I

(Seadusandlikud aktid)

DIREKTIIVID

EUROOPA PARLAMENDI JA NÕUKOGU DIREKTIIV (EL) 2016/1148,

6. juuli 2016,

meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus

EUROOPA PARLAMENT JA EUROOPA LIIDU NÕUKOGU,

võttes arvesse Euroopa Liidu toimimise lepingut, eriti selle artiklit 114,

võttes arvesse Euroopa Komisjoni ettepanekut,

olles edastanud seadusandliku akti eelnõu liikmesriikide parlamentidele,

võttes arvesse Euroopa Majandus- ja Sotsiaalkomitee arvamust ([1]),

toimides seadusandliku tavamenetluse kohaselt ([2])

ning arvestades järgmist:

(1) Võrgu- ja infosüsteemidel ning -teenustel on ühiskonnas eluliselt tähtis koht. Nende usaldusväärsus ja turvalisus on majandus- ja ühiskondliku tegevuse ning ennekõike siseturu toimimise jaoks hädavajalik.

(2) Turvaintsidentide ulatus, sagedus ja mõju suurenevad ning see kujutab endast suurt ohtu võrgu- ja infosüsteemide toimimisele. Need süsteemid võivad saada ka tahtliku kahjustamise sihtmärgiks, millega tahetakse süsteemide tööd häirida või seda katkestada. Sellised intsidendid võivad takistada majandustegevust, põhjustada olulist finantskahju, vähendada kasutajate usaldust ja tekitada liidu majandusele suurt kahju.

(3) Võrgu- ja infosüsteemidel ning eelkõige internetil on oluline roll kaupade, teenuste ja inimeste piiriülese liikumise hõlbustamisel. Sellisest riikidevahelisusest tulenevalt võib nende süsteemide töö kas tahtlik või tahtmatu oluline katkestus olenemata katkestuse kohast mõjutada üksikuid liikmesriike ja liitu tervikuna. Seepärast on võrgu- ja infosüsteemide turvalisus siseturu sujuvaks toimimiseks hädavajalik.

(4) Arvestades liikmesriikide Euroopa foorumi märkimisväärset edu heade poliitiliste tavade üle peetud arutelude ja teabevahetuse soodustamisel, kaasa arvatud Euroopa küberkriisialase koostöö põhimõtete väljatöötamist, tuleks moodustada liikmesriikide, komisjoni ja Euroopa Liidu Võrgu- ja Infoturbeameti (ENISA) esindajatest koosnev koostöörühm, et toetada ja hõlbustada liikmesriikidevahelist võrgu- ja infosüsteemide turvalisuse alast strateegilist

([1]) ELT C 271, 19.9.2013, lk 133.

([2]) Euroopa Parlamendi 13. märtsi 2014. aasta seisukoht (*Euroopa Liidu Teatajas* seni avaldamata) ja nõukogu 17. mai 2016. aasta esimese lugemise seisukoht (*Euroopa Liidu Teatajas* seni avaldamata). Euroopa Parlamendi 6. juuli 2016. aasta seisukoht (*Euroopa Liidu Teatajas* seni avaldamata).

koostööd. Selleks et selline rühm oleks tõhus ja kaasav, on oluline, et kõigil liikmesriikidel oleks miinimumsuutlikkus ja strateegia võrgu- ja infosüsteemide turvalisuse kõrge taseme tagamiseks oma territooriumil. Lisaks tuleks turva- ja teavitamisnõudeid kohaldada oluliste teenuste operaatorite ja digitaalse teenuse osutajate suhtes, et edendada riskihalduse kultuuri ja tagada, et kõige raskematest intsidentidest teatatakse.

(5) Praegune suutlikkus ei ole liidus võrgu- ja infosüsteemide turvalisuse kõrge taseme tagamiseks piisav. Liikmesriikide valmisoleku tase on väga erinev ning see põhjustab liidu lõikes lähenemisviiside killustatuse. Selle tulemusel ei ole tarbijad ja ettevõtjad võrdselt kaitstud ning samuti langeb võrgu- ja infosüsteemide turvalisuse üldine tase liidus. Oluliste teenuste operaatorite ja digitaalse teenuse osutajate suhtes kohaldatavate ühiste miinimumnõuete puudumine muudab omakorda võimatuks üldise tõhusa koostöömehhanismi loomise liidu tasandil. Ülikoolid ja teaduskeskused etendavad otsustavat rolli teadusuuringute, arendustegevuse ja innovatsiooni edendamises kõnealustes valdkondades.

(6) Tulemuslik reageerimine võrgu- ja infosüsteemide turvalisusega seotud probleemidele eeldab seega liidu tasandil üldist lähenemist, mis hõlmaks ühise miinimumsuutlikkuse loomist ja kavandamisnõudeid, teabevahetust, koostööd ning ühiseid turvanõudeid oluliste teenuste operaatoritele ja digitaalse teenuse osutajatele. Oluliste teenuste operaatoritele ja digitaalse teenuse osutajatele ei tehta takistusi käesolevas direktiivis sätestatutest rangemate turvameetmete kohaldamiseks.

(7) Selleks et hõlmatud oleks kõik asjakohased intsidendid ja riskid, tuleks käesolevat direktiivi kohaldada nii oluliste teenuste operaatorite kui ka digitaalse teenuse osutajate suhtes. Oluliste teenuste operaatoritele ja digitaalse teenuse osutajatele pandud kohustusi ei tuleks siiski kohaldada ettevõtjate suhtes, kes pakuvad üldkasutatavaid sidevõrke või üldkasutatavaid elektroonilisi sideteenuseid Euroopa Parlamendi ja nõukogu direktiivi 2002/21/EÜ ([1]) tähenduses ja kelle suhtes kehtivad konkreetsed turva- ja terviklusnõuded, mis on sätestatud nimetatud direktiivis, ning neid ei tuleks kohaldada ka usaldusteenuse osutajate suhtes Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 ([2]) tähenduses, kelle suhtes kehtivad nimetatud määruses sätestatud turvanõuded.

(8) Käesolev direktiiv ei tohiks piirata liikmesriikide võimalust võtta vajalikke meetmeid, et tagada oma oluliste julgeolekuhuvide kaitse, tagada avalik kord ja julgeolek ning võimaldada kriminaalkuritegude uurimist, avastamist ja nende eest vastutusele võtmist. Vastavalt Euroopa Liidu toimimise lepingu (ELi toimimise leping) artiklile 346 ei tohi ühtki liikmesriiki kohustada andma teavet, mille avalikustamist ta peab oma oluliste julgeolekuhuvide vastaseks. Selles kontekstis on asjakohased nõukogu otsus 2013/488/EL, ([3]) mitteavalikustamise kokkulepped või mitteametlikud mitteavalikustamise kokkulepped, näiteks protokoll teabe tundlikkuse märgistamise kohta fooritulede analoogia põhjal.

(9) Teatavate majandussektorite suhtes juba kohaldatakse või võidakse hakata tulevikus kohaldama sektoripõhiseid liidu õigusakte, mis sisaldavad võrgu- ja infosüsteemide turvalisusega seotud eeskirju. Kui liidu õigusaktid sisaldavad sätteid, millega kehtestatakse võrgu- ja infosüsteemide turvalisust või intsidentidest teatamist käsitlevad nõuded, tuleks kohaldada neid sätteid, kui need sisaldavad nõudeid, mis on toimelt vähemalt samaväärsed käesolevas direktiivis sisalduvate kohustustega. Liikmesriigid peaksid seega kohaldama sektoripõhiste liidu õigusaktide sätteid, sealhulgas jurisdiktsiooniga seotud sätteid, ning mitte rakendama oluliste teenuste operaatorite identifitseerimise protsessi, nagu on määratletud käesolevas direktiivis. Seoses sellega peaksid liikmesriigid teavitama komisjoni selliste eriõigusaktide kohaldamisest. Et teha kindlaks, kas sektoripõhistes liidu õigusaktides sisalduvad nõuded võrgu- ja infosüsteemide turvalisuse ja intsidentidest teatamise kohta on samaväärsed käesolevas direktiivis sisalduvate nõuetega, tuleks arvesse võtta üksnes asjakohaste liidu õigusaktide sätteid ja nende kohaldamist liikmesriikides.

(10) Veetranspordisektoris hõlmavad ettevõtjate, laevade, sadamarajatiste, sadamate ja laevaliiklusteenuste turvanõuded liidu õigusaktide kohaselt kõiki tegevusi, sealhulgas raadio- ja telekommunikatsioonisüsteeme, arvutisüsteeme ja -võrke. Osa kohustuslikest menetlustest puudutab kõigist intsidentidest teatamist ja seetõttu tuleks neid käsitada eriõigusaktina, niivõrd kui nimetatud nõuded on vähemalt samaväärsed käesoleva direktiivi vastavate sätetega.

([1]) Euroopa Parlamendi ja nõukogu 7. märtsi 2002. aasta direktiiv 2002/21/EÜ elektrooniliste sidevõrkude ja -teenuste ühise reguleeriva raamistiku kohta (raamdirektiiv) (EÜT L 108, 24.4.2002, lk 33).

([2]) Euroopa Parlamendi ja nõukogu 23. juuli 2014. aasta määrus (EL) nr 910/2014 e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93/EÜ (ELT L 257, 28.8.2014, lk 73).

([3]) Nõukogu 23. septembri 2013. aasta otsus 2013/488/EL ELi salastatud teabe kaitseks vajalike julgeolekueeskirjade kohta (ELT L 274, 15.10.2013, lk 1).

(11) Veetranspordisektori operaatorite identifitseerimisel peaksid liikmesriigid arvesse võtma olemasolevaid ja tulevasi, eelkõige Rahvusvahelise Mereorganisatsiooni poolt välja töötatud rahvusvahelisi eeskirju ja suuniseid, et iga meretranspordiettevõtja saaks kasutada ühtset lähenemisviisi.

(12) Panganduse ja finantsturutaristute puhul on regulatsioon ja järelevalve liidu tasandil äärmiselt ühtlustatud liidu esmase ja teisese õiguse ning koos Euroopa järelevalveasutustega välja töötatud normide abil. Pangandusliidus on kõnealuste nõuete kohaldamine ja nende täitmise järelevalve tagatud ühtse järelevalvemehhanismi abil. Pangandusliitu mittekuuluvate liikmesriikide puhul tagatakse see vastavate liikmesriikide pangandust reguleerivate asutuste poolt. Finantssektori muudes reguleerimisvaldkondades tagab Euroopa Finantsjärelevalve Süsteem järelevalvetavade ühtsuse ja lähendamise. Euroopa Väärtpaberiturujärelevalve teostab samuti otsest järelevalvet ka teatavate üksuste (reitinguagentuurid ja kauplemisteabehoidlad) üle.

(13) Panganduse ja finantsturutaristute sektori puhul on usaldatavusnõuete järgimise ja järelevalve oluliseks osaks operatsioonirisk. See hõlmab kõiki operatsioone, sealhulgas võrgu- ja infosüsteemide turvalisust, terviklikkust ja vastupidavust. Nimetatud süsteemide suhtes kohaldatavad nõuded, mis on sageli rangemad käesoleva direktiivi nõuetest, on sätestatud mitmes liidu õigusaktis, sealhulgas eeskirjades, mis käsitlevad krediidiasutuste tegevuse alustamise tingimusi ning krediidiasutuste ja investeerimisühingute usaldatavusnõuete täitmise järelevalvet ning eeskirjades krediidiasutuste ja investeerimisühingute suhtes kohaldatavate usaldatavusnõuete kohta, mis sisaldavad operatsiooniriski nõudeid; eeskirjades finantsinstrumentide turgude kohta, mis sisaldavad investeerimisühingute ja reguleeritud turgude riskihindamise nõudeid; eeskirjades börsiväliste tuletisinstrumentide, kesksete vastaspoolte ja kauplemisteabehoidlate kohta, mis sisaldavad kesksete vastaspoolte ja kauplemisteabehoidlate operatsiooniriski nõudeid, ning väärtpaberiarvelduse parandamist liidus ja väärtpaberite keskdepositooriume käsitlevates eeskirjades, mis sisaldavad operatsiooniriski nõudeid. Samuti on intsidentidest teatamise nõuded osa finantssektori tavapärasest järelevalvetavast ning need lisatakse sageli järelevalve käsiraamatutesse. Liikmesriigid peaksid nimetatud eeskirju ja nõudeid arvesse võtma eriõigusaktide kohaldamisel.

(14) Nagu Euroopa Keskpank oma 25. juuli 2014. aasta arvamuses ([1]) märkis, ei mõjuta käesolev direktiiv liidu õiguse kohast eurosüsteemi makse- ja arveldussüsteemi järelevalve korda. Järelevalve eest vastutavatel asutustel oleks asjakohane vahetada võrgu- ja infosüsteemide turvalisuse alaseid kogemusi käesoleva direktiivi kohaselt pädevate asutustega. Sama kehtib Euroopa Keskpankade Süsteemi eurotsooni mittekuuluvate liikmete kohta, kes teostavad makse- ja arveldussüsteemi järelevalvet siseriiklike õigus- ja haldusnormide kohaselt.

(15) Internetipõhine kauplemiskoht võimaldab tarbijatel ja kauplejatel sõlmida kauplejatega internetipõhiseid müügi- või teenuse osutamise lepinguid ning see on selliste lepingute sõlmimise lõplik sihtkoht. See ei peaks hõlmama internetipõhiseid teenuseid, mille abil üksnes vahendatakse kolmandate isikute teenuseid ja mille abil saab lõpuks lepingu sõlmida. Seetõttu ei peaks see hõlmama internetipõhiseid teenuseid, mis võrdlevad erinevate kauplejate konkreetsete toodete või teenuste hinda ning suunavad kasutaja seejärel eelistatud kaupleja juurde toodet ostma. Internetipõhise kauplemiskoha pakutavad andmetöötlusteenused võivad hõlmata tehingute töötlemist, andmete koondamist või kasutajate profiilianalüüsi. Tarkvarapoode, mis tegutsevad kolmandate isikute loodud rakenduste või tarkvaraprogrammide digitaalset levitamist võimaldavate veebipoodidena, tuleks käsitada internetipõhise kauplemiskoha ühe liigina.

(16) Internetipõhine otsingumootor võimaldab kasutajal teha mis tahes teemal esitatud päringu alusel otsinguid üldiselt kõikidel veebisaitidel. Teise võimalusena võib otsingumootor keskenduda mõnes kindlas keeles veebisaitidele. Käesolevas direktiivis esitatud internetipõhise otsingumootori määratlus ei peaks hõlmama teatavaid otsingufunktsioone, mis piirduvad konkreetse veebisaidi sisuga, olenemata sellest, kas otsingufunktsiooni võimaldab väline otsingumootor. Samuti ei peaks see hõlmama internetipõhiseid teenuseid, mis võrdlevad erinevate kauplejate konkreetsete toodete või teenuste hinda ning suunavad kasutaja seejärel eelistatud kaupleja juurde toodet ostma.

(17) Pilvandmetöötlusteenused hõlmavad suurt hulka toiminguid, mida saab pakkuda erinevate mudelite kohaselt. Käesolevas direktiivis tähendab mõiste „pilvandmetöötlusteenus“ teenust, mis võimaldab juurdepääsu jagatavate andmetöötlusressursside skaleeritavale ja paindlikule kogumile. Andmetöötlusressursid hõlmavad selliseid ressursse nagu võrgud, serverid või muu taristu, hoidlad, rakendused ja teenused. Mõiste „skaleeritav“ osutab andmetöötlusressurssidele, mis on nõudluse kõikumisega toimetulekuks pilveteenuse osutaja poolt paindlikult jaotatud, olenemata ressursside geograafilisest asukohast. Mõistet „paindlik kogum“ kasutatakse selliste andmetöötlusressursside kirjeldamiseks, mida pakutakse ja mis tehakse kättesaadavaks vastavalt nõudlusele, et kiiresti

([1]) ELT C 352, 7.10.2014, lk 4.

suurendada või vähendada kättesaadavaid ressursse vastavalt töökoormusele. Mõistet „jagatav“ kasutatakse selliste andmetöötlusressursside kirjeldamiseks, mida pakutakse paljudele kasutajatele, kellel on ühine juurdepääs teenusele, kuid andmete töötlemine toimub eraldi iga kasutaja jaoks, kuigi teenust osutatakse samade elektrooniliste seadmete abil.

(18) Interneti vahetuspunkti (IXP, *Internet Exchange Point*) ülesanne on võrkude omavaheline ühendamine. IXP ei paku juurdepääsu võrgule ega toimi transiiditeenuse osutaja ega edastajana. Samuti ei osuta IXP muid teenuseid, mis ei seondu võrkude ühendamisega, kuigi see ei välista võimalust, et IXP operaator osutab ka võrkude ühendamisega mitteseotud teenuseid. IXP on olemas selleks, et ühendada omavahel tehniliselt ja organisatsiooniliselt eraldiseisvaid võrke. Tehniliselt eraldiseisva võrgu kirjeldamiseks kasutatakse mõistet „autonoomne süsteem“.

(19) Liikmesriikide ülesandeks peaks olema määrata kindlaks, millised üksused vastavad oluliste teenuste operaatori määratluse kriteeriumitele. Järjepideva lähenemisviisi tagamiseks peaksid kõik liikmesriigid kohaldama oluliste teenuste operaatori määratlust ühetaoliselt. Sel eesmärgil on käesoleva direktiiviga ette nähtud konkreetsetes sektorites ja allsektorites tegutsevate üksuste hindamine, oluliste teenuste loetelu kehtestamine, ühise sektoriteüleste tegurite loetelu kaalumine, et teha kindlaks, kas potentsiaalsel intsidendil on oluline häiriv mõju, asjaomaseid liikmesriike hõlmav konsulteerimisprotsess üksuste puhul, kes osutavad teenuseid mitmes liikmesriigis, ning koostöörühma toetamine identifitseerimisprotsessis. Selleks et tagada võimalike turumuutuste täpne kajastamine, peaksid liikmesriigid identifitseeritud operaatorite loetelu regulaarselt läbi vaatama ja vajaduse korral seda ajakohastama. Liikmesriigid peaksid esitama komisjonile teabe, mis on vajalik selle hindamiseks, mil määral selline ühine metoodika on võimaldanud liikmesriikidel kõnealuse määratluse järjepidevat kohaldamist.

(20) Oluliste teenuste operaatorite identifitseerimise protsessi käigus peaksid liikmesriigid vähemalt iga käesolevas direktiivis osutatud allsektori puhul hindama, milliseid teenuseid tuleb pidada elutähtsa ühiskondliku ja majandustegevuse säilitamise seisukohast olulisteks, ning seda, kas üksused, kes käesolevas direktiivis osutatud sektorites ja allsektorites kõnealuseid teenuseid osutavad, vastavad operaatorite identifitseerimise kriteeriumitele. Hindamaks seda, kas üksus osutab teenust, mis on oluline elutähtsa ühiskondliku või majandustegevuse säilitamise seisukohast, on piisav uurida, kas konkreetne üksus osutab teenuste loetelus sisalduvat teenust. Lisaks sellele tuleks näidata, et olulise teenuse osutamine sõltub võrgu- ja infosüsteemidest. Hindamaks seda, kas intsidendil oleks oluliselt häiriv mõju teenuste osutamisele, peaksid liikmesriigid võtma arvesse mitmeid sektoriüleseid tegureid, samuti sektoripõhiseid tegureid, kui see on asjakohane.

(21) Oluliste teenuste operaatorite identifitseerimisel eeldab tegevuskoht liikmesriigis tegelikku ja tulemuslikku tegutsemist ning stabiilset tegevuskorraldust. Tegevuse õiguslik vorm (kas filiaali või juriidilisest isikust tütarettevõtja kaudu) ei ole selles osas määrav.

(22) On võimalik, et käesolevas direktiivis osutatud sektorites ja allsektorites tegutsevad üksused osutavad nii olulisi kui ka mitteolulisi teenuseid. Näiteks lennutranspordi sektoris võivad lennujaamad osutada teenuseid, mida liikmesriik võib pidada olulisteks (näiteks lennuradade haldamine), kuid ka mitmesuguseid teenuseid, mida võib pidada mitteolulisteks (näiteks ostualade pakkumine). Oluliste teenuste operaatorite suhtes tuleks kohaldada konkreetseid turvanõudeid üksnes seoses nende teenustega, mida peetakse olulisteks. Operaatorite identifitseerimiseks peaksid liikmesriigid seetõttu kehtestama oluliseks peetavate teenuste loetelu.

(23) Teenuste loetelu peaks sisaldama kõiki liikmesriigi territooriumil osutatavaid teenuseid, mis vastavad käesoleva direktiivi nõuetele. Liikmesriikidel peaks olema võimalik täiendada olemasolevat loetelu uute teenuste lisamisega. Teenuste loetelu peaks olema liikmesriikidele lähtealuseks, mis võimaldab oluliste teenuste operaatorite identifitseerimist. Selle eesmärk on teha kindlaks oluliste teenuste liigid käesolevas määruses osutatud sektorites, eristades neid mitteolulistest tegevustest, millega asjaomases sektoris tegutsev üksus võib tegeleda. Liikmesriikide kehtestatud teenuste loetelud oleksid täiendav alus kõikide liikmesriikide reguleerimistavade hindamiseks, pidades silmas identifitseerimisprotsessi järjepidevuse üldise taseme tagamist liikmesriikides.

(24) Kui üksus osutab olulist teenust kahes või enamas liikmesriigis, siis peaksid asjaomased liikmesriigid identifitseerimisprotsessi eesmärgil pidama omavahel kahe- või mitmepoolseid arutelusid. Arutelude korraldamine peaks aitama neil hinnata operaatori tähtsust piiriülese mõju seisukohast ning võimaldama igal asjaomasel liikmesriigil esitada oma seisukohad operaatori osutatavate teenustega seotud riskide kohta. Asjaomased liikmesriigid peaksid selle protsessi käigus üksteise seisukohti arvesse võtma ja neil peaks seejuures olema võimalik paluda abi koostöörühmalt.

(25) Identifitseerimisprotsessi tulemusel peaksid liikmesriigid võtma vastu siseriiklikud meetmed, et määrata kindlaks, milliste üksuste suhtes kehtivad võrgu- ja infosüsteemide turvalisuse alased kohustused. Nimetatud tulemuse saavutamiseks võib vastu võtta kõigi olulisi teenuseid osutavate operaatorite loetelu või võtta vastu siseriiklikud meetmed, mis sisaldavad objektiivseid kvantifitseeritavaid kriteeriume (nt operaatori tootmismaht või kasutajate arv), mis võimaldavad kindlaks määrata üksused, mille suhtes kohaldatakse võrgu- ja infosüsteemide turvalisuse alaseid kohustusi ja mille suhtes mitte. Olemasolevad või käesoleva määruse raames vastu võetud siseriiklikud meetmed peaksid hõlmama kõiki õiguslikke meetmeid, haldusmeetmeid ja poliitikaid, mis võimaldavad oluliste teenuste operaatorite identifitseerimist vastavalt käesolevale direktiivile.

(26) Selleks et näidata oluliste teenuste identifitseeritud operaatori tähtsust asjaomases sektoris, peaksid liikmesriigid arvesse võtma nende operaatorite arvu ja suurust (näiteks turuosa või tootmismaht) ilma kohustuseta esitada teavet, mis avalikustaks identifitseeritud operaatorid.

(27) Selleks et teha kindlaks, kas intsidendil oleks oluline häiriv mõju teenuse osutamisele, peaksid liikmesriigid arvesse võtma paljusid erinevaid tegureid, nagu asjaomasest teenusest era- või kutsealasel eesmärgil sõltuvate kasutajate arvu. Kõnealuse teenuse kasutamine võib toimuda otse, kaudselt või vahendaja kaudu. Hinnates intsidendi võimalikku mõju (raskusaste ja kestus) ühiskondlikule ja majandustegevusele või avalikule julgeolekule, peaksid liikmesriigid hindama ka seda, kui palju kulub tõenäoliselt aega, enne kui teenuse katkemine hakkaks avaldama negatiivset mõju.

(28) Selleks et teha kindlaks, kas intsidendil oleks oluline häiriv mõju teenuse osutamisele, tuleks lisaks sektoriülestele teguritele arvesse võtta ka sektoripõhiseid tegureid. Energiatarnijate puhul võiksid sellised tegurid hõlmata mahtu või osakaalu liikmesriigi energiatootmises; naftatarnijate puhul päevast tarnemahtu; lennutranspordi, sealhulgas lennuväljade ja lennuettevõtjate, raudteetranspordi ja meresadamate puhul nende osakaalu riigi liiklusmahus ja reisijate või kaubavedude arvu aastas; panganduse ja finantsturgude taristu puhul nende süsteemset tähtsust koguvarade või koguvarade ja SKP suhtarvu alusel; tervishoiusektori puhul teenuseosutaja hoole all olevate patsientide arvu aastas; veetootmis-, -töötlemis- ja -varustusettevõtete puhul mahtu ning kasutajate arvu ja liiki, sealhulgas näiteks haiglad, avalikud teenused, organisatsioonid või üksikisikud ning alternatiivsete veeallikate olemasolu samas geograafilises piirkonnas.

(29) Selleks et saavutada võrgu- ja infosüsteemide turvalisuse kõrge tase ja see säilitada, peaks igal liikmesriigil olema riiklik võrgu- ja infosüsteemide turvalisuse strateegia, milles oleks määratletud strateegilised eesmärgid ja konkreetsed poliitilised meetmed, mida rakendada.

(30) Arvestades riikide juhtimisstruktuuride erinevusi ning selleks, et kaitsta juba kehtivat valdkondlikku korda või liidu reguleerivaid ja järelevalveasutusi ning et vältida dubleerimist, peaksid liikmesriigid saama käesoleva direktiivi alusel nimetada oluliste teenuste operaatorite ja digitaalse teenuse osutajate võrgu- ja infosüsteemide turvalisusega seotud ülesannete täitmiseks rohkem kui ühe riikliku pädeva asutuse.

(31) Piiriülese koostöö ja suhtluse hõlbustamiseks ja käesoleva direktiivi kohaselt vastu võetud sätete tõhusaks rakendamiseks on vaja, et iga liikmesriik nimetaks ühe riikliku ühtse kontaktpunkti, kes vastutab võrgu- ja infosüsteemide turvalisuse alaste küsimuste koordineerimise ning liidu tasandi piiriülese koostöö eest. Pädevatele asutustele ja ühtsele kontaktpunktile tuleks anda piisavad tehnilised, rahalised ja inimressursid, mis võimaldaksid neile määratud ülesandeid tulemuslikult ja tõhusalt täita ning seeläbi saavutada käesoleva direktiivi eesmärgid. Kuna käesoleva direktiivi eesmärk on parandada siseturu toimimist usalduse ja kindlustunde suurendamise kaudu, siis peaksid liikmesriikide asutused suutma teha tõhusat koostööd majandustegevuses osalejatega ning neil peaks olema vastav struktuur.

(32) Pädevad asutused või küberturbe intsidentide lahendamise üksused (CSIRTid, *computer security incident response teams*) peaksid saama teateid intsidentide toimumisest. Intsidentide teateid ei tuleks edastada otse ühtsetele kontaktpunktidele, välja arvatud juhul, kui need toimivad ühtlasi ka pädeva asutuse või CSIRTina. Pädev asutus või CSIRT peaks saama teha ühtsele kontaktpunktile ülesandeks edastada intsidentide teated teiste mõjutatud liikmesriikide ühtsetele kontaktpunktidele.

(33) Liikmesriikide ja komisjoni tõhusa teavitamise tagamiseks peaks ühtse kontaktpunkti poolt koostöörühmale esitatav koondaruanne olema muudetud anonüümseks, et säilitada teadete ja oluliste teenuste operaatorite ja digitaalse teenuse osutajate konfidentsiaalsust, sest parimate tavade vahetamiseks koostöörühmas ei ole andmed teavitajate identiteedi kohta vajalikud. Koondaruanne peaks sisaldama andmeid saadud teadete arvu ning teatatud intsidentide laadi kohta, näiteks turvarikkumise liik, raskusaste või kestus.

(34) Liikmesriigid peaksid olema nii tehniliselt kui ka töökorralduse mõttes piisavalt varustatud, et vältida ja avastada võrgu- ja infosüsteemidega seotud intsidente ja riske ning neile reageerida ja nende mõju leevendada. Liikmesriigid peaksid seetõttu tagama, et neil oleks hästi toimivad ja olulistele nõuetele vastavad CSIRTid, mida tuntakse ka infoturbeintsidentidega tegelevate rühmadena (CERT), et tagada tulemuslik ja ühilduv suutlikkus tulla toime intsidentide ja riskidega ning tagada liidu tasandil tõhus koostöö. Selleks et igat liiki oluliste teenuste operaatorid ja digitaalse teenuse osutajad sellisest suutlikkusest ja koostööst kasu saaksid, peaksid liikmesriigid tagama, et kõigi liikide jaoks oleks kindlaks määratud vastav CSIRT. Arvestades küberturbealase rahvusvahelise koostöö tähtsust, peaks CSIRTidel olema võimalik lisaks käesoleva direktiivi kohaselt loodud CSIRTide võrgustikule osaleda ka rahvusvahelistes koostöövõrgustikes.

(35) Enamik võrgu- ja infosüsteemide operaatoreid on eraettevõtjad ning seepärast on avaliku ja erasektori koostöö hädavajalik. Tuleks soodustada oluliste teenuste operaatorite ja digitaalse teenuse osutajate endi mitteametlikke koostöömehhanisme võrgu- ja infosüsteemide turvalisuse tagamiseks. Koostöörühmal peaks vajaduse korral olema võimalus kutsuda aruteludes osalema asjaomaseid sidusrühmi. Selleks et soodustada tulemuslikult teabe ja parimate tavade vahetamist, on tähtis tagada, et teabevahetuses osalevad oluliste teenuste operaatorid ja digitaalse teenuse osutajad ei oleks oma koostöö tõttu ebasoodsamas olukorras.

(36) ENISA peaks liikmesriike ja komisjoni abistama, pakkudes neile oma teadmisi ja andes nõu ning toetades parimate tavade vahetamist. Eelkõige peaksid komisjon ja liikmesriigid saama ENISAga konsulteerida käesoleva direktiivi kohaldamise üle. Liikmesriikide suutlikkuse ja teadmiste parandamise huvides peaks koostöörühm pakkuma võimalusi ka parimate tavade vahetamiseks, liikmesriikide suutlikkuse ja valmisoleku alasteks aruteludeks ning vabatahtlikkuse põhimõttel aitama oma liikmetel hinnata riiklikke võrgu- ja infosüsteemide turvalisuse strateegiaid, suurendada suutlikkust ning hinnata võrgu- ja infosüsteemide turvalisusega seotud õppusi.

(37) Võimaluse korral peaks liikmesriigid saama käesoleva direktiivi kohaldamisel kasutada või kohandada olemasolevat organisatsioonilist struktuuri või olemasolevaid strateegiaid.

(38) Koostöörühma ja ENISA vastavad ülesanded on vastastikku sõltuvad ja üksteist täiendavad. Üldiselt peaks ENISA abistama koostöörühma tema ülesannete täitmisel kooskõlas Euroopa Parlamendi ja nõukogu määruses (EL) nr 526/2013 ([1]) sätestatud ENISA eesmärgiga aidata liidu institutsioonidel, organitel, asutustel ja ametitel ning liikmesriikidel ellu viia olemasolevate ja tulevaste liidu õigusaktide võrgu- ja infosüsteemide turvanõuetele vastavat poliitikat. Eelkõige peaks ENISA pakkuma abi valdkondades, mis vastavad tema enda ülesannetele, mis on sätestatud määruses (EL) nr 526/2013, nimelt analüüsida võrgu- ja infosüsteemide turvalisuse strateegiaid, toetada liidu võrgu- ja infosüsteemide turvalisusega seotud õppuste korraldamist ja läbiviimist ning teabevahetust ja parimaid tavasid teadlikkuse suurendamise ja koolituse alal. ENISA peaks samuti osalema sektoripõhiste kriteeriumide alaste suuniste väljatöötamises, mida kasutatakse intsidendi mõju olulisuse kindlaks tegemiseks.

([1]) Euroopa Parlamendi ja nõukogu 21. mai 2013. aasta määrus (EL) nr 526/2013, mis käsitleb Euroopa Liidu Võrgu- ja Infoturbeametit (ENISA) ning millega tunnistatakse kehtetuks määrus (EÜ) nr 460/2004 (ELT L 165, 18.6.2013, lk 41).

(39) Selleks et edendada paremat võrgu- ja infosüsteemide turvalisust, peaks koostöörühm tegema asjakohastel juhtudel koostööd asjaomaste liidu institutsioonide, organite, asutuste ja ametitega, et vahetada oskusteavet ja parimaid tavasid ning anda nõu selliste võrgu- ja infosüsteemide turvalisuse aspektide kohta, mis võivad mõjutada nende tööd, järgides samas piiratud juurdepääsuga teabe vahetamise suhtes kehtivat korda. Õiguskaitseasutustega koostöö tegemisel võrgu- ja infosüsteemide turvalisuse küsimustes, mis võivad nende tööd mõjutada, peaks koostöörühm arvestama olemasolevate teabekanalite ja rajatud võrgustikega.

(40) Teave intsidentide kohta on üha väärtuslikum üldsuse ja ettevõtjate, eelkõige väikeste ja keskmise suurusega ettevõtjate jaoks. Mõningatel juhtudel esitatakse sellist teavet juba riiklikul tasandil veebisaitide kaudu, konkreetse riigi keeles ja keskendudes peamiselt riikliku ulatusega intsidentidele ja juhtumitele. Arvestades seda, et ettevõtjad tegutsevad üha rohkem piiriüleselt ja kodanikud kasutavad internetipõhiseid teenuseid, tuleks intsidente puudutav teave esitada koondkujul liidu tasandil. CSIRTide võrgustiku sekretariaati julgustatakse looma veebisaiti või pakkuma mõnel olemasoleval veebisaidil erilehekülge, millel esitatakse üldsusele üldist teavet intsidentide kohta kogu liidus, keskendudes eelkõige ettevõtjate huvidele ja vajadustele. CSIRTide võrgustikus osalevaid CSIRTe julgustatakse esitama vabatahtlikult teavet sellisel veebisaidil avaldamiseks, ilma et seal avaldataks konfidentsiaalset või tundlikku teavet.

(41) Kui teavet peetakse konfidentsiaalseks vastavalt liidu ja liikmesriikide ärisaladust käsitlevatele eeskirjadele, tuleks käesolevas direktiivis sätestatud toimingute tegemisel ja direktiivi eesmärkide täitmisel tagada konfidentsiaalsus.

(42) Liikmesriikide võrgu- ja infosüsteemide turvalisuse alase valmisoleku ja koostöö katsetamiseks on olulised küberjulgeolekuõppused, millel simuleeritakse reaalajas toimuvate intsidentide stsenaariume. ENISA poolt koordineeritavad ja liikmesriikide osalusel toimuvad tsükli CyberEurope õppused on kasulikuks vahendiks, mille abil testida ja koostada soovitusi selle kohta, kuidas tuleks intsidentidele reageerimist liidu tasandil aja jooksul parandada. Kuna praegu ei ole liikmesriigid kohustatud ei õppusi kavandama ega neil osalema, siis peaks CSIRTide võrgustiku loomine vastavalt käesolevale direktiivile võimaldama liikmesriikidel õppustel osalemist täpsete kavade ja strateegiliste valikute alusel. Käesoleva direktiivi alusel loodud koostöörühm peaks arutama õppusi puudutavaid strateegilisi otsuseid, eelkõige, kuid mitte ainult, õppuste regulaarset korraldamist ja stsenaariumide koostamist. ENISA peaks vastavalt oma mandaadile toetama üleliiduliste õppuste korraldamist ja läbiviimist, pakkudes oma teadmisi ja nõuandeid koostöörühmale ja CSIRTide võrgustikule.

(43) Arvestades võrgu- ja infosüsteemide turvalisusega seotud probleemide globaalsust, on vaja teha tihedamat rahvusvahelist koostööd, et parandada turbestandardeid ja teabevahetust ning edendada ühtset üleilmselt lähenemist turvalisuse küsimustele.

(44) Vastutus võrgu- ja infosüsteemide turvalisuse tagamise eest lasub suuresti oluliste teenuste operaatoritel ja digitaalse teenuse osutajatel. Asjakohaste regulatiivsete nõuete ja asjaomase valdkonna vabatahtlike tegutsemisviiside kaudu tuleks levitada ja arendada riskihalduskultuuri, mis hõlmaks riskihindamist ja riskist lähtuvalt asjakohaste turvameetmete rakendamist. Samuti on oluline kehtestada usaldusväärsed võrdsed tingimused, et koostöörühm ja CSIRTide võrgustik saaks tulemuslikult toimida ja et tagatud oleks kõigi liikmesriikide tulemuslik koostöö.

(45) Käesolevat direktiivi kohaldatakse üksnes selliste ametiasutuste suhtes, mis on identifitseeritud oluliste teenuste operaatoritena. Liikmesriikide ülesanne on tagada käesoleva direktiivi kohaldamisalast välja jäävate ametiasutuste võrgu- ja infosüsteemide turvalisus.

(46) Riskihaldamismeetmed hõlmavad meetmeid igasuguste intsidendiriskide kindlakstegemiseks, riskide vältimise, avastamise ja käsitlemise ning riskide mõju leevendamise meetmeid. Võrgu- ja infosüsteemide turvalisus hõlmab salvestatud, edastatud ja töödeldud andmete turvalisust.

(47) Pädevatel asutustel peaks olema võimalik võtta vastu riiklikke suuniseid selle kohta, milliste asjaolude puhul nõutakse oluliste teenuste operaatoritelt intsidentidest teatamist.

(48) Paljud liidu ettevõtjad sõltuvad teenuste osutamisel digitaalse teenuse osutajatest. Kuna mõned digitaalsed teenused võivad olla nende kasutajate, sealhulgas oluliste teenuste operaatorite jaoks tähtis ressurss ning kuna sellistel kasutajatel ei pruugi alati olla alternatiivseid võimalusi, siis tuleks käesolevat direktiivi kohaldada ka selliste teenuste osutajate suhtes. Käesolevas direktiivis osutatud digitaalsete teenuste liigi turvalisus, pidevus ja töökindlus on oluline paljude ettevõtjate ladusaks tegevuseks. Mõne kõnealuse digitaalse teenuse katkemine võiks takistada sellest sõltuvate muude teenuste osutamist ning avaldada seega mõju olulisele ühiskondlikule ja majandustegevusele liidus. Seetõttu võib sellistel digitaalsetel teenustel olla otsustav tähtsus neist sõltuvate ettevõtjate ladusa tegevuse jaoks ning samuti kõnealuste ettevõtjate siseturul ja piiriüleses kaubanduses osalemise jaoks kogu liidus. Käesoleva direktiivi kohaldamisalasse kuuluvad digitaalse teenuse osutajad on sellised teenuseosutajad, kes osutavad digitaalseid teenuseid, millest paljud liidu ettevõtjad üha enam sõltuvad.

(49) Digitaalse teenuse osutajad peaksid tagama turvalisuse taseme, mis on võrdväärne nende osutatavate digitaalsete teenuste turvalisust ohustava riski suurusega, arvestades nende teenuste tähtsust muude ettevõtjate tegevuse jaoks liidus. Digitaalse teenuse osutajatega võrreldes on praktikas risk suurem oluliste teenuste operaatorite puhul, kes on sageli olulised elutähtsa ühiskondliku ja majandustegevuse säilitamise seisukohast. Seetõttu peaks digitaalse teenuse osutajate turvanõuded olema leebemad. Digitaalse teenuse osutajatel peaks olema õigus vabalt otsustada, milliseid meetmeid nad peavad asjakohaseks oma võrgu- ja infosüsteemide turvalisust ohustavate riskide haldamiseks. Digitaalse teenuse osutajate piiriülese olemuse tõttu tuleks nende suhtes kohaldada liidu tasandil ühtsemat lähenemisviisi. Rakendusaktidega tuleks hõlbustada selliste meetmete täpsustamist ja rakendamist.

(50) Kuigi riistvaratootjad ja tarkvaraarendajad ei ole oluliste teenuste operaatorite või digitaalse teenuse osutajatega võrreldavad ettevõtjad, suurendavad nende tooted võrgu- ja infosüsteemide turvalisust. Seetõttu on neil tähtis roll oluliste teenuste operaatorite ja digitaalse teenuse osutajate toetamisel oma võrgu- ja infosüsteemide turvalisuse tagamisel. Kõnealuste riist- ja tarkvaratoodete suhtes juba kohaldatakse kehtivaid tootjavastutuse eeskirju.

(51) Oluliste teenuste operaatorite ja digitaalse teenuse osutajate suhtes kehtestatud tehnilised ja korralduslikud meetmed ei tohiks tähendada, et konkreetset turustatavat info- ja kommunikatsioonitehnoloogilist toodet tuleks projekteerida, arendada või toota konkreetsel viisil.

(52) Oluliste teenuste operaatorid ja digitaalse teenuse osutajad peaksid tagama nende kasutatava võrgu- ja infosüsteemide turvalisuse. Eelkõige on tegemist eravõrgu ja erainfosüsteemidega, mida haldavad kas asutuse enda IT-töötajad või mille turvalisusega seotud teenused ostetakse sisse. Turvalisuse ja intsidentidest teatamisega seotud nõudeid tuleks asjaomaste oluliste teenuste operaatorite ja digitaalse teenuse osutajate suhtes kohaldada olenemata sellest, kas nad hooldavad oma võrgu- ja infosüsteeme ise või ostavad selle teenuse sisse.

(53) Vältimaks oluliste teenuste operaatorite ja digitaalse teenuse osutajate ebaproportsionaalset finants- ja halduskoormust, peaksid nõuded olema proportsionaalsed asjaomase võrgu- ja infosüsteemi puhul esineva riskiga, võttes seejuures arvesse selliste meetmete kõrget tehnilist taset. Digitaalse teenuse osutajate puhul ei tuleks neid nõudeid kohaldada mikro- ja väikeste ettevõtjate suhtes.

(54) Kui liikmesriikide ametiasutused kasutavad digitaalse teenuse osutajate pakutavaid teenuseid, eelkõige pilvandmetöötlusteenuseid, võivad nad soovida teenuste osutajatelt täiendavaid turvameetmeid lisaks digitaalse teenuse osutajate poolt käesoleva direktiivi nõuete kohaselt tavapäraselt pakutavatele. Nad peaksid saama seda nõuda lepinguliste kohustuste abil.

(55) Käesolevas direktiivis esinevaid internetipõhise kauplemiskoha, internetipõhise otsingumootori ja pilvandmetöötlusteenuse määratlusi kasutatakse üksnes käesoleva direktiivi kohaldamise eesmärgil ning see ei piira nende mõistete määratlemist muudes õigusaktides.

(56) Käesolev direktiiv ei tohiks takistada liikmesriikidel võtta vastu siseriiklikke meetmeid, millega kohustatakse avaliku sektori asutusi tagama konkreetseid turvanõudeid pilvandmetöötlusteenuste lepingute puhul. Selliseid siseriiklikke meetmeid tuleks kohaldada avaliku sektori asjaomase asutuse, mitte pilvandmetöötlusteenuse osutaja suhtes.

(57) Arvestades põhimõttelisi erinevusi, mis esinevad oluliste teenuste operaatorite (eelkõige nende otsene seotus füüsilise taristuga) ja digitaalse teenuse osutajate (eelkõige nende piiriülene olemus) vahel, tuleks nimetatud kahe rühma suhtes esitatavate nõuete ühtlustamise puhul kasutada käesolevas direktiivis diferentseeritud lähenemisviisi. Oluliste teenuste operaatorite puhul peaks liikmesriikidel olema võimalus identifitseerida asjaomased operaatorid ja kehtestada nende suhtes käesolevas direktiivis sätestatutest rangemad nõuded. Liikmesriigid ei peaks identifitseerima digitaalse teenuse osutajaid, sest käesolevat direktiivi tuleks kohaldada kõigi selle kohaldamisalasse kuuluvate digitaalse teenuse osutajate suhtes. Lisaks peaksid käesolev direktiiv ja selle alusel vastu võetud rakendusaktid tagama digitaalse teenuse osutajate suhtes kehtivate nõuete ühtlustamise kõrge taseme turvalisuse ja intsidentidest teatamise valdkonnas. See peaks võimaldama digitaalse teenuse osutajate ühetaolist kohtlemist kogu liidus proportsionaalselt nende olemusega ja võimaliku riski tasemega.

(58) Käesolev direktiiv ei tohiks takistada liikmesriikidel kehtestada turvalisuse ja intsidentidest teatamisega seotud nõudeid üksustele, mis ei ole käesoleva direktiivi kohaldamisalasse kuuluvad digitaalse teenuse osutajad, ilma et see mõjutaks liikmesriikide liidu õiguse kohaseid kohustusi.

(59) Pädevad asutused peaksid pöörama nõuetekohast tähelepanu mitteametlike ja usaldusväärsete infovahetuskanalite säilitamisele. Pädevatele asutustele teatatud intsidentide avalikustamisel tuleks seada tasakaalu üldsuse huvi saada ohtudest teada ning kahju, mida selline avalikustamine võib põhjustada intsidendist teatanud oluliste teenuste operaatorite ja digitaalse teenuse osutajate mainele ja kaubandustegevusele. Teatamiskohustuse rakendamisel peaksid pädevad asutused ja CSIRTid pöörama erilist tähelepanu sellele, et teave toote nõrkuste kohta jääks rangelt konfidentsiaalseks kuni asjakohase turvaparanduse avaldamiseni.

(60) Digitaalse teenuse osutajate suhtes tuleks kohaldada paindlikku ja reageerivat järgnevat järelevalvet, mis on nende teenuste ja tegevuse laadist tulenevalt põhjendatud. Seetõttu peaks asjaomane pädev asutus võtma meetmeid üksnes tõendite saamisel, näiteks digitaalse teenuse osutajalt endalt, teiselt pädevalt asutuselt, sealhulgas teise liikmesriigi pädevalt asutuselt, või teenuse kasutajalt selle kohta, et digitaalse teenuse osutaja ei järgi käesoleva direktiivi nõudeid, võttes meetmeid eelkõige pärast intsidendi toimumist. Seega ei peaks pädeval asutusel olema üldist kohustust teostada järelevalvet digitaalse teenuse osutajate üle.

(61) Pädevatel asutustel peaksid olema oma ülesannete täitmiseks vajalikud vahendid, sealhulgas õigus saada piisavat teavet võrgu- ja infosüsteemi turvalisuse taseme hindamiseks.

(62) Intsidendid võivad tuleneda kuritegevusest, mille ennetamist, uurimist ja mille eest vastutusele võtmist toetab oluliste teenuste operaatorite, digitaalse teenuse osutajate, pädevate asutuste ja õiguskaitseasutuste vaheline koordineerimine ja koostöö. Kui kahtlustatakse, et intsident on seotud liidu või liikmesriigi õiguses määratletud raske kuriteoga, peaksid liikmesriigid julgustama oluliste teenuste operaatoreid ja digitaalse teenuse osutajaid arvatavalt raske kuritegevusega seotud intsidentidest asjakohastele õiguskaitseasutustele teatama. Asjakohasel juhul on soovitav, et erinevate liikmesriikide pädevate asutuste ja õiguskaitseasutuste vahelist koordineerimist hõlbustaksid Euroopa küberkuritegevuse vastase võitluse keskus (EC3) ja ENISA.

(63) Sageli on intsidendi tagajärjeks isikuandmete kaitstuse rikkumine. Sellises olukorras peaksid pädevad asutused ja andmekaitseasutused omavahel koostööd tegema ja vahetama teavet kõigis asjaomastes küsimustes, et tulla toime intsidendi tagajärjel toimunud isikuandmetega seotud rikkumisega.

(64) Jurisdiktsioon digitaalse teenuse osutajate üle tuleks omistada liikmesriigile, kus on asjaomase digitaalse teenuse osutaja peamine tegevuskoht liidus, mis põhimõtteliselt tähendab riiki, kus paikneb teenuseosutaja peakontor liidus. Tegevuskoht eeldab tegelikku ja tulemuslikku tegutsemist ning stabiilset tegevuskorraldust. Tegevuse õiguslik vorm (kas filiaali või juriidilisest isikust tütarettevõtja kaudu) ei ole selles osas määrav. See kriteerium ei

tohiks sõltuda võrgu- ja infosüsteemide füüsilisest paiknemisest teatavas kohas; selliste süsteemide olemasolu ja kasutamine iseenesest ei tähenda peamist tegevuskohta ning ei ole seetõttu kriteeriumid, mille alusel teha kindlaks peamist tegevuskohta.

(65) Kui digitaalse teenuse osutaja, kelle asukoht ei ole liidus, osutab teenuseid liidu piires, peaks ta nimetama oma esindaja. Selgitamaks välja, kas digitaalse teenuse osutaja pakub teenuseid liidu piires, tuleks kindlaks teha, kas on ilmne, et digitaalse teenuse osutaja kavatseb osutada teenuseid ühes või mitmes liikmesriigis asuvatele isikutele. Kavatsuse kindlakstegemiseks ei piisa vaid sellest, et liidus on juurdepääs digitaalse teenuse osutaja või vahendaja veebisaidile, e-posti aadressile või muudele kontaktandmetele, samuti ei piisa digitaalse teenuse osutaja asukohariigiks oleva kolmanda riigi üldkasutatava keele kasutamisest. Digitaalse teenuse osutaja kavatsus pakkuda teenuseid liidu piires võib ilmneda sellistest asjaoludest nagu ühes või mitmes liikmesriigis üldiselt kasutatava keele või vääringu kasutamine koos võimalusega tellida teenuseid selles teises keeles või liidus paiknevate klientide või kasutajate nimetamine. Esindaja peaks tegutsema digitaalse teenuse osutaja nimel ning pädevatel asutustel või CSIRTil peaks olema võimalik esindajaga ühendust võtta. Digitaalse teenuse osutaja peaks kirjaliku volitusega sõnaselgelt määrama esindaja tema nimel tegutsema seoses käesoleva direktiivi kohaste kohustustega, sealhulgas intsidentidest teatamise kohustusega.

(66) Turvanõuete standardimine on turu poolt tingitud protsess. Selleks et tagada turvastandardite ühtne kohaldamine, peaksid liikmesriigid julgustama konkreetsete standardite järgimist ja vastavust neile, et tagada liidu tasandil võrgu- ja infosüsteemide turvalisuse kõrge tase. ENISA peaks abistama liikmesriike nõuannete ja suunistega. Sel eesmärgil võib abi olla ühtlustatud standardite koostamisest, mida tuleks teha kooskõlas Euroopa Parlamendi ja nõukogu määrusega (EL) nr 1025/2012 ([1]).

(67) Käesoleva direktiivi kohaldamisalast välja jäävates üksustes võib toimuda intsidente, millel on oluline mõju nende osutatavatele teenustele. Kui need üksused leiavad, et sellistest intsidentidest teatamine on avalikes huvides, siis peaks neil olema võimalik teha seda vabatahtlikult. Pädev asutus või CSIRT peaksid sellised teated läbi vaatama, kui selline läbivaatamine ei ole asjaomaste liikmesriikide jaoks ebaproportsionaalselt ega liigselt koormav.

(68) Selleks et tagada käesoleva direktiivi ühetaolised rakendamistingimused, tuleks komisjonile anda rakendamisvolitused, et määrata kindlaks koostöörühma toimimiseks vajalik menetluskord ja digitaalse teenuse osutajate suhtes kohaldatavad turva- ja teatamisnõuded. Neid volitusi tuleks teostada kooskõlas Euroopa Parlamendi ja nõukogu määrusega (EL) nr 182/2011 ([2]). Koostöörühma toimimiseks vajaliku menetluskorraga seotud rakendusaktide vastuvõtmisel peaks komisjon võimalikult suurel määral arvesse võtma ENISA arvamust.

(69) Digitaalse teenuse osutajate turvanõudeid käsitlevate rakendusaktide vastuvõtmisel peaks komisjon võimalikult suurel määral arvesse võtma ENISA arvamust ning konsulteerima huvitatud sidusrühmadega. Lisaks julgustatakse komisjoni arvesse võtma järgmisi aspekte: süsteemide ja rajatiste turvalisuse puhul: füüsiline ja keskkonnaga seotud turvalisus, tarnete turvalisus, võrgu- ja infosüsteemide juurdepääsu kontroll ning võrgu- ja infosüsteemide terviklus; intsidentide käsitlemise puhul: intsidentide käsitlemise kord, intsidentide avastamise suutlikkus, intsidentidest teatamine ja teavitamine; talitluspidevuse haldamise puhul: teenuse järjepidevuse strateegia ja hädaolukorra lahendamise kavad, avariitaastesuutlikkus, ning seire, auditeerimise ja testimise puhul: seire- ja logipoliitika, hädaolukorra lahendamise harjutuskavad, võrgu- ja infosüsteemide testimine, turvalisuse hindamine ja nõuetele vastavuse seire.

(70) Käesoleva direktiivi rakendamisel peaks komisjon pidama vastavalt asjakohast sidet asjaomaste valdkondlike komiteede ja asjaomaste organitega, mis on loodud liidu tasandil käesoleva direktiiviga hõlmatud valdkondades.

([1]) Euroopa Parlamendi ja nõukogu 25. oktoobri 2012. aasta määrus (EL) nr 1025/2012, mis käsitleb Euroopa standardimist ning millega muudetakse nõukogu direktiive 89/686/EMÜ ja 93/15/EMÜ ning Euroopa Parlamendi ja nõukogu direktiive 94/9/EÜ, 94/25/EÜ, 95/16/EÜ, 97/23/EÜ, 98/34/EÜ, 2004/22/EÜ, 2007/23/EÜ, 2009/23/EÜ ja 2009/105/EÜ ning millega tunnistatakse kehtetuks nõukogu otsus 87/95/EMÜ ning Euroopa Parlamendi ja nõukogu otsus nr 1673/2006/EÜ (ELT L 316, 14.11.2012, lk 12).

([2]) Euroopa Parlamendi ja nõukogu 16. veebruari 2011. aasta määrus (EL) nr 182/2011, millega kehtestatakse eeskirjad ja üldpõhimõtted, mis käsitlevad liikmesriikide läbiviidava kontrolli mehhanisme, mida kohaldatakse komisjoni rakendamisvolituste teostamise suhtes (ELT L 55, 28.2.2011, lk 13).

(71) Komisjon peaks huvitatud sidusrühmadega konsulteerides käesoleva direktiivi sätted regulaarselt läbi vaatama, eelkõige selleks, et teha kindlaks, kas neid on vaja muuta seoses ühiskondlike, poliitiliste, tehnoloogia ja turutingimuste muutumisega.

(72) Koostöörühmas ja CSIRTide võrgustikus riskide ja intsidentide kohta teabe jagamine ning intsidentidest riigi pädevatele asutustele või CSIRTidele teatamise nõude järgimine võib tingida isikuandmete töötlemist. Töötlemine peaks toimuma kooskõlas Euroopa Parlamendi ja nõukogu direktiiviga 95/46/EÜ ([1]) ning Euroopa Parlamendi ja nõukogu määrusega (EÜ) nr 45/2001 ([2]). Käesoleva direktiivi kohaldamisel tuleks asjakohasel juhul kohaldada Euroopa Parlamendi ja nõukogu määrust (EÜ) nr 1049/2001 ([3]).

(73) Euroopa Andmekaitseinspektoriga konsulteeriti vastavalt määruse (EÜ) nr 45/2001 artikli 28 lõikele 2 ning ta esitas oma arvamuse 14. juunil 2013 ([4]).

(74) Kuna käesoleva direktiivi eesmärki, nimelt võrgu- ja infosüsteemide turvalisuse kõrge taseme tagamist liidus, ei suuda liikmesriigid piisavalt saavutada, küll aga saab seda meetme toime tõttu paremini saavutada liidu tasandil, võib liit võtta meetmeid kooskõlas Euroopa Liidu lepingu artiklis 5 sätestatud subsidiaarsuse põhimõttega. Kõnealuses artiklis sätestatud proportsionaalsuse põhimõtte kohaselt ei lähe käesolev direktiiv nimetatud eesmärgi saavutamiseks vajalikust kaugemale.

(75) Käesolevas direktiivis järgitakse Euroopa Liidu põhiõiguste hartas tunnustatud põhiõigusi ja põhimõtteid, eelkõige õigust eraelu ja edastatavate sõnumite puutumatusele, isikuandmete kaitset, ettevõtlusvabadust, õigust omandile ning õigust tõhusale õiguskaitsevahendile kohtus ja õiglasele kohtulikule arutamisele. Käesolevat direktiivi tuleks rakendada kooskõlas nimetatud õiguste ja põhimõtetega,

ON VASTU VÕTNUD KÄESOLEVA DIREKTIIVI:

I PEATÜKK

ÜLDSÄTTED

Artikkel 1

Reguleerimisese ja kohaldamisala

1. Käesolevas direktiivis sätestatakse meetmed võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge taseme saavutamiseks liidus, parandades seeläbi siseturu toimimist.

2. Selle eesmärgi saavutamiseks tehakse käesoleva direktiiviga järgmist:

a) sätestatakse kõigile liikmesriikidele kohustus võtta vastu riiklik võrgu- ja infosüsteemide turvalisuse strateegia;

b) luuakse koostöörühm, mille eesmärk on toetada ja hõlbustada strateegilist koostööd ja teabevahetust ning luua usaldust ja kindlustunnet liikmesriikide vahel;

c) luuakse küberturbe intsidentide lahendamise üksuste võrgustik („CSIRTide võrgustik"), et aidata luua liikmesriikide vahel usaldust ja kindlustunnet ning edendada kiiret ja tõhusat operatiivkoostööd;

([1]) Euroopa Parlamendi ja nõukogu 24. oktoobri 1995. aasta direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta (EÜT L 281, 23.11.1995, lk 31).
([2]) Euroopa Parlamendi ja nõukogu 18. detsembri 2000. aasta määrus (EÜ) nr 45/2001 üksikisikute kaitse kohta isikuandmete töötlemisel ühenduse institutsioonides ja asutustes ning selliste andmete vaba liikumise kohta (EÜT L 8, 12.1.2001, lk 1).
([3]) Euroopa Parlamendi ja nõukogu 30. mai 2001. aasta määrus (EÜ) nr 1049/2001 üldsuse juurdepääsu kohta Euroopa Parlamendi, nõukogu ja komisjoni dokumentidele (EÜT L 145, 31.5.2001, lk 43).
([4]) ELT C 32, 4.2.2014, lk 19.

d) luuakse turva- ja teatamisnõuded oluliste teenuste operaatoritele ja digitaalse teenuse osutajatele;

e) sätestatakse liikmesriikidele kohustused määrata riiklikud pädevad asutused, ühtsed kontaktpunktid ja CSIRTid, mille ülesanded on seotud võrgu- ja infosüsteemide turvalisusega.

3. Käesoleva direktiiviga ette nähtud turva- ja teatamisnõudeid ei kohaldata ettevõtjatele, kelle suhtes kohaldatakse direktiivi 2002/21/EÜ artiklite 13a ja 13b nõudeid, ega usaldusteenuse osutajatele, kelle suhtes kohaldatakse määruse (EL) nr 910/2014 artikli 19 nõudeid.

4. Käesolev direktiiv ei piira nõukogu direktiivi 2008/114/EÜ ([1]) ega Euroopa Parlamendi ja nõukogu direktiivide 2011/93/EL ([2]) ja 2013/40/EL ([3]) kohaldamist.

5. Ilma et see piiraks ELi toimimise lepingu artikli 346 kohaldamist, tuleks teavet, mis on liidu ja siseriiklike õigusnormide, näiteks ärisaladust käsitlevate õigusnormide kohaselt konfidentsiaalne, vahetada komisjoni ja teiste asjakohaste asutustega ainult siis, kui selline teabevahetus on vajalik käesoleva direktiivi kohaldamiseks. Vahetada võib ainult teavet, mis on teabevahetuse eesmärgi seisukohast oluline ja proportsionaalne. Teabevahetus peab tagama asjaomase teabe konfidentsiaalsuse ning oluliste teenuste operaatorite ja digitaalse teenuse osutajate turvalisuse ja ärihuvide kaitse.

6. Käesolev direktiiv ei piira liikmesriikide võetavaid meetmeid, mille eesmärk on tagada riigi põhifunktsioonid ja eelkõige riigi julgeolek, sealhulgas sellise teabe kaitsmise meetmed, mille avalikustamist ta peab oma oluliste julgeolekuhuvide vastaseks, ning säilitada avalik kord, eelkõige selleks, et võimaldada kuritegude uurimist, avastamist ja nende eest vastutusele võtmist.

7. Kui sektoripõhine liidu õigusakt nõuab oluliste teenuste operaatoritelt või digitaalse teenuse osutajatelt nende võrgu- ja infosüsteemide turvalisuse tagamist või intsidentidest teatamist, tingimusel et sellised nõuded on toimelt vähemalt samaväärsed käesolevas direktiivis sätestatud kohustustega, kohaldatakse kõnealuse sektoripõhise liidu õigusakti sätteid.

Artikkel 2

Isikuandmete töötlemine

1. Isikuandmete töötlemine käesoleva direktiivi alusel toimub kooskõlas direktiiviga 95/46/EÜ.

2. Käesoleva direktiivi kohane isikuandmete töötlemine liidu institutsioonide ja asutuste poolt toimub kooskõlas määrusega (EÜ) nr 45/2001.

Artikkel 3

Minimaalne ühtlustamine

Ilma et see piiraks artikli 16 lõike 10 kohaldamist ja liidu õigusest tulenevaid liikmesriikide kohustusi, võivad liikmesriigid võtta vastu või säilitada sätteid eesmärgiga saavutada võrgu- ja infosüsteemide turvalisuse kõrgem tase.

([1]) Nõukogu 8. detsembri 2008. aasta direktiiv 2008/114/EÜ Euroopa elutähtsate infrastruktuuride identifitseerimise ja määramise ning nende kaitse parandamise vajaduse hindamise kohta (ELT L 345, 23.12.2008, lk 75).

([2]) Euroopa Parlamendi ja nõukogu 13. detsembri 2011. aasta direktiiv 2011/93/EL, mis käsitleb laste seksuaalse kuritarvitamise ja ärakasutamise ning lasteporno vastast võitlust ja mis asendab nõukogu raamotsuse 2004/68/JSK (ELT L 335, 17.12.2011, lk 1).

([3]) Euroopa Parlamendi ja nõukogu 12. augusti 2013. aasta direktiiv 2013/40/EL, milles käsitletakse infosüsteemide vastu suunatud rünneid ja millega asendatakse nõukogu raamotsus 2005/222/JSK (ELT L 218, 14.8.2013, lk 8).

Artikkel 4

Mõisted

Käesolevas direktiivis kasutatakse järgmisi mõisteid:

1) „võrgu- ja infosüsteem“ –

   a) elektrooniline sidevõrk direktiivi 2002/21/EÜ artikli 2 punktis a sätestatud tähenduses;

   b) seade või omavahel ühendatud või seotud seadmete rühm, millest vähemalt ühes toimub mõne programmi kohaselt digitaalsete andmete automaatne töötlemine, või

   c) digitaalsed andmed, mida salvestatakse, töödeldakse, saadakse päringutega või edastatakse punktidega a ja b hõlmatud komponentide poolt nende töö, kasutamise, kaitsmise või hooldamise jaoks;

2) „võrgu- ja infosüsteemide turvalisus“ – võrgu- ja infosüsteemi võime panna teatava kindlusega vastu mis tahes tegevusele, mis seab ohtu salvestatud, edastatud või töödeldud andmete või nendega seotud, võrgu- ja infosüsteemi kaudu pakutavate või juurdepääsetavate teenuste kättesaadavuse, autentsuse, tervikluse ja konfidentsiaalsuse;

3) „riiklik võrgu- ja infosüsteemide turvalisuse strateegia“ – raamistik, mis näeb ette võrgu- ja infosüsteemide turvalisuse liikmesriigi tasandi strateegilised eesmärgid ja prioriteedid;

4) „oluliste teenuste operaator“ – II lisas osutatud liiki avaliku või erasektori üksus, mis vastab artikli 5 lõikes 2 sätestatud kriteeriumidele;

5) „digitaalne teenus“ – Euroopa Parlamendi ja nõukogu direktiivi (EL) 2015/1535 ([1]) artikli 1 lõike 1 punktis b määratletud teenus, mis kuulub ühte III lisas loetletud liiki;

6) „digitaalse teenuse osutaja“ – juriidiline isik, kes pakub digitaalset teenust;

7) „intsident“ – sündmus, mis tegelikult kahjustab võrgu- ja infosüsteemide turvalisust;

8) „intsidendi käsitlemine“ – intsidendi tuvastamist, analüüsimist ja ohjeldamist ning intsidendile reageerimist toetavad protseduurid;

9) „risk“ – mõistlikult tuvastatav asjaolu või sündmus, mis võib kahjustada võrgu- ja infosüsteemide turvalisust;

10) „esindaja“ – liidus asuv füüsiline või juriidiline isik, kes on sõnaselgelt määratud tegutsema väljaspool liitu asuva digitaalse teenuse osutaja nimel ja kelle poole võib liikmesriigi pädev asutus või CSIRT pöörduda digitaalse teenuse osutaja asemel seoses digitaalse teenuse osutaja käesolevast direktiivist tulenevate kohustustega;

11) „standard“ – määruse (EL) nr 1025/2012 artikli 2 punktis 1 määratletud standard;

12) „spetsifikatsioon“ – määruse (EL) nr 1025/2012 artikli 2 punktis 4 määratletud tehniline spetsifikatsioon;

13) „interneti vahetuspunkt (IXP, *Internet Exchange Point*)“ – võrgustik, mis võimaldab rohkem kui kahe sõltumatu autonoomse süsteemi omavahelist ühendamist, eelkõige selleks, et hõlbustada internetiliikluse vahetamist;, IXP võimaldab üksnes autonoomsete süsteemide omavahelist ühendamist; IXP ei nõua ühegi kahe osaleva autonoomse süsteemi vahel kulgeva internetiliikluse kulgemist mõne kolmanda autonoomse süsteemi kaudu, ei muuda sellist liiklust ega sekku sellesse mingil muul viisil;

14) „domeeninimede süsteem“ – hierarhilise jaotamise põhimõttel toimuv nimede andmise süsteem võrgus, mis edastab domeeninimede päringuid;

([1]) Euroopa Parlamendi ja nõukogu 9. septembri 2015. aasta direktiiv (EL) 2015/1535, millega nähakse ette tehnilistest eeskirjadest ning infoühiskonna teenuste eeskirjadest teatamise kord (ELT L 241, 17.9.2015, lk 1).

15) „domeeninimede süsteemi teenuse osutaja“ – üksus, mis osutab internetis domeeninimede süsteemi teenuseid;

16) „tippdomeeninimede register“ – üksus, mis haldab ja teostab interneti domeeninimede registreerimist konkreetse tippdomeeni all;

17) „internetipõhine kauplemiskoht“ – digitaalne teenus, mis võimaldab Euroopa Parlamendi ja nõukogu direktiivi 2013/11/EL ([1]) artikli 4 lõike 1 punktis a määratletud tarbijatel ja punktis b määratletud kauplejatel sõlmida kauplejatega internetipõhiseid müügi- või teenuse osutamise lepinguid kas internetipõhise kauplemiskoha veebisaidil või kaupleja veebisaidil, mis kasutab internetipõhise kauplemiskoha pakutavaid andmetöötlusteenuseid;

18) „internetipõhine otsingumootor“ – digitaalne teenus, mis võimaldab kasutajatel teha otsinguid üldjuhul kõikidel veebisaitidel või konkreetses keeles veebisaitidel mis tahes teemal võtmesõna, fraasi või muu sisendi vormis päringu alusel ning saadab vastuseks lingid, kust võib leida teavet taotletud sisu kohta;

19) „pilvandmetöötlusteenus“ – digitaalne teenus, mis võimaldab juurdepääsu skaleeritavale ja paindlikule jagatavate andmetöötlusressursside kogumile.

Artikkel 5

Oluliste teenuste operaatorite identifitseerimine

1. 9. novembriks 2018 identifitseerivad liikmesriigid iga II lisas osutatud sektori ja allsektori puhul need oluliste teenuste operaatorid, kelle tegevuskoht on nende territooriumil.

2. Artikli 4 punktis 4 osutatud oluliste teenuste operaatori identifitseerimise kriteeriumid on järgmised:

a) üksus osutab teenust, mis on oluline elutähtsa ühiskondliku ja/või majandustegevuse säilitamise seisukohast;

b) kõnealuse teenuse osutamine sõltub võrgu- ja infosüsteemidest ning

c) intsidendil oleks oluliselt häiriv mõju nimetatud teenuse osutamisele.

3. Lõike 1 kohaldamiseks koostab iga liikmesriik lõike 2 punktis a osutatud teenuste loetelu.

4. Lõike 1 kohaldamiseks, juhul kui üksus osutab lõike 2 punktis a osutatud teenust kahes või enamas liikmesriigis, konsulteerivad kõnealused liikmesriigid üksteisega. Konsulteerimine toimub enne identifitseerimist käsitleva otsuse tegemist.

5. Liikmesriigid vaatavad korrapäraselt ja vähemalt iga kahe aasta tagant pärast 9. maid 2018 läbi identifitseeritud oluliste teenuste operaatorite nimekirja ja vajaduse korral ajakohastavad seda.

6. Koostöörühma roll on kooskõlas artiklis 11 osutatud ülesannetega toetada liikmesriike järjepideva lähenemisviisi võtmisel oluliste teenuste operaatorite identifitseerimise protsessis.

7. Artiklis 23 osutatud läbivaatamise eesmärgil ja 9. novembriks 2018 ning pärast seda iga kahe aasta tagant esitavad liikmesriigid komisjonile vajaliku teabe, et komisjon saaks hinnata käesoleva direktiivi rakendamist, eelkõige liikmesriikide lähenemisviiside järjepidevust seoses oluliste teenuste operaatorite identifitseerimisega. Kõnealune teave hõlmab vähemalt järgmist:

a) riiklikud meetmed, mis võimaldavad oluliste teenuste operaatorite identifitseerimist;

([1]) Euroopa Parlamendi ja nõukogu 21. mai 2013. aasta direktiiv 2013/11/EL tarbijavaidluste kohtuvälise lahendamise kohta, millega muudetakse määrust (EÜ) nr 2006/2004 ja direktiivi 2009/22/EÜ (tarbijavaidluste kohtuvälise lahendamise direktiiv) (ELT L 165, 18.6.2013, lk 63).

b) lõikes 3 osutatud teenuste loetelu;

c) iga II lisas osutatud sektori puhul identifitseeritud oluliste teenuste operaatorite arv ning operaatori tähtsus asjaomases sektoris;

d) piirmäärad (kui need on olemas), mille abil määrata kindlaks asjakohane teenuse osutamise tase viitega artikli 6 lõike 1 punktis a osutatud teenusest sõltuvate kasutajate arvule või asjaomase oluliste teenuste operaatori tähtsusele, millele on osutatud artikli 6 lõike 1 punktis f.

Komisjon võib selleks, et aidata kaasa võrreldava teabe esitamisele, võtta vastu asjakohased tehnilised suunised käesolevas lõikes osutatud teabe parameetrite kohta, võttes seejuures võimalikult suurel määral arvesse ENISA arvamust.

Artikkel 6

Oluline häiriv mõju

1. Artikli 5 lõike 2 punktis c osutatud häiriva mõju olulisuse kindlakstegemisel võtavad liikmesriigid arvesse vähemalt järgmisi sektoritevahelisi tegureid:

a) asjaomase üksuse poolt osutatavatest teenustest sõltuvate kasutajate arv;

b) muude II lisas osutatud sektorite sõltumine üksuse poolt pakutavast teenusest;

c) intsidentide võimalik mõju (raskusaste ja kestus) majandus- ja ühiskondlikule tegevusele või avalikule julgeolekule;

d) üksuse turuosa;

e) intsidendist mõjutatud geograafilise ala võimalik ulatus;

f) üksuse tähtsus teenuse piisava kvaliteedi säilitamisel, võttes arvesse alternatiivide olemasolu kõnealuse teenuse osutamiseks.

2. Selleks et teha kindlaks, kas intsidendil oleks oluline häiriv mõju, võtavad liikmesriigid asjakohasel juhul arvesse ka sektoripõhiseid tegureid.

II PEATÜKK

RIIKLIKUD VÕRGU- JA INFOSÜSTEEMIDE TURVALISUSE RAAMISTIKUD

Artikkel 7

Riiklik võrgu- ja infosüsteemide turvalisuse strateegia

1. Iga liikmesriik võtab vastu riikliku võrgu- ja infosüsteemide turvalisuse strateegia, milles määratletakse strateegilised eesmärgid ning asjakohased poliitilised ja regulatiivsed meetmed, mille abil saavutada võrgu- ja infosüsteemide turvalisuse kõrge tase ja seda säilitada, ning mis hõlmab vähemalt II lisas osutatud sektoreid ja III lisas osutatud teenuseid. Eelkõige käsitletakse riiklikus võrgu- ja infosüsteemide turvalisuse strateegias järgmisi küsimusi:

a) riikliku võrgu- ja infosüsteemide turvalisuse strateegia eesmärgid ja prioriteedid;

b) juhtimisraamistik, mille toel riikliku võrgu- ja infosüsteemide turvalisuse strateegia eesmärgid ja prioriteedid ellu viia; see hõlmab valitsusasutuste ning muude asjaomaste osalejate ülesandeid ja vastutust;

c) valmisoleku-, reageerimis- ja taastemeetmete, sh avaliku ja erasektori koostöö kindlaksmääramine;

d) riikliku võrgu- ja infosüsteemide turvalisuse strateegiaga seotud haridus-, teadlikkuse suurendamise ja koolitusprogrammide kirjeldus;

e) riikliku võrgu- ja infosüsteemide turvalisuse strateegiaga seotud teadus- ja arendustegevuse kavade kirjeldus;

f) riski hindamise kava riskide kindlakstegemiseks;

g) riikliku võrgu- ja infosüsteemide turvalisuse strateegia rakendamises osalevate erinevate osalejate loetelu.

2. Liikmesriigid võivad paluda ENISA abi riiklike võrgu- ja infosüsteemide turvalisuse strateegiate väljatöötamisel.

3. Liikmesriigid edastavad oma riikliku võrgu- ja infosüsteemide turvalisuse strateegia komisjonile kolme kuu jooksul pärast selle vastuvõtmist. Seda tehes võivad liikmesriigid jätta välja strateegia elemendid, mis on seotud riikliku julgeolekuga.

Artikkel 8

Riiklikud pädevad asutused ja ühtne kontaktpunkt

1. Iga liikmesriik määrab võrgu- ja infosüsteemide turbe vallas ühe või mitu riiklikku pädevat asutust („pädev asutus“), kes hõlmavad vähemalt II lisas osutatud sektoreid ja III lisas osutatud teenuseid. Liikmesriigid võivad määrata selle ülesande olemasolevale asutusele või olemasolevatele asutustele.

2. Pädevad asutused jälgivad käesoleva direktiivi kohaldamist riigi tasandil.

3. Iga liikmesriik määrab võrgu- ja infosüsteemide turbe vallas riikliku ühtse kontaktpunkti („ühtne kontaktpunkt“). Liikmesriigid võivad määrata selle ülesande olemasolevale asutusele. Kui liikmesriik nimetab ainult ühe pädeva asutuse, siis on see pädev asutus ka ühtne kontaktpunkt.

4. Ühtne kontaktpunkt täidab sidepidamisfunktsiooni, et tagada liikmesriikide asutuste piiriülene koostöö teiste liikmesriikide asjaomaste asutuste, artiklis 11 osutatud koostöörühma ja artiklis 12 osutatud CSIRTide võrgustikuga.

5. Liikmesriigid tagavad, et pädevatel asutustel ja ühtsetel kontaktpunktidel on piisavad ressursid, et oma ülesandeid tulemuslikult ja tõhusalt täita ning seeläbi saavutada käesoleva direktiivi eesmärgid. Liikmesriigid tagavad määratud esindajate tõhusa, tulemusliku ja turvalise koostöö koostöörühmas.

6. Pädevad asutused ja ühtne kontaktpunkt peavad vajaduse korral ja kooskõlas siseriikliku õigusega konsulteerima ja tegema koostööd asjakohaste riiklike õiguskaitse- ja andmekaitseasutustega.

7. Iga liikmesriik teatab komisjonile viivitamata pädeva asutuse ja ühtse kontaktpunkti määramisest, nende ülesannetest ja nende hilisemast muutmisest. Iga liikmesriik avalikustab määratud pädeva asutuse ja ühtse kontaktpunkti. Komisjon avaldab määratud ühtsete kontaktpunktide loetelu.

Artikkel 9

Küberturbe intsidentide lahendamise üksused (CSIRTid)

1. Iga liikmesriik määrab ühe või mitu I lisa punktis 1 sätestatud nõuetele vastava CSIRTi, kes hõlmavad vähemalt II lisas osutatud sektoreid ja III lisas osutatud teenuseid ning kes vastutavad riskide ja intsidentide käsitlemise eest põhjalikult määratletud protseduuri kohaselt. CSIRTi võib luua pädeva asutuse osana.

2. Liikmesriigid tagavad, et CSIRTidel on I lisa punktis 2 osutatud ülesannete tulemuslikuks täitmiseks piisavad ressursid.

Liikmesriigid tagavad oma CSIRTide tõhusa, tulemusliku ja turvalise koostöö artiklis 12 osutatud CSIRTide võrgustikus.

3. Liikmesriigid tagavad, et CSIRTidel on riigi tasandil juurdepääs asjakohasele, turvalisele ja töökindlale side- ja infotaristule.

4. Liikmesriigid teatavad komisjonile, millised on CSIRTide volitused ja intsidentide käsitlemise protseduuri peamised elemendid.

5. Liikmesriigid võivad paluda ENISA abi riiklike CSIRTide väljatöötamisel.

Artikkel 10

Koostöö liikmesriigi tasandil

1. Kui sama liikmesriigi pädev asutus, ühtne kontaktpunkt ja CSIRT on üksteisest eraldiseisvad, teevad nad käesolevas direktiivis sätestatud kohustuste täitmiseks koostööd.

2. Liikmesriigid tagavad, et pädevad asutused või CSIRTid saavad käesoleva direktiivi kohaselt esitatud teated intsidentide kohta. Kui liikmesriik otsustab, et CSIRTid ei saa teateid, tuleb CSIRTidele anda nende ülesannete täitmiseks vajalikus ulatuses juurdepääs andmetele intsidentide kohta, millest on teatanud oluliste teenuste operaatorid artikli 14 lõigete 3 ja 5 kohaselt või digitaalse teenuse osutajad artikli 16 lõigete 3 ja 6 kohaselt.

3. Liikmesriigid tagavad, et pädevad asutused või CSIRTid teavitavad ühtseid kontaktpunkte käesoleva direktiivi kohaselt esitatud intsidente käsitlevatest teadetest.

Ühtne kontaktpunkt esitab 9. augustiks 2018 ning pärast seda üks kord aastas koostöörühmale saadud teadete kohta koondaruande, mis sisaldab teadete arvu ja teatatud intsidentide laadi ning vastavalt artikli 14 lõigetele 3 ja 5 ning artikli 16 lõigetele 3 ja 6 võetud meetmeid.

III PEATÜKK

KOOSTÖÖ

Artikkel 11

Koostöörühm

1. Käesolevaga luuakse koostöörühm, et toetada ja hõlbustada liikmesriikidevahelist strateegilist koostööd ja infovahetust, luua usaldust ja kindlustunnet ning saavutada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase liidus.

Koostöörühm täidab oma ülesandeid kaheaastaste tööprogrammide alusel, nagu on osutatud lõike 3 teises lõigus.

2. Koostöörühm koosneb liikmesriikide, komisjoni ja ENISA esindajatest.

Kui see on asjakohane, võib koostöörühm kutsuda oma töös osalema asjakohaste sidusrühmade esindajaid.

Komisjon tagab sekretariaadi teenused.

3. Koostöörühmal on järgmised ülesanded:

a) anda strateegilisi suuniseid artikli 12 kohaselt loodud CSIRTide võrgustiku tegevuse kohta;

b) vahetada parimaid tavasid artikli 14 lõigetes 3 ja 5 ja artikli 16 lõigetes 3 ja 6 osutatud intsidentidest teatamisega seotud teabevahetuse kohta;

c) vahetada parimaid tavasid liikmesriikide vahel ning aidata koostöös ENISAga liikmesriike võrgu- ja infosüsteemide turvalisuse alase suutlikkuse suurendamise alal;

d) arutada liikmesriikide suutlikkust ja valmisolekut ning hinnata vabatahtlikkuse alusel riiklikke võrgu- ja infosüsteemide turvalisuse strateegiaid ja CSIRTide tõhusust ning teha kindlaks parimad tavad;

e) vahetada teavet ja parimaid tavasid teadlikkuse suurendamise ja koolituse kohta;

f) vahetada teavet ja parimaid tavasid võrgu- ja infosüsteemide turvalisusega seotud teadus- ja arendustegevuse kohta;

g) kui see on asjakohane, siis vahetada kogemusi võrgu- ja infosüsteemide turvalisuse küsimustes liidu asjakohaste institutsioonide, organite ja asutustega;

h) arutada asjakohaste Euroopa standardiorganisatsioonide esindajatega artiklis 19 osutatud standardeid ja spetsifikatsioone;

i) koguda parimaid tavasid riskide ja intsidentide kohta;

j) analüüsida igal aastal artikli 10 lõike 3 teises lõigus osutatud koondaruandeid;

k) arutada võrgu- ja infosüsteemide turvalisusega seotud õppuste, haridusprogrammide ja koolituse osas tehtud tööd, sealhulgas ENISA tööd;

l) vahetada ENISA abiga parimaid tavasid seoses oluliste teenuste operaatorite identifitseerimisega liikmesriikide poolt, sealhulgas mis puudutab riskide ja intsidentidega seotud piiriüleseid sõltuvusseoseid;

m) arutada artiklites 14 ja 16 osutatud intsidentidest teatamise korda.

Koostöörühm koostab 9. veebruariks 2018 ja seejärel iga kahe aasta tagant tööprogrammi eesmärkide ja ülesannete täitmiseks võetavate meetmete kohta, mis peab olema kooskõlas käesoleva direktiivi eesmärkidega.

4. Koostöörühm esitab artiklis 23 osutatud ülevaate jaoks ja 9. augustiks 2018 ning pärast seda iga pooleteise aasta tagant aruande, milles hinnatakse käesoleva artikli kohaselt tehtud strateegilisest koostööst saadud kogemusi.

5. Komisjon võtab vastu rakendusaktid, millega kehtestatakse koostöörühma toimimiseks vajalik menetluskord. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 22 lõikes 2 osutatud kontrollimenetlusega.

Esimese lõigu kohaldamise eesmärgil esitab komisjon esimese rakendusakti eelnõu artikli 22 lõikes 1 osutatud komiteele hiljemalt 9. veebruariks 2017.

Artikkel 12

CSIRTide võrgustik

1. Käesolevaga luuakse riiklike CSIRTide võrgustik, et aidata luua liikmesriikide vahel usaldust ja kindlustunnet ning edendada kiiret ja tõhusat operatiivkoostööd.

2. CSIRTide võrgustik koosneb liikmesriikide CSIRTide ja CERT-EU esindajatest. Komisjon osaleb CSIRTide võrgustikus vaatlejana. ENISA tagab sekretariaadi töö ja toetab aktiivselt CSIRTide-vahelist koostööd.

3. CSIRTide võrgustikul on järgmised ülesanded:

a) vahetada teavet CSIRTide teenuste, tegevuste ja koostöösuutlikkuse kohta;

b) intsidendist potentsiaalselt mõjutatud liikmesriigi CSIRTi esindaja taotlusel vahetada ja arutada asjaomast intsidenti ja sellega seonduvaid riske käsitlevat mittetundlikku äriteavet, aga samas võib iga liikmesriigi CSIRT keelduda sellesse arutellu panustamast, kui on olemas oht, et see kahjustab intsidendi uurimist;

c) vahetada ja teha vabatahtlikkuse alusel kättesaadavaks mittekonfidentsiaalset teavet üksikute intsidentide kohta;

d) liikmesriigi CSIRT esindaja taotlusel arutada koordineeritud reageerimist sama liikmesriigi jurisdiktsioonis tuvastatud intsidendile ning võimaluse korral määratleda koordineeritud reageerimine;

e) toetada liikmesriike piiriüleste intsidentide käsitlemisel nende vabatahtliku vastastikuse abistamise põhimõttel;

f) arutada, uurida ja teha kindlaks täiendavaid operatiivkoostöö vorme, sealhulgas seoses järgmisega:

   i) riskide ja intsidentide kategooriad;

   ii) varajased hoiatused;

   iii) vastastikune abi;

   iv) koostöö põhimõtted ja kord juhtudeks, kui liikmesriigid reageerivad piirülestele riskidele ja intsidentidele;

g) teavitada koostöörühma oma tegevusest ja punkti f kohaselt arutatud täiendavatest operatiivkoostöö vormidest ning taotleda sellega seonduvaid suuniseid;

h) arutada võrgu- ja infosüsteemide turvalisusega seotud õppustelt, sealhulgas ENISA korraldatud õppustelt, saadud kogemusi;

i) arutada üksiku CSIRT taotlusel kõnealuse CSIRT suutlikkust ja valmisolekut;

j) anda suuniseid, et hõlbustada operatiivsete tavade lähendamist seoses käesoleva artikli operatiivkoostööd käsitlevate sätete kohaldamisega.

4. Artiklis 23 osutatud läbivaatamise eesmärgil ja 9. augustiks 2018 ning pärast seda iga pooleteise aasta tagant esitab CSIRTide võrgustik aruande, milles hinnatakse käesoleva artikli kohaselt tehtud operatiivkoostööst saadud kogemusi ning mis sisaldab järeldusi ja soovitusi. See aruanne esitatakse ka koostöörühmale.

5. CSIRTide võrgustik sätestab oma töökorra.

Artikkel 13

Rahvusvaheline koostöö

Liit võib kooskõlas ELi toimimise lepingu artikliga 218 sõlmida kolmandate riikide või rahvusvaheliste organisatsioonidega rahvusvahelisi lepinguid, mis võimaldavad neil osaleda ja korraldada nende osalust mõningates koostöörühma tegevustes. Sellistes lepingutes arvestatakse vajadusega tagada andmete piisav kaitse.

IV PEATÜKK

OLULISTE TEENUSTE OPERAATORITE VÕRGU- JA INFOSÜSTEEMIDE TURVALISUS

Artikkel 14

Turvanõuded ja intsidentidest teatamine

1. Liikmesriigid tagavad, et oluliste teenuste operaatorid võtavad asjakohased ja proportsionaalsed tehnilised ja korralduslikud meetmed, et hallata riske, mis ohustavad nende töös kasutatavate võrgu- ja infosüsteemide turvalisust. Tehnika taset arvesse võttes tagatakse nende meetmetega olemasolevale ohule vastav võrgu- ja infosüsteemide turvalisuse tase.

2. Liikmesriigid tagavad, et oluliste teenuste operaatorid võtavad asjakohased meetmed, selleks et ennetada ja minimeerida oluliste teenuste osutamiseks kasutatavate võrgu- ja infosüsteemide turvalisust kahjustavate intsidentide mõju, eesmärgiga tagada kõnealuste teenuste järjepidevus.

3. Liikmesriigid tagavad, et oluliste teenuste operaatorid teatavad põhjendamatu viivituseta pädevale asutusele või CSIRTile intsidentidest, millel on oluline mõju nende pakutavate oluliste teenuste järjepidevusele. Teated peavad sisaldama teavet, mis võimaldab pädeval asutusel või CSIRTil teha kindlaks intsidendi igasugune piiriülene mõju. Teatamine ei suurenda teavitava osapoole vastutust.

4. Intsidendi mõju olulisuse kindlakstegemiseks võetakse arvesse eriti järgmisi parameetreid:

a) olulise teenuse katkemisest mõjutatud kasutajate arv;

b) intsidendi kestus;

c) intsidendist mõjutatud geograafilise ala ulatus.

5. Oluliste teenuste operaatori teates esitatud teabe põhjal teavitab pädev asutus või CSIRT teisi mõjutatud liikmesriike, juhul kui intsidendil on oluline mõju oluliste teenuste järjepidevusele asjaomases liikmesriigis. Seda tehes kaitseb pädev asutus või CSIRT kooskõlas liidu õigusega või liidu õigusele vastavate siseriiklike õigusaktidega oluliste teenuste operaatori turvalisust ja ärihuve ning tema poolt teates esitatud teabe konfidentsiaalsust.

Kui olukord seda võimaldab, esitab pädev asutus või CSIRT teate esitanud oluliste teenuste operaatorile asjakohase teabe intsidendist teatamise järelmeetmete kohta, näiteks teabe, mis võib aidata intsidenti tõhusalt käsitleda.

Pädeva asutuse või CSIRT taotlusel edastab ühtne kontaktpunkt esimeses lõigus osutatud teated teiste puudutatud liikmesriikide ühtsetele kontaktpunktidele.

6. Pärast konsulteerimist teate esitanud oluliste teenuste operaatoriga võib teate saanud pädev asutus või CSIRT teavitada üldsust üksikutest intsidentidest, juhul kui üldsuse teadlikkus on vajalik intsidendi ärahoidmiseks või käimasoleva intsidendi lahendamiseks.

7. Koostöörühmas koos tegutsevad pädevad asutused võivad koostada ja võtta vastu suuniseid olukordade kohta, kus oluliste teenuste operaatoritelt nõutakse intsidentidest teatamist, sealhulgas parameetrite kohta, millega määratakse kindlaks intsidendi mõju olulisus, nagu on osutatud lõikes 4.

Artikkel 15

Rakendamine ja jõustamine

1. Liikmesriigid tagavad, et pädevatel asutustel on vajalikud õigused ja vahendid, et hinnata seda, kas oluliste teenuste operaatorid täidavad artiklist 14 tulenevaid kohustusi, ning selle mõju võrgu- ja infosüsteemide turvalisusele.

2. Liikmesriigid tagavad, et pädeval asutusel on õigused ja vahendid nõudmaks, et oluliste teenuste operaatorid esitaksid

a) oma võrgu- ja infosüsteemide turvalisuse hindamiseks vajaliku teabe, sealhulgas dokumenteeritud turvapõhimõtted;

b) tõendid turvapõhimõtete tõhusa rakendamise kohta, näiteks pädeva asutuse või tunnustatud audiitori poolt läbi viidud turvaauditi tulemused, ning viimasel juhul teeksid need tulemused ja nende aluseks olevad tõendid kättesaadavaks pädevale asutusele.

Teabe või tõendite esitamist taotledes esitavad pädevad asutused taotluse eesmärgi ja täpsustavad, millist teavet nõutakse.

3. Pärast lõikes 2 osutatud teabe või turvaauditite tulemuste hindamist võivad pädevad asutused anda oluliste teenuste operaatoritele siduvaid juhiseid nende töö parandamiseks.

4. Kui intsident põhjustab isikuandmetega seotud rikkumise, teeb pädev asutus selle lahendamisel tihedat koostööd andmekaitseasutustega.

V PEATÜKK

DIGITAALSE TEENUSE OSUTAJATE VÕRGU- JA INFOSÜSTEEMIDE TURVALISUS

Artikkel 16

Turvanõuded ja intsidentidest teatamine

1. Liikmesriigid tagavad, et digitaalse teenuse osutajad teevad kindlaks riskid, mis ohustavad nende võrgu- ja infosüsteemide turvalisust, mida nad kasutavad III lisas osutatud teenuste osutamisel liidus, ning võtavad asjakohased ja proportsionaalsed tehnilised ja korralduslikud meetmed, et neid riske juhtida. Tehnika taset arvesse võttes tagatakse nende meetmetega olemasolevale ohule vastav võrgu- ja infosüsteemide turvalisuse tase ning võetakse arvesse järgmisi elemente:

a) süsteemide ja rajatiste turvalisus,

b) intsidentide käsitlemine,

c) talitluspidevuse haldamine,

d) seire, auditeerimine ja testimine,

e) vastavus rahvusvahelistele standarditele.

2. Liikmesriigid tagavad, et digitaalse teenuse osutajad võtavad meetmeid, et vältida ja minimeerida nende intsidentide mõju, mis kahjustavad nende poolt III lisas sätestatud teenuste liidus osutamiseks kasutatavate võrgu- ja infosüsteemide turvalisust, eesmärgiga tagada kõnealuste teenuste järjepidevus.

3. Liikmesriigid tagavad, et digitaalse teenuse osutajad teatavad pädevale asutusele või CSIRTile põhjendamatu viivituseta igast intsidendist, millel on oluline mõju nende poolt liidus osutatavale III lisas sätestatud teenusele. Teated peavad sisaldama teavet, mis võimaldab pädeval asutusel või CSIRTil teha kindlaks intsidendi piiriülese mõju olulisus. Teatamine ei suurenda teavitava osapoole vastutust.

4. Intsidendi mõju olulisuse hindamiseks võetakse arvesse eelkõige järgmisi parameetreid:

a) intsidendist mõjutatud kasutajate ja eelkõige nende kasutajate arv, kes sõltuvad asjaomasest teenusest oma teenuste osutamisel;

b) intsidendi kestus;

c) intsidendist mõjutatud geograafilise ala ulatus;

d) teenuse toimimise katkemise ulatus;

e) majandus- ja ühiskondlikule tegevusele avalduva mõju ulatus.

Intsidendist teatamise kohustust kohaldatakse üksnes juhul, kui digitaalse teenuse osutajal on juurdepääs teabele, mis on vajalik esimeses lõigus osutatud kriteeriumide täitmise hindamiseks.

5. Kui oluliste teenuste operaator sõltub tähtsa ühiskondliku ja majandustegevuse säilitamiseks olulise teenuse osutamisel kolmandast isikust digitaalse teenuse osutajast, peab operaator teatama digitaalse teenuse osutajat kahjustava intsidendi mis tahes olulisest mõjust oluliste teenuste järjepidevusele.

6. Kui see on asjakohane ja eelkõige juhul, kui lõikes 3 osutatud intsident puudutab kahte või enamat liikmesriiki, peab pädev asutus või CSIRT teavitama teisi mõjutatud liikmesriike. Seda tehes kaitsevad pädevad asutused, CSIRTid ja ühtsed kontaktpunktid kooskõlas liidu õigusega või liidu õigusele vastavate siseriiklike õigusaktidega digitaalse teenuse osutaja turvalisust ja ärihuve ning esitatud teabe konfidentsiaalsust.

7. Pärast konsulteerimist asjaomase digitaalse teenuse osutajaga võivad pädev asutus või CSIRTid ja, kui see on asjakohane, teiste asjaomaste liikmesriikide asutused või CSIRTid teavitada üldsust üksikutest intsidentidest või nõuda, et digitaalse teenuse osutaja seda teeks, juhul kui üldsuse teadlikkus on vajalik intsidendi ärahoidmiseks või käimasoleva intsidendi lahendamiseks või kui intsidendi avalikustamine on muul moel üldsuse huvides.

8. Komisjonil on õigus võtta vastu rakendusakte, et täpsustada veelgi käesoleva artikli lõikes 1 osutatud elemente ja lõikes 4 loetletud parameetreid. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 22 lõikes 2 osutatud kontrollimenetlusega hiljemalt 9. augustiks 2017.

9. Komisjon võib võtta vastu rakendusakte, millega kehtestada teatamisnõuete suhtes kohaldatavad formaadid ja menetlused. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 22 lõikes 2 osutatud kontrollimenetlusega.

10. Liikmesriigid ei kehtesta digitaalse teenuse osutajate suhtes täiendavaid turva- või teatamisnõudeid, ilma et see piiraks artikli 1 lõike 6 kohaldamist.

11. V peatükki ei kohaldata komisjoni soovituses 2003/361/EÜ ([1]) määratletud mikro- ja väikeste ettevõtjate suhtes.

([1]) Komisjoni 6. mai 2003. aasta soovitus 2003/361/EÜ mikro-, väikeste ja keskmise suurusega ettevõtjate määratlemise kohta (ELT L 124, 20.5.2003, lk 36).

Artikkel 17

Rakendamine ja jõustamine

1. Liikmesriigid tagavad, et pädevad asutused võtavad vajaduse korral meetmeid järgneva järelevalve käigus, kui neile esitatakse tõendid, et digitaalse teenuse osutaja ei täida artiklis 16 sätestatud nõudeid. Tõendid võib esitada teise liikmeriigi pädev asutus, kus teenust osutatakse.

2. Lõike 1 kohaldamisel on pädevatel asutustel vajalikud õigused ja vahendid, et nõuda digitaalse teenuse osutajatelt

a) nende võrgu- ja infosüsteemide turvalisuse hindamiseks vajaliku teabe, sealhulgas dokumenteeritud turvapõhimõtete esitamist;

b) artiklis 16 sätestatud nõuete täitmata jätmise heastamist.

3. Kui digitaalse teenuse osutaja peamine tegevuskoht või esindaja asuvad ühes liikmesriigis, kuid tema võrgu- ja infosüsteemid asuvad ühes või mitmes teises liikmesriigis, teevad peamise tegevuskoha või esindaja liikmesriigi pädev asutus ja kõnealuste teiste liikmesriikide pädevad asutused koostööd ja vajaduse korral abistavad üksteist. Abi ja koostöö võivad sisaldada asjaomaste pädevate asutuste vahelist teabevahetust ja taotlusi võtta lõikes 2 osutatud järelevalvemeetmed.

Artikkel 18

Jurisdiktsioon ja territoriaalsus

1. Käesoleva direktiivi kohaldamise eesmärgil käsitatakse digitaalse teenuse osutajat selle liikmesriigi jurisdiktsiooni alla kuuluvana, kus on tema peamine tegevuskoht. Digitaalse teenuse osutaja peamiseks asukohaks loetakse liikmesriiki, kui tema peakorter asub kõnealuses liikmesriigis.

2. Digitaalse teenuse osutaja, kelle asukoht ei ole liidus, kuid kes osutab liidus III lisas osutatud teenuseid, peab määrama oma esindaja liidus. Esindaja asukohaks on üks nendest liikmesriikidest, kus teenuseid osutatakse. Digitaalse teenuse osutajat käsitatakse selle liikmesriigi jurisdiktsiooni alla kuuluvana, kus on esindaja asukoht.

3. Esindaja määramine digitaalse teenuse osutaja poolt ei piira kohtumenetlusi, mida võiks algatada digitaalse teenuse osutaja enda vastu.

VI PEATÜKK

STANDARDIMINE JA VABATAHTLIK TEATAMINE

Artikkel 19

Standardimine

1. Selleks et edendada artikli 14 lõigete 1 ja 2 ning artikli 16 lõigete 1 ja 2 ühtset rakendamist, innustavad liikmesriigid võrgu- ja infosüsteemide turvalisust käsitlevate Euroopa või rahvusvaheliselt heaks kiidetud standardite ja spetsifikatsioonide kasutamist, ilma et nad seejuures nõuaksid või soosiksid konkreetset tüüpi tehnoloogia kasutamist.

2. ENISA koostab koostöös liikmesriikidega nõuanded ja suunised seoses tehniliste valdkondadega, mida tuleks lõike 1 puhul arvesse võtta, ning seoses olemasolevate, sealhulgas liikmesriikide standarditega, mis võimaldaksid neid valdkondi hõlmata.

Artikkel 20

Vabatahtlik teatamine

1. Ilma et see piiraks artikli 3 kohaldamist, võivad üksused, mis ei ole määratletud kui oluliste teenuste operaatorid ega digitaalse teenuse osutajad, teatada vabatahtlikult intsidentidest, millel on oluline mõju nende osutatavate teenuste järjepidevusele.

2. Teadete läbivaatamisel järgivad liikmesriigid artiklis 14 sätestatud menetlust. Liikmesriigid võivad vaadata kohustuslikud teated läbi enne vabatahtlikke teateid. Vabatahtlikud teated vaadatakse läbi üksnes juhul, kui selline läbivaatamine ei ole asjaomaste liikmesriikide jaoks ebaproportsionaalselt ega liigselt koormav.

Vabatahtlik teade ei pane teate esitanud üksusele mingeid kohustusi, mida tal ei oleks tekkinud juhul, kui ta ei oleks kõnealust teadet esitanud.

VII PEATÜKK

LÕPPSÄTTED

Artikkel 21

Karistused

Liikmesriigid kehtestavad sätted karistuste kohta, mida rakendatakse käesoleva direktiivi kohaselt vastu võetud siseriiklike õigusnormide rikkumise korral, ning võtavad kõik vajalikud meetmed nende rakendamise tagamiseks. Kehtestatud karistused peavad olema tõhusad, proportsionaalsed ja hoiatavad. Liikmesriigid teatavad kõnealustest sätetest ja meetmetest komisjonile hiljemalt 9. maiks 2018, samuti teatavad nad viivitamata kõigist neid mõjutavatest hilisematest muudatustest.

Artikkel 22

Komiteemenetlus

1. Komisjoni abistab võrgu- ja infoturbesüsteemide komitee. Nimetatud komitee on komitee määruse (EL) nr 182/2011 tähenduses.

2. Käesolevale lõikele viitamisel kohaldatakse määruse (EL) nr 182/2011 artiklit 5.

Artikkel 23

Läbivaatamine

1. Komisjon esitab 9. maiks 2019 Euroopa Parlamendile ja nõukogule aruande, milles antakse hinnang liikmesriikide lähenemisviiside järjepidevusele oluliste teenuste operaatorite identifitseerimisel.

2. Komisjon vaatab käesoleva direktiivi toimimise korrapäraselt läbi ning esitab aruande Euroopa Parlamendile ja nõukogule. Sel eesmärgil ning strateegilise ja operatiivkoostöö täiendavaks edendamiseks võtab komisjon arvesse koostöörühma ja CSIRTide võrgustiku aruandeid strateegilisel ja operatiivtasandil saadud kogemuste kohta. Komisjon hindab läbivaatamise käigus ka II ja III lisas esitatud loetelusid ning järjepidevust oluliste teenuste operaatorite ja teenuste identifitseerimisel II lisas osutatud sektorites. Esimene aruanne esitatakse 9. maiks 2021.

Artikkel 24

Üleminekumeetmed

1. Ilma et see piiraks artikli 25 kohaldamist ja selleks, et anda liikmesriikidele lisavõimalusi teha ülevõtmisperioodil asjakohast koostööd, alustavad koostöörühm ja CSIRTide võrgustik oma vastavalt artikli 11 lõikes 3 ja artikli 12 lõikes 3 sätestatud ülesannete täitmist 9. veebruariks 2017.

2. Ajavahemikuks 9. veebruarist 2017 kuni 9. novembrini 2018 ning selleks, et toetada liikmesriikide järjepidevat lähenemisviisi oluliste teenuste operaatorite identifitseerimisel, arutab koostöörühm nende riiklike meetmete protsessi, sisu ja liiki, mis võimaldavad identifitseerida oluliste teenuste operaatorid konkreetses sektoris vastavalt artiklites 5 ja 6 sätestatud kriteeriumidele. Koostöörühm arutab liikmesriigi taotlusel ka asjaomase liikmesriigi konkreetseid riiklike meetmete kavandeid, mis võimaldavad identifitseerida oluliste teenuste operaatorid konkreetses sektoris vastavalt artiklites 5 ja 6 sätestatud kriteeriumidele.

3. Liikmesriigid tagavad 9. veebruariks 2017 ja käesoleva artikli kohaldamisel asjakohase esindatuse koostöörühmas ja CSIRTide võrgustikus.

Artikkel 25

Ülevõtmine

1. Liikmesriigid võtavad vastu ja avaldavad käesoleva direktiivi järgimiseks vajalikud õigus- ja haldusnormid 9. maiks 2018. Liikmesriigid teatavad nendest viivitamata komisjonile.

Nad kohaldavad kõnealuseid meetmeid alates 10. maist 2018.

Kui liikmesriigid need sätted vastu võtavad, lisavad nad nendesse või nende ametliku avaldamise korral nende juurde viite käesolevale direktiivile. Sellise viitamise viisi näevad ette liikmesriigid.

2. Liikmesriigid edastavad komisjonile käesoleva direktiiviga reguleeritavas valdkonnas nende poolt vastu võetud põhiliste siseriiklike õigusnormide teksti.

Artikkel 26

Jõustumine

Käesolev direktiiv jõustub kahekümnendal päeval pärast selle avaldamist *Euroopa Liidu Teatajas*.

Artikkel 27

Adressaadid

Käesolev direktiiv on adresseeritud liikmesriikidele.

Strasbourg, 6. juuli 2016

Euroopa Parlamendi nimel	*Nõukogu nimel*
president	*eesistuja*
M. SCHULZ	I. KORČOK

I LISA

KÜBERTURBE INTSIDENTIDE LAHENDAMISE ÜKSUSELE (CSIRT) ESITATAVAD NÕUDED JA ÜKSUSE ÜLESANDED

CSIRTile esitatavad nõuded ja tema ülesanded tuleb määratleda piisavalt ja selgelt ning riigi poliitika ja/või õigusnormid peavad neid toetama. Need hõlmavad järgmist.

1) CSIRTile esitatavad nõuded

   a) CSIRT peab tagama oma sideteenuste laialdase kättesaadavuse, vältides nõrku lülisid, ning kasutama mitmesuguseid vahendeid, mis võimaldavad neil teistega ja teistel nendega igal ajal ühendust võtta. Lisaks peavad sidekanalid olema selgelt nimetatud ning kasutajatele ja koostööpartneritele hästi teada.

   b) CSIRTi ametiruumide ja tema tööd toetavate infosüsteemide asukoht peab olema turvaline.

   c) Talitluspidevus:

      i) CSIRTil peab olema taotluste haldamiseks ja suunamiseks sobiv süsteem, et hõlbustada üleandmisi:

      ii) CSIRTil peab olema piisavalt töötajaid, et tagada alaline kättesaadavus:

      iii) CSIRTi kasutatava taristu pidevus peab olema tagatud. Selleks peavad olema kasutada liiased süsteemid ja varutöökeskkond.

   d) CSIRTil peab olema soovi korral võimalik osaleda rahvusvahelistes koostöövõrgustikes.

2) CSIRTi ülesanded

   a) CSIRTi ülesanded peavad sisaldama vähemalt järgmist:

      i) intsidentide seire riigis;

      ii) riskide ja intsidentide kohta varajaste hoiatuste, hoiatuste ja teadaannete esitamine ning teabe levitamine asjakohastele sidusrühmadele;

      iii) intsidentidele reageerimine;

      iv) pidev riskide ja intsidentide analüüsimine ja teadlikkus olukorrast;

      v) osalemine CSIRTide võrgustikus.

   b) CSIRT peab sisse seadma koostöö erasektoriga.

   c) Koostöö hõlbustamiseks peab CSIRT toetama ühiste või standardtoimingute vastuvõtmist ja kasutamist järgmistes valdkondades:

      i) intsidentide ja riskide käsitlemise menetlused;

      ii) intsidentide, riskide ja teabe liigitamise kavad.

II LISA

ÜKSUSTE LIIGID ARTIKLI 4 PUNKTI 4 KOHALDAMISEL

Sektor	Allsektor	Üksuse liik
1. Energeetika	a) Elekter	— Euroopa Parlamendi ja nõukogu direktiivi 2009/72/EÜ ([1]) artikli 2 punktis 35 määratletud elektriettevõtja, kes täidab nimetatud direktiivi artikli 2 punktis 19 määratletud tarnimise ülesannet
		— Direktiivi 2009/72/EÜ artikli 2 punktis 6 määratletud jaotusvõrguettevõtjad
		— Direktiivi 2009/72/EÜ artikli 2 punktis 4 määratletud põhivõrguettevõtjad
	b) Nafta	— Naftajuhtmete operaatorid
		— Nafta tootmise, rafineerimise ja töötlemise rajatiste ning hoiustamise ja ülekandmisega tegelevad operaatorid
	c) Gaas	— Euroopa Parlamendi ja nõukogu direktiivi 2009/73/EÜ ([2]) artikli 2 punktis 8 määratletud tarneettevõtjad
		— Direktiivi 2009/73/EÜ artikli 2 punktis 6 määratletud jaotussüsteemi haldurid
		— Direktiivi 2009/73/EÜ artikli 2 punktis 4 määratletud ülekandesüsteemi haldurid
		— Direktiivi 2009/73/EÜ artikli 2 punktis 10 määratletud hoidlatevõrgu haldurid
		— Direktiivi 2009/73/EÜ artikli 2 punktis 12 määratletud maagaasi veeldusjaamade haldurid
		— Direktiivi 2009/73/EÜ artikli 2 punktis 1 määratletud maagaasiettevõtjad
		— Maagaasi rafineerimise ja töötlemise rajatiste haldurid
2. Transport	a) Lennutransport	— Euroopa Parlamendi ja nõukogu määruse (EÜ) nr 300/2008 ([3]) artikli 3 punktis 4 määratletud lennuettevõtjad
		— Euroopa Parlamendi ja nõukogu direktiivi 2009/12/EÜ ([4]) artikli 2 punktis 2 määratletud lennujaama juhtorganid, nimetatud direktiivi artikli 2 punktis 1 määratletud lennujaamad, sealhulgas Euroopa Parlamendi ja nõukogu määruse (EL) nr 1315/2013 ([5]) II lisa 2. jaos loetletud põhivõrgu lennujaamad ning lennujaamades olevaid abirajatisi käitavad üksused

Sektor	Allsektor	Üksuse liik
		— Euroopa Parlamendi ja nõukogu määruse (EÜ) nr 549/2004 ([6]) artikli 2 punktis 1 määratletud lennujuhtimise teenust osutavad liikluskorraldusettevõtjad
	b) Raudteetransport	— Euroopa Parlamendi ja nõukogu direktiivi 2012/34/EL ([7]) artikli 3 punktis 2 määratletud raudteeinfrastruktuuri-ettevõtjad
		— Direktiivi 2012/34/EL artikli 3 punktis 1 määratletud raudteeveo-ettevõtjad, sealhulgas direktiivi 2012/34/EL artikli 3 punktis 12 määratletud teenindusrajatiste käitajad
	c) Veetransport	— Euroopa Parlamendi ja nõukogu määruse (EÜ) nr 725/2004 ([8]) I lisas meretranspordi puhul määratletud reisijate ja kauba vedamisega sisevetes, merel ja rannavetes tegelevad ettevõtjad, v.a kõnealuste ettevõtjate käitatud üksikud laevad
		— Euroopa Parlamendi ja nõukogu direktiivi 2005/65/EÜ ([9]) artikli 3 punktis 1 määratletud sadamate valdajad, sealhulgas nende määruse (EÜ) nr 725/2004 artikli 2 punktis 11 määratletud sadamarajatised ning sadamates tööde ja varustuse haldamisega tegelevad üksused
		— Euroopa Parlamendi ja nõukogu direktiivi 2002/59/EÜ ([10]) artikli 3 punktis o määratletud laevaliikluse juhtimise keskuste operaatorid
	d) Maanteetransport	— Komisjoni delegeeritud määruse (EL) 2015/962 ([11]) artikli 2 punktis 12 määratletud maanteeametid, kes vastutavad liikluskorralduse eest
		— Euroopa Parlamendi ja nõukogu direktiivi 2010/40/EL ([12]) artikli 4 punktis 1 määratletud intelligentsete transpordisüsteemide operaatorid
3. Pangandus		Euroopa Parlamendi ja nõukogu määruse (EL) nr 575/2013 ([13]) artikli 4 punktis 1 määratletud krediidiasutused
4. Finantsturu taristu		— Euroopa Parlamendi ja nõukogu direktiivi 2014/65/EL ([14]) artikli 4 punktis 24 määratletud kauplemiskohtade korraldajad
		— Euroopa Parlamendi ja nõukogu määruse (EL) nr 648/2012 ([15]) artikli 2 punktis 1 määratletud keskne vastaspool
5. Tervishoiusektor	Tervishoiuasutused (kaasa arvatud haiglad ja erakliinikud)	Euroopa Parlamendi ja nõukogu direktiivi 2011/24/EL ([16]) artikli 3 punktis g määratletud tervishoiuteenuse osutajad

Sektor	Allsektor	Üksuse liik
6. Joogivee varustus ja jaotamine		Nõukogu direktiivi 98/83/EÜ [17] artikli 2 punkti 1 alapunktis a määratletud olmeveega varustajad ja olmevee jaotajad, v.a jaotajad, kelle puhul olmevee jaotamine moodustab vaid ühe osa nende muude tarbekaupade ja kaupade tarnimisega, mida ei loeta oluliseks teenuseks, seotud üldisest tegevusest
7. Digitaalne taristu		— IXPd
		— Domeeninimede süsteemi teenuse osutajad
		— Tippdomeeninimede registrid

(1) Euroopa Parlamendi ja nõukogu 13. juuli 2009. aasta direktiiv 2009/72/EÜ, mis käsitleb elektrienergia siseturu ühiseeskirju ning millega tunnistatakse kehtetuks direktiiv 2003/54/EÜ (ELT L 211, 14.8.2009, lk 55).
(2) Euroopa Parlamendi ja nõukogu 13. juuli 2009. aasta direktiiv 2009/73/EÜ, mis käsitleb maagaasi siseturu ühiseeskirju ning millega tunnistatakse kehtetuks direktiiv 2003/55/EÜ (ELT L 211, 14.8.2009, lk 94).
(3) Euroopa Parlamendi ja nõukogu 11. märtsi 2008. aasta määrus (EÜ) nr 300/2008, mis käsitleb tsiviillennundusjulgestuse ühiseeskirju ja millega tunnistatakse kehtetuks määrus (EÜ) nr 2320/2002 (ELT L 97, 9.4.2008, lk 72).
(4) Euroopa Parlamendi ja nõukogu 11. märtsi 2009. aasta direktiiv 2009/12/EÜ, lennujaamatasude kohta (ELT L 70, 14.3.2009, lk 11).
(5) Euroopa Parlamendi ja nõukogu 11. detsembri 2013. aasta määrus (EL) nr 1315/2013 üleeuroopalise transpordivõrgu arendamist käsitlevate liidu suuniste kohta ja millega tunnistatakse kehtetuks otsus nr 661/2010/EL (ELT L 348, 20.12.2013, lk 1).
(6) Euroopa Parlamendi ja nõukogu 10. märtsi 2004. aasta määrus (EÜ) nr 549/2004, millega sätestatakse raamistik ühtse Euroopa taeva loomiseks (raammäärus) (ELT L 96, 31.3.2004, lk 1).
(7) Euroopa Parlamendi ja nõukogu 21. novembri 2012. aasta direktiiv 2012/34/EL, millega luuakse ühtne Euroopa raudteepiirkond (ELT L 343, 14.12.2012, lk 32).
(8) Euroopa Parlamendi ja nõukogu 31. märtsi 2004. aasta määrus (EÜ) nr 725/2004 laevade ja sadamarajatiste turvalisuse tugevdamise kohta (ELT L 129, 29.4.2004, lk 6).
(9) Euroopa Parlamendi ja nõukogu 26. oktoobri 2005. aasta direktiiv 2005/65/EÜ sadamate turvalisuse tugevdamise kohta (ELT L 310, 25.11.2005, lk 28).
(10) Euroopa Parlamendi ja nõukogu 27. juuni 2002. aasta direktiiv 2002/59/EÜ, millega luuakse ühenduse laevaliikluse seire- ja teabesüsteem ning tunnistatakse kehtetuks nõukogu direktiiv 93/75/EMÜ (EÜT L 208, 5.8.2002, lk 10).
(11) Komisjoni 18. detsembri 2014. aasta delegeeritud määrus (EL) 2015/962, millega täiendatakse Euroopa Parlamendi ja nõukogu direktiivi 2010/40/EL kogu ELis reaalajas saadava liiklusteabe teenuste pakkumise osas (ELT L 157, 23.6.2015, lk 21).
(12) Euroopa Parlamendi ja nõukogu 7. juuli 2010. aasta direktiiv 2010/40/EL, mis käsitleb raamistikku intelligentsete transpordisüsteemide kasutuselevõtmiseks maanteetranspordis ja liideste jaoks teiste transpordiliikidega (ELT L 207, 6.8.2010, lk 1).
(13) Euroopa Parlamendi ja nõukogu 26. juuni 2013. aasta määrus (EL) nr 575/2013 krediidiasutuste ja investeerimisühingute suhtes kohaldatavate usaldatavusnõuete kohta ja määruse (EL) nr 648/2012 muutmise kohta (ELT L 176, 27.6.2013, lk 1).
(14) Euroopa Parlamendi ja nõukogu 15. mai 2014. aasta direktiiv 2014/65/EL finantsinstrumentide turgude kohta ning millega muudetakse direktiive 2002/92/EÜ ja 2011/61/EL (ELT L 173, 12.6.2014, lk 349).
(15) Euroopa Parlamendi ja nõukogu 4. juuli 2012. aasta määrus (EL) nr 648/2012 börsiväliste tuletisinstrumentide, kesksete vastaspoolte ja kauplemisteabehoidlate kohta (ELT L 201, 27.7.2012, lk 1).
(16) Euroopa Parlamendi ja nõukogu 9. märtsi 2011. aasta direktiiv 2011/24/EL patsiendiõiguste kohaldamise kohta piiriüleses tervishoius (ELT L 88, 4.4.2011, lk 45).
(17) Nõukogu 3. novembri 1998. aasta direktiiv 98/83/EÜ olmevee kvaliteedi kohta (EÜT L 330, 5.12.1998, lk 32).

III LISA

DIGITAALSETE TEENUSTE LIIGID ARTIKLI 4 PUNKTI 5 KOHALDAMISEL

1. Internetipõhine kauplemiskoht
2. Internetipõhine otsingumootor
3. Pilvandmetöötlusteenus