KOMISJONI RAKENDUSMÄÄRUS (EL) 2018/151,

30. jaanuar 2018,

millega nähakse ette Euroopa Parlamendi ja nõukogu direktiivi (EL) 2016/1148 kohaldamise eeskirjad, et täpsustada elemendid, mida digitaalse teenuse osutajad peavad võrgu- ja infosüsteemide turvalisust ohustavate riskide haldamiseks arvesse võtma, ja parameetrid, mille põhjal tehakse kindlaks intsidendi mõju olulisus

EUROOPA KOMISJON,

võttes arvesse Euroopa Liidu toimimise lepingut,

võttes arvesse Euroopa Parlamendi ja nõukogu 6. juuli 2016. aasta direktiivi (EL) 2016/1148 meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus, ([1]) eriti selle artikli 16 lõiget 8,

ning arvestades järgmist:

(1) Direktiivi (EL) 2016/1148 kohaselt on digitaalse teenuse osutajatel vabadus võtta tehnilisi ja korralduslikke meetmeid, mida nad peavad oma võrgu- ja infosüsteemide turvalisust ohustavate riskide haldamiseks asjakohaseks ja proportsionaalseks, tingimusel et nende meetmetega tagatakse asjakohane turvalisuse tase ning võetakse arvesse direktiiviga ette nähtud elemente.

(2) Asjakohaste ja proportsionaalsete tehniliste ja korralduslike meetmete kindlakstegemiseks peaks digitaalse teenuse osutaja käsitlema infoturvet süsteemselt, rakendades riskipõhist lähenemisviisi.

(3) Süsteemide ja rajatiste turvalisuse tagamiseks peaksid digitaalse teenuse osutajad korraldama hindamisi ja analüüse. Need peaksid käsitlema järgimisi aspekte: võrgu- ja infosüsteemide süsteemne haldamine, füüsiline ja keskkonnaga seotud turvalisus, tarnete turvalisus ning juurdepääsukontroll.

(4) Kui digitaalse teenuse osutajad teevad võrgu- ja infosüsteemide süsteemse haldamise raames riskianalüüsi, tuleks neil soovitada välja selgitada spetsiifilised riskid ja kirjeldada kvantitatiivsete näitajate abil nende olulisust, näiteks võiks kindlaks teha elutähtsat vara ähvardavad ohud ja nende võimaliku mõju tegevusele ning otsustada, kuidas neid olemasoleva suutlikkuse ja nõutavate ressursside alusel kõige paremini leevendada.

(5) Personalipoliitika võiks hõlmata oskuste kujundamist, sealhulgas turvalisusega seotud oskuste arendamist ja teadlikkuse suurendamist puudutavaid aspekte. Tegevuse turvalisust käsitlevate põhimõtete üle otsustamisel peaksid digitaalse teenuse osutajad võtma arvesse muutuste juhtimise, haavatavustegurite haldamise, tegevus- ja haldustavade formaliseerimise ja süsteemide kaardistamise aspekte.

(6) Turvaarhitektuuri põhimõtted võiksid eelkõige hõlmata võrkude ja süsteemide lahusust ning konkreetseid turbemeetmeid elutähtsate toimingute, nagu haldustoimingute jaoks. Võrkude ja süsteemide lahusus võiks võimaldada digitaalse teenuse osutajal eristada selliseid elemente nagu andmevood ja andmetöötlusressursid, mis kuuluvad kliendile, klientide rühmale, digitaalse teenuse osutajale või kolmandatele isikutele.

(7) Füüsilise ja keskkonnaga seotud turvalisuse kindlustamiseks võetavad meetmed peaksid tagama organisatsiooni võrgu- ja infosüsteemide turvalisuse selliste ohtude põhjustatud intsidentide puhul nagu vargus, tulekahju, üleujutus või muud ilmastikuolud, telekommunikatsiooniprobleemid või voolukatkestused.

(8) Elektri-, kütuse- või jahutusenergiaga varustamise kindlus võiks katta ka tarneahelat, mis hõlmab eelkõige väliste töövõtjate ja alltöövõtjate ning nende juhtimisega seotud turvalisust. Elutähtsate tarnete jälgitavus tähendab digitaalse teenuse osutaja suutlikkust teha kindlaks ja registreerida nende tarnete allikad.

(9) Digitaalse teenuse kasutajatena tuleks käsitada füüsilisi ja juriidilisi isikuid, kes on internetipõhise kauplemiskoha või pilvandmetöötlusteenuse kliendid või tellijad või kes külastavad internetipõhise otsingumootori veebisaiti märksõnaotsingu tegemiseks.

([1]) ELT L 194, 19.7.2016, lk 1.

(10) Intsidendi mõju olulisuse kindlaksmääramisel tuleks käesolevas määruses nimetatud juhtumitesse suhtuda kui oluliste intsidentide mitteammendavasse loetelusse. Käesoleva määruse rakendamisest ja tööst, mida koostöörühm teeb, et koguda parimaid tavasid riskide ja intsidentide kohta ning arutada intsidentidest teatamise korra üle vastavalt direktiivi (EL) 2016/1148 artikli 11 lõike 3 punktidele i ja m, tuleks teha järeldusi. Tulemuseks võiksid olla põhjalikud suunised selle kohta, milliste teatamisparameetrite kvantitatiivsete piirmäärade ületamise korral tekib digitaalse teenuse osutajal direktiivi (EL) 2016/1148 artikli 16 lõike 3 kohane teatamiskohustus. Kui see on asjakohane, võiks komisjon kaaluda ka määruses praegu sätestatud piirmäärade läbivaatamist.

(11) Selleks et pädevaid asutusi oleks võimalik potentsiaalsetest uutest riskidest teavitada, tuleks julgustada digitaalse teenuse pakkujaid vabatahtlikult teatama intsidentidest, mille omadustega nad ei ole varem kokku puutunud, nagu uued nõrkuste ärakasutamise moodused, ründevektorid või ohusubjektid, haavatavused ja ohud.

(12) Käesolevat määrust tuleks hakata kohaldama alates direktiivi (EL) 2016/1148 ülevõtmise tähtaja möödumisele järgnevast päevast.

(13) Käesoleva määrusega ette nähtud meetmed on kooskõlas direktiivi (EL) 2016/1148 artiklis 22 nimetatud võrgu- ja infoturbesüsteemide komitee arvamusega,

ON VASTU VÕTNUD KÄESOLEVA MÄÄRUSE:

Artikkel 1

Reguleerimisese

Käesolevas määruses täpsustatakse, milliseid elemente peavad digitaalse teenuse pakkujad arvesse võtma, kui nad määravad kindlaks ja võtavad meetmeid, et tagada direktiivi (EL) 2016/1148 III lisas nimetatud teenuste osutamiseks kasutatavate võrgu- ja infosüsteemide turvalisus, ning täpsustatakse parameetrid, mida võetakse arvesse intsidendi mõju olulisuse kindlakstegemiseks.

Artikkel 2

Turvalisuse elemendid

1. Direktiivi (EL) 2016/1148 artikli 16 lõike 1 punktis a nimetatud süsteemide ja rajatiste turvalisus tähendab võrgu- ja infosüsteemide ning nende füüsilise keskkonna turvalisust ja hõlmab järgimisi elemente:

a) võrgu- ja infosüsteemide süsteemne haldamine, mis tähendab infosüsteemide kaardistamist ja asjakohaste põhimõtete väljatöötamist infoturbe haldamise, sealhulgas riskianalüüsi, personali, toimingute turvalisuse, turvaarhitektuuri, andmete ja süsteemi elutsükli turvalise haldamise ning vajaduse korral krüpteerimise ja selle haldamise jaoks;

b) füüsiline ja keskkonnaga seotud turvalisus, mis tähendab, et olemas on meetmed, millega kaitstakse digitaalse teenuse osutaja võrgu- ja infosüsteemide turvalisust kahju eest, rakendades kõiki ohte hõlmavat riskipõhist lähenemisviisi, mille puhul tegeldakse näiteks süsteemitõrgete, inimeksimuste, pahatahtliku tegevuse ja loodusnähtustega;

c) tarnete turvalisus, mis tähendab asjakohaste põhimõtete väljatöötamist ja säilitamist, et tagada teenuste osutamiseks kasutatavate peamiste tarnete kättesaadavus ja vajaduse korral jälgitavus;

d) võrgu- ja infosüsteemidele juurdepääsu kontroll, mis tähendab, et olemas on meetmed, millega tagatakse, et võrgu- ja infosüsteemide füüsilise ja loogilise juurdepääsu, sealhulgas võrgu- ja infosüsteemide haldusturvalisuse jaoks kasutatakse talitlus- ja turvanõuetel põhinevaid volitusi ja piiranguid.

2. Direktiivi (EL) 2016/1148 artikli 16 lõike 1 punktis b nimetatud intsidentide käsitlemisel hõlmavad digitaalse teenuse osutaja võetavad meetmed järgmist:

a) tuvastamisprotsessid ja -menetlused, mida hoitakse alal ja testitakse, et tagada õigeaegne ja piisav teadlikkus anomaalsetest juhtumitest;

b) intsidentidest teatamise ja infosüsteemide nõrkade kohtade ja haavatavuste kindlakstegemise protsessid ja põhimõtted;

c) kehtestatud korra kohane reageerimine ja võetud meetmete tulemustest teatamine;

d) intsidendi raskusastme hindamine, intsidendianalüüsi põhjal saadud teadmuse dokumenteerimine ja sellise asjakohase info kogumine, mida saab kasutada tõendusmaterjalina ja mille põhjal saab protsesse pidevalt täiustada.

3. Direktiivi (EL) 2016/1148 artikli 16 lõike 1 punktis c nimetatud talitluspidevuse haldamine tähendab organisatsiooni suutlikkust säilitada või vajaduse korral taastada pärast häirivat intsidenti teenuste osutamine varem kokku lepitud vastuvõetaval tasemel ja see hõlmab järgmist:

a) toime analüüsi põhjal koostatud hädaolukorra lahendamise kavade koostamine ja kasutamine, et tagada digitaalse teenuse osutajate poolse teenuse pakkumise järjepidevus, mida hinnatakse ja testitakse regulaarselt, näiteks õppuste kaudu;

b) avariitaastesuutlikkus, mida hinnatakse ja testitakse regulaarselt, näiteks õppuste kaudu.

4. Direktiivi (EL) 2016/1148 artikli 16 lõike 1 punktis d nimetatud seire, auditeerimine ja testimine hõlmab põhimõtete väljatöötamist ja rakendamist, et reguleerida järgmist:

a) vaatluste või mõõtmiste kavandatud seeriate korraldamine, et hinnata, kas võrgu- ja infosüsteemid toimivad eesmärgipäraselt;

b) inspekteerimine ja kontrollimine, et teha kindlaks, kas standardeid või suuniseid järgitakse, andmed on täpsed ning täidetakse tõhususe ja tulemuslikkuse eesmärke;

c) protsess, mille eesmärk on tuvastada puudused võrgu- ja infosüsteemide turvamehhanismides, millega kaitstakse andmeid ja tagatakse eesmärgipärane toimimine. Selline protsess hõlmab toiminguvooga seotud tehnilisi protsesse ja personali.

5. Direktiivi (EL) 2016/1148 artikli 16 lõike 1 punktis e nimetatud rahvusvahelised standardid tähendavad standardeid, mille on vastu võtnud Euroopa Parlamendi ja nõukogu määruse (EL) nr 1025/2012 ([1]) artikli 2 lõike 1 punktis a nimetatud rahvusvaheline standardiorganisatsioon. Direktiivi (EL) 2016/1148 artikli 19 kohaselt võib kasutada ka Euroopas või rahvusvaheliselt heaks kiidetud võrgu- ja infosüsteemide turvalisuse alaseid standardeid ja spetsifikatsioone, sealhulgas liikmesriikide standardeid.

6. Digitaalse teenuse osutajad tagavad, et neil on olemas asjakohased dokumendid, mille alusel pädevad asutused saavad kontrollida, kas lõigetes 1, 2, 3, 4 ja 5 nimetatud turvalisuse elementidest peetakse kinni.

Artikkel 3

Parameetrid, mida tuleb intsidendi mõju olulisuse kindlakstegemiseks arvesse võtta

1. Direktiivi (EL) 2016/1148 artikli 16 lõike 4 punktis a nimetatud intsidendist mõjutatud kasutajate ja eelkõige nende kasutajate arvu osas, kes sõltuvad asjaomasest teenusest oma teenuste osutamisel, peab digitaalse teenuse osutajal olema võimalik hinnata üht järgmistest:

a) selliste mõjutatud füüsiliste ja juriidiliste isikute arv, kellega on teenuse osutamiseks sõlmitud leping, või

b) teenust kasutanud mõjutatud kasutajate arv, mille aluseks on eelkõige varasemad andmeliiklusandmed.

2. Artikli 16 lõike 4 punktis b nimetatud intsidendi kestus tähendab ajavahemikku alates hetkest, mil teenuse osutamine katkeb käideldavuse, autentsuse, tervikluse või konfidentsiaalsuse seisukohast, kuni selle taastamiseni.

3. Direktiivi (EL) 2016/1148 artikli 16 lõike 4 punktis c nimetatud intsidendist mõjutatud geograafilise ala ulatuse osas peab digitaalse teenuse pakkujal olema võimalik kindlaks teha, kas intsident mõjutab tema teenuste osutamist konkreetsetes liikmesriikides.

4. Direktiivi (EL) 2016/1148 artikli 16 lõike 4 punktis d nimetatud teenuse toimimise katkestuse ulatuse mõõtmisel võetakse arvesse üht või mitut järgmistest komponentidest, mida intsident on kahjustanud: andmete või seonduvate teenuste käideldavus, autentsus, terviklus ja konfidentsiaalsus.

([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).

5. Direktiivi (EL) 2016/1148 artikli 16 lõike 4 punktis e nimetatud majandus- ja ühiskondlikule tegevusele avalduva mõju ulatuse osas on digitaalse teenuse osutajal võimalik otsustada selliste näitajate alusel nagu tema ja kliendi lepinguliste suhete laad, või kui see on asjakohane, mõjutatud kasutajate potentsiaalne arv, kas intsident on põhjustanud kasutajatele märkimisväärset materiaalset või mittemateriaalset kahju, näiteks seoses tervise, ohutuse või varalise kahjuga.

6. Lõigete 1, 2, 3, 4 ja 5 kohaldamisel ei kohustata digitaalse teenuse osutajat koguma täiendavat infot, millele tal puudub juurdepääs.

Artikkel 4

Intsidendi oluline mõju

1. Intsidendi mõju peetakse oluliseks, kui esinenud on vähemalt üks järgmistest olukordadest:

a) digitaalse teenuse osutaja pakutav teenus ei olnud kättesaadav üle 5 000 000 kasutajatunni, kusjuures kasutajatund tähendab liidus asuvate mõjutatud kasutajate arvu kuuekümne minuti jooksul;

b) intsident on põhjustanud salvestatud, edastatud või töödeldud andmete või digitaalse teenuse osutaja võrgu- ja infosüsteemi kaudu pakutavate või juurdepääsetavate asjaomaste teenuste tervikluse, autentsuse või konfidentsiaalsuse kadu, mis mõjutab rohkem kui 100 000 kasutajat liidus;

c) intsident on seadnud ohtu avaliku ohutuse, avaliku julgeoleku või inimelu;

d) intsident on põhjustanud liidus vähemalt ühele kasutajale materiaalset kahju, mis ületab 1 000 000 eurot.

2. Komisjon võib lõikes 1 sätestatud piirmäärad läbi vaadata, tuginedes parimatele tavadele, mida koostöörühm on kogunud, täites direktiivi (EL) 2016/1148 artikli 11 lõikest 3 tulenevaid ülesandeid, ja artikli 11 lõike 3 punkti m kohastele aruteludele.

Artikkel 5

Jõustumine

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

2. Seda kohaldatakse alates 10. maist 2018.

Käesolev määrus on tervikuna siduv ja vahetult kohaldatav kõikides liikmesriikides.

Brüssel, 30. jaanuar 2018

Komisjoni nimel

president

Jean-Claude JUNCKER