2024/1772

25.6.2024.

KOMISIJAS DELEĢĒTĀ REGULA (ES) 2024/1772

(2024. gada 13. marts),

ar ko Eiropas Parlamenta un Padomes Regulu (ES) 2022/2554 papildina attiecībā uz regulatīvajiem tehniskajiem standartiem, kuros precizēti kritēriji ar IKT saistītu incidentu un kiberdraudu klasifikācijai, nosakot būtiskuma robežvērtības un precizējot sīkāku informāciju, kas ietverama ziņojumos par būtiskiem incidentiem

(Dokuments attiecas uz EEZ)

EIROPAS KOMISIJA,

ņemot vērā Līgumu par Eiropas Savienības darbību,

ņemot vērā Eiropas Parlamenta un Padomes Regulu (ES) 2022/2554 (2022. gada 14. decembris) par finanšu nozares digitālās darbības noturību un ar ko groza Regulas (EK) Nr. 1060/2009, (ES) Nr. 648/2012, (ES) Nr. 600/2014, (ES) Nr. 909/2014 un (ES) 2016/1011 ([1]), un jo īpaši tās 18. panta 4. punkta trešo daļu,

tā kā:

(1) Ņemot vērā to, ka Regulas (ES) 2022/2554 mērķis ir saskaņot un racionalizēt prasības ar IKT saistītu incidentu un ar maksājumiem saistītu darbības vai drošības incidentu paziņošanai, kas skar kredītiestādes, maksājumu iestādes, konta informācijas pakalpojumu sniedzējus un elektroniskās naudas iestādes ("incidenti"). Ņemot vērā to, ka ziņošanas prasības attiecas uz 20 dažādiem finanšu vienību veidiem, klasifikācijas kritēriji un būtiskuma robežvērtības būtisku incidentu un būtisku kiberdraudu noteikšanai būtu jāprecizē vienkāršā, saskaņotā un konsekventā veidā, ņemot vērā visu attiecīgo finanšu vienību pakalpojumu un darbību specifiku.

(2) Lai nodrošinātu proporcionalitāti, klasifikācijas kritērijiem un būtiskuma robežvērtībām būtu jāatspoguļo visu finanšu vienību lielums un vispārējais riska profils, kā arī pakalpojumu veids, mērogs un sarežģītība. Turklāt kritēriji un būtiskuma robežvērtības būtu jāizstrādā tā, lai tie vienādi attiektos uz visām finanšu vienībām neatkarīgi no to lieluma un riska profila un neradītu nesamērīgu ziņošanas slogu mazākām finanšu vienībām. Tomēr, lai risinātu situācijas, kad incidents ietekmē ievērojamu skaitu klientu, bet kas nepārsniedz piemērojamo robežvērtību, būtu jānosaka absolūta robežvērtība, kas galvenokārt vērsta uz lielākām finanšu vienībām.

(3) Attiecībā uz incidentu ziņošanas sistēmām, kas pastāvēja pirms Regulas (ES) 2022/2554 stāšanās spēkā, būtu jānodrošina finanšu vienību darbības nepārtrauktība. Tāpēc klasifikācijas kritēriji un būtiskuma robežvērtības būtu jāsaskaņo ar EBI pamatnostādnēm par ziņošanu par būtiskiem incidentiem saskaņā ar Eiropas Parlamenta un Padomes Direktīvu (ES) 2015/2366 ([2]), Pamatnostādnēm par periodisku informāciju un būtisku izmaiņu paziņošanu, kas darījumu reģistriem jāsniedz EVTI, ECB/VUM kiberincidentu ziņošanas sistēmu un citiem būtiskiem norādījumiem. Klasifikācijas kritērijiem un būtiskuma robežvērtībām vajadzētu būt piemērotām arī tādām finanšu vienībām, uz kurām pirms Regulas (ES) 2022/2554 stāšanās spēkā neattiecās ziņošanas prasības par incidentiem.

(4) Attiecībā uz klasifikācijas kritēriju "skarto darījumu apjoms un skaits" darījumu jēdziens ir plašs un aptver dažādas darbības un pakalpojumus visos finanšu vienībām piemērojamajos nozaru tiesību aktos. Minētā klasifikācijas kritērija nolūkā būtu jāaptver maksājumu darījumi un visu veidu apmaiņa ar finanšu instrumentiem, kriptoaktīviem, precēm vai jebkuriem citiem aktīviem, tostarp drošības rezerves, nodrošinājuma vai ķīlas veidā gan pret naudu, gan pret jebkuru citu aktīvu. Klasifikācijas nolūkā būtu jāņem vērā visi darījumi, kas ietver aktīvus, kuru vērtību var izteikt naudas summā.

([1]) OV L 333, 27.12.2022., 1. lpp., ELI: http://data.europa.eu/eli/reg/2022/2554/oj.

([2]) Eiropas Parlamenta un Padomes Direktīva (ES) 2015/2366 (2015. gada 25. novembris) par maksājumu pakalpojumiem iekšējā tirgū, ar ko groza Direktīvas 2002/65/EK, 2009/110/EK un 2013/36/ES un Regulu (ES) Nr. 1093/2010 un atceļ Direktīvu 2007/64/EK (OV L 337, 23.12.2015., 35. lpp., ELI: http://data.europa.eu/eli/dir/2015/2366/oj).

(5) Klasifikācijas kritērijiem būtu jānodrošina, ka tiek aptverti visi attiecīgie būtisku incidentu veidi. Kiberuzbrukumi, kas saistīti ar ielaušanos tīklos vai informācijas sistēmās, var nebūt ietverti daudzos klasifikācijas kritērijos. Tomēr tie ir svarīgi, jo jebkāda ielaušanās tīklu un informācijas sistēmās var kaitēt finanšu vienībai. Tādēļ klasifikācijas kritēriji "skartie kritiskie pakalpojumi" un "datu zudumi" būtu jāprecizē tā, lai aptvertu šāda veida būtiskus incidentus, jo īpaši neatļautu ielaušanos, kas, pat ja ietekme nav uzreiz zināma, var radīt nopietnas sekas, jo īpaši datu aizsardzības pārkāpumus un datu noplūdi.

(6) Tā kā uz kredītiestādēm attiecas gan Regulas (ES) 2022/2554 18. pantā izklāstītā incidentu klasifikācijas sistēma, gan operacionālā riska regulējums saskaņā ar Komisijas Deleģēto regulu (ES) 2018/959 ([3]), pieejai incidenta ekonomiskās ietekmes novērtēšanai, kuras pamatā ir izmaksu un zaudējumu aprēķins, vajadzētu būt pēc iespējas konsekventākai abos regulējumos, lai izvairītos no nesaderīgu vai pretrunīgu prasību ieviešanas.

(7) Regulas (ES) 2022/2554 18. panta 1. punkta c) apakšpunktā izklāstītajam kritērijam attiecībā uz incidenta ģeogrāfisko izplatību būtu jākoncentrējas uz incidenta pārrobežu ietekmi, jo incidenta ietekme uz finanšu vienības darbībām vienā jurisdikcijā tiks aptverta ar citiem minētajā pantā izklāstītajiem kritērijiem.

(8) Ņemot vērā to, ka klasifikācijas kritēriji ir savstarpēji atkarīgi un savstarpēji saistīti, pieeja tādu būtisku incidentu identificēšanai, par kuriem jāziņo saskaņā ar Regulas (ES) 2022/2554 19. panta 1. punktu, būtu jābalsta uz kritēriju kombināciju, kurā dažiem kritērijiem, kas ir cieši saistīti ar Regulas (ES) 2022/2554 3. panta 8. un 10. punktā izklāstītajām ar IKT saistīta incidenta un būtiska ar IKT saistīta incidenta definīcijām, vajadzētu būt lielākai nozīmei būtisku incidentu klasifikācijā nekā citiem.

(9) Lai nodrošinātu, ka ziņojumi un paziņojumi par būtiskiem incidentiem, ko kompetentās iestādes saņēmušas saskaņā ar Regulas (ES) 2022/2554 19. panta 1. punktu, kalpo gan uzraudzības mērķiem, gan kaitīgas ietekmes izplatīšanās novēršanai visā finanšu nozarē, būtiskuma robežvērtībām būtu jāļauj aptvert būtiskus incidentus, cita starpā koncentrējoties uz ietekmi uz vienībai specifiskiem kritiskiem pakalpojumiem, konkrētām absolūtām un relatīvām klientu vai finanšu partneru robežvērtībām, darījumiem, kas norāda uz būtisku ietekmi uz finanšu vienību, un ietekmes būtiskumu citās dalībvalstīs.

(10) Incidenti, kas ietekmē tādus IKT pakalpojumus vai tīklu un informācijas sistēmas, ar ko atbalsta kritiski svarīgas vai svarīgas funkcijas, vai finanšu pakalpojumus, uz kuriem attiecas prasība saņemt atļauju, vai ļaunprātīga neatļauta piekļuve tīklu un informācijas sistēmām, ar ko atbalsta kritiski svarīgas vai svarīgas funkcijas, būtu jāuzskata par incidentiem, kas ietekmē finanšu vienību kritiski svarīgos pakalpojumus. Ļaunprātīga, neatļauta piekļuve tīklu un informācijas sistēmām, ar ko atbalsta finanšu vienību kritiski svarīgas vai svarīgas funkcijas, rada nopietnus riskus finanšu vienībai un var ietekmēt citas finanšu vienības, tāpēc tā vienmēr būtu jāuzskata par būtisku incidentu, par kuru ir jāziņo.

(11) Daudzkārtēji incidenti, kas ir saistīti ar līdzīgu acīmredzamu pamatcēloni un kas atsevišķi netiek uzskatīti par būtiskiem incidentiem, var norādīt uz būtiskiem trūkumiem un nepilnībām finanšu vienības incidenta un riska pārvaldības procedūrās. Tāpēc daudzkārtēji incidenti kopā būtu jāuzskata par būtiskiem, ja tie atkārtojas noteiktā laikposmā.

(12) Ņemot vērā to, ka kiberdraudiem var būt negatīva ietekme uz finanšu vienību un nozari, finanšu vienībām, ziņojot par būtiskajiem kiberdraudiem, būtu jānorāda uz īstenošanās iespējamību un iespējamās ietekmes kritiskumu. Attiecīgi, lai nodrošinātu skaidru un konsekventu novērtējumu par kiberdraudu nozīmīgumu, kiberdrauda klasificēšanai par būtisku vajadzētu būt atkarīgai no iespējamības, ka, ja apdraudējums īstenotos, tiktu izpildīti būtisku incidentu klasifikācijas kritēriji un sasniegta to robežvērtība, kā arī atkarīgai no kiberdraudu veida un finanšu vienībai pieejamās informācijas.

([3]) Komisijas Deleģētā regula (ES) 2018/959 (2018. gada 14. marts), ar ko attiecībā uz regulatīviem tehniskiem standartiem par novērtējuma metodikas precizējumu, saskaņā ar kuru kompetentās iestādes atļauj iestādēm izmantot attīstītās mērīšanas pieejas operacionālajam riskam, papildina Eiropas Parlamenta un Padomes Regulu (ES) Nr. 575/2013 (OV L 169, 6.7.2018., 1. lpp., ELI: http://data.europa.eu/eli/reg_del/2018/959/oj).

(13) Ņemot vērā to, ka citu dalībvalstu kompetentās iestādes ir jāinformē par incidentiem, kas ietekmē finanšu vienības un klientus to jurisdikcijā, ietekmes novērtējums citā jurisdikcijā saskaņā ar Regulas (ES) 2022/2554 19. panta 7. punktu būtu jābalsta uz incidenta pamatcēloni, iespējamo kaitīgās ietekmes izplatīšanos ar trešo personu, kas ir pakalpojumu sniedzēji, un finanšu tirgus infrastruktūru starpniecību, kā arī ietekmi uz nozīmīgām klientu grupām vai finanšu darījumu partneriem.

(14) Regulas (ES) 2022/2554 19. panta 6. un 7. punktā minētajiem ziņošanas un paziņošanas procesiem būtu jāļauj attiecīgajiem saņēmējiem novērtēt incidentu ietekmi. Tāpēc nosūtītajā informācijā būtu jāietver visa informācija, kas ietverta ziņojumos par incidentu, kurus finanšu vienība iesniegusi kompetentajai iestādei.

(15) Ja incidents ir personas datu aizsardzības pārkāpums saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) 2016/679 ([4]) un Eiropas Parlamenta un Padomes Direktīvu 2002/58/EK ([5]), šai regulai nebūtu jāietekmē minētajos Savienības tiesību aktos noteiktie datu aizsardzības pārkāpumu reģistrēšanas un paziņošanas pienākumi. Kompetentajām iestādēm būtu jāsadarbojas un jāapmainās ar informāciju par visiem attiecīgajiem jautājumiem ar iestādēm, kas minētas Regulā (ES) 2016/679 un Direktīvā 2002/58/EK.

(16) Šīs regulas pamatā ir regulatīvo tehnisko standartu projekts, ko Komisijai iesniegušas Eiropas uzraudzības iestādes, apspriežoties ar Eiropas Savienības Kiberdrošības aģentūru (*ENISA*) un Eiropas Centrālo banku (ECB).

(17) Eiropas uzraudzības iestāžu apvienotā komiteja, kas minēta Eiropas Parlamenta un Padomes Regulas (ES) Nr. 1093/2010 ([6]) 54. pantā, Eiropas Parlamenta un Padomes Regulas (ES) Nr. 1094/2010 ([7]) 54. pantā un Eiropas Parlamenta un Padomes Regulas (ES) Nr. 1095/2010 ([8]) 54. pantā, ir rīkojusi atklātu sabiedrisko apspriešanu par regulatīvajiem tehniskajiem standartiem, uz kuriem balstīta šī regula, analizējusi ierosināto standartu potenciālās izmaksas un radītos ieguvumus un lūgusi padomu Banku nozares ieinteresēto personu grupai, kas izveidota saskaņā ar Regulas (ES) Nr. 1093/2010 37. pantu, Apdrošināšanas un pārapdrošināšanas nozares ieinteresēto personu grupai un Aroda pensiju nozares ieinteresēto personu grupai, kas izveidotas saskaņā ar Regulas (ES) Nr. 1094/2010 37. pantu, un Vērtspapīru un tirgu nozares ieinteresēto personu grupai, kas izveidota saskaņā ar Regulas (ES) Nr. 1095/2010 37. pantu.

([4]) Eiropas Parlamenta un Padomes Regula (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula) (OV L 119, 4.5.2016., 1. lpp., ELI: http://data.europa.eu/eli/reg/2016/679/oj)

([5]) Eiropas Parlamenta un Padomes Direktīva 2002/58/EK (2002. gada 12. jūlijs) par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (direktīva par privāto dzīvi un elektronisko komunikāciju) (OV L 201, 31.7.2002., 37. lpp., ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([6]) Eiropas Parlamenta un Padomes Regula (ES) Nr. 1093/2010 (2010. gada 24. novembris), ar ko izveido Eiropas Uzraudzības iestādi (Eiropas Banku iestādi), groza Lēmumu Nr. 716/2009/EK un atceļ Komisijas Lēmumu 2009/78/EK (OV L 331, 15.12.2010., 12. lpp., ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([7]) Eiropas Parlamenta un Padomes Regula (ES) Nr. 1094/2010 (2010. gada 24. novembris), ar ko izveido Eiropas Uzraudzības iestādi (Eiropas Apdrošināšanas un aroda pensiju iestādi), groza Lēmumu Nr. 716/2009/EK un atceļ Komisijas Lēmumu 2009/79/EK (OV L 331, 15.12.2010., 48. lpp., ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([8]) Eiropas Parlamenta un Padomes Regula (ES) Nr. 1095/2010 (2010. gada 24. novembris), ar ko izveido Eiropas Uzraudzības iestādi (Eiropas Vērtspapīru un tirgu iestādi), groza Lēmumu Nr. 716/2009/EK un atceļ Komisijas Lēmumu 2009/77/EK (OV L 331, 15.12.2010., 84. lpp., ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

(18) Saskaņā ar Eiropas Parlamenta un Padomes Regulas (ES) 2018/1725 ([9]) 42. panta 1. punktu ir notikusi apspriešanās ar Eiropas Datu aizsardzības uzraudzītāju, kas sniedza atzinumu 2024. gada 24. janvārī,

IR PIEŅĒMUSI ŠO REGULU.

I NODAĻA

KLASIFIKĀCIJAS KRITĒRIJI

1. pants

Klienti, finanšu darījumu partneri un darījumi

1. To klientu skaits, kurus skāris incidents, kā minēts Regulas (ES) 2022/2554 18. panta 1. punkta a) apakšpunktā, atspoguļo visu skarto klientu (fizisko vai juridisko personu) skaitu, kuri incidenta laikā nevar izmantot vai nevarēja izmantot finanšu vienības sniegto pakalpojumu vai kurus incidents ir nelabvēlīgi ietekmējis. Minētajā skaitā iekļauj arī trešās personas, uz kurām nepārprotami attiecas līgumiskā vienošanās starp finanšu vienību un klientu kā skartā pakalpojuma saņēmēju.

2. Incidenta skarto finanšu darījumu partneru skaits, kā minēts Regulas (ES) 2022/2554 18. panta 1. punkta a) apakšpunktā, atspoguļo visu to skarto finanšu darījumu partneru skaitu, kuri ir noslēguši līgumisku vienošanos ar finanšu vienību.

3. Attiecībā uz to klientu un finanšu partneru nozīmīgumu, kurus skāris incidents, kā minēts Regulas (ES) 2022/2554 18. panta 1. punkta a) apakšpunktā, finanšu vienība ņem vērā to, cik lielā mērā ietekme uz klientu vai finanšu darījumu partneri ietekmēs finanšu vienības darījumdarbības mērķu īstenošanu, kā arī incidenta iespējamo ietekmi uz tirgus efektivitāti.

4. Attiecībā uz to skarto darījumu apjomu vai skaitu, kā minēts Regulas (ES) 2022/2554 18. panta 1. punkta a) apakšpunktā, finanšu vienība ņem vērā visus skartos darījumus, kas saistīti ar naudas summu, ja vismaz viena darījuma daļa tiek veikta Savienībā.

5. Ja skarto klientu vai finanšu darījumu partneru faktisko skaitu vai skarto darījumu faktisko skaitu vai summu nevar noteikt, finanšu vienība aplēš šos skaitļus vai summas, pamatojoties uz pieejamajiem datiem par salīdzināmiem atsauces periodiem.

2. pants

Ietekme uz reputāciju

1. Lai noteiktu incidenta ietekmi uz reputāciju, kā minēts Regulas (ES) 2022/2554 18. panta 1. punkta a) apakšpunktā, finanšu vienības uzskata, ka ir radusies ietekme uz reputāciju, ja ir izpildīts vismaz viens no šādiem kritērijiem:

a) incidents ir atspoguļots plašsaziņas līdzekļos;

b) incidenta rezultātā ir atkārtoti saņemtas sūdzības no dažādiem klientiem vai finanšu darījumu partneriem par pakalpojumiem, kas orientēti uz klientiem, vai kritiski svarīgām darījumattiecībām;

c) incidenta rezultātā finanšu vienība nespēs vai varētu nespēt izpildīt regulatīvās prasības;

d) incidenta rezultātā finanšu vienība zaudēs vai varētu zaudēt klientus vai finanšu darījumu partnerus, kam ir būtiska ietekme uz tās uzņēmējdarbību.

([9]) Eiropas Parlamenta un Padomes Regula (ES) 2018/1725 (2018. gada 23. oktobris) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Savienības iestādēs, struktūrās, birojos un aģentūrās un par šādu datu brīvu apriti un ar ko atceļ Regulu (EK) Nr. 45/2001 un Lēmumu Nr. 1247/2002/EK (OV L 295, 21.11.2018., 39. lpp., ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

2. Novērtējot incidenta ietekmi uz reputāciju, finanšu vienības ņem vērā pamanāmības līmeni, ko incidents ir ieguvis vai varētu iegūt saistībā ar katru 1. punktā uzskaitīto kritēriju.

3. pants

Incidenta ilgums un pakalpojuma nepieejamība

1. Finanšu vienības mēra Regulas (ES) 2022/2554 18. panta 1. punkta b) apakšpunktā minētā incidenta ilgumu no brīža, kad incidents ir iestājies, līdz brīdim, kad incidents tika novērsts.

Ja finanšu vienības nespēj noteikt incidenta iestāšanās brīdi, tās mēra incidenta ilgumu no brīža, kad tas tika konstatēts. Ja finanšu vienības uzzina par incidenta atgadījumu pirms tā konstatēšanas, tās mēra ilgumu no brīža, kad incidents ir reģistrēts tīkla vai sistēmas žurnālos vai citos datu avotos.

Ja finanšu vienības vēl nezina, kad incidents tiks novērsts, vai nespēj pārbaudīt ierakstus žurnālos vai citos datu avotos, tās piemēro aplēses.

2. Finanšu vienības mēra ar incidentu saistīto pakalpojuma nepieejamību, kas minēta Regulas (ES) 2022/2554 18. panta 1. punkta b) apakšpunktā, no brīža, kad pakalpojums ir pilnībā vai daļēji nepieejams klientiem, finanšu darījumu partneriem vai citiem iekšējiem vai ārējiem lietotājiem, līdz brīdim, kad regulārās darbības vai operācijas ir atjaunotas tādā līmenī, kāds tika sniegts pirms incidenta. Ja pakalpojuma nepieejamības dēļ tiek kavēta pakalpojumu sniegšana pēc tam, kad ir atjaunotas regulārās darbības vai operācijas, attiecīgo nepieejamību mēra no incidenta sākuma līdz brīdim, kad šis aizkavētais pakalpojums tiek pilnībā sniegts.

Ja finanšu vienības nespēj noteikt brīdi, kad sakās pakalpojuma nepieejamība, tās mēra pakalpojuma nepieejamības ilgumu no brīža, kad tā tika konstatēta.

4. pants

Ģeogrāfiskā izplatība

Lai noteiktu ģeogrāfisko izplatību attiecībā uz incidenta skartajām teritorijām, kā minēts Regulas (ES) 2022/2554 18. panta 1. punkta c) apakšpunktā, finanšu vienības novērtē, vai incidents ietekmē vai ir ietekmējis citas dalībvalstis, un jo īpaši ietekmes nozīmīgumu saistībā ar kādu no turpmāk minētajiem:

a) klienti un finanšu darījumu partneri citās dalībvalstīs;

b) filiāles vai citas grupā esošās finanšu vienības, kas veic darbības citās dalībvalstīs;

c) finanšu tirgus infrastruktūras vai trešās personas, kas sniedz pakalpojumus, kas var ietekmēt finanšu vienības citās dalībvalstīs, kurās tie sniedz pakalpojumus, ciktāl šāda informācija ir pieejama.

5. pants

Datu zudumi

Lai noteiktu datu zudumus, ko radījis incidents, kā noteikts Regulas (ES) 2022/2554 18. panta 1. punkta d) apakšpunktā, finanšu vienības ņem vērā turpmāk minēto:

a) attiecībā uz datu pieejamību – vai incidents pēc finanšu vienības, tās klientu vai darījumu partneru pieprasījuma ir padarījis datus uz laiku vai pastāvīgi nepieejamus vai neizmantojamus;

b) attiecībā uz datu autentiskumu – vai incidents ir apdraudējis datu avota uzticamību;

c) attiecībā uz datu integritāti – vai incidenta rezultātā ir notikusi neatļauta datu modificēšana, kas tos padarījusi neprecīzus vai nepilnīgus;

d) attiecībā uz datu konfidencialitāti – vai incidenta rezultātā nepilnvarotai pusei vai sistēmai ir bijusi piekļuve datiem vai tie ir izpausti nepilnvarotai pusei vai sistēmai.

6. pants

Skarto pakalpojumu kritiskums

Lai noteiktu ietekmēto pakalpojumu kritiskumu, kā minēts Regulas (ES) 2022/2554 18. panta 1. punkta e) apakšpunktā, finanšu vienības novērtē, vai incidents:

a) ietekmē vai ir ietekmējis IKT pakalpojumus vai tīklu un informācijas sistēmas, ar ko atbalsta finanšu vienības kritiski svarīgas vai svarīgas funkcijas;

b) ietekmē vai ir ietekmējis finanšu pakalpojumus, ko sniedz finanšu vienība, kurai nepieciešama atļauja, reģistrācija vai kuru uzrauga kompetentās iestādes;

c) izraisa vai ir izraisījis sekmīgu, ļaunprātīgu un neatļautu piekļuvi finanšu vienības tīklam un informācijas sistēmām.

7. pants

Ekonomiskā ietekme

1. Lai noteiktu incidenta ekonomisko ietekmi, kas minēta Regulas (ES) 2022/2554 18. panta 1. punkta f) apakšpunktā, finanšu vienības, neskaitot atgūtos finanšu līdzekļus, ņem vērā šādus tiešo un netiešo izmaksu un zaudējumu veidus, kas tām radušies incidenta rezultātā:

a) ekspropriēti līdzekļi vai finanšu aktīvi, par kuriem tās ir atbildīgas, tostarp zādzības rezultātā zaudēti aktīvi;

b) programmatūras, aparatūras vai infrastruktūras nomaiņas vai pārvietošanas izmaksas;

c) personāla izmaksas, tostarp izmaksas, kas saistītas ar personāla aizstāšanu vai pārcelšanu, papildu darbinieku pieņemšanu darbā, virsstundu atalgojumu un zaudēto vai ietekmēto prasmju atgūšanu;

d) maksas par līgumiskās vienošanās neizpildi;

e) izmaksas par tiesisko aizsardzību un kompensāciju klientiem;

f) zaudēto ieņēmumu dēļ radušies zaudējumi;

g) izmaksas, kas saistītas ar iekšējo un ārējo komunikāciju;

h) konsultāciju izmaksas, tostarp izmaksas, kas saistītas ar juridiskajām konsultācijām, tiesu ekspertīzes pakalpojumiem un izlabošanas pakalpojumiem.

2. Šā panta 1. punktā minētās izmaksas un zaudējumi neietver izmaksas, kas nepieciešamas uzņēmuma ikdienas darbībai, jo īpaši:

a) infrastruktūras, aprīkojuma, aparatūras un programmatūras vispārējās uzturēšanas izmaksas un personāla prasmju atjaunināšanas izmaksas;

b) iekšējās vai ārējās izmaksas uzņēmējdarbības uzlabošanai pēc incidenta, tostarp jauninājumi, uzlabojumi un riska novērtēšanas iniciatīvas;

c) apdrošināšanas prēmijas.

3. Finanšu vienības aprēķina izmaksu un zaudējumu summas, pamatojoties uz ziņošanas laikā pieejamajiem datiem. Ja faktiskās izmaksu un zaudējumu summas nevar noteikt, finanšu vienības aplēš šīs summas.

4. Novērtējot incidenta ekonomisko ietekmi, finanšu vienības summē 1. punktā minētās izmaksas un zaudējumus.

II NODAĻA

BŪTISKI INCIDENTI UN BŪTISKUMA ROBEŽVĒRTĪBAS

8. pants

Būtiski incidenti

1. Incidentu uzskata par būtisku incidentu Regulas (ES) 2022/2554 19. panta 1. punkta nolūkā, ja tas ir ietekmējis 6. pantā minētos kritiskos pakalpojumus un ja ir izpildīts kāds no turpmāk minētajiem nosacījumiem:

a) ir sasniegta 9. panta 5. punkta b) apakšpunktā minētā būtiskuma robežvērtība;

b) ir sasniegtas divas vai vairākas citas 9. panta 1.–6. punktā minētās būtiskuma robežvērtības.

2. Daudzkārtējus incidentus, kas atsevišķi netiek uzskatīti par būtisku incidentu saskaņā ar 1. punktu, uzskata par vienu būtisku incidentu, ja tie atbilst visiem turpmāk minētajiem nosacījumiem:

a) tie ir notikuši vismaz divas reizes sešu mēnešu laikā;

b) tiem ir tāds pats acīmredzamais pamatcēlonis, kā minēts Regulas (ES) 2022/2554 20. panta pirmās daļas b) punktā;

c) tie kopā atbilst 1. punktā izklāstītajiem kritērijiem, lai tos uzskatītu par būtisku incidentu.

Finanšu vienības reizi mēnesī novērtē daudzkārtēju incidentu esamību.

Šo punktu nepiemēro mikrouzņēmumiem un finanšu vienībām, kas uzskaitītas Regulas (ES) 2022/2554 16. panta 1. punktā.

9. pants

Būtiskuma robežvērtības būtisku incidentu noteikšanai

1. Būtiskuma robežvērtība attiecībā uz kritēriju "klienti, finanšu darījumu partneri un darījumi" ir sasniegta, ja ir izpildīts kāds no turpmāk minētajiem nosacījumiem:

a) ietekmēto klientu skaits pārsniedz 10 % no visiem klientiem, kuri izmanto skarto pakalpojumu;

b) ietekmēto klientu skaits, kuri izmanto skarto pakalpojumu, ir lielāks par 100 000;

c) ietekmēto finanšu darījumu partneru skaits ir lielāks par 30 % no visiem finanšu darījumu partneriem, kas veic darbības saistībā ar skartā pakalpojuma sniegšanu;

d) ietekmēto darījumu skaits pārsniedz 10 % no finanšu vienības veikto darījumu dienas vidējā skaita saistībā ar skarto pakalpojumu;

e) ietekmēto darījumu summa ir lielāka par 10 % no finanšu vienības veikto darījumu dienas vidējās vērtības saistībā ar skarto pakalpojumu;

f) ir ietekmēti klienti vai finanšu darījumu partneri, kas noteikti kā būtiski saskaņā ar 1. panta 3. punktu.

Ja ietekmēto klientu vai finanšu darījumu partneru faktisko skaitu vai ietekmēto darījumu faktisko skaitu vai summu nevar noteikt, finanšu vienība aplēš šos skaitļus vai summas, pamatojoties uz pieejamajiem datiem par salīdzināmiem atsauces periodiem.

2. Būtiskuma robežvērtība attiecībā uz kritēriju "ietekme uz reputāciju" ir sasniegta, ja ir izpildīts kāds no 2. panta 1. punkta a)–d) apakšpunktā izklāstītajiem nosacījumiem.

3. Būtiskuma robežvērtība attiecībā uz kritēriju "incidenta ilgums un pakalpojuma nepieejamība" ir sasniegta, ja ir izpildīts kāds no turpmāk minētajiem nosacījumiem:

a) incidenta ilgums pārsniedz 24 stundas;

b) pakalpojuma nepieejamība pārsniedz 2 stundas IKT pakalpojumiem, ar ko atbalsta kritiski svarīgas vai svarīgas funkcijas.

4. Būtiskuma robežvērtība attiecībā uz kritēriju "ģeogrāfiskā izplatība" ir sasniegta, ja saskaņā ar 4. pantu incidentam ir ietekme divās vai vairākās dalībvalstīs.

5. Būtiskuma robežvērtība attiecībā uz kritēriju "datu zudumi" ir sasniegta, ja ir izpildīts kāds no turpmāk minētajiem nosacījumiem:

a) jebkāda 5. pantā minētā ietekme uz datu pieejamību, autentiskumu, integritāti vai konfidencialitāti negatīvi ietekmē vai negatīvi ietekmēs finanšu vienības darījumdarbības mērķu īstenošanu vai tās spēju izpildīt regulatīvās prasības;

b) notiek jebkāda sekmīga, ļaunprātīga un neatļauta piekļuve, uz ko neattiecas a) apakšpunkts, tīklu un informācijas sistēmām, ja šāda piekļuve var izraisīt datu zudumus.

6. Būtiskuma robežvērtība attiecībā uz kritēriju "ekonomiskā ietekme" ir sasniegta, ja izmaksas un zaudējumi, kas finanšu vienībai radušies incidenta rezultātā, ir pārsnieguši vai, iespējams, pārsniegs 100 000 EUR.

III NODAĻA

BŪTISKI KIBERDRAUDI

10. pants

Augstas būtiskuma robežvērtības būtisku kiberdraudu noteikšanai

Regulas (ES) 2022/2554 18. panta 2. punkta nolūkā kiberdraudus uzskata par nozīmīgiem, ja ir izpildīti visi turpmāk minētie nosacījumi:

a) kiberdraudi, ja tie būtu materializējušies, varētu ietekmēt vai būtu varējuši ietekmēt finanšu vienības kritiski svarīgās vai svarīgās funkcijas vai varētu ietekmēt citas finanšu vienības, trešās personas, kas ir pakalpojumu sniedzēji, klientus vai finanšu darījumu partnerus, pamatojoties uz finanšu vienībai pieejamo informāciju;

b) pastāv augsta iespējamība, ka kiberdraudi īstenosies finanšu vienībā vai citās finanšu vienībās, ņemot vērā vismaz šādus elementus:

   i) piemērojamos riskus, kas saistīti ar a) apakšpunktā minētajiem kiberdraudiem, tostarp finanšu vienības sistēmu potenciālās nepilnības, kuras var izmantot;

   ii) apdraudētāju spējas un nodomus, ciktāl tie ir zināmi finanšu vienībai;

   iii) apdraudējuma noturību un visas uzkrātās zināšanas par incidentiem, kas ietekmējuši finanšu vienību vai tās trešo personu, kas sniedz pakalpojumus, klientus vai finanšu partnerus;

c) kiberdraudi, ja tie materializētos, varētu atbilst kādam no turpmāk minētajiem:

   i) Regulas (ES) 2022/2554 18. panta 1. punkta e) apakšpunktā noteiktajam pakalpojumu kritērijam par kritiskumu, kā norādīts šīs regulas 6. pantā;

   ii) būtiskuma robežvērtībai, kas noteikta šīs regulas 9. panta 1. punktā;

   iii) būtiskuma robežvērtībai, kas noteikta šīs regulas 9. panta 4. punktā.

Ja atkarībā no kiberdraudu veida un pieejamās informācijas finanšu vienība secina, ka 9. panta 2., 3., 5. un 6. punktā noteiktās būtiskuma robežvērtības varētu tikt sasniegtas, var ņemt vērā arī minētās robežvērtības.

IV NODAĻA

BŪTISKU INCIDENTU NOZĪMĪGUMS KOMPETENTAJĀM IESTĀDĒM CITĀS DALĪBVALSTĪS UN SĪKĀKA ZIŅOJUMOS IETVERAMĀ INFORMĀCIJA, KAS JĀKOPLIETO AR CITĀM KOMPETENTAJĀM IESTĀDĒM

11. pants

Būtisku incidentu nozīmīgums kompetentajām iestādēm citās dalībvalstīs

Novērtējumu par to, vai būtisks incidents ir nozīmīgs citu dalībvalstu kompetentajām iestādēm, kā minēts Regulas (ES) 2022/2554 19. panta 7. punktā, balsta uz to, vai incidenta pamatcēlonis ir radies citā dalībvalstī, vai incidentam ir vai ir bijusi būtiska ietekme citā dalībvalstī uz kādu no turpmāk minētajiem aspektiem:

a) klientiem vai finanšu darījumu partneriem;

b) finanšu vienības filiāli vai citu finanšu vienību grupas ietvaros;

c) finanšu tirgus infrastruktūru vai trešo personu, kas sniedz pakalpojumus, kas var ietekmēt finanšu vienības, kurām tie sniedz pakalpojumus.

12. pants

Sīkāka informācija par būtiskiem incidentiem, kas jākoplieto ar citām kompetentajām iestādēm

Sīkāka informācija par būtiskiem incidentiem, kas kompetentajām iestādēm jāiesniedz citām kompetentajām iestādēm saskaņā ar Regulas (ES) 2022/2554 19. panta 6. punktu, un paziņojumi, kas EBI, EVTI vai EAAPI un ECB jāiesniedz attiecīgajām kompetentajām iestādēm citās dalībvalstīs saskaņā ar minētās regulas 19. panta 7. punktu, ietver tādu pašu informācijas līmeni bez anonimizācijas kā paziņojumos un ziņojumos par būtiskiem incidentiem, kas no finanšu vienībām saņemti saskaņā ar Regulas (ES) 2022/2554 19. panta 4. punktu.

V NODAĻA

NOBEIGUMA NOTEIKUMI

13. pants

Stāšanās spēkā

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

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

Briselē, 2024. gada 13. martā

Komisijas vārdā –
priekšsēdētāja
Ursula VON DER LEYEN