EUROPOS AUDITO RŪMAI

LT

Pranešimas spaudai

Liuksemburgas, 2022 m. kovo 29 d.

ES įstaigos turi stiprinti savo kibernetinio saugumo parengtį

Kibernetinių išpuolių prieš ES įstaigas skaičius smarkiai didėja. ES įstaigų kibernetinio saugumo parengties lygis skiriasi ir iš esmės neatitinka didėjančių grėsmių. Kadangi ES įstaigos yra glaudžiai tarpusavyje susijusios, dėl vienos iš jų trūkumo gali kilti grėsmių kitų įstaigų saugumui. Tokia išvada padaryta Europos Audito Rūmų specialiojoje ataskaitoje, kurioje nagrinėjama, kaip ES valdymo subjektai yra pasirengę kovoti su kibernetinėmis grėsmėmis. Auditoriai rekomenduoja nustatyti privalomas kibernetinio saugumo taisykles ir padidinti Kompiuterinių incidentų tyrimo tarnybos (CERT-EU) turimus išteklius. Auditoriai teigia, kad Europos Komisija taip pat turėtų skatinti tolesnį ES įstaigų bendradarbiavimą, o CERT-EU ir Europos Sąjungos kibernetinio saugumo agentūra turėtų daugiau dėmesio skirti toms ES įstaigoms, kurios turi mažiau kibernetinio saugumo valdymo patirties.

2018–2021 m. reikšmingų kibernetinio saugumo incidentų ES įstaigose padaugėjo daugiau nei dešimt kartų; nuotolinis darbas gerokai padidino galimų prieigos taškų, kuriais gali pasinaudoti užpuolikai, skaičių. Reikšmingus incidentus dažniausiai sukelia sudėtingi kibernetiniai išpuoliai, kurie paprastai susiję su naujų metodų ir technologijų naudojimu. Gali prireikti savaičių, jei ne mėnesių, kad jie būtų ištirti ir būtų nuo jų atsigauta. Vienas pavyzdžių – kibernetinis išpuolis prieš Europos vaistų agentūrą, kai neskelbtini duomenys buvo nutekinti ir manipuliuojami taip, kad būtų pakenkta pasitikėjimui vakcinomis.

„ES institucijos, įstaigos ir agentūros yra patrauklūs taikiniai galimiems užpuolikams, visų pirma grupėms, kurios gali vykdyti itin sudėtingas slaptas atakas kibernetinio šnipinėjimo ir kitais nusikalstamais tikslais, – teigė auditui vadovavusi Audito Rūmų narė Bettina Jakobsen. – *Tokie išpuoliai gali turėti didelių politinių pasekmių, pakenkti bendrai ES reputacijai ir pasitikėjimui jos institucijomis. ES turi dėti daugiau pastangų, kad apsaugotų savo organizacijas.“*

Pagrindinis auditorių nustatytas faktas buvo tas, kad ES institucijos, įstaigos ir agentūros ne visada yra gerai apsaugotos nuo kibernetinių grėsmių. Jos nevertina kibernetinio saugumo problemos nuosekliai, ne visada taikomos esminės kontrolės priemonės ir ne visada atsižvelgiama į pagrindinę gerąją kibernetinio saugumo patirtį, o mokymai kibernetinio saugumo klausimais nėra rengiami sistemingai. Ištekliai, skiriami kibernetiniam saugumui užtikrinti, labai skiriasi, o kai kurių ES įstaigų išlaidos yra gerokai mažesnės nei panašių kitų subjektų išlaidos. Nors teoriškai kibernetinio saugumo lygių skirtumus būtų galima pagrįsti skirtingais kiekvienos organizacijos rizikos profiliais

Šio pranešimo spaudai tikslas – pateikti Europos Audito Rūmų specialiosios ataskaitos pagrindines mintis. Visa ataskaita pateikta eca.europa.eu.

ECA Press

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

ir įvairiais jų tvarkomų duomenų opumo lygiais, auditoriai pabrėžia, kad dėl vienos ES įstaigos kibernetinio saugumo trūkumų kelioms kitoms organizacijoms gali kilti kibernetinio saugumo grėsmių (visos ES įstaigos yra susijusios tarpusavyje, jos dažnai yra susietos su viešosiomis ir privačiomis organizacijomis valstybėse narėse).

Kompiuterinių incidentų tyrimo tarnyba (CERT-EU) ir Europos Sąjungos kibernetinio saugumo agentūra (ENISA) yra du pagrindiniai ES subjektai, kuriems pavesta teikti paramą kibernetinio saugumo srityje. Tačiau dėl ribotų išteklių ar prioritetų kitose srityse jos ES įstaigoms negalėjo suteikti visos reikalingos paramos. Auditoriai teigia, kad dalijimasis informacija taip pat yra trūkumas: pavyzdžiui, ne visos ES įstaigos laiku praneša apie pažeidžiamumą ir reikšmingus kibernetinio saugumo incidentus, kurie padarė joms poveikį ir gali daryti poveikį kitoms įstaigoms.

Bendroji informacija

Šiuo metu ES institucijose, agentūrose ir įstaigose nėra informacijos saugumo ir kibernetinio saugumo teisinės sistemos. Joms netaikomi plačiausi ES kibernetinio saugumo teisės aktai, 2016 m. TIS direktyva ar siūloma peržiūrėta jos redakcija, TIS 2 direktyva. Taip pat nėra išsamios informacijos apie sumą, kurią ES įstaigos išleido kibernetiniam saugumui užtikrinti. Bendros visų ES įstaigų informacijos saugumo ir kibernetinio saugumo taisyklės įtrauktos į 2020 m. liepos mėn. Komisijos paskelbtą komunikatą dėl 2020–2025 m. laikotarpio ES saugumo sąjungos strategijos. 2020 m. gruodžio mėn. paskelbtoje ES skaitmeninio dešimtmečio kibernetinio saugumo strategijoje Komisija įsipareigojo pasiūlyti reglamentą dėl bendrų kibernetinio saugumo taisyklių visoms ES įstaigoms. Ji taip pat pasiūlė sukurti naują CERT-EU teisinį pagrindą, kad būtų sustiprinti jos įgaliojimai ir finansavimas.

Specialioji ataskaita 05/2022 *„ES institucijų, įstaigų ir agentūrų kibernetinis saugumas. Parengties lygis iš esmės neatitinka grėsmių“* paskelbta Audito Rūmų interneto svetainėje. Audito Rūmai į veiksmingos ES kibernetinio saugumo politikos iššūkius atkreipė dėmesį ir 2019 m. apžvalgoje.

Kontaktai spaudai

Audito Rūmų spaudos tarnyba: press@eca.europa.eu

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