EUROPOS KOMISIJOS ATSAKYMAI

Į EUROPOS AUDITO RŪMŲ SPECIALIOSIOS ATASKAITOS PASTABAS

ES institucijų, įstaigų ir agentūrų kibernetinis saugumas. Grėsmių neatitinkantis parengties lygis

Turinys

I. KOMISIJOS ATSAKYMAI GLAUSTAI 2

a) Bendras įvadas 2

b) Komisijos pozicija dėl pagrindinių Audito Rūmų pastabų ir rekomendacijų 2

c) Aktualios naujausios tendencijos ir tolesni veiksmai 3

II. KOMISIJOS ATSAKYMAI Į PAGRINDINES EUROPOS AUDITO RŪMŲ PASTABAS 3

1. EUIBA kibernetinio saugumo brandos lygiai 3

2. EUIBA bendradarbiavimo mechanizmai 4

3. Dalijimasis informacija apie reikšmingus incidentus ar pažeidžiamumą 4

III. KOMISIJOS ATSAKYMAI Į EUROPOS AUDITO RŪMŲ IŠVADAS IR REKOMENDACIJAS 5

1 rekomendacija. Gerinti EUIBA kibernetinio saugumo parengtį taikant bendras privalomas taisykles ir didinant CERT-EU išteklius 5

2 rekomendacija. Pasisakyti už tolesnę EUIBA sąveiką pasirinktose srityse 5

3 rekomendacija. CERT-EU ir ENISA daugiau dėmesio skirti mažiau brandžioms EUIBA 6

Šiame dokumente pateikiami Europos Komisijos atsakymai į Europos Audito Rūmų specialiosios ataskaitos pastabas pagal Finansinio reglamento 259 straipsnį, kurie turi būti paskelbti kartu su specialiąja ataskaita.

I. KOMISIJOS ATSAKYMAI GLAUSTAI

a) Bendras įvadas

Kibernetinis saugumas tapo svarbiausiu Europos Komisijos politiniu ir veiklos prioritetu. COVID-19 krizė padidino mūsų priklausomybę nuo skaitmeninių paslaugų (debesijos kompiuterijos, mobiliųjų įrenginių, dirbtinio intelekto). Per pastaruosius dvejus metus imta masiškai dirbti iš namų. Tai reiškia, kad internete taip pat dideliu mastu plačiai paplito tiek kibernetinis nusikalstamumas, tiek kibernetinis šnipinėjimas – dvi pagrindinės grėsmės, su kuriomis susiduria EUIBA (Europos Sąjungos institucijos, įstaigos ir agentūros). Šią tendenciją Komisija pripažįsta. Ji parodė nuoseklią ir ryžtingą lyderystę kibernetinio saugumo srityje. 2019 m. įsigaliojo Kibernetinio saugumo aktas, kuriuo, *inter alia*, išplėsti ENISA įgaliojimai ir jie įtvirtinti kaip nuolatiniai. Šiuo aktu taip pat nustatytas oficialus ENISA ir CERT-EU (kompiuterinių incidentų tyrimo tarnybos, padedančios visoms EUIBA) bendradarbiavimas. 2020 m. Komisija pasiūlė sugriežtinti Tinklų ir informacijos saugumo direktyvą ir dėl to beveik susitarta su teisės aktų leidėjais.

2020 m. kibernetinio saugumo strategijoje taip pat numatyti trys veiksmai, susiję su EUIBA kibernetiniu saugumu. Joje paskelbta apie Reglamentą dėl informacijos saugumo ES institucijose, įstaigose ir agentūrose, Reglamentą dėl ES institucijų, įstaigų ir agentūrų bendrų kibernetinio saugumo taisyklių ir ketinimą suteikti naują teisinį pagrindą CERT-EU, kad būtų sustiprinti jos įgaliojimai ir padidintas finansavimas – taip užtikrinti, kad ji turėtų pakankamai išteklių, atsižvelgiant į didėjančias grėsmes, riziką ir incidentus.

Padaryta pažanga rengiant šiuos pasiūlymus. Nors Kolegija jų dar nepriėmė, tikimasi, kad jie bus priimti 2022 m. pirmąjį ketvirtį. Svarbūs klausimai, kuriuos institucijos aptarė šiame parengiamajame etape, yra susiję su pasiūlymo teisiniu pagrindu ir visų EUIBA biudžeto pajėgumu patenkinti reikalavimus, susijusius su jų pačių kibernetinio saugumo poreikių finansavimu, ir rasti reikiamų išteklių CERT-EU, biudžetui ir ypač pareigybėms remti.

ES institucijų, įstaigų ir agentūrų kibernetinio saugumo brandos lygiai skiriasi. Kelių EUBIA rezultatai kibernetinės parengties srityje yra geri, todėl jos ir toliau turėtų būti lyderės, skatinančios ir įkvepiančios daryti pažangą ir tolesnius patobulinimus visoje kibernetinio saugumo aplinkoje. Siekiant išmatuojamos pažangos, svarbu pripažinti skirtingą EUIBA brandos lygį ir nustatyti prioritetus – visų pirma tobulinimo veiksmus skirti toms EUIBA, kuriose dėl nustatytų trūkumų kyla didžiausia rizika.

b) Komisijos pozicija dėl pagrindinių Audito Rūmų pastabų ir rekomendacijų

Komisija palankiai vertina Audito Rūmų ataskaitą dėl ES institucijų, įstaigų ir agentūrų kibernetinio saugumo. Ji atkreipia dėmesį į tai, kad ataskaitoje pabrėžiama bendrų teisinių sistemų svarba visoms EUIBA informacijos saugumo ir kibernetinio saugumo srityje siekiant padidinti bendrą visuotinį kibernetinio saugumo lygį. Komisija pažymi, kad pagrindinės Audito Rūmų pastabos ir rekomendacijos skirtos ne pačios Komisijos operatyviniam kibernetiniam saugumui, o Komisijos politiniam vaidmeniui siūlant teisės aktus, kuriais siekiama padidinti EUIBA kibernetinę brandą.

Būsimame reglamente dėl informacijos saugumo ES institucijose, įstaigose ir agentūrose ir reglamente dėl bendrų kibernetinio saugumo taisyklių ES institucijoms, įstaigoms ir agentūroms bus

nustatytos bendros taisyklės, kuriomis siekiama aukšto lygio informacijos saugumo ir kibernetinio saugumo, tačiau už jų įgyvendinimą, atsižvelgiant į kiekvienos EUIBA organizacines ir veiklos aplinkybes (visų pirma jų grėsmės ir rizikos profilius), ir toliau savarankiškai atsako EUIBA. Siūlomame reglamente dėl kibernetinio saugumo bus nustatyti atitikties užtikrinimo mechanizmai, kurie atitinka naujų taisyklių tikslą ir taikymo sritį ir yra jiems proporcingi, nedarant poveikio institucijų, įstaigų ir agentūrų autonomijai.

Šiuo metu Komisija pirmininkauja Tarpinstitucinio skaitmeninės transformacijos komiteto (ICDT) kibernetinio saugumo pogrupiui, o jam pirmininkaujama rotacijos tvarka (iki dvejų metų). Pažymima, kad pogrupio darbui neskiriama jokių specialių išteklių: visi veiksmai grindžiami tik dalyvių savanoriškomis pastangomis.

Komisija pritaria bendrajam principui, kad reikia stiprinti CERT-EU išteklius ir įgaliojimus.

Laikydamasi tokio požiūrio Komisija pritaria pagrindinėms ataskaitoje pateiktoms pastaboms ir rekomendacijoms. Mūsų išsami pozicija paaiškinta III skirsnyje pateiktose papildomose pastabose. Kalbant apie rekomendacijas, Komisija pritaria 1a, b, c, d, e, f, g ir 2a, b, c rekomendacijoms.

c) Aktualios naujausios tendencijos ir tolesni veiksmai

Užbaigtos oficialios konsultacijos su EUIBA generaliniais direktoriais dėl abiejų reglamentų (informacijos saugumas, kibernetinis saugumas) konsoliduotų projektų, o gautos grįžtamosios informacijos vertinimas tebevyksta. Paskui bus baigtas rengti dokumentų rinkinys ir Kolegija jį priims 2022 m. pirmąjį ketvirtį.

II. KOMISIJOS ATSAKYMAI Į PAGRINDINES EUROPOS AUDITO RŪMŲ PASTABAS

1. EUIBA kibernetinio saugumo brandos lygiai

Komisija sutinka, kad stebint EUIBA išlaidų kibernetiniam saugumui lygį svarbu atsižvelgti į grėsmes ir riziką.

Panašiai, kalbant apie žmogiškųjų išteklių aspektą, EUIBA personalo skaičiaus stabilumui įtakos turi keletas veiksnių. Vis sudėtingesnė tampa specializuotų kibernetinio saugumo ekspertų įdarbinimo rinka. Daugeliu atvejų žmogiškųjų išteklių taisyklės nėra pritaikytos specializuotiems profiliams (įdarbinimas, karjeros raida, mokymas). Be to, dėl biudžeto valdymo institucijos daromo bendro spaudimo, susijusio su darbuotojų skaičiumi visose EUIBA, naujose prioritetinėse srityse, kaip antai kibernetinis saugumas, vis dar trūksta etatų, visų pirma vidaus operatyvinėse tarnybose.

Vertinant pažangą valdymo ir rizikos valdymo srityje reikėtų atsižvelgti į tai, kad iš bandomojo atitikties stebėsenos etapo dabar pereinama į visiško įdiegimo etapą. Taigi normalu, kad iki šiol aprėptis gana maža. Šis atitikties projektas yra kitas ilgalaikio kibernetinės brandos gerinimo proceso etapas, kuris prasidėjo apibrėžiant bendrą rizikos metodiką, kuriant bendras priemones, diegiant pažeidžiamumo valdymą ir turto inventorizacijos stebėseną, testavimą ir patvirtinimą. Nepaisant sudėtingos Komisijos turto bazės, kurioje daugiau kaip 1 000 informacinių sistemų valdo daugiau kaip 50 generalinių direktoratų ir vykdomųjų įstaigų, einant šiuo ilgu keliu padaryta pažanga.

2. EUIBA bendradarbiavimo mechanizmai

CERT-EU yra fenomenalus sėkmės pavyzdys, kaip galima skatinti bendradarbiavimą ne tik tarp EUIBA, bet ir Europos lygmeniu, nes ji yra visateisė CSIRT tinklo, sukurto pagal TIS direktyvą, narė. Todėl CERT-EU yra pavyzdys, kaip galima sustiprinti bendradarbiavimą ir kibernetinio saugumo paslaugas. Iš Audito Rūmų pastabų dėl CERT-EU labai aiškiai matyti, kokį išskirtinį darbą atlieka CERT-EU susiduriant su vis priešiškesne kibernetinių grėsmių aplinka ir nuolatiniu išteklių trūkumu.

Pagal šį tarpinstitucinį susitarimą ES decentralizuotoms agentūroms ir bendrosioms įmonėms CERT-EU valdyboje oficialiai atstovauja ENISA. Be to, jų nuomonę valdybos posėdžiuose išreiškia IRT patariamojo komiteto (ICTAC) atstovas, kuriam leidžiama dalyvauti siekiant padėti ENISA atstovauti agentūroms, tačiau jis neturi oficialios būstinės ar balsavimo teisės. Tinkamo atstovavimo agentūroms CERT-ES valdyboje klausimas bus sprendžiamas siūlomame reglamente į valdybos sudėtį įtraukiant ne daugiau kaip tris Sąjungos agentūrų tinklo (EUAN) paskirtus atstovus, remiantis jos IRT patariamojo komiteto pasiūlymu.

Dalyvavimas ICDT kibernetinio saugumo pogrupio veikloje vyksta dedant visas pastangas ir lygiu, kurį nustato kiekviena EUIBA. Rengiant naują kibernetinio saugumo preliminariąją sutartį sprendžiama, kaip patobulinti dalijimąsi informacija apie viešuosius pirkimus, nes jie yra svarbi Kibernetinio saugumo pogrupio 2 darbo grupės veiklos sritis.

Kalbant apie bendras priemones, skirtas tokioms paslaugoms, kaip e. paštas ir vaizdo konferencija, Komisija yra įdiegusi priemonę, leidžiančią naudotis SECEM-2 sistema visoms EUIBA: šifruotu e. paštu, kuris priklauso nuo veiksmingo šifravimo raktų ir sertifikatų valdymo. Be to, šiuo metu kuriama SECABC priemonė, kuria naudojantis galima užšifruoti tarp institucijų siunčiamus elektroninius laiškus, siekiant nuo 2022 m. suteikti prieigą prie jos kiekvienai suinteresuotai EUIBA. Saugių vaizdo konferencijų priemonė, skirta SNC tarnyboms, jau įdiegta, ja naudotis gali būti suteikta galimybė ir kitoms EUIBA *ad hoc* pagrindu, administruojant posėdžio dalyvių tapatybę. Siūlomame reglamente dėl informacijos saugumo taip pat bus nuostatų dėl keitimosi neskelbtina informacija (t. y. taikant bendrą ženklinimą ir žymėjimą).

3. Dalijimasis informacija apie reikšmingus incidentus ar pažeidžiamumą

Tai, kad ne visos EUIBA praneša CERT-EU apie reikšmingus incidentus ar pažeidžiamumą, sprendžiama kibernetinio saugumo reglamento projekte, atsižvelgiant į Komisijos pasiūlymą, pateiktą TIS 2 direktyvoje[1]. Įgyvendinimo lygis priklausys nuo papildomų išteklių, kuriuos tam skirs autonominės EUIBA. Dėl EUIBA institucinės autonomijos tokių pranešimų pateikimo užtikrinimo galimybės tebėra ribotos, be kita ko, pagal siūlomą reglamentą, kaip šiuo metu planuojama. Siūlomame reglamente dėl kibernetinio saugumo bus nustatyti atitikties užtikrinimo mechanizmai, kurie atitinka naujų taisyklių tikslą ir taikymo sritį ir yra jiems proporcingi, nedarant poveikio institucijų, įstaigų ir agentūrų autonomijai.

[1] Pasiūlymas dėl Europos Parlamento ir Tarybos direktyvos dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria panaikinama Direktyva (ES) 2016/1148, COM/2020/823 *final*.

III. KOMISIJOS ATSAKYMAI Į EUROPOS AUDITO RŪMŲ IŠVADAS IR REKOMENDACIJAS

1 rekomendacija. Gerinti EUIBA kibernetinio saugumo parengtį taikant bendras privalomas taisykles ir didinant CERT-EU išteklius

Į siūlomą reglamento tekstą bus įtrauktos konkrečios priemonės, kuriomis siekiama toliau didinti bendrą kibernetinio saugumo lygį. Minėtos priemonės bus perkeltos į kibernetinio saugumo planus, apibrėžtus ir įgyvendinamus EUIBA lygmeniu pagal jų pačių kibernetinio saugumo valdymo sistemą.

Komisija pritaria šiai rekomendacijai. Dėl konkrečių smulkesnių rekomendacijų Komisija atkreipia dėmesį į tai, kad:

a) Komisija pritaria 1a rekomendacijai. Siekiant užtikrinti veiksmingą ir apdairų visos kibernetinio saugumo rizikos valdymą, į reglamento projektą bus įtrauktos nuostatos dėl kiekvienos EUIBA aukščiausio lygio vykdomosios vadovybės valdymo ir kontrolės sistemų;
b) Komisija pritaria 1b rekomendacijai. Reglamento projekte bus labiau pabrėžiamas rizika grindžiamas požiūris į kibernetinio saugumo valdymą, aiškiai nurodant, kad veiksmai, IT saugumo planai ir faktinis esminių kontrolės priemonių įgyvendinimas turėtų atitikti vertinimus;
c) Komisija pritaria 1c rekomendacijai. Kibernetinio saugumo švietimo, informuotumo didinimo ir mokymo programos reglamento projekte bus nurodytos kaip kibernetinio saugumo bazinio lygio dalis;
d) Komisija pritaria 1d rekomendacijai. Remiantis mūsų patirtimi, nors reguliarūs auditai ir bandymai yra labai svarbūs, jų nepakanka, kad būtų užtikrinta pažanga. Todėl būtina reguliariai teikti ataskaitas ir užtikrinti skaidrumą įgyvendinant a punkte minimą kibernetinio saugumo valdymo sistemą;
e) Komisija pritaria 1e rekomendacijai. Į reglamento projektą bus įtrauktos nuostatos, susijusios su EUIBA pranešimu apie dideles kibernetines grėsmes, pažeidžiamumą ir incidentus CERT-EU;
f) Komisija pritaria 1f rekomendacijai. Komisija pritaria, kad reikia stiprinti CERT-EU išteklius. Į reglamento projekto tekstą bus įtrauktos nuostatos, susijusios su EUIBA aprūpinimu darbuotojais ir finansiniais įnašais;
g) Komisija pritaria 1g rekomendacijai. Siūlomame reglamente bus numatyti atitikties užtikrinimo mechanizmai, kurie atitinka nuostatų tikslą ir taikymo sritį ir yra jiems proporcingi, atsižvelgiant į EUIBA institucinę autonomiją. Būsimo reglamento turinys priklauso nuo teisėkūros procedūros rezultatų ir yra ES teisės aktų leidėjo sprendimo dėl Komisijos pateikto pasiūlymo rezultatas.

2 rekomendacija. Pasisakyti už tolesnę EUIBA sąveiką pasirinktose srityse

Komisija, šiuo metu pirmininkaujanti Tarpinstitucinio skaitmeninės transformacijos komiteto Kibernetinio saugumo pogrupiui (ICDT), pritaria rekomendacijoms skatinti sprendimus, kaip nuosekliai ir saugiai dalytis neskelbtina informacija, sistemingai keistis informacija apie kibernetinio

saugumo projektus ir bendras viešųjų pirkimų sistemas bei sutartis dėl kibernetinio saugumo paslaugų.

Komisija pritaria šiai rekomendacijai. Dėl konkrečių smulkesnių rekomendacijų Komisija atkreipia dėmesį į tai, kad:

a) Komisija pritaria 2a rekomendacijai. Komisija siūlo technines iniciatyvas ir paslaugas ICDT Kibernetinio saugumo pogrupiui, siekdama skatinti ir remti bendras keitimosi neskelbtina informacija priemones, kuriomis sudaromos sąlygos teikti tokias paslaugas kaip e. paštas ir vaizdo konferencijos. Taip pat atkreipiame dėmesį į tai, kad siūlomame reglamente dėl informacijos saugumo bus aptartas bendros neskelbtinos neįslaptintos informacijos žymėjimas ir bendros tvarkymo taisyklės;
b) Komisija pritaria 2b rekomendacijai. ICDT Kibernetinio saugumo pogrupio darbo grupės sprendžia šį klausimą ir jis toliau bus plėtojamas. Rengiant naują kibernetinio saugumo preliminariąją sutartį siekiama gerinti dalijimąsi informacija apie viešuosius pirkimus;
c) Komisija pritaria 2c rekomendacijai. EUIBA jau turi galimybę sudaryti tarpinstitucines preliminariąsias sutartis IRT, kurias valdo Komisija, srityje. Naujos kibernetinio saugumo preliminariosios sutarties rengimas bus koordinuojamas su ICDT kibernetinio saugumo pogrupiu.

3 rekomendacija. CERT-EU ir ENISA daugiau dėmesio skirti mažiau brandžioms EUIBA

Ši rekomendacija skirta CERT-EU ir ENISA.