanje na področjih skupnega interesa. Svetovalni odbor za IKT (ICTAC) je podskupina EUAN, ki je pristojna za spodbujanje sodelovanja na področju IKT, tudi na področju kibernetske varnosti.

Svetovalni odbor za informacijsko in komunikacijsko tehnologijo (ICTAC)

Svetovalni odbor za informacijsko in komunikacijsko tehnologijo spodbuja sodelovanje na področju IKT med agencijami in skupnimi podjetji. Njegov cilj je poiskati izvedljive in gospodarne rešitve skupnih težav, izmenjati informacije in po potrebi sprejeti skupna stališča. V skladu z njegovim mandatom se dvakrat letno organizirajo skupščine, ki se jih udeležijo vsi njegovi člani. Organizirajo se tudi redni mesečni sestanki predstavnikov svetovalnega odbora za informacijsko in komunikacijsko tehnologijo v projektnih skupinah podskupine za kibernetsko varnost, ki deluje v okviru medinstitucionalnega odbora za digitalno preobrazbo, predstavnika svetovalnega odbora za informacijsko in komunikacijsko tehnologijo v tej podskupini in trojke svetovalnega odbora za informacijsko in komunikacijsko tehnologijo. Trojko sestavljajo sedanji, prejšnji in prihodnji predsedniki svetovalnega odbora za informacijsko in komunikacijsko tehnologijo (mandat vsakega od predsednikov traja eno leto). Vloga trojke je podpirati sedanjega predsednika pri vseh zadevah, povezanih z njegovo vlogo, vključno z njegovo zamenjavo, če to zahtevajo okoliščine.

Kratice in okrajšave

CERT-EU: skupina za odzivanje na računalniške grožnje za evropske institucije, organe in agencije

CISO: pooblaščena oseba za varnost informacij

CSIRT: skupina za odzivanje na incidente na področju računalniške varnosti

ENISA: Agencija Evropske unije za kibernetsko varnost

EPDČ: ekvivalent polnega delovnega časa

eu-LISA: Agencija Evropske unije za operativno upravljanje obsežnih informacijskih sistemov s področja svobode, varnosti in pravice

GD DIGIT: Generalni direktorat za informatiko

GD HR: Generalni direktorat za človeške vire in varnost

ICDT CSSG: podskupina za kibernetsko varnost, ki deluje v okviru medinstitucionalnega odbora za digitalno preobrazbo

ICDT: medinstitucionalni odbor za digitalno preobrazbo

ICTAC: svetovalni odbor za informacijsko in komunikacijsko tehnologijo

IKT: informacijska in komunikacijska tehnologija

ISACA: Združenje za revizijo in kontrolo informacijskih sistemov

ITCB: Odbor za informacijsko tehnologijo in kibernetsko varnost

KIS: komunikacijski in informacijski sistem

NIS: varnost omrežij in informacij

SLA: sporazum o ravni storitve

Glosar

Etični heking: realistična simulacija kibernetskih napadov z uporabo elementa presenečenja in tehnik, ki so bile nedavno opažene v resničnem svetu, s poudarkom na specifičnih ciljih in v okviru več vrst napadov.

Kibernetska varnost: ukrepi za zaščito omrežij in infrastrukture IT ter informacij, ki jih ti vsebujejo, pred zunanjimi grožnjami.

Kibernetski prostor: globalno spletno okolje, v katerem ljudje, programska oprema in storitve komunicirajo prek omrežij računalnikov in drugih povezanih naprav.

Kibernetsko vohunjenje: dejanje ali praksa pridobivanja skrivnosti in informacij z interneta, omrežij ali posameznih računalnikov brez dovoljenja in vednosti imetnika teh informacij.

Lažno predstavljanje: pošiljanje elektronskih sporočil, ki so videti, kot da prihajajo iz zanesljivega vira, in tako prejemnike zavedejo, da odprejo zlonamerne povezave ali posredujejo osebne podatke.

Napredna trajna grožnja: napad, v katerem nepooblaščeni uporabnik vstopi v sistem ali omrežje z namenom kraje občutljivih podatkov in ostane tam dlje časa.

Penetracijsko testiranje: metoda ocenjevanja varnosti sistema IT, pri kateri se skušajo zaobiti varnostni zaščitni ukrepi z orodji in tehnikami, ki jih običajno uporabljajo napadalci.

Skupina za odzivanje na računalniške grožnje za evropske institucije, organe in agencije: koordinacijsko središče za izmenjavo informacij o kibernetski varnosti in za odzivanje na incidente, katerega stranke („udeleženci”) so institucije, organi in agencije EU.

Socialni inženiring: psihološka manipulacija na področju varnosti informacij, namenjena zavajanju ljudi, da nekaj storijo ali razkrijejo zaupne informacije.

Odgovori Komisije

https://www.eca.europa.eu/sl/Pages/DocItem.aspx?did=60922

Odgovori skupin CERT-EU in agencije ENISA

https://www.eca.europa.eu/sl/Pages/DocItem.aspx?did=60922

Časovni okvir

https://www.eca.europa.eu/sl/Pages/DocItem.aspx?did=60922

AVTORSKE PRAVICE

PDF	ISBN 978-92-847-7580-4	1977-5784	doi:10.2865/30482	QJ-AB-22-003-SL-N
HTML	ISBN 978-92-847-7575-0	1977-5784	doi:10.2865/5569	QJ-AB-22-003-SL-Q

Število kibernetskih napadov na institucije, organe in agencije EU se močno povečuje. Ker so institucije, organi in agencije EU med seboj tesno povezani, so lahko zaradi slabosti enega varnostnim grožnjam izpostavljeni tudi drugi. Sodišče je preučilo, ali imajo institucije, organi in agencije EU ustrezne ureditve za zaščito pred kibernetskimi grožnjami. Ugotovilo je, da njihova raven pripravljenosti na splošno ni sorazmerna z grožnjami in da imajo zelo različne ravni zrelosti na področju kibernetske varnosti. Priporoča, naj Komisija izboljša njihovo pripravljenost, in sicer tako, da predlaga uvedbo zavezujočih pravil o kibernetski varnosti in poveča vire za skupino za odzivanje na računalniške grožnje (CERT-EU). Poleg tega naj Komisija spodbuja nadaljnje sinergije med institucijami, organi in agencijami EU, skupina CERT-EU in Agencija Evropske unije za kibernetsko varnost pa naj svojo podporo osredotočita na manj zrele institucije, organe in agencije EU.

Posebno poročilo Sodišča v skladu z drugim pododstavkom člena 287(4) PDEU.

EVROPSKO RAČUNSKO SODIŠČE

Urad za publikacije Evropske unije

EVROPSKO RAČUNSKO SODIŠČE
12, rue Alcide De Gasperi
1615 Luxembourg
LUKSEMBURG

Tel. +352 4398-1

Vprašanja: eca.europa.eu/sl/Pages/ContactForm.aspx
Spletišče: eca.europa.eu
Twitter: @EUAuditors