EIROPAS
REVĪZIJAS
PALĀTA

LV

Preses relīze

Luksemburgā, 2022. gada 29. martā

ES struktūrām jāstiprina kiberdrošības sagatavotība

Strauji pieaug kiberuzbrukumu skaits ES struktūrām. ES struktūru kiberdrošības sagatavotības līmenis ir atšķirīgs un kopumā neatbilst arvien pieaugošajam apdraudējumam. Tā kā starp ES struktūrām pastāv cieša saikne, nepilnības vienā iestādē var pakļaut drošības apdraudējumam citas iestādes. Tā ir secināts Eiropas Revīzijas palātas īpašajā ziņojumā, kurā analizēta ES pārvaldes struktūru sagatavotība pret kiberdraudiem. Revidenti iesaka ieviest saistošus kiberdrošības noteikumus un palielināt datorapdraudējumu reaģēšanas vienībai (*CERT-EU*) pieejamos resursus. Revidenti norāda, ka Eiropas Komisijai arī jāsekmē turpmāka ES struktūru sadarbība, savukārt *CERT-EU* un Eiropas Savienības Kiberdrošības aģentūrai vairāk uzmanības jāpievērš tām ES struktūrām, kurām ir mazāka pieredze kiberdrošības pārvaldībā.

No 2018. līdz 2021. gadam būtiski kiberdrošības incidenti ES struktūrās ir pieauguši vairāk nekā desmitkārt; attālināts darbs ir ievērojami palielinājis uzbrucēju potenciālo piekļuves punktu skaitu. Būtiskus incidentus parasti izraisa sarežģīti kiberuzbrukumi, kas visbiežāk ir saistīti ar jaunu metožu un tehnoloģiju izmantošanu, un to izmeklēšana un seku pārvarēšana var ilgt vairākas nedēļas un pat mēnešus. Kā piemēru var minēt kiberuzbrukumu Eiropas Zāļu aģentūrai, kad tika nopludināti sensitīvi dati un ar tiem manipulēja tā, lai mazinātu uzticēšanos vakcīnām.

"*ES iestādes, struktūras un aģentūras ir pievilcīgi mērķi iespējamajiem uzbrucējiem, jo īpaši grupām, kuras spēj veikt augstas sarežģītības maskētus uzbrukumus kiberspiegošanas un citos negodīgos nolūkos*," sacīja par šo revīziju atbildīgā ERP locekle *Bettina Jakobsen*. "*Šādiem uzbrukumiem var būt nozīmīgas politiskas sekas, tie var kaitēt ES reputācijai kopumā un mazināt uzticēšanos tās iestādēm. ES ir jāpastiprina centieni aizsargāt savas organizācijas*."

Galvenais revidentu konstatējums bija: ES iestādes, struktūras un aģentūras ne vienmēr ir labi aizsargātas pret kiberdraudiem. Tām trūkst konsekventas pieejas kiberdrošībai, ne vienmēr ir ieviesti būtiski kontroles mehānismi un svarīga laba kiberdrošības prakse, un kiberdrošības apmācība netiek nodrošināta sistemātiski. Kiberdrošībai piešķirtie resursi ļoti atšķiras, un vairākas ES struktūras tērē ievērojami mazāk nekā tām līdzīgas struktūras. Lai gan kiberdrošības līmeņa atšķirības teorētiski varētu pamatot ar katras organizācijas atšķirīgo riska profilu un tajās apstrādāto datu dažādajiem sensitivitātes līmeņiem, revidenti uzsver, ka kiberdrošības nepilnības vienā ES struktūrā var pakļaut kiberdrošības apdraudējumiem vairākas citas organizācijas (visas

Šī preses relīze sniedz kopsavilkumu par Eiropas Revīzijas palātas sagatavoto īpašo ziņojumu. Tā pilns teksts ir pieejams Palātas tīmekļa vietnē www.eca.europa.eu.

ECA Press

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

ES struktūras ir saistītas savā starpā, kā arī bieži vien ar publiskām un privātām organizācijām dalībvalstīs).

ES iestāžu un aģentūru datorapdraudējumu reaģēšanas vienība (*CERT-EU*) un Eiropas Savienības Kiberdrošības aģentūra (*ENISA*) ir divas galvenās vienības, kuru uzdevums ir nodrošināt atbalstu kiberdrošības jomā. Tomēr tās nav spējušas sniegt ES struktūrām visu vajadzīgo atbalstu, jo resursi ir ierobežoti vai prioritāte tiek piešķirta citām jomām. Viens no trūkumiem attiecas arī uz informācijas apmaiņu, proti, revidenti apgalvo, ka ne visas ES struktūras laikus ziņo par ievainojamību un būtiskiem kiberdrošības incidentiem, kas tās ir ietekmējuši un var ietekmēt citas iestādes.

Vispārīga informācija

Pašlaik ES iestāžu, aģentūru un struktūru informācijas drošībai un kiberdrošībai nav juridiskā satvara. Uz tām neattiecas plašākie ES tiesību akti par kiberdrošību, 2016. gada TID direktīva, kā arī tās ierosinātā pārskatītā redakcija – TID2 direktīva. Tāpat arī nav visaptverošas informācijas par summu, ko ES struktūras tērē kiberdrošībai. Vienoti noteikumi par informācijas drošību un kiberdrošību ES struktūrām ir iekļauti Komisija 2020. gada jūlijā publicētajā paziņojumā par ES Drošības savienības stratēģiju 2020.–2025. gadam. ES Kiberdrošības stratēģijā digitālajai desmitgadei, kas ir publicēta 2020. gada decembrī, Komisija apņēmās ierosināt regulu par vienotiem kiberdrošības noteikumiem visām ES struktūrām. Tāpat arī Komisija ierosināja izveidot jaunu *CERT-EU* juridisko pamatu, lai stiprinātu vienības pilnvaras un finansējumu.

Īpašais ziņojums Nr. 05/2022 *"ES iestāžu, struktūru un aģentūru kiberdrošība: sagatavotības līmenis kopumā neatbilst apdraudējumam"* ir pieejams ERP tīmekļa vietnē. ERP norādīja uz problēmām, kas traucē īstenot efektīvu ES kiberdrošības politiku, arī 2019. gada apskatā.

Kontaktinformācija presei:

ERP preses birojs: press@eca.europa.eu

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