EUROOPA KONTROLLIKODA

ET

Pressiteade

Luxembourg, 29. märts 2022

ELi asutused peavad parandama oma küberturvalisuse alast valmisolekut

ELi asutuste vastu suunatud küberrünnete arv kasvab järsult. Samas on ELi asutuste küberturvalisuse alane valmisolek organisatsiooniti erinev ja üldiselt ei vasta see pidevalt suurenevatele ohtudele. Kuna ELi asutused on omavahel tihedalt seotud, võivad ühe asutuse nõrgad kohad tekitada turvaohte ka teistele. Sellele järeldusele jõuti Euroopa Kontrollikoja eriaruandes, milles uuritakse, kui hästi on ELi asutused küberohtudeks valmis. Audiitorid soovitavad kehtestada siduvad küberturvalisuse alased eeskirjad ja suurendada infoturbeintsidentidega tegeleva rühma (CERT-EU) ressursse. Audiitorite sõnul peaks Euroopa Komisjon edendama ka ELi asutuste vahelist koostööd. CERT-EU ja Euroopa Liidu Küberturvalisuse Amet peaksid ka pöörama rohkem tähelepanu küberturvalisuse alal vähem kogenud ELi asutustele.

Aastatel 2018–2021 suurenes oluliste intsidentide arv enam kui kümme korda. See on ründajate jaoks märkimisväärselt suurendanud võimalike juurdepääsupunktide arvu. Olulisi intsidente põhjustavad üldiselt väga keerukad ründed. Tavaliselt hõlmavad need uusi meetodeid ja tehnoloogiaid ning nende uurimiseks ja neist taastumiseks võib kuluda nädalaid või isegi kuid. Üks hiljutine näide oli küberrünne Euroopa Ravimiameti vastu, mille käigus lekitati ja manipuleeriti tundlikke andmeid eesmärgiga õõnestada usaldust vaktsiinide vastu.

„ELi institutsioonid, organid ja asutused kujutavad endast huvitavaid sihtmärke võimalike ründajate jaoks, kelleks on eelkõige rühmitused, kes suudavad toime panna väga keerukaid varjatud ründeid küberspionaaži ja muudel eesmärkidel," ütles auditit juhtinud kontrollikoja liige Bettina Jakobsen. „Sellistel rünnetel võivad olla märkimisväärsed poliitilised tagajärjed, need võivad kahjustada ELi üldist mainet ja õõnestada usaldust liidu institutsioonide vastu. EL peab suurendama jõupingutusi oma organisatsioonide kaitsmiseks."

Audiitorite peamine järeldus oli, et ELi institutsioonid, organid ja asutused ei ole küberohtude eest alati hästi kaitstud. Nad ei tegele küberturvalisuse teemadega järjepidevalt ega rakenda alati olulisi kontrollimehhanisme ja küberturvalisuse peamisi häid tavasid, lisaks ei pakuta ka süstemaatiliselt küberturvalisuse alast koolitust. Küberturvalisusele eraldatakse ressursse väga erineval määral ning mõned ELi asutused kulutavad sellele oluliselt vähem kui teised sarnase suurusega ELi asutused. Kuigi küberturvalisuse erinevat taset võib teoreetiliselt põhjendada iga organisatsiooni erineva riskiprofiili ja käideldavate andmete erineva tundlikkusega, rõhutavad audiitorid, et ühe

Pressiteate eesmärk on edastada Euroopa Kontrollikoja eriaruande põhisõnumid. Aruanne on tervikuna kättesaadav veebisaidil eca.europa.eu.

ECA Press

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

ELi asutuse nõrgad kohad võivad tekitada küberohte ka teistele organisatsioonidele (nad on seotud nii omavahel kui ka sageli liikmesriikide avaliku ja erasektori organisatsioonidega).

ELi institutsioonide ja ametite infoturbeintsidentidega tegelev rühm (CERT-EU) ja Euroopa Liidu Küberturvalisuse Amet (ENISA) on kaks peamist üksust, mille ülesanne on pakkuda tuge küberturvalisuse valdkonnas. Ressursside piiratuse või muude valdkondade eelistamise tõttu ei ole nad aga suutnud pakkuda ELi asutustele kogu vajalikku tuge. Audiitorite sõnul on probleemiks ka teabevahetus: näiteks ei anna kõik ELi asutused õigeaegselt teada oma nõrkadest kohtadest ja neid tabanud olulistest küberturvalisuse intsidentidest, mis võivad ka teisi mõjutada.

Selgitav taustteave

Praegu puudub ELi institutsioonidel, asutustel ja organitel infoturbe ja küberturvalisuse küsimuste jaoks õigusraamistik. Nende suhtes ei kohaldata kõige üldisemat küberturvalisust käsitlevat ELi õigusakti (2016. aasta võrgu- ja infoturbe direktiiv) ning neid ei puuduta ka selle kavandatav läbivaatamine (küberturvalisuse 2. direktiiv). Samuti puudub põhjalik teave selle kohta, kui palju on ELi asutused küberturbele kulutanud. Kõigile ELi asutustele kehtivad infoturbe ja küberturvalisuse ühised eeskirjad on esitatud teatises ELi julgeolekuliidu strateegia kohta ajavahemikuks 2020–2025, mille komisjon avaldas 2020. aasta juulis. 2020. aasta detsembris avaldatud ELi küberturvalisuse strateegias digikümnendi jaoks võttis komisjon kohustuse teha ettepanek võtta vastu määrus, mis käsitleks ELi asutuste jaoks kehtivaid ühiseid küberturvalisuse norme. Samuti tegi komisjon ettepaneku luua CERT-EU jaoks uus õiguslik alus, mis tugevdaks selle volitusi ja rahastamist.

Eriaruanne 05/2022 „ELi institutsioonide, organite ja asutuste küberturvalisus: üldine valmisoleku tase ei vasta ohtudele“ on kättesaadav kontrollikoja veebisaidil. Kontrollikoda käsitles ELi küberturvalisuse poliitika tõhusust mõjutavaid probleeme ka ühes oma 2019. aasta ülevaates.

Pressikontakt

Kontrollikoja pressibüroo: press@eca.europa.eu

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