ODGOVORI EVROPSKE KOMISIJE

NA POSEBNO POROČILO EVROPSKEGA RAČUNSKEGA SODIŠČA

Kibernetska varnost institucij, organov in agencij EU: raven pripravljenosti na splošno ni sorazmerna z grožnjami

SL

SL

Kazalo

V tem dokumentu so predstavljeni odgovori Evropske komisije na opažanja iz posebnega poročila Evropskega računskega sodišča v skladu s členom 259 finančne uredbe in se objavi skupaj s posebnim poročilom.

I. ODGOVORI KOMISIJE NA KRATKO

(a) Splošni uvod

Kibernetska varnost je postala glavna politična in operativna prednostna naloga Evropske komisije. Kriza zaradi COVID-19 je pospešila našo odvisnost od digitalnih storitev (računalništvo v oblaku, mobilne naprave, umetna inteligenca). V zadnjih dveh letih smo doživeli velik prehod na delo od doma. To pomeni, da sta se na splet v veliki meri preselila tudi kibernetska kriminaliteta in kibernetsko vohunjenje, ki sta glavni grožnji, s katerima se soočajo institucije, organi in agencije EU. Komisija se zaveda tega trenda. Na področju kibernetske varnosti je pokazala dosledno in odločno vodenje. Leta 2019 je začela veljati uredba o kibernetski varnosti, ki je med drugim razširila mandat agencije ENISA in jo vzpostavila kot stalno agencijo. S to uredbo je bilo vzpostavljeno tudi formalno sodelovanje med agencijo ENISA in skupino CERT-EU (skupina za odzivanje na računalniške grožnje za evropske institucije, organe in agencije). Komisija je leta 2020 predlagala okrepitev direktive o varnosti omrežij in informacij, ki je blizu dogovoru v zakonodajnem organu.

Tudi strategija za kibernetsko varnost iz leta 2020 je vsebovala tri ukrepe, povezane s kibernetsko varnostjo institucij, organov in agencij EU. V strategiji so bile napovedane uredba o informacijski varnosti v institucijah, organih in agencijah EU, uredba o skupnih pravilih o kibernetski varnosti za institucije, organe in agencije EU ter namera Komisije, da zagotovi novo pravno podlago za skupino CERT-EU, ki bi okrepila njen mandat in financiranje ter ji tako ob vse večjih grožnjah, tveganjih in incidentih zagotovila ustrezne vire.

Priprava teh predlogov je napredovala. Čeprav jih kolegij še ni sprejel, se pričakuje, da bodo sprejeti v prvem četrtletju leta 2022. Pomembna vprašanja, o katerih so v tej pripravljalni fazi razpravljale institucije, se nanašajo na pravno podlago predloga in proračunsko zmogljivost vseh institucij, organov in agencij EU za izpolnjevanje zahtev glede financiranja lastnih potreb na področju kibernetske varnosti ter za iskanje potrebnih virov za podporo proračunu skupine CERT-EU, in zlasti delovnim mestom.

Ravni pripravljenosti institucij, organov in agencij EU na področju kibernetske varnosti so različne zrelosti. Več institucij, organov in agencij EU je zelo uspešnih v smislu kibernetske pripravljenosti in bi morali še naprej delovati kot voditelji, ki predstavljajo spodbudo in zgled za napredek in nadaljnje izboljšave na celotnem področju kibernetske varnosti. Da bi dosegli merljiv napredek, je pomembno priznati različne ravni zrelosti institucij, organov in agencij EU ter določiti prednostne naloge, tako da se ukrepi za izboljšanje namenijo predvsem tistim institucijam, organom in agencijam EU, v katerih ugotovljene vrzeli povzročajo največjo izpostavljenost tveganju.

(b) Stališče Komisije o ključnih opažanjih in priporočilih Evropskega računskega sodišča

Komisija pozdravlja poročilo Evropskega računskega sodišča o kibernetski varnosti institucij, organov in agencij EU. Ugotavlja, da je v poročilu poudarjen pomen skupnih pravnih okvirov za vse institucije, organe in agencije EU na področju informacijske in kibernetske varnosti, da bi se na splošno povečala skupna raven kibernetske varnosti. Komisija ugotavlja, da glavna opažanja in priporočila Evropskega računskega sodišča niso namenjena operativni kibernetski varnosti Komisije kot taki, temveč njeni vlogi na področju politik kot predlagateljici zakonodaje za dvig kibernetske zrelosti institucij, organov in agencij EU.

Prihodnji uredbi o informacijski varnosti v institucijah, organih in agencijah EU ter o skupnih pravilih o kibernetski varnosti za institucije, organe in agencije EU bosta določili skupna pravila za doseganje visoke ravni informacijske in kibernetske varnosti, vendar njuno izvajanje v organizacijskem in operativnem kontekstu vsake evropske institucije, organa ali agencije EU (zlasti njihovih profilov groženj in tveganj) ostaja v avtonomni pristojnosti vsake od njih. Predlagana uredba o kibernetski varnosti bo vsebovala mehanizme za izpolnjevanje zahtev, ki bodo ustrezni in sorazmerni s ciljem in področjem uporabe novih pravil, brez poseganja v avtonomijo institucij, organov in agencij.

Komisija trenutno predseduje podskupini za kibernetsko varnost, ki deluje v okviru medinstitucionalnega odbora za digitalno preobrazbo (ICDT); predsedovanje se izvaja po načelu rotacije (za obdobje do dveh let). Opozoriti je treba, da za delo podskupine niso bila dodeljena nobena namenska sredstva: vsi ukrepi temeljijo na najboljših prizadevanjih udeležencev na prostovoljni osnovi.

Komisija se strinja s splošno idejo o okrepitvi virov in pooblastil skupine CERT-EU.

Komisija ob takem razumevanju podpira ključne ugotovitve in priporočila iz poročila. Naše podrobno stališče je pojasnjeno v dodatnih pripombah v oddelku III. Kar zadeva priporočila, Komisija sprejema priporočila 1(a), (b), (c), (d), (e), (f), (g) in 2(a), (b), (c).

(c) Relevanten najnovejši razvoj dogodkov in naslednji koraki

Na ravni generalnih direktorjev institucij, organov in agencij EU je bilo zaključeno uradno posvetovanje o konsolidiranih osnutkih obeh uredb (informacijska varnost, kibernetska varnost), ocena prejetih povratnih informacij pa še poteka, preden bo sveženj dokončan in ga bo kolegij sprejel v prvem četrtletju leta 2022.

II. ODGOVORI KOMISIJE NA GLAVNA OPAŽANJA EVROPSKEGA RAČUNSKEGA SODIŠČA

1. Stopnje zrelosti institucij, organov in agencij EU na področju kibernetske varnosti

Komisija se strinja, da je pri opazovanju ravni porabe institucij, organov in agencij EU za kibernetsko varnost pomembno upoštevati grožnje in tveganja.

Podobno s kadrovskega vidika na stabilnost števila zaposlenih v institucijah, organih in agencijah EU vplivajo številni dejavniki. Trg za zaposlovanje specializiranih strokovnjakov za kibernetsko varnost je vse bolj kompleksen. V številnih primerih pravila o človeških virih niso prilagojena specializiranim profilom (zaposlovanje, poklicni razvoj, usposabljanje). Poleg tega splošni pritisk proračunskega organa na število zaposlenih v institucijah, organih in agencijah EU pomeni, da je za nova prednostna področja, kot je kibernetska varnost, še vedno na voljo premalo delovnih mest, zlasti v notranjih operativnih službah.

Pri sklicevanju na napredek pri upravljanju in obvladovanju tveganja bi bilo treba upoštevati dejstvo, da spremljanje izpolnjevanja zahtev zdaj prehaja s pilotnega izvajanja na popolno uvedbo. Zato je običajno, da je dosedanja pokritost precej nizka. Ta projekt za izpolnjevanje zahtev je naslednja faza dolgoročnega procesa izboljšanja kibernetske zrelosti, ki se je začel z opredelitvijo skupne metodologije tveganja, oblikovanjem skupnih orodij, uvedbo upravljanja ranljivosti ter spremljanjem, preskušanjem in potrjevanjem evidence sredstev. Na tej dolgi poti je bil kljub kompleksnosti baze sredstev Komisije z več kot 1 000 informacijskimi sistemi, ki jih upravlja več kot 50 generalnih direktoratov in izvajalskih agencij, dosežen napredek.

2. Mehanizmi institucij, organov in agencij EU za sodelovanje

Skupina CERT-EU je izjemna zgodba o uspehu pri spodbujanju sodelovanja ne le med institucijami, organi in agencijami EU, temveč tudi na evropski ravni, in sicer z njenim sodelovanjem kot polnopravna članica v mreži CSIRT, vzpostavljeni na podlagi direktive o varnosti omrežij in informacij. S tem je skupina CERT-EU zgled za to, kako je mogoče okrepiti sodelovanje in storitve kibernetske varnosti. Opažanja Evropskega računskega sodišča o skupini CERT-EU zelo jasno ponazarjajo izjemno delo, ki ga CERT-EU opravlja v vse bolj sovražnem okolju kibernetskih groženj in s kronično nezadostnimi viri.

V skladu s sedanjim medinstitucionalnim dogovorom decentralizirane agencije in skupna podjetja EU v usmerjevalnem odboru skupine CERT-EU uradno zastopa agencija ENISA. Poleg tega njihova stališča na sejah usmerjevalnega odbora izrazi predstavnik svetovalnega odbora za IKT (ICTAC), ki se jih lahko udeleži, da agenciji ENISA pomaga pri zastopanju agencij, vendar nima uradnega sedeža ali glasu. Vprašanje ustrezne zastopanosti agencij v usmerjevalnem odboru skupine CERT-EU bo obravnavano v predlagani uredbi z dopolnitvijo sestave usmerjevalnega odbora z do tremi predstavniki, ki jih imenuje mreža agencij Unije na predlog svojega svetovalnega odbora za IKT.

Sodelovanje v podskupini ICDT za kibernetsko varnost temelji na najboljših prizadevanjih, in sicer na ravni sodelovanja, ki jo določi vsaka institucija, organ ali agencija EU posebej. Pri pripravi nove okvirne pogodbe za kibernetsko varnost se obravnavajo izboljšave v zvezi z izmenjavo informacij o javnem naročanju, ki je pomembna tema v okviru projektne skupine 2 podskupine za kibernetsko varnost.

Kar zadeva skupna orodja za storitve, kot sta elektronska pošta in videokonference, že obstaja možnost uporabe sistema SECEM-2, ki ga Komisija izvaja za vse institucije, organe in agencije EU, za šifrirano elektronsko pošto, odvisno od uspešnega upravljanja šifrirnih ključev in potrdil. Poleg tega se razvija orodje SECABC, ki bo omogočalo šifriranje elektronske pošte med institucijami, z namenom, da se vsem zainteresiranim institucijam, organom in agencijam EU ponudi dostop do njega od leta 2022. Varna videokonferenčna povezava za storitve prenosa občutljivih netajnih podatkov je že dosežena in se lahko *ad hoc* razširi na druge institucije, organe in agencije EU z upravljanjem identitet udeležencev sestanka. Izmenjava občutljivih informacij bo obravnavana tudi v predlagani uredbi o informacijski varnosti (tj. s skupnim etiketiranjem in označevanjem).

3. Izmenjava informacij o pomembnih incidentih ali šibkih točkah

V osnutku uredbe o kibernetski varnosti je v skladu s predlogom Komisije iz direktive o varnosti omrežij in informacij 2 obravnavano dejstvo, da vse institucije, organi in agencije EU ne priglasijo pomembnih incidentov ali šibkih točk skupini CERT-EU[1]. Raven izvajanja bo odvisna od dodatnih virov, ki jih bodo za to namenili avtonomni institucije, organi in agencije EU. Možnosti za izvrševanje takih obvestil ostajajo tudi v okviru predlagane uredbe, kot je trenutno načrtovana, omejene zaradi institucionalne avtonomije institucij, organov in agencij EU. Predlagana uredba o kibernetski varnosti bo vsebovala mehanizme za izpolnjevanje zahtev, ki bodo ustrezni in sorazmerni s ciljem in področjem uporabe novih pravil, brez poseganja v avtonomijo institucij, organov in agencij.

III. ODGOVORI KOMISIJE NA ZAKLJUČKE IN PRIPOROČILA EVROSPKEGA RAČUNSKEGA SODIŠČA

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

Predlagano besedilo uredbe bo vključevalo posebne ukrepe za nadaljnje povečanje skupne ravni kibernetske varnosti. Navedeni ukrepi bodo preneseni v načrte za kibernetsko varnost, ki bodo opredeljeni in izvedeni na ravni institucij, organov in agencij EU v okviru njihovega okvira upravljanja kibernetske varnosti.

Komisija sprejema to priporočilo. V zvezi s specifičnimi podpriporočili Komisija ugotavlja naslednje:

(a) Komisija sprejema priporočilo 1(a.) Osnutek uredbe bo vključeval določbe o okvirih upravljanja in kontrole, vzpostavljenih na najvišji ravni izvršnega upravljanja vsake institucije, organa in agencije EU, da se zagotovi učinkovito in preudarno upravljanje vseh tveganj za kibernetsko varnost.

(b) Komisija sprejema priporočilo 1(b). Osnutek uredbe bo v večji meri poudaril pristop k upravljanju kibernetske varnosti na podlagi tveganja, tako da bo pojasnil, da bi morali ukrepi, varnostni načrti za IT in dejansko izvajanje bistvenih kontrol slediti ocenam.

(c) Komisija sprejema priporočilo 1(c). Programi izobraževanja, ozaveščanja in usposabljanja na področju kibernetske varnosti bodo v osnutku uredbe navedeni kot del izhodišča za kibernetsko varnost.

(d) Komisija sprejema priporočilo 1(d). Čeprav so po naših izkušnjah redne revizije in preskusi bistvenega pomena, ne zadostujejo za zagotovitev napredka. Zato sta kot del okvira upravljanja kibernetske varnosti iz točke (a) potrebna redno poročanje in preglednost.

[1] Predlog direktive Evropskega parlamenta in Sveta o ukrepih za visoko skupno raven kibernetske varnosti v Uniji in razveljavitvi Direktive (EU) 2016/1148 (COM(2020) 823 final).

(e) Komisija sprejema priporočilo 1(e). Osnutek uredbe bo vključeval določbe v zvezi z obveščanjem skupine CERT-EU o pomembnih kibernetskih grožnjah, šibkih točkah in incidentih s strani institucij, organov in agencij EU.
(f) Komisija sprejema priporočilo 1(f). Komisija podpira potrebo po okrepitvi virov skupine CERT-EU. Določbe v zvezi z osebjem in finančnimi prispevki institucij, organov in agencij EU bodo vključene v besedilo osnutka uredbe.
(g) Komisija sprejema priporočilo 1(g). Predlagana uredba bo imela mehanizme za izpolnjevanje zahtev, ki bodo ustrezni in sorazmerni s ciljem in področjem uporabe določb, ob upoštevanju institucionalne avtonomije institucij, organov in agencij EU. Vsebina prihodnje uredbe je odvisna od izida zakonodajnega postopka in je rezultat odločitve zakonodajalca EU o predlogu Komisije.

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

Komisija, ki trenutno predseduje podskupini za kibernetsko varnost, ki deluje v okviru medinstitucionalnega odbora za digitalno preobrazbo (ICDT), se strinja s priporočili za spodbujanje rešitev za dosledno in varno izmenjavo občutljivih informacij, za sistematično izmenjavo informacij o projektih kibernetske varnosti ter za skupne okvire javnega naročanja in pogodbe za storitve kibernetske varnosti.

Komisija sprejema to priporočilo. V zvezi s specifičnimi podpriporočili Komisija ugotavlja naslednje:

(a) Komisija sprejema priporočilo 2(a). Komisija predlaga tehnične pobude in storitve podskupini ICDT za kibernetsko varnost, da bi spodbujala in podpirala skupna orodja za izmenjavo občutljivih informacij, ki omogočajo storitve, kot sta elektronska pošta in videokonferenca. Ugotavljamo tudi, da bodo v predlagani uredbi o varnosti podatkov obravnavani skupno označevanje in skupna pravila za obravnavanje občutljivih netajnih informacij.
(b) Komisija sprejema priporočilo 2(b). To točko obravnavajo in jo bodo nadalje razvile obstoječe projektne skupine v okviru podskupine ICDT za kibernetsko varnost. Pri pripravi nove okvirne pogodbe za kibernetsko varnost se obravnavajo izboljšave v zvezi z izmenjavo informacij o javnem naročanju.
(c) Komisija sprejema priporočilo 2(c) Institucije, organi in agencije EU že imajo dostop do medinstitucionalnih okvirnih pogodb na področju IKT, ki jih upravlja Komisija. Priprava nove okvirne pogodbe za kibernetsko varnost bo usklajena s podskupino ICDT za kibernetsko varnost.

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

To priporočilo je naslovljeno na skupino CERT-EU in agencijo ENISA.