ODGOVORI EUROPSKE KOMISIJE

NA TEMATSKO IZVJEŠĆE EUROPSKOG REVIZORSKOG SUDA

Kibersigurnost institucija, tijela i agencija EU-a: razina pripravnosti nije razmjerna prijetnjama

HR

HR

Sadržaj

Ovaj dokument sadržava odgovore Europske komisije na opažanja iz tematskog izvješća Europskog revizorskog suda, u skladu s člankom 259. Financijske uredbe, i objavit će se zajedno s tematskim izvješćem.

I. SAŽETAK ODGOVORÂ KOMISIJE

a) Uvod

Kibersigurnost je postala glavni politički i operativni prioritet Europske komisije. Kriza uzrokovana bolešću COVID-19 povećala je našu ovisnost o digitalnim uslugama (računalstvo u oblaku, mobilni uređaji, umjetna inteligencija). Protekle dvije godine svjedočili smo velikom pomaku prema radu od kuće. To znači da su se kiberkriminal i kiberšpijunaža, najveće dvije prijetnje s kojima se suočavaju institucije, tijela i agencije Europske unije, uvelike preselili na internet. Komisija je to uočila i reagirala je kvalitetnim i odlučnim vodstvom u području kibersigurnosti. Akt o kibersigurnosti stupio je na snagu 2019. i njime se, među ostalim, Agencija Europske komisije za kibersigurnost (ENISA) uspostavlja kao stalna agencija i produžuje joj se mandat. Tim se Aktom uspostavlja i službena suradnja između ENISA-e i tima CERT-EU (tim za hitne računalne intervencije koji podržava sve organe EU-a). Komisija je 2020. predložila jačanje Direktive o sigurnosti mrežnih i informacijskih sustava, o kojoj je dogovor u zakonodavnom tijelu blizu.

Strategija za kibersigurnost iz 2020. sadržava i tri mjere povezane s kibersigurnošću u organima EU-a. U strategiji su najavljene uredba o informacijskoj sigurnosti u institucijama, tijelima i agencijama EU-a, uredba o zajedničkim pravilima o kibersigurnosti za institucije, tijela i agencije EU-a i namjera Komisije da pruži novu pravnu osnovu na temelju koje bi tim CERT-EU ojačao svoj mandat i financiranje, da bi osigurao odgovarajuća sredstva s obzirom na rastuće prijetnje, rizike i incidente.

Izrada tih prijedloga je napredovala. Iako ih kolegij još nije donio, očekuje se da će to učiniti u prvom tromjesečju 2022. Važna pitanja o kojima su institucije raspravljale tijekom ove pripremne faze odnose se na pravnu osnovu prijedloga i proračunski kapacitet svakog organa EU-a da ispuni zahtjeve za financiranje vlastitih potreba kibersigurnosti i pronađe neophodna sredstva za potporu timu CERT-EU, za proračun i pogotovo za radna mjesta.

Razine pripravnosti institucija, tijela i agencija EU-a u području kibersigurnosti razlikuju se po stupnjevima osviještenosti. Nekoliko organa EU-a vrlo je uspješno s obzirom na kiberpripravnost i oni bi trebali i dalje biti predvodnici u podržavanju i promicanju napretka te daljnjih poboljšanja u cijelom području kibersigurnosti. Kako bi se postigao mjerljivi napredak, važno je odrediti različite stupnjeve osviještenosti u organima EU-a i utvrditi prioritete tako da se mjere poboljšanja usmjere na one organe EU-a kod kojih su utvrđeni nedostaci koji predstavljaju najveću izloženost riziku.

b) Stajalište Komisije o ključnim opažanjima i preporukama Europskog revizorskog suda

Komisija pozdravlja izvješće Europskog revizorskog suda i kibersigurnosti institucija, tijela i agencija EU-a. Napominje da se u izvješću naglašava važnost zajedničkih pravnih okvira za sve organe EU-a u području informacijske sigurnosti i kibersigurnosti kako bi se općenito povećala ukupna razina kibersigurnosti. Komisija napominje da glavna opažanja i preporuke Europskog revizorskog suda nisu usmjereni na operativnu kibersigurnost Komisije, već na političku ulogu Komisije u predloženom zakonodavstvu čiji je cilj povećati kiberosviještenost organa EU-a.

Budućim uredbama o „informacijskoj sigurnosti u institucijama, tijelima i agencijama EU-a” te „zajedničkim pravilima o kibersigurnosti za institucije, tijela i agencije EU-a” utvrdit će se zajednička

pravila za postizanje visoke razine informacijske sigurnosti i kibersigurnosti, ali njihova provedba u organizacijskom i operativnom kontekstu svakog organa EU-a (posebno njihovi profili prijetnji i rizičnosti) i dalje je autonomna odgovornost tih organa EU-a. Predložena uredba o kibersigurnosti sadržavat će mehanizme za postizanje sukladnosti koji odgovaraju i proporcionalni su cilju i području primjene novih pravila, ne dovodeći u pitanje autonomiju institucija, tijela i agencija.

Komisija trenutačno predsjeda podskupinom za kibersigurnost u okviru Međuinstitucijskog odbora za digitalnu transformaciju (ICDT); predsjedanje je rotirajuće (na razdoblje do dvije godine). Treba napomenuti da za rad podskupine nisu dodijeljena namjenska sredstva: sve se mjere temelje na dobrovoljnom trudu sudionika.

Komisija se slaže s općom idejom povećanja sredstava i jačanja mandata tima CERT-EU.

S obzirom na to, Komisija podržava ključna opažanja i preporuke izvješća. Naše je stajalište detaljno objašnjeno u dodatnim primjedbama u odjeljku III. Što se tiče preporuka, Komisija prihvaća točke (a), (b), (c), (d), (e), (f) i (g) 1. preporuke te točke (a), (b) i (c) 2. preporuke.

c) Relevantni nedavni događaji i sljedeći koraci

Na razini glavnih direktora organa EU-a završeno je službeno savjetovanje o konsolidiranim nacrtima obaju propisa (informacijska sigurnost, kibersigurnost), a još traje procjena primljenih povratnih informacija, prije nego što se paket dovrši i kolegij ga usvoji u prvom tromjesečju 2022.

II. ODGOVORI KOMISIJE NA GLAVNA OPAŽANJA EUROPSKOG REVIZORSKOG SUDA

1. Stupnjevi osviještenosti o kibersigurnosti organa EU-a

Komisija se slaže da je pri praćenju razine potrošnje organa EU-a na kibersigurnost važno uzeti u obzir prijetnje i rizike.

Isto tako, u kontekstu ljudskih resursa, na stabilnost broja osoblja u organima EU-a utječe niz čimbenika. Tržište za zapošljavanje specijaliziranih stručnjaka za kibersigurnost sve je složenije. U mnogim slučajevima pravila o ljudskim resursima nisu prilagođena specijaliziranim profilima (zapošljavanje, profesionalni razvoj, osposobljavanje). Osim toga, opći pritisak proračunskog tijela na broj zaposlenih u svim organima EU-a znači da je još premalo radnih mjesta za nova visokoprioritetna područja kao što je područje kibersigurnosti, posebno u internim operativnim službama.

Kod upućivanja na napredak u upravljačkoj strukturi i upravljanju rizikom trebalo bi uzeti u obzir činjenicu da praćenje usklađenosti sada prelazi s pilot-provedbe u potpunu provedbu. Stoga je normalno da je trenutačna pokrivenost poprilično niska. Taj projekt usklađenosti sljedeća je faza u dugoročnom procesu povećanja kiberosviještenosti koji je počeo definiranjem zajedničke metodologije procjene rizika, razvojem zajedničkog alata, uvođenjem upravljanja slabim točkama i praćenja, ispitivanja i provjere popisa resursa. Unatoč složenosti baze resursa Komisije s više od 1 000 informacijskih sustava kojima upravlja više od 50 glavnih uprava i izvršnih agencija, postignut je napredak.

2. Mehanizmi organa EU-a za suradnju

Tim CERT-EU izuzetno uspješno promiče suradnju među organima EU-a i na europskoj razini, zato što je punopravni član mreže timova za odgovor na računalne sigurnosne incidente (CSIRT) koja je uspostavljena u skladu s Direktivom o sigurnosti mrežnih i informacijskih sustava. Tim CERT-EU zato je izuzetan primjer poboljšanja suradnje i usluga kibersigurnosti. Opažanja Europskog revizorskog suda o timu CERT-EU vrlo jasno prikazuju odličan rad tima CERT-EU u okruženju sve brojnijih i ozbiljnijih kiberprijetnji s kronično nedovoljnim resursima.

U skladu s postojećim Međuinstitucijskim sporazumom (IIA), decentralizirane agencije i zajednička poduzeća EU-a u Upravljačkom odboru tima CERT-EU službeno zastupa ENISA. Nadalje, njihova stajališta na sastancima Upravljačkog odbora iznosi predstavnik Savjetodavnog odbora za IKT (ICTAC), koji smije prisustvovati kako bi pomogao ENISA-i u zastupanju agencija, ali nema službeno mjesto ili pravo glasa. Pitanje odgovarajuće zastupljenosti agencija u Upravljačkom odboru tima CERT-EU bit će obrađeno u predloženoj uredbi dopunom sastava Upravljačkog odbora s najviše tri zastupnika koje imenuje Mreža agencija Europske unije (EUAN) na prijedlog svog Savjetodavnog odbora za IKT.

Sudjelovanje u podskupini ICDT-a za kibersigurnost najviše se temelji na angažmanu o kojem odlučuje svaki organ EU-a. U pripremi novog okvirnog sporazuma o kibersigurnosti razmatraju se poboljšanja u razmjeni informacija o javnoj nabavi, što je važna tema u radnoj skupini 2 podskupine za kibersigurnost.

Već postoji mogućnost upotrebe sustava SECEM-2 koji je Komisija uvela za sve organe EU-a kao zajedničkog alata za usluge kao što su e-pošta i videokonferencije, za šifriranu e-poštu ovisno o učinkovitosti upravljanja ključevima za šifriranje i certifikatima. Osim toga, u izradi je i SECABC, alat za šifriranje e-pošte koja se razmjenjuje među institucijama, s ciljem da od 2022. postane dostupan svim zainteresiranim organima EU-a. Već je postignuta sigurna videokonferencijska veza za usluge prijenosa osjetljivih podataka koji nisu povjerljivi i može se *ad hoc* proširiti na druge organe EU-a tako da se upravlja identitetom sudionika na sastanku. Razmjenom osjetljivih informacija bavit će se i predložena uredba o informacijskoj sigurnosti (kroz zajedničko označivanje i oznake).

3. Razmjena informacija o ozbiljnim incidentima ili slabim točkama

Nacrt uredbe o kibersigurnosti, u skladu s prijedlogom Komisije u direktivi o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije (NIS-2)[1], bavi se činjenicom da ne prijavljuju svi organi EU-a ozbiljne incidente ili slabe točke. Razina provedbe ovisit će o dodatnim sredstvima koja joj dodijele autonomni organi EU-a. Zbog institucijske autonomije organa EU-a u sadašnjem prijedlogu te uredbe područje primjene takvih obavijesti ostaje ograničeno. Predložena uredba o kibersigurnosti sadržavat će mehanizme za postizanje sukladnosti koji odgovaraju i proporcionalni su cilju i području primjene novih pravila, ne dovodeći u pitanje autonomiju institucija, tijela i agencija.

[1] Prijedlog Direktive Europskog parlamenta i Vijeća o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije i stavljanju izvan snage Direktive (EU) 2016/1148, COM/2020/823 final

III. ODGOVORI KOMISIJE NA ZAKLJUČKE I PREPORUKE EUROPSKOG REVIZORSKOG SUDA

1. preporuka – Potrebno je poboljšati pripravnost svih organa EU-a u području kibersigurnosti s pomoću zajedničkih obvezujućih pravila i povećanjem resursa za tim CERT-EU

Predloženi tekst uredbe uključivat će posebne mjere za daljnje povećanje ukupne razine kibersigurnosti. Te će se mjere pretočiti u planove za kibersigurnost koji će se definirati i provoditi na razini organa EU-a prema njihovu okviru upravljačke strukture za kibersigurnost.

Komisija prihvaća ovu preporuku. S obzirom na posebne potpreporuke, Komisija ističe sljedeće:

a) Komisija prihvaća točku (a) 1. preporuke. Nacrt uredbe uključivat će odredbe o okvirima upravljačke strukture i kontrole, uspostavljenima na najvišoj razini izvršne vlasti svakog organa EU-a, kako bi se osiguralo učinkovito i razborito upravljanje svim rizicima za kibersigurnost.
b) Komisija prihvaća točku (b) 1. preporuke. U nacrtu uredbe naglasit će se pristup upravljanju kibersigurnošću koji se temelji na riziku, jasnim navođenjem da mjere, planovi informacijske sigurnosti i stvarna provedba bitnih kontrola trebaju pratiti procjene.
c) Komisija prihvaća točku (c) 1. preporuke. Edukacija o kibersigurnosti, programi jačanja svijesti i osposobljavanja bit će navedeni u nacrtu uredbe kao dio osnove kibersigurnosti.
d) Komisija prihvaća točku (d) 1. preporuke. Iako su, prema našem iskustvu, redovite revizije i testiranja bitni, oni nisu dovoljni za osiguranje napretka. Stoga je potrebno redovito izvješćivanje i transparentnost, kao dio okvira upravljačke strukture za kibersigurnost iz točke (a).
e) Komisija prihvaća točku (e) 1. preporuke. Nacrt uredbe uključivat će odredbe o obavijestima koje organi EU-a dostavljaju timu CERT-EU.
f) Komisija prihvaća točku (f) 1. preporuke. Komisija podržava potrebu za povećanje sredstava za tim CERT-EU. Odredbe o doprinosu broja osoblja i financijskom doprinosu organima EU-a bit će uključene u tekst nacrta uredbe.
g) Komisija prihvaća točku (g) 1. preporuke. Predložena uredba imat će mehanizme usklađenosti koji su primjereni i razmjerni cilju i području primjene novih odredbi, uzimajući u obzir institucionalnu autonomiju organa EU-a. Sadržaj buduće uredbe ovisi o ishodu zakonodavnog postupka i rezultat je odluke zakonodavca EU-a na prijedlog Komisije.

2. preporuka – Potrebno je zagovarati dublju sinergiju među organima EU-a u odabranim područjima

Komisija, koja trenutačno predsjeda podskupinom za kibersigurnost u okviru Međuinstitucijskog odbora za digitalnu transformaciju (ICDT), slaže se s preporukama za promicanje rješenja za dosljednu i sigurnu razmjenu osjetljivih informacija, sustavnu razmjenu informacija o projektima kibersigurnosti i za zajedničke okvire nabave te ugovore za usluge kibersigurnosti.

Komisija prihvaća ovu preporuku. S obzirom na posebne potpreporuke, Komisija ističe sljedeće:

a) Komisija prihvaća točku (a) 2. preporuke. Omogućujući pružanje usluga kao što su e-pošta i videokonferencije, Komisija šalje tehničke inicijative i usluge podskupini za kibersigurnost u okviru ICDT-a kako bi promovirala i podržala zajedničke alate za razmjenu osjetljivih informacija. Ističemo da će se u predloženoj uredbi o informacijskoj sigurnosti obraditi zajedničke oznake i zajednička pravila za postupanje osjetljivim podacima koji nisu zaštićeni.
b) Komisija prihvaća točku (b) 2. preporuke. Ovu točku rješavaju i dalje će je razvijati postojeće radne skupine unutar podskupine za kibersigurnost u okviru ICDT-a. U pripremi novog okvirnog sporazuma o kibersigurnosti razmatraju se poboljšanja u razmjeni informacija o javnoj nabavi.
c) Komisija prihvaća točku (c) 2. preporuke. Organi EU-a već imaju pristup međuinstitucijskim okvirnim sporazumima o IKT-u kojim upravlja Komisija. Priprema novog okvirnog sporazuma o kibersigurnosti bit će koordinirana s podskupinom za kibersigurnost u okviru ICDT-a.

3. preporuka – Potrebno je povećati usredotočenost ENISA-e i tima CERT-EU na manje osviještene organe EU-a

Ova je preporuka upućena timu CERT-EU i ENISA-i.