EUROPOS
KOMISIJA

Briuselis, 2017 10 04
COM(2017) 476 final

NOTE
This language version reflects the corrections done to the original EN version transmitted under COM(2017) 476 final of 13.9.2017 and retransmitted (with corrections) under COM(2017) 476 final/2 of 4.10.2017

KOMISIJOS KOMUNIKATAS EUROPOS PARLAMENTUI IR TARYBAI

Racionaliausias tinklų ir informacijos saugumas. Kaip veiksmingai įgyvendinti Direktyvą (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti

LT

Įvadas

2016 m. liepos 6 d. priimta Direktyva (ES) 2016/1148 dėl tinklų ir informacinių sistemų saugumo visoje Sąjungoje[1] (toliau – TIS direktyva, arba Direktyva) yra pirmas kibernetinio saugumo iššūkiams skirtas ES horizontalusis teisės aktas. Jį priėmus Europoje kibernetinio saugumo srities atsparumas ir bendradarbiavimas keičiasi iš esmės.

Pagrindiniai direktyvos tikslai yra trys:

- gerinti nacionalinius kibernetinio saugumo pajėgumus,
- stiprinti ES lygmens bendradarbiavimą ir
- ugdyti pagrindinių ekonominės veiklos vykdytojų, visų pirma visuomenei ir ekonomikai didelę reikšmę turinčias esmines paslaugas teikiančių operatorių ir skaitmeninių paslaugų teikėjų, nuostatą valdyti riziką ir pranešti apie incidentus.

TIS direktyva suteikia ES pagrindą reaguoti į didėjančias kibernetines grėsmes ir iššūkius, kylančius skaitmeninant mūsų ekonominį ir socialinį gyvenimą, todėl jos įgyvendinimas yra svarbi 2017 m. rugsėjo 13 d. pateikto kibernetinio saugumo dokumentų rinkinio dalis. Kol visos ES valstybės narės į savo teisę nėra perkėlusios visų TIS direktyvos nuostatų, ES atsakomieji veiksmai nėra labai efektyvūs. Ši esminė problema pripažinta 2016 m. Komisijos komunikate „Europos kibernetinio atsparumo sistemos stiprinimas“[2].

Iššūkiams, kurių kyla visiems subjektams siekiant laiku užtikrinti sėkmingą TIS direktyvos perkėlimą, reikia skirti ypatingą dėmesį, nes Direktyva naujoviška, be to, reikia skubiai reaguoti į sparčiai kintančią kibernetinių grėsmių įvairovę. Turėdama omeny perkėlimo terminą 2018 m. gegužės 9 d. ir esminių paslaugų operatorių identifikavimo terminą 2018 m. lapkričio 9 d., Komisija rėmė valstybių narių pastangas perkelti Direktyvą į nacionalinę teisę ir jų darbą Bendradarbiavimo grupėje, skirtą šiam tikslui.

Rašant šį komunikatą ir jo priedą pasinaudota Komisijos parengiamuoju darbu ir ligšiolinio TIS direktyvos įgyvendinimo analize, Europos tinklų ir informacijos apsaugos agentūros (ENISA) įnašu ir perkeliant Direktyvą vykusiomis diskusijomis su valstybėmis narėmis, konkrečiai Bendradarbiavimo grupės posėdžiuose[3]. Šis komunikatas papildo dideles iki šiol dėtas pastangas, visų pirma:

- intensyvų darbą Bendradarbiavimo grupėje. Grupė susitarė dėl darbo plano, pirmiausiai skirto TIS direktyvos perkėlimui, ypač esminių paslaugų operatorių identifikavimo ir su saugumo reikalavimais bei pranešimais apie incidentus susijusių jų pareigų klausimams. Direktyvoje leista savo nuožiūra spręsti dėl perkėlimo

[1] 2016 m. liepos 6 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti. Direktyva įsigaliojo 2016 m. rugpjūčio 8 d.
[2] COM(2016) 410 *final*.
[3] Veikla laikantis TIS direktyvos 11 straipsnyje numatyto valstybių narių strateginio bendradarbiavimo mechanizmo.

nuostatų, susijusių su esminių paslaugų operatoriais, tačiau valstybės narės pripažino, kad svarbu šiuo klausimo laikytis suderinto požiūrio[4];

- reagavimo į kompiuterinius saugumo incidentus tarnybų (toliau – CSIRT) tinklo sukūrimą ir greitai pradėtą operatyvinę veiklą pagal Direktyvos 12 straipsnio 1 dalį. Nuo to laiko šis tinklas pradėjo dėti pamatus struktūriniam Europos lygmens operatyviniam bendradarbiavimui.

Siekiant tikslo – bendro aukšto tinklų ir informacinių sistemų saugumo lygio Sąjungoje, labai svarbu, kad visos valstybės narės aktyviai dalyvautų abiejose struktūrose, kurių viena yra politikos, kita operatyvinio lygmens.

Šis komunikatas ir jo priedas papildys šias pastangas, nes juose skelbiama ir lyginama geriausia Direktyvos įgyvendinimo reikmėms naudinga valstybių narių patirtis, pateikiama daugiau Direktyvos įgyvendinimo gairių ir išsamiau paaiškinamos atskiros nuostatos. Visa apimantis tikslas – padėti valstybėms narėms užtikrinti veiksmingą ir suderintą TIS direktyvos įgyvendinimą visoje ES.

Šį komunikatą toliau papildys remiantis TIS direktyvos 16 straipsnio 8 dalimi rengiamas Komisijos įgyvendinimo reglamentas dėl elementų ir parametrų, susijusių su skaitmeninių paslaugų teikėjams keliamais saugumo ir pranešimo apie incidentus reikalavimais, patikslinimo. Įgyvendinimo reglamentu bus palengvintas skaitmeniniams paslaugų teikėjams Direktyvoje numatytų pareigų įgyvendinimas[5].

Komunikate pateikiamos pagrindinės aspektų, kurie perkeliant Direktyvą į nacionalinę teisę laikomi svarbiais atspirties taškais ir galimais orientyrais, analizės išvados. Dokumente daugiausia dėmesio skiriama valstybių narių pajėgumams ir su subjektais, kuriems taikoma Direktyva, susijusiems įpareigojimams. Priede išsamiau nagrinėjami klausimai, kuriems spręsti, Komisijos nuomone, labiausiai verta pateikti praktines perkėlimo gaires: paaiškinti tam tikras Direktyvos nuostatas, nurodyti, kaip Komisija jas interpretuoja, ir pristatyti geriausią praktiką ir iki šiol sukauptą Direktyvos įgyvendinimo patirtį.

Pasirengimas veiksmingai įgyvendinti TIS direktyvą

TIS direktyvos tikslas – pasiekti bendrą aukštą tinklų ir informacinių sistemų saugumo lygį Europos Sąjungoje. Tai reiškia, kad turi būti didinamas interneto ir privačių tinklų bei informacinių sistemų, palaikančių mūsų visuomenės ir ekonomikos funkcionavimą, saugumas. Šiuo aspektu pirmiausia svarbi valstybių narių parengtis. Ją reikėtų užtikrinti parengiant nacionalines kibernetinio saugumo strategijas, kaip aprašyta Direktyvoje. Tai

[4] Bendradarbiavimo grupė šiuo metu rengia pagalbinius rekomendacinius dokumentus, be kita ko, dėl: kriterijų, kuriais remiantis pagal Direktyvos 5 straipsnio 2 dalį apibrėžiama, koks operatoriaus yra ypatingos svarbos; aplinkybių, kuriomis esminių paslaugų operatoriai privalo pranešti apie incidentus pagal Direktyvos 14 straipsnio 7 dalį, ir saugumo reikalavimų esminių paslaugų operatoriams, pagal 14 straipsnio 1 ir 2 dalis.

[5] Nuomonę dėl įgyvendinimo reglamento projekto visuomenė gali pareikšti adresu https://ec.europa.eu/info/law/better-regulation/have-your-say_en.

turėtų atlikti reagavimo į kompiuterinius saugumo incidentus tarnybos ir kompetentingos nacionalinės institucijos.

Nacionalinių strategijų išsamumas

Valstybėms narėms svarbu pasinaudoti TIS direktyvos įgyvendinimu, kaip proga peržiūrėti savo nacionalines kibernetinio saugumo strategijas: remiantis priedu šalinti spragas, perimti geriausią praktiką ir reaguoti į naujus iššūkius.

Suprantama, kad Direktyvoje daugiausia dėmesio skiriama toms įmonėms ir paslaugoms, kurių svarba ypač didelė, tačiau reikia visapusiškai ir nuosekliai spręsti visos ekonomikos ir visuomenės kibernetinio saugumo uždavinį, nes priklausomybė nuo informacinių ir ryšių technologijų vis didėja. Todėl priėmus visapusiškas nacionalines strategijas, kuriomis siekiama daugiau, negu minimaliai reikalaujama TIS direktyvoje (t. y. strategijas taikant ne vien Direktyvos II priede išvardytiems sektoriams ir III priede nurodytoms paslaugoms), padidėtų bendras tinklų ir informacijos sistemų saugumo lygis.

Kadangi kibernetinis saugumas yra palyginti nauja ir sparčiai besiplečianti viešosios politikos sritis, daugeliu atveju reikia naujų investicijų, net kai bendra viešųjų finansų padėtis reikalauja apkarpyti išlaidas ir taupyti. Todėl siekiant pasiekti Direktyvos tikslus būtina priimti didelio užmojo sprendimus – skirti adekvačių finansinių ir žmogiškųjų išteklių, kurie neišvengiami norint veiksmingai įgyvendinti nacionalines strategijas. Be kita ko, reikia suteikti pakankamų išteklių nacionalinėms kompetentingoms institucijoms ir CSIRT.

Įgyvendinimo ir vykdymo užtikrinimo veiksmingumas

Direktyvos 8 straipsnyje nurodyta, kad reikia paskirti atitinkamas nacionalines kompetentingas institucijas ir bendruosius informacinius centrus. Tai būtina veiksmingo TIS direktyvos įgyvendinimo ir tarpvalstybinio bendradarbiavimo sąlyga. Valstybės narės pasirinko taikyti tiek centralizuotus, tiek decentralizuotus modelius. Kai valstybės narės pasirinko labiau decentralizuotą nacionalinių kompetentingų institucijų skyrimo modelį, paaiškėjo, kad labai svarbu užtikrinti sklandžią gausių institucijų ir bendrojo informacinio centro bendradarbiavimo tvarką (*žr. priedo 3.2 skirsnio 1 lentelę*). Tai padidintų įgyvendinimo ir vykdymo užtikrinimo veiksmingumą.

Ankstesnė su ypatingos svarbos informacinės infrastruktūros apsauga susijusi patirtis gali padėti valstybėms narėms suprojektuoti optimalų valdymo modelį, kad būtų užtikrintas ir veiksmingas TIS direktyvos įgyvendinimas atskiruose sektoriuose, ir nuoseklus kompleksinis požiūris (*žr. priedo 3.1 skirsnį*).

Nacionalinių CSIRT pajėgumų didinimas

Be veiksmingų adekvačius išteklius turinčių CSIRT, kurios numatytos TIS direktyvos 9 straipsnyje, ES tarpvalstybinių kibernetinių grėsmių akivaizdoje bus pernelyg pažeidžiama. Todėl valstybės narės galėtų apsvarstyti galimybę į CSIRT veikimo sritį įtraukti ir tuos sektorius bei paslaugas, kurios nėra numatytos pagal Direktyvą (*žr. priedo 3.3 skirsnį*). Tai leistų nacionalinėms CSIRT teikti operatyvinę paramą, kai kibernetiniai incidentai įvyksta įmonėse ir organizacijose, kurios svarbios visuomenei ir ekonomikai, nors joms Direktyva ir netaikoma. Be to, valstybės narės galėtų visapusiškai pasinaudoti papildomomis Europos infrastruktūros tinklų priemonės Kibernetinio saugumo skaitmeninių paslaugų infrastruktūros programos teikiamomis finansavimo galimybėmis, kurių tikslas – stiprinti nacionalinių CSIRT pajėgumus ir jų bendradarbiavimą (*žr. priedo 3.5 skirsnį*).

Esminių paslaugų operatorių identifikavimo proceso nuoseklumas

Pagal TIS direktyvos 5 straipsnį valstybės narės privalo iki 2018 m. lapkričio 9 d. identifikuoti subjektus, laikytinus esminių paslaugų operatoriais. Atlikdamos šią užduotį, valstybės narės galėtų nuspręsti, kad šiame komunikate pateiktas apibrėžtis ir gaires tikslinga taikyti nuosekliai siekiant užtikrinti, kad panašaus tipo ir panašų vaidmenį vidaus rinkoje turintys subjektai ir kitose valstybėse narėse būtų nuosekliai identifikuojami kaip esminių paslaugų operatoriai. Valstybės narės galėtų nuspręsti į TIS direktyvos taikymo sritį įtraukti viešojo administravimo įstaigas, atsižvelgiant į jų reikšmę visai visuomenei ir ekonomikai (*žr. priedo 2.1. ir 4.1.3 skirsnius*).

Būtų labai naudinga kuo labiau suderinti nacionalinius esminių paslaugų operatorių identifikavimo modelius, laikantis Bendradarbiavimo grupės parengtų gairių (*žr. priedo 4.1.2 skirsnį*), nes tai užtikrintų labiau suderintą Direktyvos nuostatų taikymą ir taip sumažintų rinkos susiskaidymo riziką. Tais atvejais, kai esminių paslaugų operatoriai esmines paslaugas teikia dviejose ar daugiau valstybių narių, labai svarbu, kad valstybės narės konsultuodamosi, kaip numatyta 5 straipsnio 4 dalyje, siektų susitarimo dėl nuoseklaus subjektų identifikavimo (*žr. priedo 4.1.7 skirsnį*), nes taip būtų išvengta skirtingo to paties subjekto reguliavimo skirtingų valstybių narių jurisdikcijose.

Informacijos apie esminių paslaugų operatorių identifikavimą pateikimas Komisijai

Pagal 5 straipsnio 7 dalį reikalaujama, kad valstybės narės pateiktų Komisijai informaciją apie nacionalines priemones, leidžiančias identifikuoti esminių paslaugų operatorius, esminių paslaugų sąrašą, identifikuotų esminių paslaugų operatorių skaičių ir tų operatorių svarbą sektoriui. Be to, valstybių narių reikalaujama nurodyti identifikavimo procese taikomas ribas, jei jų esama, siekiant nustatyti atitinkamą tiekimo lygį arba konkretaus esminių paslaugų operatoriaus svarbą pakankamam paslaugos lygiui išlaikyti. Valstybės narės taip pat galėtų nuspręsti pateikti Komisijai identifikuotų esminių paslaugų operatorių sąrašus, jei būtina, konfidencialiai, nes tai padėtų pagerinti Komisijos vertinimo tikslumą ir kokybę (*žr. priedo 4.1.5 ir 4.1.6 skirsnius*).

Suderinti požiūriai į esminių paslaugų operatoriams keliamus saugumo ir pranešimo apie incidentus reikalavimus

Kiek tai susiję su 14 straipsnio 1–3 dalyse nustatytomis esminių paslaugų operatorių pareigomis laikytis saugumo reikalavimų ir pranešti apie incidentus, suderintas požiūris į saugumo reikalavimus ir pranešimus apie incidentus siekiant, kad esminių paslaugų operatoriams būtų lengviau atitikti reikalavimus keliose ES valstybėse narėse, maksimaliai sustiprintų teigiamą bendrosios rinkos poveikį. Šiuo klausimu reikia atsižvelgti į Bendradarbiavimo grupėje vykdomą rekomendacinio dokumento rengimo darbą (*žr. priedo 4.2 ir 4.3 skirsnius*).

Jei kelias valstybes nares ištiktų didelio masto kibernetinis incidentas, labai tikėtina, kad privaloma tvarka pranešimą apie incidentą pateiktų esminių paslaugų operatorius ar skaitmeninių paslaugų teikėjas pagal 14 straipsnio 3 dalį ir 16 straipsnio 3 dalį arba savanoriškai kitas subjektas, kuriam Direktyva netaikoma, pagal 20 straipsnio 1 dalį. Laikantis Komisijos rekomendacijos dėl koordinuoto atsako į didelio masto kibernetinio saugumo incidentus ir krizes, valstybės narės galėtų nuspręsti suderinti nacionalinius požiūrius taip, kad tais pranešimais pagrįstą svarbią informaciją jos galėtų kuo greičiau pateikti kitų suinteresuotų valstybių narių kompetentingoms institucijoms ar CSIRT. Tiksli praktiška informacija labai padėtų sumažinti užkrėtimų skaičių ir pašalinti saugumo spragas, kol jomis dar nepasinaudota.

Veikdama pagal partnerystės principą ir siekdama, kad TIS direktyva būtų kuo naudingesnė, Komisija ketina plėsti pagal Europos infrastruktūros tinklų priemonę teikiamą pagalbą visiems suinteresuotiesiems subjektams, su kuriais susijęs šis teisės aktas. Pirmiausia finansavimo Europos infrastruktūros tinklų priemonės lėšomis buvo siekiama stiprinti CSIRT pajėgumus ir sukurti platformą, kurioje vyktų spartus ir veiksmingas operatyvinis bendradarbiavimas, ir taip sustiprinti CSIRT tinklą. Dabar Komisija svarstys, kaip šiomis lėšomis galima padėti taip pat nacionalinėms kompetentingoms institucijoms ir esminių paslaugų operatoriams bei skaitmeninių paslaugų teikėjams.

Išvada

Artėjant TIS direktyvos perkėlimo į nacionalinės teisės aktus terminui 2018 m. gegužės 9 d. ir esminių paslaugų operatorių identifikavimo terminui 2018 m. lapkričio 9 d., valstybės narės turėtų tinkamai užtikrinti, kad TIS direktyvos nuostatos ir bendradarbiavimo modeliai galėtų tapti pačiomis geriausiomis ES lygmens priemonėmis bendram aukštam tinklų ir informacinių sistemų saugumo lygiui Sąjungoje pasiekti. Komisija ragina valstybes nares per šį procesą apsvarstyti šiame komunikate pateiktą aktualią informaciją, gaires ir rekomendacijas.

Šis komunikatas gali būti toliau papildomas kitais veiksmais, be kita ko, tais, kurie inicijuojami vykdant tęstinį Bendradarbiavimo grupės darbą.