KOMISIJAS ĪSTENOŠANAS REGULA (ES) 2018/151

(2018. gada 30. janvāris),

ar ko paredz noteikumus Eiropas Parlamenta un Padomes Direktīvas (ES) 2016/1148 piemērošanai attiecībā uz tādu elementu precizēšanu, kuri jāņem vērā digitālo pakalpojumu sniedzējiem, lai pārvaldītu riskus, kas tiek radīti tīklu un informācijas sistēmu drošībai, un tādu rādītāju precizēšanu, kuri jāņem vērā, lai noteiktu, vai incidentam ir būtiska ietekme

EIROPAS KOMISIJA,

ņemot vērā Līgumu par Eiropas Savienības darbību,

ņemot vērā Eiropas Parlamenta un Padomes 2016. gada 6. jūlija Direktīvu (ES) 2016/1148 par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā [1] un jo īpaši tās 16. panta 8. punktu,

tā kā:

(1) Saskaņā ar Direktīvu (ES) 2016/1148 digitālo pakalpojumu sniedzēji saglabā rīcības brīvību veikt tehniskus un organizatoriskus pasākumus, kurus uzskata par atbilstīgiem un samērīgiem, lai pārvaldītu risku, kas tiek radīts to tīklu un informācijas sistēmu drošībai, ar nosacījumu, ka minētie pasākumi nodrošina pienācīgu drošības līmeni un tajos ņemti vērā minētajā direktīvā noteiktie elementi.

(2) Nosakot atbilstīgus un samērīgus tehniskus un organizatoriskus pasākumus, digitālo pakalpojumu sniedzējam informācijas drošība būtu jāskata sistēmiski, izmantojot uz risku balstītu pieeju.

(3) Lai nodrošinātu sistēmu un iekārtu drošību, digitālo pakalpojumu sniedzējiem būtu jāveic novērtēšanas un analīzes procedūras. Šīm darbībām būtu jāattiecas uz tīklu un informācijas sistēmu sistemātisku pārvaldību, fizisko un vides drošību, piegādes drošību un piekļuves kontroli.

(4) Digitālo pakalpojumu sniedzēji būtu jāmudina, veicot riska analīzi tīklu un informācijas sistēmu sistemātiskā pārvaldībā, identificēt konkrētus riskus un skaitliski izmērīt to būtiskumu, piemēram, identificējot svarīgākajiem objektiem radītu apdraudējumu, nosakot, kā tas var ietekmēt darbības, kā arī to, kā labāk novērst minēto apdraudējumu, izmantojot pašreizējās spējas un vajadzīgos resursus.

(5) Cilvēkresursu politika varētu attiekties uz prasmju pārvaldību, ieskaitot aspektus, kuri saistīti ar tādu prasmju pilnveidi, kas attiecas uz drošību, un informētības uzlabošanu. Digitālo pakalpojumu sniedzēji būtu jāmudina, lemjot par atbilstīgu politiku attiecībā uz darbības drošību, ņemt vērā izmaiņu pārvaldības, ievainojamības pārvaldības, darbības un administratīvās prakses formalizēšanas un sistēmas kartēšanas aspektus.

(6) Politika, kas attiecas uz drošības arhitektūru, jo īpaši varētu aptvert tīklu un sistēmu nodalīšanu, kā arī konkrētus drošības pasākumus svarīgākajām darbībām, piemēram, administrēšanas darbībām. Tīklu un sistēmu nodalīšana varētu ļaut digitālo pakalpojumu sniedzējam tādus elementus kā datu plūsmas nošķirt no skaitļošanas resursiem, kas pieder klientam, klientu grupai, digitālo pakalpojumu sniedzējam vai trešām personām.

(7) Pasākumiem, kas veikti attiecībā uz fizisko un vides drošību, būtu jānodrošina organizācijas tīklu un informācijas sistēmu drošība no kaitējuma, ko rada tādi incidenti kā zādzība, ugunsgrēks, plūdi vai cita laikapstākļu iedarbība, telesakaru vai elektroapgādes pārtraukumi.

(8) Piegādes – piemēram, elektroenerģijas, degvielas vai dzesēšanas piegādes – drošībai būtu jāaptver piegādes ķēdes drošība, kas jo īpaši ietver ārējo darbuzņēmēju un apakšuzņēmēju drošību un to pārvaldības drošību. Svarīgāko piegāžu izsekojamība attiecas uz digitālo pakalpojumu sniedzēja spēju noteikt un reģistrēt minēto piegāžu avotus.

(9) Digitālo pakalpojumu lietotāja jēdzienam būtu jāaptver fiziskas un juridiskas personas, kas ir tiešsaistes tirdzniecības vietas vai mākoņdatošanas pakalpojuma klienti vai abonenti vai kas apmeklē tiešsaistes meklētājprogrammas vietni, lai veiktu meklēšanu pēc atslēgvārdiem.

[1] OV L 194, 19.7.2016., 1. lpp.

(10) Nosakot incidenta ietekmes būtiskumu, šajā regulā izklāstītie gadījumi būtu jāuzskata par būtisku incidentu neizsmeļošu sarakstu. No šīs regulas īstenošanas un Sadarbības grupas darba būtu jāizdara secinājumi par Direktīvas (ES) 2016/1148 11. panta 3. punkta attiecīgi i) un m) apakšpunktā minēto tādas paraugprakses informācijas vākšanu, kas attiecas uz riskiem un incidentiem, un tādas kārtības apspriešanu, kas paredzēta ziņošanai par paziņojumiem par incidentiem. Pamatojoties uz šiem secinājumiem, varētu izstrādāt visaptverošas pamatnostādnes par paziņošanas rādītāju kvantitatīvām robežvērtībām, kuras sasniedzot digitālo pakalpojumu sniedzējiem būtu jāziņo saskaņā ar Direktīvas (ES) 2016/1148 16. panta 3. punktu. Komisija attiecīgā gadījumā var arī apsvērt šajā regulā noteikto robežvērtību pārskatīšanu.

(11) Lai kompetentās iestādes varētu tikt informētas par potenciāliem jauniem riskiem, digitālo pakalpojumu sniedzēji būtu jāmudina brīvprātīgi ziņot par visiem incidentiem, kuru īpašības tiem iepriekš nav bijušas zināmas, piemēram, par jauniem mūķiem, uzbrukuma vektoriem vai apdraudējuma radītājiem, ievainojamību un apdraudējumiem.

(12) Šī regula būtu jāpiemēro nākamajā dienā pēc Direktīvas (ES) 2016/1148 transponēšanas termiņa beigām.

(13) Šajā regulā paredzētie pasākumi atbilst Direktīvas (ES) 2016/1148 22. pantā minētās Tīklu un informācijas sistēmu drošības komitejas atzinumam,

IR PIEŅĒMUSI ŠO REGULU.

1. pants

Priekšmets

Šī regula precizē elementus, kas digitālo pakalpojumu sniedzējiem jāņem vērā, nosakot un veicot pasākumus, lai nodrošinātu zināmu drošību tīklu un informācijas sistēmām, kuras tie izmanto saistībā ar Direktīvas (ES) 2016/1148 III pielikumā minēto pakalpojumu sniegšanu, un precizē rādītājus, kas jāņem vērā, lai noteiktu, vai incidentam ir būtiska ietekme uz minēto pakalpojumu sniegšanu.

2. pants

Drošības elementi

1. Direktīvas (ES) 2016/1148 16. panta 1. punkta a) apakšpunktā minētā sistēmu un iekārtu drošība ir tīklu un informācijas sistēmu un to fiziskās vides drošība, un tā iekļauj šādus elementus:

a) tīklu un informācijas sistēmu sistemātiska pārvaldība – informācijas sistēmu kartēšana un tādu atbilstīgu politikas pasākumu kopuma izstrāde, kas attiecas uz informācijas drošības pārvaldību, ieskaitot riska analīzi, cilvēkresursus, darbību drošību, drošības arhitektūru, drošus datus un sistēmas dzīves cikla pārvaldību, kā arī attiecīgā gadījumā šifrēšanu un tās pārvaldību;

b) fiziskā un vides drošība – tāda pasākumu kopuma pieejamība, kas ļauj aizsargāt digitālo pakalpojumu sniedzēju tīklu un informācijas sistēmu drošību no kaitējuma, izmantojot visus apdraudējumus aptverošu uz risku balstītu pieeju, kas ņem vērā, piemēram, sistēmas atteici, cilvēka kļūdu, ļaunprātīgu darbību vai dabas parādības;

c) piegādes drošība – tādas atbilstīgas politikas izveide un uzturēšana, kuras mērķis ir nodrošināt svarīgāko piegāžu, kas tiek izmantotas pakalpojumu sniegšanā, pieejamību un attiecīgā gadījumā izsekojamību;

d) piekļuves tīklu un informācijas sistēmām kontrole – tāda pasākumu kopuma pieejamība, kas nodrošina, lai fiziskā un loģiskā piekļuve tīklu un informācijas sistēmām, ieskaitot tīklu un informācijas sistēmu administratīvo drošību, būtu atļauta un ierobežota, pamatojoties uz darbības nodrošināšanas un drošības prasībām.

2. Attiecībā uz Direktīvas (ES) 2016/1148 16. panta 1. punkta b) apakšpunktā minēto incidentu risināšanu digitālo pakalpojumu sniedzēja īstenotie pasākumi ietver:

a) atklāšanas procesus un procedūras, kas tiek uzturētas un testētas, lai nodrošinātu laicīgu un pienācīgu informētību par anomāliem notikumiem;

b) procesus un politiku, kas attiecas uz ziņošanu par incidentiem un trūkumu un ievainojamības konstatēšanu tā informācijas sistēmā;

c) reaģēšanu saskaņā ar noteiktajām procedūrām un veikto pasākumu rezultātu paziņošanu;

d) incidenta smaguma pakāpes novērtējumu, incidenta analīzes rezultātā iegūto zināšanu dokumentēšanu un tādas attiecīgas informācijas vākšanu, kas var kalpot par pierādījumu un sekmēt nepārtrauktu uzlabojumu procesu.

3. Direktīvas (ES) 2016/1148 16. panta 1. punkta c) apakšpunktā minētā darbības nepārtrauktības pārvaldība ir organizācijas spēja uzturēt vai attiecīgā gadījumā pēc traucējumus radījuša incidenta atjaunot pakalpojumu sniegšanu pieņemamā iepriekš noteiktā līmenī, un tā ietver:

a) tādu ārkārtas rīcības plānu izstrādi un izmantošanu, kuru pamatā ir ietekmes uz darbību analīze, kuri paredzēti digitālo pakalpojumu sniedzēju sniegto pakalpojumu nepārtrauktības nodrošināšanai un kurus regulāri novērtē un testē, piemēram, mācību pasākumos;

b) negadījuma seku novēršanas spējas, ko regulāri novērtē un testē, piemēram, mācību pasākumos.

4. Direktīvas (ES) 2016/1148 16. panta 1. punkta d) apakšpunktā minētās uzraudzība, revīzijas un pārbaudes ietver tādas politikas izstrādi un uzturēšanu, kura attiecas uz:

a) plānotu, secīgu novērojumu vai mērījumu veikšanu, lai novērtētu, vai tīklu un informācijas sistēmas darbojas tā, kā paredzēts;

b) inspicēšanu un verificēšanu, lai pārbaudītu atbilstību standartam vai vadlīniju kopumam, uzskaites pareizību un efektivitātes un rezultativitātes mērķu izpildi;

c) procesu, kas paredzēts, lai atklātu trūkumus tīklu un informācijas sistēmas drošības mehānismos, kas atbilstīgā veidā aizsargā datus un uztur funkcijas. Šādi procesi iekļauj tehniskos procesus un personālu, kas iesaistīts darba plūsmā.

5. Direktīvas (ES) 2016/1148 16. panta 1. punkta e) apakšpunktā minētie starptautiskie standarti ir standarti, ko pieņem starptautiska standartizācijas iestāde, kas minēta Eiropas Parlamenta un Padomes Regulas (ES) Nr. 1025/2012 ([1]) 2. panta 1. punkta a) apakšpunktā. Saskaņā ar Direktīvas (ES) 2016/1148 19. pantu var izmantot arī Eiropas vai starptautiski atzītus standartus un specifikācijas, tostarp esošus dalībvalstu standartus, kas attiecas uz tīklu un informācijas sistēmu drošību.

6. Digitālo pakalpojumu sniedzēji nodrošina atbilstošu dokumentāciju, kas ir pieejama, lai kompetentā iestāde varētu pārbaudīt atbilstību drošības elementiem, kas noteikti 1., 2., 3., 4. un 5. punktā.

3. pants

Rādītāji, kas jāņem vērā, lai noteiktu, vai incidentam ir būtiska ietekme

1. Attiecībā uz incidenta skarto lietotāju – īpaši to, kuri attiecīgo pakalpojumu izmanto paši savu pakalpojumu sniegšanai, – skaitu, kas minēts Direktīvas (ES) 2016/1148 16. panta 4. punkta a) apakšpunktā, digitālo pakalpojumu sniedzējam jāspēj aplēst vai nu:

a) tādu incidenta skarto fizisko un juridisko personu skaitu, ar kurām ir noslēgts līgums par pakalpojuma sniegšanu; vai

b) to incidenta skarto lietotāju skaitu, kuri ir izmantojuši attiecīgo pakalpojumu, un šo skaitu nosaka, galvenokārt pamatojoties uz iepriekšējās informācijas plūsmas datiem.

2. 16. panta 4. punkta b) apakšpunktā minētais incidenta ilgums ir laika periods no brīža, kad pakalpojuma pienācīga sniegšana pārtraukta pieejamības, autentiskuma, integritātes vai konfidencialitātes ziņā, līdz atkopes brīdim.

3. Attiecībā uz Direktīvas (ES) 2016/1148 16. panta 4. punkta c) apakšpunktā minēto ģeogrāfisko izplatību attiecībā uz incidenta skarto vidi digitālo pakalpojumu sniedzējam jāspēj noteikt, vai incidents ietekmē tā pakalpojumu sniegšanu konkrētās dalībvalstīs.

4. Direktīvas (ES) 2016/1148 16. panta 4. punkta d) apakšpunktā minēto traucētas pakalpojumu darbības apmēru mēra attiecībā uz vienu vai vairākiem no šiem incidenta skartajiem aspektiem: datu vai saistīto pakalpojumu pieejamība, autentiskums, integritāte vai konfidencialitāte.

([1]) Eiropas Parlamenta un Padomes 2012. gada 25. oktobra Regula (ES) Nr. 1025/2012 par Eiropas standartizāciju, ar ko groza Padomes Direktīvas 89/686/EEK un 93/15/EEK un Eiropas Parlamenta un Padomes Direktīvas 94/9/EK, 94/25/EK, 95/16/EK, 97/23/EK, 98/34/EK, 2004/22/EK, 2007/23/EK, 2009/23/EK un 2009/105/EK un ar ko atceļ Padomes Lēmumu 87/95/EEK un Eiropas Parlamenta un Padomes Lēmumu Nr. 1673/2006/EK (OV L 316, 14.11.2012., 12. lpp.).

5. Attiecībā uz Direktīvas (ES) 2016/1148 16. panta 4. punkta e) apakšpunktā minēto tādas ietekmes apmēru, kas radīta uz ekonomiskajām un sabiedriskajām darbībām, digitālo pakalpojumu sniedzējam, pamatojoties uz tādām norādēm kā tā un klienta līgumisko attiecību raksturs vai attiecīgā gadījumā skarto lietotāju potenciālais skaits, jāspēj secināt, vai incidents ir radījis būtiskus materiālus vai nemateriālus zaudējumus lietotājiem, piemēram, saistībā ar veselību, drošību vai kaitējumu īpašumam.

6. Piemērojot šā panta 1., 2., 3., 4. un 5. punktu, digitālo pakalpojumu sniedzējiem nav pienākuma vākt papildu informāciju, kas tiem nav pieejama.

4. pants

Incidenta būtiska ietekme

1. Uzskatāms, ka incidentam ir būtiska ietekme, ja ir radusies vismaz viena no šādām situācijām:

a) digitālo pakalpojumu sniedzēja sniegtais pakalpojums nav bijis pieejams vairāk kā 5 000 000 lietotājstundu, un "lietotājstunda" šajā gadījumā ir sešdesmit minūšu laikā skarto lietotāju skaits Savienībā;

b) incidenta rezultātā ir zudusi glabāto, nosūtīto vai apstrādāto datu vai saistīto pakalpojumu, kurus sniedz vai kam var piekļūt ar digitālo pakalpojumu sniedzēja tīklu un informācijas sistēmas palīdzību, integritāte, autentiskums vai konfidencialitāte, un tas ir ietekmējis vairāk nekā 100 000 lietotāju Savienībā;

c) incidents ir radījis briesmas sabiedrībai, risku sabiedrības drošībai vai draudus dzīvībai;

d) incidents ir radījis materiālus zaudējumus vismaz vienam lietotājam Savienībā, ja minētajam lietotājam radītie zaudējumi pārsniedz EUR 1 000 000.

2. Pamatojoties uz paraugpraksi, ko saskaņā ar Direktīvas (ES) 2016/1148 11. panta 3. punktu apzinājusi Sadarbības grupa, un apspriešanu saskaņā ar minētās direktīvas 11. panta 3. punkta m) apakšpunktu, Komisija var pārskatīt 1. punktā noteiktās robežvērtības.

5. pants

Stāšanās spēkā

1. Šī regula stājas spēkā divdesmitajā dienā pēc tās publicēšanas *Eiropas Savienības Oficiālajā Vēstnesī*.

2. To piemēro no 2018. gada 10. maija.

Šī regula uzliek saistības kopumā un ir tieši piemērojama visās dalībvalstīs.

Briselē, 2018. gada 30. janvārī

Komisijas vārdā –
priekšsēdētājs
Jean-Claude JUNCKER