EVROPSKO RAČUNSKO SODIŠČE

SL

Sporočilo za javnost

Luxembourg, 29. marca 2022

Organi EU morajo okrepiti svojo pripravljenost na področju kibernetske varnosti

Število kibernetskih napadov na organe EU se močno povečuje. Raven pripravljenosti na področju kibernetske varnosti se po organih EU razlikuje in na splošno ni sorazmerna z vse večjimi grožnjami. Ker so organi EU med seboj tesno povezani, so lahko zaradi slabosti enega varnostnim grožnjam izpostavljeni tudi drugi. To je bilo ugotovljeno v posebnem poročilu Evropskega računskega sodišča (Sodišča), ki je preučilo pripravljenost organov upravljanja EU na kibernetske grožnje. Revizorji priporočajo uvedbo zavezujočih pravil o kibernetski varnosti in povečanje virov za skupino za odzivanje na računalniške grožnje (CERT-EU). Pravijo tudi, naj Evropska komisija spodbuja nadaljnje sodelovanje med organi EU, skupina CERT-EU in Agencija Evropske unije za kibernetsko varnost pa naj se bolj osredotočita na tiste organe EU, ki imajo manj izkušenj z upravljanjem kibernetske varnosti.

Med letoma 2018 in 2021 se je število pomembnih incidentov v organih EU povečalo za več kot desetkrat. Delo na daljavo je znatno povečalo število možnih točk dostopa za napadalce. Pomembni incidenti so navadno posledica kompleksnih kibernetskih napadov, ki običajno vključujejo uporabo novih metod in tehnologij, da se raziščejo in da se ponovno vzpostavi prejšnje stanje pa lahko traja več tednov ali celo mesecev. Tak primer je bil kibernetski napad na Evropsko agencijo za zdravila, pri katerem so bili občutljivi podatki razkriti in manipulirani, da bi se spodkopalo zaupanje v cepiva.

„*Institucije, organi in agencije EU so privlačne tarče potencialnih napadalcev, zlasti skupin, ki so sposobne izvajati visoko izpopolnjene prikrite napade za namene kibernetskega vohunjenja in druge škodljive namene*,“ je povedala članica Sodišča Bettina Jakobsen, ki je vodila revizijo. „*Takšni napadi imajo lahko znatne politične posledice ter lahko škodujejo splošnemu ugledu EU in spodkopavajo zaupanje v njene institucije. EU mora okrepiti prizadevanja za zaščito svojih organizacij.*“

Glavna ugotovitev revizorjev je bila, da institucije, organi in agencije EU niso vedno dobro zaščiteni pred kibernetskimi grožnjami. Kibernetske varnosti namreč ne obravnavajo usklajeno, bistvene kontrole in ključne dobre prakse na področju kibernetske varnosti niso vedno vzpostavljene, usposabljanje na tem področju pa se ne zagotavlja sistematično. Dodeljevanje sredstev za

Namen tega sporočila za javnost je predstaviti glavna sporočila posebnega poročila, ki ga je sprejelo Evropsko računsko sodišče. Celo poročilo je na voljo na eca.europa.eu.

ECA Press

12, rue Alcide De Gasperi – L-1615 Luxembourg
E: press@eca.europa.eu @EUAuditors eca.europa.eu

kibernetsko varnost je zelo različno in številni organi EU za to porabijo precej manj kot primerljivi drugi. Različne ravni kibernetske varnosti bi bilo sicer teoretično mogoče upravičiti z različnimi profili tveganja posameznih organizacij in ravnmi občutljivosti podatkov, ki jih obdelujejo, vendar revizorji poudarjajo, da je lahko zaradi slabosti na področju kibernetske varnosti v enem organu EU kibernetskim grožnjam izpostavljenih tudi več drugih organizacij (organi EU so namreč povezani drug z drugim, pogosto pa tudi z javnimi in zasebnimi organizacijami v državah članicah).

Skupina za odzivanje na računalniške grožnje (CERT-EU) in Agencija Evropske unije za kibernetsko varnost (ENISA) sta glavna subjekta EU, zadolžena za zagotavljanje podpore na področju kibernetske varnosti. Vendar pa organom EU nista mogla zagotoviti vse podpore, ki jo potrebujejo, ker imata omejene vire ali ker se druga področja obravnavajo prednostno. Po mnenju revizorjev med pomanjkljivosti spada tudi izmenjava informacij, saj vsi organi EU na primer ne poročajo pravočasno o šibkih točkah in pomembnih kibernetskih incidentih, ki so vplivali nanje in bi lahko vplivali na druge.

Splošne informacije

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 iz leta 2016 niti predlog za njeno spremembo (tj. revidirana direktiva o varnosti omrežij in informacij). Prav tako ni izčrpnih informacij o sredstvih, ki so jih organi EU porabili za kibernetsko varnost. Skupna pravila o varnosti informacij in kibernetski varnosti za vse organe EU so vključena v sporočilo o strategiji EU za varnostno unijo za obdobje 2020–2025, ki ga je Komisija objavila julija 2020. Komisija se je v strategiji EU za kibernetsko varnost v digitalnem desetletju, objavljeni decembra 2020, zavezala, da bo predlagala uredbo o skupnih pravilih o kibernetski varnosti za vse organe EU. Predlagala je tudi vzpostavitev nove pravne podlage za okrepitev pooblastil in financiranja skupine CERT-EU.

Posebno poročilo št. 5/2022 z naslovom *Kibernetska varnost institucij, organov in agencij EU – Stopnja pripravljenosti na splošno ni sorazmerna z grožnjami* je na voljo na spletišču Sodišča. Sodišče je izzive za uspešno politiko EU za kibernetsko varnost obravnavalo tudi v pregledu iz leta 2019.

Kontakt za medije

Tiskovni urad Sodišča: press@eca.europa.eu

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