2024/1772

25.6.2024

KOMISJONI DELEGEERITUD MÄÄRUS (EL) 2024/1772,

13. märts 2024,

millega täiendatakse Euroopa Parlamendi ja nõukogu määrust (EL) 2022/2554 regulatiivsete tehniliste standarditega, millega määratakse kindlaks IKT intsidentide ja küberohtude liigitamise kriteeriumid, kehtestatakse olulisuse läved ja täpsustatakse tõsiste intsidentide kohta esitatavate raportite üksikasju

(EMPs kohaldatav tekst)

EUROOPA KOMISJON,

võttes arvesse Euroopa Liidu toimimise lepingut,

võttes arvesse Euroopa Parlamendi ja nõukogu 14. detsembri 2022. aasta määrust (EL) 2022/2554, mis käsitleb finantssektori digitaalset tegevuskerksust ning millega muudetakse määrusi (EÜ) nr 1060/2009, (EL) nr 648/2012, (EL) nr 600/2014, (EL) nr 909/2014 ja (EL) 2016/1011, ([1]) eriti selle artikli 18 lõike 4 kolmandat lõiku,

ning arvestades järgmist:

(1) Määruse (EL) 2022/2554 eesmärk on ühtlustada ja sujundada krediidiasutuste, makseasutuste, kontoteabe teenuse pakkujate ja e-raha asutustega seotud IKT intsidentidest ning tegevust või turvalisust mõjutavatest maksetega seotud intsidentidest teatamise nõudeid (edaspidi „intsidendid“). Võttes arvesse, et teatamisnõuded hõlmavad 20 eri liiki finantssektori ettevõtjaid, tuleks tõsiste intsidentide ja oluliste küberohtude kindlaksmääramiseks kasutatavad liigitamiskriteeriumid ja olulisuse läved kindlaks määrata lihtsal, ühtsel ja järjepideval viisil, võttes arvesse kõigi asjaomaste finantssektori ettevõtjate teenuste ja tegevuse eripära.

(2) Proportsionaalsuse tagamiseks peaksid liigitamiskriteeriumid ja olulisuse läved kajastama kõigi finantssektori ettevõtjate suurust ja üldist riskiprofiili ning teenuste laadi, ulatust ja keerukust. Lisaks tuleks kriteeriumid ja olulisuse läved kehtestada nii, et neid kohaldatakse järjepidevalt kõigi finantssektori ettevõtjate suhtes, olenemata nende suurusest ja riskiprofiilist, ning need ei tekita väiksematele finantssektori ettevõtjatele ebaproportsionaalset aruandluskoormust. Selleks et lahendada olukordi, kus oluline arv kliente on mõjutatud intsidendist, mis iseenesest ei ületa kohaldatavat läve, tuleks kehtestada peamiselt suurematele finantssektori ettevõtjatele suunatud absoluutne lävi.

(3) Seoses intsidentidest teatamise raamistikega, mis kehtisid juba enne määruse (EL) 2022/2554 jõustumist, tuleks finantssektori ettevõtjate jaoks tagada järjepidevus. Seepärast tuleks liigitamiskriteeriumid ja olulisuse läved viia kooskõlla EBA suunistega tõsistest intsidentidest teatamise kohta Euroopa Parlamendi ja nõukogu direktiivi (EL) 2015/2366 ([2]) alusel, suunistega kauplemisteabehoidlate poolt ESMA-le perioodilise teabe esitamise ja olulistest muudatuste teatamise kohta, EKP/ühtse järelevalvemehhanismi küberintsidentidest teatamise raamistikuga ning muude asjakohaste suunistega. Liigitamiskriteeriumid ja läved peaksid sobima ka finantssektori ettevõtjatele, kelle suhtes intsidentidest teatamise nõudeid enne määrust (EL) 2022/2554 ei kohaldatud.

(4) Seoses liigitamiskriteeriumiga „mõjutatud tehingute summa ja arv“ on tehingute mõiste lai ning hõlmab finantssektori ettevõtjate suhtes kohaldatavates valdkondlikes õigusaktides sätestatud eri tegevusi ja teenuseid. Kõnealuse liigitamiskriteeriumi kohaldamisel tuleks hõlmata maksetehingud ning finantsinstrumentide, krüptovara, kaupade või muu vara (sealhulgas võimendustagatise, tagatise või pandi kujul) igasugune vahetamine nii sularaha kui ka mis tahes muu vara vastu. Liigitamisel tuleks arvesse võtta kõiki tehinguid, mis hõlmavad varasid, mille väärtust saab väljendada rahalises summas.

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

([2]) Euroopa Parlamendi ja nõukogu 25. novembri 2015. aasta direktiiv (EL) 2015/2366 makseteenuste kohta siseturul, direktiivide 2002/65/EÜ, 2009/110/EÜ ning 2013/36/EL ja määruse (EL) nr 1093/2010 muutmise ning direktiivi 2007/64/EÜ kehtetuks tunnistamise kohta (ELT L 337, 23.12.2015, lk 35, ELI: http://data.europa.eu/eli/dir/2015/2366/oj).

(5) Liigitamiskriteeriumidega tuleks tagada, et hõlmatud on kõik asjakohased tõsiste intsidentide liigid. Paljud liigitamiskriteeriumid ei pruugi tingimata hõlmata võrgu- või infosüsteemidesse sissetungiga seotud küberründe id. Kuid need on siiski olulised, sest mis tahes sissetung võrgu- ja infosüsteemidesse võib finantssektori ettevõtjat kahjustada. Sellest tulenevalt tuleks täpsustada liigitamiskriteeriume „mõjutatud kriitilise tähtsusega teenused" ja „andmekadu" nii, et need hõlmaksid seda liiki tõsiseid intsidente, eelkõige loata sissetunge, mis võivad isegi juhul, kui mõju ei ole kohe teada, tuua kaasa tõsiseid tagajärgi, eelkõige andmetega seotud rikkumisi ja andmelekkeid.

(6) Kuna krediidiasutuste suhtes kohaldatakse nii määruse (EL) 2022/2554 artikli 18 kohast intsidentide liigitamise raamistikku kui ka komisjoni delegeeritud määruse (EL) 2018/959 ([3]) kohast operatsiooniriski raamistikku, peaks lähenemisviis intsidendi majandusliku mõju hindamiseks kulude ja kahju arvutamise alusel olema mõlemas raamistikus võimalikult järjepidev, et vältida sobimatute või vastuoluliste nõuete kehtestamist.

(7) Intsidendi geograafilise ulatuse kriteerium, nagu on sätestatud määruse (EL) 2022/2554 artikli 18 lõike 1 punktis c, peaks keskenduma intsidendi piiriülesele mõjule, kuna intsidendi mõju finantssektori ettevõtja tegevusele ühes jurisdiktsioonis hõlmavad muud kõnealuses artiklis sätestatud kriteeriumid.

(8) Võttes arvesse, et liigitamiskriteeriumid on üksteisest sõltuvad ja omavahel seotud, peaks määruse (EL) 2022/2554 artikli 19 lõike 1 kohaselt teatatavate tõsiste intsidentide kindlakstegemise lähenemisviis põhinema kriteeriumide kombinatsioonil, mille puhul mõnel kriteeriumil, mis on tihedalt seotud määruse (EL) 2022/2554 artikli 3 lõigetes 8 ja 10 sätestatud IKT intsidendi ja tõsise IKT intsidendi määratlustega, olema tõsiste intsidentide liigitamisel suurem tähtsus kui muudel kriteeriumidel.

(9) Tagamaks, et määruse (EL) 2022/2554 artikli 19 lõike 1 kohaselt pädevatele asutustele esitatavad rapordid ja teated tõsiste intsidentide kohta on kasulikud nii järelevalve eesmärgil kui ka finantssektoris leviku ärahoidmiseks, peaksid olulisuse läved võimaldama hõlmata tõsiseid intsidente, keskendudes muu hulgas mõjule üksuse konkreetsetele kriitilise tähtsusega teenustele, klientide, finantssektori vastaspoolte või tehingute konkreetsetele absoluutsetele ja suhtelistele lävedele, mis osutavad finantssektori ettevõtjale avalduvale olulisele mõjule, ning mõju olulisusele teistes liikmesriikides.

(10) Intsidente, mis mõjutavad IKT-teenuseid või võrgu- ja infosüsteeme, mis toetavad kriitilise tähtsusega või olulisi funktsioone või puudutavad finantsteenuseid, mille osutamiseks on vaja luba, või pahatahtlikku loata juurdepääsu võrgu- ja infosüsteemidele, mis toetavad kriitilise tähtsusega või olulisi funktsioone, tuleks käsitada intsidentidena, mis mõjutavad finantssektori ettevõtjate kriitilise tähtsusega teenuseid. Pahatahtlik loata juurdepääs võrgu- ja infosüsteemidele, mis toetavad finantssektori ettevõtja kriitilise tähtsusega või olulisi funktsioone, kujutab endast tõsist ohtu finantssektori ettevõtjale ning, kuna see võib mõjutada teisi finantssektori ettevõtjaid, tuleks seda alati käsitada tõsise intsidendina, millest tuleb teatada.

(11) Korduvad intsidendid, mis on omavahel seotud sarnase ilmse algpõhjuse kaudu ja mis eraldi ei ole tõsised intsidendid, võivad osutada märkimisväärsetele puudustele ja nõrkustele finantssektori ettevõtja intsidendi- ja riskijuhtimismenetlustes. Seepärast tuleks korduvaid intsidente pidada kollektiivselt tõsiseks, kui need toimuvad teatava ajavahemiku jooksul korduvalt.

(12) Võttes arvesse, et küberohud võivad finantssektori ettevõtjat ja sektorit negatiivselt mõjutada, peaksid finantssektori ettevõtjad olulistest küberohtudest teatamisel täpsustama nende realiseerumise tõenäosust ja võimaliku mõju kriitilist tähtsust. Selleks et tagada küberohtude olulisuse selge ja järjepidev hindamine, peaks küberohu liigitamine oluliseks sõltuma tõenäosusest, et ohu realiseerumise korral on tõsiste intsidentide liigitamise kriteeriumid täidetud ja nende lävi ületatud, küberohu liigist ja finantssektori ettevõtjale kättesaadavast teabest.

([3]) Komisjoni 14. märtsi 2018. aasta delegeeritud määrus (EL) 2018/959, millega täiendatakse Euroopa Parlamendi ja nõukogu määrust (EL) nr 575/2013 seoses regulatiivsete tehniliste standarditega, mis käsitlevad sellise hindamismetoodika kindlaksmääramist, mille alusel pädevad asutused lubavad krediidiasutustel kasutada operatsiooniriski puhul täiustatud mõõtmismudelil põhinevaid meetodeid (ELT L 169, 6.7.2018, lk 1, ELI: http://data.europa.eu/eli/reg_del/2018/959/oj).

(13) Võttes arvesse, et teiste liikmesriikide pädevaid asutusi tuleb teavitada intsidentidest, mis mõjutavad finantssektori ettevõtjaid ja kliente nende jurisdiktsioonis, peaks määruse (EL) 2022/2554 artikli 19 lõike 7 kohane mõju hindamine teises jurisdiktsioonis põhinema intsidendi algpõhjusel, võimalikul levikul kolmandast isikust teenuseosutajate ja finantsturutaristute kaudu ning intsidendi mõjul olulistele kliendi- või finantssektori vastaspoolte rühmadele.

(14) Määruse (EL) 2022/2554 artikli 19 lõigetes 6 ja 7 osutatud aruandlus- ja teavitamismenetlused peaksid võimaldama asjaomastel saajatel hinnata intsidentide mõju. Seepärast peaks edastatud teave hõlmama kõiki üksikasju, mis sisalduvad finantssektori ettevõtja poolt pädevale asutusele intsidendi kohta esitatud raportis.

(15) Kui intsident kujutab endast isikuandmetega seotud rikkumist vastavalt Euroopa Parlamendi ja nõukogu määrusele (EL) 2016/679 ([4]) ning Euroopa Parlamendi ja nõukogu direktiivile 2002/58/EÜ ([5]), ei tohiks käesolev määrus mõjutada kõnealuste liidu õigusaktide kohaseid isikuandmetega seotud rikkumiste registreerimise ja nendest teavitamise kohustusi. Pädevad asutused peaksid kõigis asjakohastes küsimustes tegema koostööd ning vahetama teavet määruses (EL) 2016/679 ja direktiivis 2002/58/EÜ osutatud asutustega.

(16) Käesolev määrus põhineb regulatiivsete tehniliste standardite eelnõul, mille on komisjonile esitanud Euroopa järelevalveasutused, konsulteerides Euroopa Liidu Küberturvalisuse Ameti ja Euroopa Keskpangaga.

(17) Euroopa Parlamendi ja nõukogu määruse (EL) nr 1093/2010 ([6]) artiklis 54, Euroopa Parlamendi ja nõukogu määruse (EL) nr 1094/2010 ([7]) artiklis 54 ning Euroopa Parlamendi ja nõukogu määruse (EL) nr 1095/2010 ([8]) artiklis 54 osutatud Euroopa järelevalveasutuste ühiskomitee on korraldanud käesoleva määruse aluseks olevate regulatiivsete tehniliste standardite eelnõude kohta avalikud konsultatsioonid, analüüsinud kavandatud standardite võimalikke kulusid ja kasu ning küsinud nõu määruse (EL) nr 1093/2010 artikli 37 kohaselt loodud pangandussektori sidusrühmade kogult, määruse (EL) nr 1094/2010 artikli 37 kohaselt loodud kindlustuse ja edasikindlustuse sidusrühmade kogult ja tööandjapensionide sidusrühmade kogult ning määruse (EL) nr 1095/2010 artikli 37 kohaselt loodud väärtpaberituru sidusrühmade kogult.

([4]) Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus) (ELT L 119, 4.5.2016, lk 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([5]) Euroopa Parlamendi ja nõukogu 12. juuli 2002. aasta direktiiv 2002/58/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv) (ELT L 201, 31.7.2002, lk 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([6]) Euroopa Parlamendi ja nõukogu 24. novembri 2010. aasta määrus (EL) nr 1093/2010, millega asutatakse Euroopa Järelevalveasutus (Euroopa Pangandusjärelevalve), muudetakse otsust nr 716/2009/EÜ ning tunnistatakse kehtetuks komisjoni otsus 2009/78/EÜ (ELT L 331, 15.12.2010, lk 12, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([7]) Euroopa Parlamendi ja nõukogu 24. novembri 2010. aasta määrus (EL) nr 1094/2010, millega asutatakse Euroopa Järelevalveasutus (Euroopa Kindlustus- ja Tööandjapensionide Järelevalve), muudetakse otsust nr 716/2009/EÜ ning tunnistatakse kehtetuks komisjoni otsus 2009/79/EÜ (ELT L 331, 15.12.2010, lk 48, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([8]) Euroopa Parlamendi ja nõukogu 24. novembri 2010. aasta määrus (EL) nr 1095/2010, millega asutatakse Euroopa Järelevalveasutus (Euroopa Väärtpaberiturujärelevalve), muudetakse otsust nr 716/2009/EÜ ning tunnistatakse kehtetuks komisjoni otsus 2009/77/EÜ (ELT L 331, 15.12.2010, lk 84, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

(18) Vastavalt Euroopa Parlamendi ja nõukogu määruse (EL) 2018/1725 ([9]) artikli 42 lõikele 1 konsulteeriti Euroopa Andmekaitseinspektoriga, kes esitas oma arvamuse 24. jaanuaril 2024,

ON VASTU VÕTNUD KÄESOLEVA MÄÄRUSE:

I PEATÜKK

LIIGITAMISKRITEERIUMID

Artikkel 1

Kliendid, finantssektori vastaspooled ja tehingud

1. Intsidendist mõjutatud klientide arv, nagu on osutatud määruse (EL) 2022/2554 artikli 18 lõike 1 punktis a, kajastab kõigi selliste mõjutatud klientide arvu, olenemata sellest, kas tegemist on füüsiliste või juriidiliste isikutega, kes ei saa või ei saanud intsidendi ajal kasutada finantssektori ettevõtja pakutavat teenust või keda intsident negatiivselt mõjutas. See arv hõlmab ka kolmandaid isikuid, kes on sõnaselgelt hõlmatud finantssektori ettevõtja ja kliendi vahelise lepinguga kui mõjutatud teenusest kasu saavad isikud.

2. Intsidendist mõjutatud finantssektori vastaspoolte arv, nagu on osutatud määruse (EL) 2022/2554 artikli 18 lõike 1 punktis a, kajastab kõigi selliste mõjutatud finantssektori vastaspoolte arvu, kes on sõlminud finantssektori ettevõtjaga lepingu.

3. Seoses intsidendist mõjutatud klientide ja finantssektori vastaspoolte olulisusega, nagu on osutatud määruse (EL) 2022/2554 artikli 18 lõike 1 punktis a, võtab finantssektori ettevõtja arvesse seda, mil määral mõjutab kliendile või finantssektori vastaspoolele avalduv mõju finantssektori ettevõtja ärieesmärkide saavutamist, samuti intsidendi võimalikku mõju turu tõhususele.

4. Seoses intsidendist mõjutatud tehingute summa või arvuga, nagu on osutatud määruse (EL) 2022/2554 artikli 18 lõike 1 punktis a, võtab finantssektori ettevõtja arvesse kõiki rahalise summaga seotud mõjutatud tehinguid, kui vähemalt üks osa tehingust tehakse liidus.

5. Kui mõjutatud klientide või finantssektori vastaspoolte tegelikku arvu või mõjutatud tehingute tegelikku arvu või summat ei ole võimalik kindlaks määrata, hindab finantssektori ettevõtja neid arve või summasid võrreldavate vaatlusperioodide kättesaadavate andmete põhjal.

Artikkel 2

Mõju mainele

1. Selleks et teha kindlaks intsidendi mõju mainele, nagu on osutatud määruse (EL) 2022/2554 artikli 18 lõike 1 punktis a, leiavad finantssektori ettevõtjad, et mainele on avaldunud mõju, kui täidetud on vähemalt üks järgmistest kriteeriumidest:

a) intsidenti on kajastatud meedias;

b) intsident on toonud kaasa korduvad kaebused eri klientidelt või finantssektori vastaspooltelt kliendile suunatud teenuste või kriitilise tähtsusega ärisuhete kohta;

c) finantssektori ettevõtja ei suuda või tõenäoliselt ei suuda intsidendi tõttu täita regulatiivseid nõudeid;

d) finantssektori ettevõtja kaotab või tõenäoliselt kaotab intsidendi tõttu kliente või finantssektori vastaspooli ning sellel on oluline mõju tema äritegevusele.

([9]) Euroopa Parlamendi ja nõukogu 23. oktoobri 2018. aasta määrus (EL) 2018/1725, mis käsitleb füüsiliste isikute kaitset isikuandmete töötlemisel liidu institutsioonides, organites ja asutustes ning isikuandmete vaba liikumist, ning millega tunnistatakse kehtetuks määrus (EÜ) nr 45/2001 ja otsus nr 1247/2002/EÜ (ELT L 295, 21.11.2018, lk 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

2. Intsidendi poolt mainele avalduva mõju hindamisel võtavad finantssektori ettevõtjad iga lõikes 1 loetletud kriteeriumi puhul arvesse intsidendi nähtavuse taset, mille intsident on saavutanud või tõenäoliselt saavutab.

Artikkel 3

Kestus ja teenuse seisaku aeg

1. Finantssektori ettevõtjad mõõdavad määruse (EL) 2022/2554 artikli 18 lõike 1 punktis b osutatud intsidendi kestust alates intsidendi toimumisest kuni selle lahendamiseni.

Kui finantssektori ettevõtjatel ei ole võimalik intsidendi toimumise hetke kindlaks määrata, mõõdavad nad intsidendi kestust alates selle avastamise hetkest. Kui finantssektori ettevõtjad saavad teada, et intsident leidis aset enne selle avastamist, mõõdavad nad selle kestust alates intsidendi registreerimisest võrgu- või süsteemilogides või muudes andmeallikates.

Kui finantssektori ettevõtjad ei tea veel, millal intsident lahendatakse, või ei suuda kontrollida logides või muudes andmeallikates olevaid andmeid, kasutavad nad hinnanguid.

2. Finantssektori ettevõtjad mõõdavad intsidendist tingitud teenuse seisaku aega, nagu on osutatud määruse (EL) 2022/2554 artikli 18 lõike 1 punktis b, alates hetkest, mil teenus ei ole klientidele, finantssektori vastaspooltele või muudele sise- või väliskasutajatele täielikult või osaliselt kättesaadav, kuni hetkeni, mil tavapärane tegevus või tavapärased toimingud on taastatud enne intsidenti osutatud teenuse tasemele. Kui teenuse seisaku tõttu hilineb teenuse osutamine pärast tavapärase tegevuse või tavapäraste toimingute taastamist, mõõdetakse seisaku aega alates intsidendi algusest kuni hetkeni, mil hilinenud teenust hakatakse täielikult osutama.

Kui finantssektori ettevõtjatel ei ole võimalik teenuse seisaku aega kindlaks määrata, mõõdavad nad teenuse seisaku aega alates seisaku avastamise hetkest.

Artikkel 4

Geograafiline ulatus

Selleks et määrata kindlaks intsidendist mõjutatud piirkondade geograafiline ulatus, nagu on osutatud määruse (EL) 2022/2554 artikli 18 lõike 1 punktis c, hindavad finantssektori ettevõtjad, kas intsident avaldab või avaldas mõju teistes liikmesriikides, ning eelkõige selle mõju olulisust seoses mis tahes järgmisega:

a) kliendid ja finantssektori vastaspooled teistes liikmesriikides;

b) kontserni kuuluvad filiaalid või muud finantssektori ettevõtjad, kes tegutsevad teistes liikmesriikides;

c) finantsturutaristud või kolmandast isikust teenuseosutajad, mis võivad mõjutada teistes liikmesriikides tegutsevaid finantssektori ettevõtjaid, kellele nad teenuseid osutavad, niivõrd kui selline teave on kättesaadav.

Artikkel 5

Andmekadu

Intsidendiga kaasneva andmekao kindlaksmääramisel, nagu on osutatud määruse (EL) 2022/2554 artikli 18 lõike 1 punktis d, võtavad finantssektori ettevõtjad arvesse järgmist:

a) seoses andmete kättesaadavusega, kas intsident on muutnud finantssektori ettevõtja, tema klientide või vastaspoolte nõutavad andmed ajutiselt või püsivalt kättesaamatuks või kasutuskõlbmatuks;

b) seoses andmete autentsusega, kas intsident on seadnud ohtu andmeallika usaldusväärsuse;

c) seoses andmete usaldusväärsusega, kas intsident on kaasa toonud andmete loata muutmise, mis on muutnud need ebatäpseks või mittetäielikuks;

d) seoses andmete konfidentsiaalsusega, kas intsident on toonud kaasa selle, et loata isik või süsteem on andmetele juurde pääsenud või andmed on neile avalikustatud.

Artikkel 6

Mõjutatud teenuste kriitiline tähtsus

Mõjutatud teenuste kriitilise tähtsuse kindlaksmääramisel, nagu on osutatud määruse (EL) 2022/2554 artikli 18 lõike 1 punktis e, hindavad finantssektori ettevõtjad, kas intsident:

a) mõjutab või on mõjutanud IKT-teenuseid või võrgu- ja infosüsteeme, mis toetavad finantssektori ettevõtja kriitilise tähtsusega või olulisi funktsioone;

b) mõjutab või on mõjutanud finantssektori ettevõtja osutatavaid finantsteenuseid, mis vajavad tegevusluba või registreerimist või mille üle teevad järelevalvet pädevad asutused;

c) kujutab või on kujutanud endast edukat, pahatahtlikku ja loata juurdepääsu finantssektori ettevõtja võrgu- ja infosüsteemidele.

Artikkel 7

Majanduslik mõju

1. Intsidendi majandusliku mõju kindlaksmääramisel, nagu on osutatud määruse (EL) 2022/2554 artikli 18 lõike 1 punktis f, võtavad finantssektori ettevõtjad arvesse järgmist liiki otseseid ja kaudseid kulusid ja kahjusid (võtmata arvesse tagasi saadud summasid), mida nad on kandnud intsidendi tõttu:

a) sundvõõrandatud rahalised vahendid või finantsvarad, mille eest nad vastutavad, sealhulgas varguse tõttu kaotatud varad;

b) tarkvara, riistvara või taristu asendamise või ümberpaigutamise kulud;

c) personalikulud, sealhulgas kulud, mis on seotud töötajate asendamise või ümberpaigutamise, lisatöötajate värbamise, ületunnitöö tasustamise ning kaotatud või vähenenud oskuste taastamisega;

d) lepinguliste kohustuste täitmata jätmisest tulenevad tasud;

e) kahju heastamise ja klientidele hüvitamise kulud;

f) saamata jäänud tulust tulenev kahju;

g) sise- ja välissuhtlusega seotud kulud;

h) nõustamiskulud, sealhulgas õigusnõustamise, kohtuekspertiisi ja parandusteenustega seotud kulud.

2. Lõikes 1 osutatud kulud ja kahju ei hõlma igapäevaseks äritegevuseks vajalikke kulusid, eelkõige järgmist:

a) taristu, seadmete, riist- ja tarkvara üldise hoolduse kulud ning personali oskuste täiendamise kulud;

b) sise- ja väliskulud, mis on seotud äritegevuse edendamisega pärast intsidenti, sealhulgas ajakohastamised, täiustused ja riskihindamise algatused;

c) kindlustusmaksed.

3. Finantssektori ettevõtjad arvutavad kulu- ja kahjusummad aruandluse ajal kättesaadavate andmete põhjal. Kui tegelikke kulu- ja kahjusummasid ei ole võimalik kindlaks määrata, hindavad finantssektori ettevõtjad neid summasid.

4. Intsidendi majandusliku mõju hindamisel liidavad finantssektori ettevõtjad kokku lõikes 1 osutatud kulud ja kahjud.

II PEATÜKK

TÕSISED INTSIDENDID JA OLULISUSE LÄVED

Artikkel 8

Tõsised intsidendid

1. Intsidenti loetakse määruse (EL) 2022/2554 artikli 19 lõike 1 kohaldamisel tõsiseks intsidendiks, kui see on mõjutanud artiklis 6 osutatud kriitilise tähtsusega teenuseid ja kui on täidetud mõni järgmistest tingimustest:

a) artikli 9 lõike 5 punktis b osutatud olulisuse lävi on ületatud;

b) ületatud on kaks või enam artikli 9 lõigetes 1–6 osutatud olulisuse läve.

2. Korduvaid intsidente, mida eraldi ei käsitata tõsise intsidendina vastavalt lõikele 1, käsitatakse ühe tõsise intsidendina, kui need vastavad kõigile järgmistele tingimustele:

a) need on toimunud vähemalt kaks korda kuue kuu jooksul;

b) neil on sama ilmne algpõhjus, nagu on osutatud määruse (EL) 2022/2554 artikli 20 esimese lõigu punktis b;

c) nad vastavad ühiselt lõike 1 kohastele tõsise intsidendina käsitamise kriteeriumidele.

Finantssektori ettevõtjad hindavad korduvate intsidentide olemasolu kord kuus.

Käesolevat lõiget ei kohaldata mikroettevõtjate ja määruse (EL) 2022/2554 artikli 16 lõikes 1 loetletud finantssektori ettevõtjate suhtes.

Artikkel 9

Olulisuse läved tõsiste intsidentide kindlaksmääramiseks

1. Klientide, finantssektori vastaspoolte ja tehingute kriteeriumi olulisuse lävi on ületatud, kui on täidetud mõni järgmistest tingimustest:

a) mõjutatud klientide arv on suurem kui 10 % kõigist mõjutatud teenust kasutavatest klientidest;

b) mõjutatud teenust kasutavate mõjutatud klientide arv on suurem kui 100 000;

c) mõjutatud finantssektori vastaspoolte arv on suurem kui 30 % kõigist finantssektori vastaspooltest, kelle tegevus on seotud mõjutatud teenuse osutamisega;

d) mõjutatud tehingute arv on suurem kui 10 % finantssektori ettevõtja päeva keskmisest selliste tehingute arvust, mis on seotud mõjutatud teenusega;

e) mõjutatud tehingute summa on suurem kui 10 % finantssektori ettevõtja päeva keskmisest selliste tehingute summast, mis on seotud mõjutatud teenusega;

f) mõjutatud on artikli 1 lõike 3 kohaselt asjakohasteks tunnistatud kliendid või finantssektori vastaspooled.

Kui mõjutatud klientide või finantssektori vastaspoolte tegelikku arvu või mõjutatud tehingute tegelikku arvu või summat ei ole võimalik kindlaks määrata, hindab finantssektori ettevõtja neid arve või summasid võrreldavate vaatlusperioodide kättesaadavate andmete põhjal.

2. Mainele avalduva mõju kriteeriumi olulisuse lävi on ületatud, kui on täidetud mõni artikli 2 punktides a–d sätestatud tingimustest.

3. Kestuse ja teenuse seisaku aja kriteeriumi olulisuse lävi on ületatud, kui on täidetud mõni järgmistest tingimustest:

a) intsidendi kestus on pikem kui 24 tundi;

b) kriitilise tähtsusega või olulisi funktsioone toetavate IKT-teenuste puhul on teenuse seisaku aeg pikem kui 2 tundi.

4. Geograafilise ulatuse kriteeriumi olulisuse lävi on ületatud, kui intsidendil on mõju kahes või enamas liikmesriigis vastavalt artiklile 4.

5. Andmekao kriteeriumi olulisuse lävi on ületatud, kui on täidetud mõni järgmistest tingimustest:

a) igasugune artiklis 5 osutatud mõju andmete kättesaadavusele, autentsusele, usaldusväärsusele või konfidentsiaalsusele on avaldanud või avaldab omakorda negatiivset mõju finantssektori ettevõtja ärieesmärkide saavutamisele või tema suutlikkusele täita regulatiivseid nõudeid;

b) mis tahes edukas, pahatahtlik ja loata juurdepääs, mis ei ole hõlmatud punktiga a, võrgu- ja infosüsteemidele, kui selline juurdepääs võib põhjustada andmekadu.

6. Majandusliku mõju kriteeriumi olulisuse lävi on ületatud, kui finantssektori ettevõtjale intsidendi tõttu tekkinud kulud ja kahjud on ületanud või tõenäoliselt ületavad 100 000 eurot.

III PEATÜKK

OLULISED KÜBEROHUD

Artikkel 10

Kõrged olulisuse läved oluliste küberohtude kindlakstegemiseks

Määruse (EL) 2022/2554 artikli 18 lõike 2 kohaldamisel peetakse küberohtu oluliseks, kui on täidetud kõik järgmised tingimused:

a) finantssektori ettevõtjale kättesaadava teabe alusel võib küberoht realiseerumise korral mõjutada või oleks võinud mõjutada finantssektori ettevõtja kriitilise tähtsusega või olulisi funktsioone või muid finantssektori ettevõtjaid, kolmandast isikust teenuseosutajaid, kliente või finantssektori vastaspooli;

b) küberoht võib suure tõenäosusega realiseeruda finantssektori ettevõtjas või muudes finantssektori ettevõtjates, võttes arvesse vähemalt järgmisi elemente:

   i) punktis a osutatud küberohuga seotud kohaldatavad riskid, sealhulgas finantssektori ettevõtja süsteemide võimalikud nõrkused, mida saab ära kasutada;

   ii) ohusubjektide suutlikkus ja kavatsus niivõrd, kui see on finantssektori ettevõtjale teada;

   iii) ohu püsimine ja mis tahes kogutud teave intsidentide kohta, mis on mõjutanud finantssektori ettevõtjat või tema kolmandast isikust teenuseosutajat, kliente või finantssektori vastaspooli;

c) küberoht võib realiseerumise korral vastata mõnele järgmistest:

   i) määruse (EL) 2022/2554 artikli 18 lõike 1 punktis e sätestatud teenuste kriitilise tähtsuse kriteerium, nagu on täpsustatud käesoleva määruse artiklis 6;

   ii) artikli 9 lõikes 1 sätestatud olulisuse lävi;

   iii) artikli 9 lõikes 4 sätestatud olulisuse lävi.

Kui finantssektori ettevõtja jõuab olenevalt küberohu liigist ja kättesaadavast teabest järeldusele, et artikli 9 lõigetes 2, 3, 5 ja 6 sätestatud olulisuse läved võivad olla ületatud, võib arvesse võtta ka neid lävesid.

IV PEATÜKK

TÕSISTE INTSIDENTIDE OLULISUS TEISTE LIIKMESRIIKIDE PÄDEVATE ASUTUSTE JAOKS JA RAPORTITE ÜKSIKASJAD, MIDA JAGATAKSE TEISTE PÄDEVATE ASUTUSTEGA

Artikkel 11

Tõsiste intsidentide olulisus teiste liikmesriikide pädevate asutuste jaoks

Selle hindamisel, kas tõsine intsident on oluline teiste liikmesriikide pädevate asutuste jaoks, nagu on osutatud määruse (EL) 2022/2554 artikli 19 lõikes 7, tuginetakse sellele, kas intsidendi algpõhjus on pärit teisest liikmesriigist või kas intsident avaldab või on avaldanud teises liikmesriigis olulist mõju seoses mõne järgmisega:

a) kliendid või finantssektori vastaspooled;

b) finantssektori ettevõtja või kontserni kuuluva muu finantssektori ettevõtja filiaal;

c) finantsturutaristu või kolmandast isikust teenuseosutaja, mis võib mõjutada finantssektori ettevõtjaid, kellele nad teenuseid osutavad.

Artikkel 12

Tõsiste intsidentide üksikasjad, mida jagatakse teiste pädevate asutustega

Tõsiste intsidentide üksikasjad, mille pädevad asutused peavad esitama teistele pädevatele asutustele vastavalt määruse (EL) 2022/2554 artikli 19 lõikele 6, ning teated, mille EBA, ESMA või EIOPA ja EKP peavad esitama teiste liikmesriikide asjaomastele pädevatele asutustele vastavalt kõnealuse määruse artikli 19 lõikele 7, sisaldavad anonüümimata ja samal tasemel teavet nagu finantssektori ettevõtjatelt määruse (EL) 2022/2554 artikli 19 lõike 4 kohaselt tõsiste intsidentide kohta saadud teated ja raportid.

V PEATÜKK

LÕPPSÄTTED

Artikkel 13

Jõustumine

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

Käesolev määrus on tervikuna siduv ja vahetult kohaldatav kõikides liikmesriikides.

Brüssel, 13. märts 2024

Komisjoni nimel
president
Ursula VON DER LEYEN