EUROPSKI REVIZORSKI SUD

HR

Priopćenje za medije

Luxembourg, 29. ožujka 2022.

Tijela EU-a moraju podići razinu pripravnosti u području kibersigurnosti

Broj kibernapada na tijela EU-a u naglom je porastu. Razina pripravnosti tijela EU-a u području kibersigurnosti neujednačena je i općenito nerazmjerna rastućim prijetnjama. Budući da su tijela EU-a tijesno međusobno povezana, slaba točka jednoga može izložiti i druga tijela sigurnosnim prijetnjama. To je zaključak tematskog izvješća Europskog revizorskog suda koje donosi analizu pripravnosti upravljačkih tijela EU-a na kiberprijetnje. Revizori preporučuju da se uvedu obvezujuća kibersigurnosna pravila i povećaju resursi dostupni timu za hitne računalne intervencije (CERT-EU). Europska komisija trebala bi promicati i jaču suradnju među tijelima EU-a, tvrde revizori, dok bi se tim CERT-EU i Agencija Europske unije za kibersigurnost trebali više usmjeriti na tijela EU-a koja imaju manje iskustva u upravljanju kibersigurnošću.

U razdoblju 2018. – 2021. broj ozbiljnih incidenata u tijelima EU-a više se nego udeseterostručio; radom na daljinu znatno se povećao broj potencijalnih pristupnih točaka za napadače. Ozbiljni incidenti općenito su posljedica složenih kibernapada koji obično uključuju primjenu novih metoda i tehnologija te za istragu nad njima i oporavak od njih mogu biti potrebni tjedni, ako ne i mjeseci. Jedan od primjera bio je kibernapad na Europsku agenciju za lijekove, zbog kojeg su procurili osjetljivi podatci kojima se manipuliralo kako bi se poljuljalo povjerenje u cjepiva.

„Institucije, tijela i agencije EU-a privlačne su mete potencijalnih napadača, posebice skupina koje su u stanju izvršiti vrlo sofisticirane prikrivene napade radi kiberšpijunaže i u druge zlonamjerne svrhe”, izjavila je Bettina Jakobsen, članica Suda koja je predvodila ovu reviziju. „Takvi napadi mogu imati ozbiljne političke posljedice, naštetiti općem ugledu EU-a i narušiti povjerenje u njegove institucije. EU mora uložiti dodatne napore da zaštiti vlastite organizacije.”

Glavni zaključak revizora bio je da institucije, tijela i agencije EU-a nisu uvijek dobro zaštićeni od kiberprijetnji. Ti organi nemaju dosljedan pristup problematici kibersigurnosti, ponekad se ne primjenjuju ni osnovne kontrole i ključne dobre prakse u području kibersigurnosti, a nema ni sustavnog osposobljavanja o toj temi. Izdvajanje resursa za kibersigurnost vrlo je neujednačeno, a više tijela EU-a troši znatno manje financijskih sredstava od drugih usporedivih tijela. Iako bi se razlike u razinama kibersigurnosti teoretski mogle opravdati različitim profilima rizičnosti svake organizacije i različitim razinama osjetljivosti podataka koje te organizacije obrađuju, revizori naglašavaju da kibersigurnosne slabe točke u jednom tijelu EU-a mogu izložiti više drugih

U ovom priopćenju za medije iznesene su glavne poruke tematskog izvješća Europskog revizorskog suda. Cjeloviti tekst izvješća dostupan je na eca.europa.eu.

ECA Press

12, rue Alcide De Gasperi – L-1615 Luxembourg

E: press@eca.europa.eu @EUAuditors eca.europa.eu

organizacija kiberprijetnjama (sva su tijela EU-a povezana međusobno, a često i s javnim i privatnim organizacijama u državama članicama).

Tim za hitne računalne intervencije (CERT-EU) i Agencija Europske unije za kibersigurnost (ENISA) dva su glavna subjekta EU-a zadužena za pružanje podrške u pogledu kibersigurnosti. Međutim, zbog ograničenih resursa ili davanja prednosti drugim područjima navedeni subjekti nisu mogli pružiti tijelima EU-a svu potrebnu podršku. Nedostatci postoje i u području razmjene informacija, tvrde revizori. Primjerice, pojedina tijela EU-a ne izvješćuju na vrijeme o slabim točkama i ozbiljnim kiberincidentima kojima su bila izložena i koji bi mogli utjecati na druge.

Kontekst

U institucijama, agencijama i tijelima EU-a trenutačno ne postoji pravni okvir za informacijsku sigurnost i kibersigurnost. Na njih se trenutačno ne primjenjuje najšire zakonodavstvo EU-a o kibersigurnosti, Direktiva o mrežnoj i informacijskoj sigurnosti iz 2016. niti predložena izmijenjena inačica te direktive. Ne postoje ni iscrpne informacije o iznosu sredstava koji su tijela EU-a potrošila na kibersigurnost. Zajednička pravila o informacijskoj sigurnosti i kibersigurnosti za sva tijela EU-a obuhvaćena su komunikacijom o strategiji EU-a za sigurnosnu uniju za razdoblje 2020. – 2025., koju je Komisija objavila u srpnju 2020. U Strategiji EU-a za kibersigurnost za digitalno desetljeće objavljenoj u prosincu 2020. Komisija se obvezala predložiti uredbu o zajedničkim kibersigurnosnim pravilima za sva tijela EU-a. Predložila je i uspostavu nove pravne osnove za tim CERT-EU radi jačanja njegovih ovlasti i financiranja.

Tematsko izvješće br. 5/2022 „Kibersigurnost institucija, tijela i agencija EU-a: razina pripravnosti općenito nije razmjerna prijetnjama” dostupna je na internetskim stranicama Suda. Sud je i u pregledu iz 2019. upozorio na izazove u pogledu djelotvornosti kibersigurnosne politike EU-a.

Kontakt za medije

Služba Suda za odnose s medijima: press@eca.europa.eu

- Claudia Spiti: claudia.spiti@eca.europa.eu – M: (+352) 691 553 547
- Vincent Bourgeais: vincent.bourgeais@eca.europa.eu – M: (+352) 691 551 502
- Damijan Fišer: damijan.fiser@eca.europa.eu – M: (+352) 621 552 224