EUROOPA
KOMISJON

Brüssel, 4.10.2017
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

KOMISJONI TEATIS EUROOPA PARLAMENDILE JA NÕUKOGULE

Parimate tulemuste saavutamine võrgu- ja infoturbe direktiivi rakendamisel – jõupingutused direktiivi (EL) 2016/1148 (meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus) tulemuslikuks rakendamiseks

ET

Sissejuhatus

6. juulil 2016 vastu võetud direktiiv (EL) 2016/1148 võrgu- ja infosüsteemide turvalisuse kohta kogu liidus[1] (edaspidi „võrgu- ja infoturbe direktiiv“ või „direktiiv“) on ELi esimene küberturvalisuse probleeme käsitlev horisontaalne õigusakt, mis on Euroopa kübervastupidavusvõime ja küberturvalisuse alase koostöö seisukohalt teedrajav.

Direktiivil on kolm peamist eesmärki:

- liikmesriikide suutlikkuse suurendamine küberturvalisuse valdkonnas;
- koostöö arendamine liidu tasandil ning
- riskijuhtimise ja intsidentidest teatamise kultuuri edendamine oluliste majandustegevuses osalejate, eelkõige majandus- ja ühiskondlike tegevuste säilitamiseks olulisi teenuseid osutavate operaatorite ning digitaalse teenuse osutajate seas.

Võrgu- ja infoturbe direktiiv on Euroopa Liidu tegevuse nurgakivi reageerimisel kasvavatele küberohtudele ja -probleemidele, mis kaasnevad meie majandus- ja ühiskondliku elu üleminekuga digitaaltehnoloogiale, ning selle rakendamine on seetõttu 13. septembril 2017 esitatud küberturvalisuse paketi oluline osa. ELi reageerimise tulemuslikkus on pärsitud, kuni see direktiiv ei ole kõikides liikmesriikides täielikult üle võetud. Seda peeti kriitiliseks küsimuseks ka komisjoni 2016. aasta teatises Euroopa kübervastupidavusvõime süsteemi tugevdamise kohta[2].

Võrgu- ja infoturbe direktiivi uudsus ja kiiresti muutuvate küberohtudega tegelemise pakilisus nõuavad erilise tähelepanu pööramist probleemidele, millega kõik osalejad direktiivi õigeaegsel ja edukal ülevõtmisel silmitsi seisavad. 9. mail 2018 saabuvat ülevõtmise tähtaega ja 9. novembril 2018 saabuvat oluliste teenuste operaatorite identifitseerimise tähtaega silmas pidades on komisjon toetanud liikmesriikide ülevõtmisprotsessi ja nende sellealast tööd koostöörühmas.

Käesolev teatis ja selle lisa põhinevad komisjoni ettevalmistaval tööl ja direktiivi senise rakendamisega seotud analüüsil, Euroopa Liidu Võrgu- ja Infoturbeameti (ENISA) panusel ning liikmesriikidega direktiivi ülevõtmisetapis, eelkõige koostöörühmas[3] peetud aruteludel. See teatis täiendab seniseid märkimisväärseid jõupingutusi, mis hõlmavad eelkõige järgmist:

- koostöörühma intensiivne töö, mille tulemusena on kokku lepitud töökava, mis keskendub eeskätt võrgu- ja infoturbe direktiivi ülevõtmisele, eriti oluliste teenuste operaatorite identifitseerimise küsimusele ning nende kohustustele seoses turvanõuete ja intsidentidest teatamisega. Kuigi direktiiv näeb ette kaalutlusõiguse oluliste teenuste

[1] Euroopa Parlamendi ja nõukogu 6. juuli 2016. aasta direktiiv (EL) 2016/1148 meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus. Direktiiv jõustus 8. augustil 2016.
[2] COM(2016) 410 final.
[3] Võrgu- ja infoturbe direktiivi artikli 11 kohane liikmesriikidevahelise strateegilise koostöö mehhanism.

operaatoritega seotud sätete ülevõtmisel, on liikmesriigid tunnistanud ühtlustatud lähenemisviisi tähtsust selles küsimuses[4];

- küberturbe intsidentide lahendamise üksuste (CSIRTid) võrgustiku loomine ja kiire toimimise tagamine kooskõlas direktiivi artikli 12 lõikega 1. Võrgustik on alustanud aluse panemist struktureeritud operatiivkoostööle Euroopa tasandil.

Nii poliitilisel kui ka operatiivtasandil, mida need kaks struktuuri esindavad, on väga oluline liikmesriikide täielik kaasamine, et saavutada eesmärgiks olev võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase liidus.

Käesolev teatis ja selle lisa tugevdavad neid jõupingutusi, koondades kokku direktiivi rakendamisel asjakohased liikmesriikide parimad tavad ja võrreldes neid ning andes täiendavaid suuniseid direktiivi rakendamiseks ja üksikasjalikumaid selgitusi konkreetsete sätete kohta. Üldine eesmärk on liikmesriike toetada, et saavutada võrgu- ja infoturbe direktiivi tõhus ja ühtne rakendamine kogu Euroopa Liidus.

Teatist täiendab direktiivi artikli 16 lõike 8 kohaselt vastu võetav komisjoni rakendusmäärus, milles täpsustatakse täiendavalt digitaalse teenuse osutajatele kohaldatavate turvanõuete ja intsidentidest teatamise kohustusega seotud elemente ja parameetreid. Rakendusmäärus hõlbustab direktiivi rakendamist seoses digitaalse teenuse osutajate kohustustega[5].

Teatises esitatakse peamised järeldused, mis tehti nende küsimuste analüüsi tulemusena, mida peetakse olulisteks lähtepunktideks ja millest võib juhinduda siseriiklikku õigusesse ülevõtmisel. Põhitähelepanu pälvivad sätted, mis käsitlevad liikmesriikide suutlikkust ja kohustusi seoses direktiivi kohaldamisalasse kuuluvate üksustega. Lisas on üksikasjalikumalt käsitletud valdkondi, milles komisjon näeb praktiliste ülevõtmissuuniste andmisel kõige suuremat kasutegurit, selgitades ja tõlgendades teatavaid direktiivi sätteid ning tutvustades seniseid direktiiviga seotud parimaid tavasid ja saadud kogemusi.

Jõupingutused direktiivi tulemuslikuks rakendamiseks

Võrgu- ja infoturbe direktiivi eesmärk on saavutada ELis võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase. See tähendab interneti ning ühiskonna ja majanduse toimimist toetavate eravõrkude ja -infosüsteemide turvalisuse suurendamist. Sellega seoses on esimene oluline element liikmesriikide valmisolek, mis tuleks tagada direktiivikohase riikliku küberturvalisuse strateegia kehtestamise ning CSIRTide ja riiklike pädevate asutuste tööga.

Riiklike strateegiate terviklikkus

[4] Koostöörühm töötab praegu välja viitena kasutatavaid juhenddokumente, mis käsitlevad muu hulgas järgmist: kriteeriumid, mille alusel määratakse kindlaks operaatori olulisus vastavalt direktiivi artikli 5 lõikele 2, olukorrad, kus oluliste teenuste operaatoritelt nõutakse direktiivi artikli 14 lõike 7 kohaselt intsidentidest teatamist, ja oluliste teenuste operaatoritele esitatavad turvanõuded kooskõlas artikli 14 lõigetega 1 ja 2.

[5] Rakendusmääruse eelnõu on tehtud avalikkusele tutvumiseks kättesaadavaks aadressil https://ec.europa.eu/info/law/better-regulation/have-your-say_et.

On tähtis, et liikmesriigid kasutaksid võrgu- ja infoturbe direktiivi ülevõtmisega kaasnevat võimalust oma riikliku küberturvalisuse strateegia läbivaatamiseks, võttes arvesse lisas käsitletud puudusi, parimaid tavasid ja uusi probleeme.

Kuigi direktiiv keskendub mõistagi eriti olulistele äriühingutele ja teenustele, tuleb IKTst sõltuvuse pideva suurenemise tõttu tegeleda terviklikult ja järjepidevalt majanduse ja ühiskonna küberturvalisusega tervikuna. Seepärast tõstaks direktiivi miinimumnõudeid ületavate (st rohkem kui vastavalt direktiivi II ja III lisas loetletud sektoreid ja teenuseid hõlmavate) terviklike riiklike strateegiate vastuvõtmine võrgu- ja infosüsteemide turvalisuse üldist taset.

Kuna küberturvalisus on ikka veel suhteliselt uus ja kiiresti laienev avaliku poliitika valdkond, on enamikul juhtudel vaja uusi investeeringuid, isegi kui riigi rahanduse üldine olukord nõuab kärpeid ja säästmist. Seetõttu on direktiivi eesmärkide saavutamiseks ülioluline teha kaugeleulatuvaid otsuseid, et tagada piisavad rahalised vahendid ja inimressursid, mis on hädavajalikud riiklike strateegiate tulemuslikuks rakendamiseks, sealhulgas eraldada piisavalt ressursse riiklikele pädevatele asutustele ja CSIRTidele.

Rakendamise ja täitmise tulemuslikkus

Direktiivi artiklis 8 on nimetatud asjaomaste riiklike pädevate asutuste ja ühtsete kontaktpunktide määramise vajadust, mis on direktiivi tulemusliku rakendamise ja piiriülese koostöö tagamise üks võtmeelemente. Seoses sellega on liikmesriikides tekkinud nii tsentraliseeritumaid kui ka detsentraliseeritumaid lähenemisviise. Liikmesriikides, kus riiklike pädevate asutuste määramisel järgitakse detsentraliseeritumat lähenemisviisi, on osutunud oluliseks tugevate koostöökokkulepete sõlmimine arvukate asutuste ja ühtse kontaktpunkti vahel (*vt lisa punkti 3.2 tabel 1*). See suurendab rakendamise tulemuslikkust ja hõlbustab täitmist.

Tuginemine varasematele kogemustele elutähtsa infoinfrastruktuuri kaitse alal võib aidata välja töötada liikmesriikide jaoks optimaalse juhtimismudeli, mis tagab nii direktiivi tulemusliku valdkondliku rakendamise kui ka sidusa horisontaalse lähenemisviisi (*vt lisa punkt 3.1*).

Riiklike CSIRTide suurem suutlikkus

Kui kogu ELis ei tegutse piisavate ressurssidega varustatud ja tulemuslikud riiklikud CSIRTid, nagu on ette nähtud võrgu- ja infoturbe direktiivi artiklis 9, jääb Euroopa Liit piiriüleste küberohtude suhtes liiga haavatavaks. Liikmesriigid võiksid seetõttu kaaluda CSIRTide pädevusala laiendamist direktiivi kohaldamisalast väljapoole jäävatele sektoritele ja teenustele (*vt lisa punkt 3.3*). See võimaldaks riiklikel CSIRTidel pakkuda operatiivtuge sellistes äriühingutes ja organisatsioonides toimuvate küberintsidentide puhul, mis ei kuulu

direktiivi kohaldamisalasse, kuid on ühiskonna ja majanduse jaoks samuti olulised. Peale selle võiksid liikmesriigid täielikult ära kasutada täiendavaid rahastamisvõimalusi, mida pakub Euroopa ühendamise rahastu küberturvalisuse digitaalteenuste taristu programm, mille eesmärk on suurendada riiklike CSIRTide suutlikkust ja koostööd (*vt lisa punkt 3.5*).

Oluliste teenuste operaatorite identifitseerimise protsessi järjepidevus

Vastavalt võrgu- ja infoturbe direktiivi artiklile 5 peavad liikmesriigid identifitseerima 9. novembriks 2018 üksused, keda käsitatakse oluliste teenuste operaatoritena. Liikmesriigid võiksid seoses selle ülesandega kaaluda käesolevas teatises esitatud määratluste ja suuniste järjepidevat kasutamist, et sarnast liiki üksused, kellel on siseturul sarnane roll, identifitseeritaks teistes liikmesriikides järjepidevalt oluliste teenuste operaatoritena. Liikmesriigid võiksid kaaluda ka direktiivi kohaldamisala laiendamist haldusasutustele, arvestades nende rolli ühiskonnas ja majanduses tervikuna (*vt lisa punktid 2.1 ja 4.1.3*).

Väga kasulik oleks liikmesriikide lähenemised oluliste teenuste operaatorite identifitseerimisele võimalikult ulatuslikult ühtlustada, järgides eelkõige koostöörühma koostatud suuniseid (*vt lisa punkt 4.1.2*), sest see soodustaks direktiivi sätete ühtsemat kohaldamist ja vähendaks seega turu killustatuse ohtu. Kui oluliste teenuste operaatorid osutavad olulisi teenuseid kahes või enamas liikmesriigis, on tähtis, et liikmesriigid jõuaksid üksuste järjepideva identifitseerimise suhtes artikli 5 lõike 4 kohase konsulteerimise käigus kokkuleppele (*vt lisa punkt 4.1.7*), kuna see väldib sama üksuse erinevat õiguslikku kohtlemist eri liikmesriikides.

Oluliste teenuste operaatorite identifitseerimise kohta teabe esitamine komisjonile

Vastavalt artikli 5 lõikele 7 peavad liikmesriigid esitama komisjonile teabe, mis hõlmab oluliste teenuste operaatorite identifitseerimist võimaldavaid riiklikke meetmeid, oluliste teenuste loetelu, identifitseeritud oluliste teenuste operaatorite arvu ning nende operaatorite tähtsust asjaomases sektoris. Peale selle peavad liikmesriigid esitama piirmäärad (kui need on olemas), mida kasutatakse identifitseerimisel, et kindlaks määrata asjakohane teenuse osutamise tase või asjaomase operaatori tähtsus teenuse osutamise piisava taseme säilitamisel. Liikmesriigid võiksid kaaluda ka identifitseeritud oluliste teenuste operaatorite loetelu esitamist komisjonile (vajaduse korral konfidentsiaalselt), sest see parandaks komisjoni hindamise täpsust ja kvaliteeti (*vt lisa punktid 4.1.5 ja 4.1.6*).

Ühtlustatud lähenemine seoses oluliste teenuste operaatoritele kohaldatavate turvanõuete ja intsidentidest teatamise kohustusega

Seoses oluliste teenuste operaatorite turvanõuete ja intsidentidest teatamise kohustusega (artikli 14 lõiked 1, 2 ja 3) suurendaks ühtse turu mõju kõige enam ühtlustatud lähenemine turvanõuetele ja intsidentidest teatamise kohustusele, mis hõlbustaks nõuete piiriülest järgimist oluliste teenuste operaatorite poolt. Taas kord on kohane viidata koostöörühmas juhenddokumendi koostamiseks tehtud tööle (*vt lisa punktid 4.2 ja 4.3*).

Mitut liikmesriiki mõjutava ulatusliku küberintsidendi puhul on väga tõenäoline, et oluliste teenuste operaator või digitaalse teenuse osutaja esitab artikli 14 lõike 3 või artikli 16 lõike 3 kohaselt kohustusliku intsidenditeate või muu üksus, mis ei kuulu direktiivi kohaldamisalasse, esitab artikli 20 lõike 1 kohaselt vabatahtliku teate. Kooskõlas komisjoni soovitusega koordineeritud reageerimise kohta ulatuslike küberturvalisuse intsidentide ja kriiside korral võiksid liikmesriigid kaaluda riiklike lähenemisviiside ühtlustamist, et nad saaksid nende teadete põhjal võimalikult ruttu esitada asjakohast teavet teiste asjaomaste liikmesriikide pädevatele asutustele või CSIRTile. Täpne ja meetmeid võtta võimaldav teave oleks väga vajalik nakatumiste arvu vähendamiseks või nõrkuste kõrvaldamiseks enne nende ärakasutamist.

Parimate tulemuste saavutamiseks võrgu- ja infoturbe direktiivi rakendamisel kavatseb komisjon partnerluse vaimus laiendada Euroopa ühendamise rahastu raames pakutavat toetust kõikidele nimetatud õigusakti puhul asjakohastele sidusrühmadele. Kui seni olid tähelepanu keskmes CSIRTide suutlikkuse suurendamine ning kiiret ja tõhusat operatiivkoostööd võimaldav platvorm, millega tugevdati seega CSIRTide võrgustikku, siis praegu uurib komisjon, kuidas Euroopa ühendamise rahastu raames pakutav rahastamine saab tuua kasu ka riiklikele pädevatele asutustele ning oluliste teenuste operaatoritele ja digitaalse teenuse osutajatele.

Kokkuvõte

Kuna võrgu- ja infoturbe direktiivi siseriiklikku õigusesse ülevõtmise tähtaeg on 9. mail 2018 ja oluliste teenuste operaatorite identifitseerimise tähtaeg on 9. novembril 2018, peaksid liikmesriigid võtma asjakohaseid meetmeid eesmärgiga tagada, et direktiivi sätted ja koostöömudelid annavad võimalikest parimad ELi tasandi vahendid võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge taseme saavutamiseks kogu liidus. Komisjon kutsub liikmesriike üles arvestama selle protsessi käigus käesolevas teatises esitatud asjakohast teavet, suuniseid ja soovitusi.

Käesolevat teatist võidakse veelgi täiendada muude meetmetega, sealhulgas koostöörühmas välja töötatud meetmetega.