EIROPAS KOMISIJAS ATBILDES

UZ EIROPAS REVĪZIJAS PALĀTAS ĪPAŠO ZIŅOJUMU

ES iestāžu, struktūru un aģentūru kiberdrošība: sagatavotības līmenis neatbilst draudiem

Saturs

Šajā dokumentā ir izklāstītas Eiropas Komisijas atbildes uz apsvērumiem Eiropas Revīzijas palātas īpašajā ziņojumā saskaņā ar Finanšu regulas 259. pantu, un tās tiks publicētas kopā ar īpašo ziņojumu.

I. KOMISIJAS ATBILŽU KOPSAVILKUMS

a) Vispārīgs ievads

Kiberdrošība Eiropas Komisijai ir kļuvusi par augstu politisko un darbības prioritāti. Covid-19 krīze ir paātrinājusi mūsu atkarību no digitālajiem pakalpojumiem (mākoņdatošana, mobilās ierīces, mākslīgais intelekts). Pēdējo divu gadu laikā mēs esam piedzīvojuši masveida pāreju uz darbu no mājām. Tas nozīmē, ka gan kibernoziedzība, gan kiberspiegošana, kas ir divi galvenie draudi, ar kuriem saskaras *EUIBA* (Eiropas Savienības iestādes, struktūras un aģentūras), arī ir ievērojami izplatījušās tiešsaistē. Komisija atzīst šo tendenci, un tās vadība kiberdrošības jomā ir bijusi konsekventa un izlēmīga. Kiberdrošības akts stājās spēkā 2019. gadā, ar kuru cita starpā tika paplašinātas *ENISA* pilnvaras un tai tika piešķirts pastāvīgs raksturs. Ar minēto aktu tika izveidota arī oficiāla sadarbība starp *ENISA* un *CERT-EU* (datorapdraudējumu reaģēšanas vienība visām Eiropas Savienības iestādēm, struktūrām un aģentūrām). Komisija 2020. gadā ierosināja pastiprināt Tīklu un informācijas drošības (TID) direktīvu, par kuru likumdevēji ir gandrīz panākuši vienošanos.

2020. gada kiberdrošības stratēģijā bija ietvertas arī trīs rīcības jomas saistībā ar kiberdrošību ES iestādēs, struktūrās un aģentūrās. Tajā pieteikta regula par informācijas drošību ES iestādēs, struktūrās un aģentūrās, regula par vienotiem ES iestāžu, struktūru un aģentūru kiberdrošības noteikumiem un Komisijas nodoms nodrošināt jaunu juridisko pamatu *CERT-EU*, lai stiprinātu tās pilnvaras un finansējumu nolūkā nodrošināt pienācīgus resursus, saskaroties ar pieaugošajiem draudiem, riskiem un incidentiem.

Darbs saistībā ar šo priekšlikumu sagatavošanu ir pavirzījies uz priekšu. Lai gan kolēģija tos vēl nav pieņēmusi, paredzams, ka tie tiks pieņemti 2022. gada pirmajā ceturksnī. Svarīgi jautājumi, ko iestādes apsprieda šajā sagatavošanas posmā, ir priekšlikuma juridiskais pamats, kā arī visu ES iestāžu, struktūru un aģentūru budžetspēja izpildīt prasības gan attiecībā uz savu vajadzību finansēšanu kiberdrošības jomā, gan atrast resursus, kas vajadzīgi, lai atbalstītu *CERT-EU*, budžetu un jo īpaši amata vietas.

Sagatavotības līmeņi kiberdrošības jomā dažādās ES iestādēs, struktūrās un aģentūrās ir atšķirīgi. Vairākām ES iestādēm, struktūrām un aģentūrām ir labi rezultāti kibersagatavotības ziņā, un tām arī turpmāk jāuzņemas sava vadošā loma, stimulējot un iedvesmojot progresu un turpmākus uzlabojumus visā kiberdrošības jomā. Lai panāktu izmērāmu progresu, ir svarīgi atzīt dažādos ES iestāžu, struktūru un aģentūru brieduma līmeņus un noteikt prioritātes, vispirms uzlabošanas darbības attiecinot uz tām ES iestādēm, struktūrām un aģentūrām, kurās konstatētās nepilnības rada vislielāko risku.

b) Komisijas nostāja attiecībā uz Revīzijas palātas galvenajiem apsvērumiem un ieteikumiem

Komisija atzinīgi vērtē Revīzijas palātas ziņojumu par ES iestāžu, struktūru un aģentūru kiberdrošību. Tā pieņem zināšanai, ka ziņojumā ir uzsvērts, cik nozīmīgs visām ES iestādēm, struktūrām un aģentūrām ir vienots tiesiskais regulējums informācijas drošības un kiberdrošības jomā, lai palielinātu vispārējo kiberdrošības līmeni visās jomās. Komisija norāda, ka Revīzijas palātas galvenie apsvērumi un ieteikumi nav vērsti uz pašas Komisijas operatīvo kiberdrošību, bet gan uz Komisijas politisko lomu tādu tiesību aktu ierosināšanā, kuru mērķis ir palielināt ES iestāžu, struktūru un aģentūru kiberbriedumu.

Turpmākajās regulās par "informācijas drošību ES iestādēs, struktūrās un aģentūrās" un par "vienotiem ES iestāžu, struktūru un aģentūru kiberdrošības noteikumiem" tiks paredzēti kopīgi noteikumi, lai panāktu augstu informācijas drošības un kiberdrošības līmeni, taču to īstenošana katras ES iestādes, struktūras un aģentūras organizatoriskā un darbības kontekstā (jo īpaši to apdraudējuma un riska profili) joprojām būs ES iestāžu, struktūru un aģentūru autonoma atbildība. Ierosinātajā regulā par kiberdrošību būs atbilstības mehānismi, kas ir pienācīgi un samērīgi ar jauno noteikumu mērķi un piemērošanas jomu, neskarot iestāžu, struktūru un aģentūru autonomiju.

Pašlaik Komisija vada Iestāžu komitejas digitālās pārveides jautājumos (*ICDT*) kiberdrošības apakšgrupu, kas tiek iecelta rotācijas kārtībā (uz laiku līdz diviem gadiem). Jānorāda, ka apakšgrupas darbam nav piešķirti nekādi īpaši resursi: visas darbības ir balstītas uz dalībnieku vislabākajām pūlēm pēc brīvprātības principa.

Komisija piekrīt vispārīgajai idejai par *CERT-EU* resursu palielināšanu un pilnvaru stiprināšanu.

Atbilstoši šai izpratnei Komisija atbalsta ziņojumā ietvertos galvenos apsvērumus un ieteikumus. Mūsu nostāja ir sīkāk izskaidrota papildu piezīmēs III iedaļā. Kas attiecas uz ieteikumiem, Komisija piekrīt 1. ieteikuma a), b), c), d), e), f) un g) punktam un 2. ieteikuma a), b) un c) punktam.

c) Jaunākās norises un turpmākie pasākumi

Ir pabeigta oficiāla apspriešanās ES iestāžu, struktūru un aģentūru ģenerāldirektoru līmenī par abu regulu (par informācijas drošību un kiberdrošību) konsolidētajiem projektiem, un šobrīd tiek veikta saņemto atsauksmju novērtēšana, pirms tiek pabeigts tiesību aktu kopums un pirms kolēģija to pieņem 2022. gada pirmajā ceturksnī.

II. KOMISIJAS ATBILDES UZ REVĪZIJAS PALĀTAS GALVENAJIEM APSVĒRUMIEM

1. ES iestāžu, struktūru un aģentūru kiberdrošības brieduma līmeņi

Komisija piekrīt, ka ir svarīgi ņemt vērā draudus un riskus saistībā ar ES iestāžu, struktūru un aģentūru izdevumu līmeni kiberdrošības jomā.

Tāpat attiecībā uz cilvēkresursiem ES iestāžu, struktūru un aģentūru personāla stabilitāti ietekmē vairāki faktori. Kiberdrošības speciālistu darbā pieņemšanas tirgus kļūst arvien sarežģītāks. Daudzos gadījumos noteikumi par cilvēkresursiem nav pielāgoti specializētiem profiliem (pieņemšana darbā, karjeras attīstība, apmācība). Turklāt budžeta lēmējinstitūcijas vispārējais spiediens uz darbinieku skaitu visās ES iestādēs, struktūrās un aģentūrās nozīmē, ka jaunām prioritārām jomām, piemēram, kiberdrošībai, joprojām netiek piešķirts pietiekams amata vietu skaits, jo īpaši iekšējos operatīvajos dienestos.

Saistībā ar norādi uz panākto progresu pārvaldības un riska pārvaldības jomā, būtu jāņem vērā tas, ka atbilstības uzraudzība tagad pāriet no izmēģinājuma posma uz pilnīgu ieviešanu. Līdz ar to ir normāli, ka tās tvērums līdz šim ir bijis diezgan zems. Šis atbilstības projekts ir nākamais posms ilgtermiņa kiberbrieduma uzlabošanas procesā, kas sākās ar vienotas riska metodikas noteikšanu,

kopīgu instrumentu izstrādi, ievainojamības pārvaldības ieviešanu un aktīvu inventarizācijas uzraudzību, testēšanu un apstiprināšanu. Šajā jomā ir panākts progress neatkarīgi no tā, ka Komisijas aktīvu bāze ir ļoti sarežģīta, jo vairāk nekā 1000 informācijas sistēmu pārvalda vairāk nekā 50 ģenerāldirektorāti un izpildaģentūras.

2. ES iestāžu, struktūru un aģentūru sadarbības mehānismi

CERT-EU ir neparasts veiksmes stāsts sadarbības veicināšanā ne tikai starp ES iestādēm, struktūrām un aģentūrām, bet arī Eiropas līmenī, pateicoties tam, ka tā ir pilntiesīga dalībniece *CSIRT* tīklā, kas izveidots saskaņā ar TID direktīvu. Tādējādi *CERT-EU* ir piemērs tam, kā var uzlabot sadarbību un kiberdrošības pakalpojumus. ERP apsvērumi par *CERT-EU* ļoti skaidri parāda izcilo darbu, ko *CERT-EU* veic, saskaroties ar arvien naidīgāku kiberdraudu ainu un to, ka pastāvīgi trūkst resursu.

Saskaņā ar spēkā esošo Iestāžu nolīgumu ES decentralizētās aģentūras un kopuzņēmumus *CERT-EU* valdē oficiāli pārstāv *ENISA*. Turklāt viņu viedokli valdes sanāksmēs pauž IKT konsultatīvās komitejas (*ICTAC*) pārstāvis, kuram ir ļauts būt klāt, lai palīdzētu *ENISA* pildīt aģentūru pārstāvības pienākumus, bet kuram valdē nav oficiālas vietas vai balss. Jautājums par aģentūru pienācīgu pārstāvību *CERT-EU* valdē tiks risināts ierosinātajā regulā, kurā pēc IKT konsultatīvās komitejas priekšlikuma valdes sastāvs tiks papildināts ar ne vairāk kā trim pārstāvjiem, ko iecēlis Savienības aģentūru tīkls (*EUAN*).

Dalība *ICDT* kiberdrošības apakšgrupā ir balstīta uz dalībnieku vislabākajiem centieniem, ciktāl katra ES iestāde, struktūra un aģentūra ir nolēmusi iesaistīties. Jautājums par uzlabojumiem attiecībā uz informācijas apmaiņu par iepirkumu ir svarīgs temats kiberdrošības apakšgrupas 2. darba grupas darbības jomā, un tas tiks izskatīts, sagatavojot jauno kiberdrošības pamatlīgumu.

Attiecībā uz kopīgiem rīkiem tādiem pakalpojumiem kā e-pasts un videokonference jau pastāv iespēja izmantot sistēmu *SECEM-2*, ko Komisija ieviesusi attiecībā uz visām ES iestādēm, struktūrām un aģentūrām šifrētiem e-pastiem un kas ir atkarīga no šifrēšanas atslēgu un sertifikātu efektīvas pārvaldības. Turklāt šobrīd tiek izstrādāts *SECABC* – rīks, kas ļauj iestādēm apmainīties ar šifrētiem e-pastiem –, lai no 2022. gada visām ieinteresētajām ES iestādēm, struktūrām un aģentūrām varētu piedāvāt piekļuvi šai sistēmai. Droša videokonferenču rīkošana jau ir ieviesta pakalpojumiem, kuros apmainās ar sensitīvu neklasificētu informāciju, un, pārvaldot sanāksmes dalībnieku identitāti, to uz *ad hoc* pamata var izmantot arī citām ES iestādēm, struktūrām un aģentūrām. Sensitīvas informācijas apmaiņa tiks aplūkota arī ierosinātajā regulā par informācijas drošību (vienotu marķējumu veidā).

3. Informācijas apmaiņa par būtiskiem incidentiem vai ievainojamību

Tas, ka ne visas ES iestādes, struktūras un aģentūras ziņo *CERT-EU* par būtiskiem incidentiem vai ievainojamību, ir risināts kiberdrošības regulas projektā saskaņā ar Komisijas priekšlikumu TID-2 direktīvā[1]. Īstenošanas līmenis būs atkarīgs no papildu resursiem, ko šim nolūkam piešķīrušas

[1] Priekšlikums Eiropas Parlamenta un Padomes direktīvai, ar ko paredz pasākumus nolūkā panākt vienādi augsta līmeņa kiberdrošību visā Savienībā un ar ko atceļ Direktīvu (ES) 2016/1148, COM(2020) 823 final.

autonomās ES iestādes, struktūras un aģentūras. Iespēja šādus paziņojumus noteikt par obligātiem joprojām ir ierobežota, tostarp arī saskaņā ar ierosināto regulas redakciju, ņemot vērā ES iestāžu, struktūru un aģentūru institucionālo autonomiju. Ierosinātajā regulā par kiberdrošību būs atbilstības mehānismi, kas ir pienācīgi un samērīgi ar jauno noteikumu mērķi un piemērošanas jomu, neskarot iestāžu, struktūru un aģentūru autonomiju.

III. KOMISIJAS ATBILDES UZ REVĪZIJAS PALĀTAS SECINĀJUMIEM UN IETEIKUMIEM

1. ieteikums. Uzlabot *EUIBA* sagatavotību kiberdrošības jomā, nosakot vienotus saistošus noteikumus un palielinot *CERT-EU* resursus

Ierosinātajā regulā būs iekļauti konkrēti pasākumi, kas paredzēti, lai paaugstinātu kopējo kiberdrošības līmeni. Šie pasākumi tiks pārvērsti kiberdrošības plānos, kurus izstrādās un īstenos ES iestāžu, struktūru un aģentūru līmenī atbilstoši to kiberdrošības pārvaldības satvaram.

Komisija piekrīt šim ieteikumam. Atsaucoties uz konkrētajiem apakšieteikumiem, Komisija norāda, ka:

a) Komisija piekrīt 1. ieteikuma a) punktam. Regulas projektā tiks iekļauti noteikumi par pārvaldības un kontroles satvaru, kas izveidots katras ES iestādes, struktūras un aģentūras augstākajā vadības līmenī, lai nodrošinātu visu kiberdrošības risku efektīvu un piesardzīgu pārvaldību;
b) Komisija piekrīt 1 ieteikuma b) punktam. Regulas projektā tiks pastiprināta uz risku balstīta pieeja kiberdrošības pārvaldībā, skaidri norādot, ka darbībām, IT drošības plāniem un būtisku kontroles mehānismu faktiskai īstenošanai būtu jāseko novērtējumiem;
c) Komisija piekrīt 1.ieteikumam c) punktam Izglītošana par kiberdrošību, izpratnes veidošanas un apmācības programmas regulas projektā tiks minētas kā daļa no kiberdrošības pamatscenārija;
d) Komisija piekrīt 1. ieteikuma d) punktam. Mūsu pieredze liecina, ka, lai gan regulāras revīzijas un testēšana ir būtiskas, ar tām nepietiek, lai nodrošinātu, ka tiek panākts progress. Tādēļ ir nepieciešama regulāra ziņošana un pārredzamība kā daļa no kiberdrošības pārvaldības satvara, kas izveidots saskaņā ar a) punktu;
e) Komisija piekrīt 1. ieteikuma e) punktam. Regulas projektā būs iekļauti noteikumi par ES iestāžu, struktūru un aģentūru ziņošanu *CERT-EU* par būtiskiem kiberdraudiem, ievainojamību un incidentiem;
f) Komisija piekrīt 1. ieteikuma f) punktam. Komisija atbalsta nepieciešamību palielināt *CERT-EU* resursus. Regulas projekts ietver noteikumus par ES iestāžu, struktūru un aģentūru personālu un finanšu iemaksām.
g) Komisija piekrīt 1. ieteikuma g) punktam. Ierosinātajā regulā būs atbilstības mehānismi, kas ir atbilstoši un samērīgi ar noteikumu mērķi un piemērošanas jomu un vienlaicīgi respektē ES iestāžu, struktūru un aģentūru autonomiju. Jaunās regulas saturs ir atkarīgs no likumdošanas procedūras iznākuma un izriet no lēmuma, ko Savienības likumdevējs pieņems attiecībā uz Komisijas priekšlikumu.

2. ieteikums. Iestāties par turpmāku *EUIBA* sinerģiju izraudzītās jomās

Komisija, kas pašlaik vada Iestāžu komitejas digitālās pārveides jautājumos (*ICDT*) kiberdrošības apakšgrupu, piekrīt ieteikumiem veicināt risinājumus konsekventai un drošai apmaiņai ar sensitīvu informāciju, sistemātiskai informācijas apmaiņai par projektiem saistībā ar kiberdrošību un vienotu iepirkumu satvaru un līgumiem par kiberdrošības pakalpojumiem.

Komisija piekrīt šim ieteikumam. Atsaucoties uz konkrētajiem apakšieteikumiem, Komisija norāda, ka:

a) Komisija piekrīt 2. ieteikuma a) punktam. Komisija *ICDT* kiberdrošības apakšgrupai ierosina tehniskas iniciatīvas un pakalpojumus, lai veicinātu un atbalstītu kopīgus rīkus sensitīvas informācijas apmaiņai, dodot iespēju izmantot tādus pakalpojumus kā e-pasts un videokonference. Mēs arī atzīmējam, ka ierosinātajā regulā par informācijas drošību tiks aplūkoti vienoti marķējumi un vienoti apstrādes noteikumi sensitīvai neklasificētai informācijai;
b) Komisija piekrīt 2. ieteikuma b) punktam. *ICDT* kiberdrošības apakšgrupas darba grupas šobrīd šo jautājumu izskata, un darbs pie tā tiks turpināts. Saistībā ar jaunā kiberdrošības pamatlīguma izstrādi tiek izskatīts jautājums par uzlabojumiem attiecībā uz informācijas apmaiņu par iepirkumu;
c) Komisija piekrīt 2 ieteikuma c) punktam. ES iestādēm, struktūrām un aģentūrām jau ir pieejami iestāžu pamatlīgumi IKT jomā, ko pārvalda Komisija. Jaunā kiberdrošības pamatlīguma sagatavošana tiks koordinēta ar *ICDT* kiberdrošības apakšgrupu.

3. ieteikums. Palielināt *CERT-EU* un *ENISA* koncentrēšanos uz mazāk nobriedušām *EUIBA*

Šis ieteikums ir adresēts *CERT-EU* un *ENISA*.