Publicatieblad
van de Europese Unie

NL
L-serie

2024/1772

25.6.2024

GEDELEGEERDE VERORDENING (EU) 2024/1772 VAN DE COMMISSIE

van 13 maart 2024

tot aanvulling van Verordening (EU) 2022/2554 van het Europees Parlement en de Raad met betrekking tot technische reguleringsnormen tot nadere bepaling van de criteria voor de classificatie van ICT-gerelateerde incidenten en cyberdreigingen, tot vaststelling van materialiteitsdrempels en tot bepaling van de nadere informatie van verslagen over ernstige incidenten

(Voor de EER relevante tekst)

DE EUROPESE COMMISSIE,

Gezien het Verdrag betreffende de werking van de Europese Unie,

Gezien Verordening (EU) 2022/2554 van het Europees Parlement en de Raad van 14 december 2022 betreffende digitale operationele weerbaarheid voor de financiële sector en tot wijziging van Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 en (EU) 2016/1011 ([1]), en met name artikel 18, lid 4, derde alinea,

Overwegende hetgeen volgt:

(1) Verordening (EU) 2022/2554 heeft tot doel de rapportagevereisten voor ICT-gerelateerde incidenten en betalingsgerelateerde operationele of beveiligingsincidenten die kredietinstellingen, betalingsinstellingen, aanbieders van rekeninginformatiediensten en instellingen voor elektronisch geld betreffen ("incidenten") te harmoniseren en te stroomlijnen. Aangezien de rapportagevereisten betrekking hebben op twintig verschillende soorten financiële entiteiten, moeten de classificatiecriteria en de materialiteitsdrempels voor het bepalen van ernstige incidenten en significante cyberdreigingen op eenvoudige, geharmoniseerde en consistente wijze worden gespecificeerd, waarbij rekening wordt gehouden met de specifieke kenmerken van de diensten en activiteiten van alle relevante financiële entiteiten.

(2) Met het oog op proportionaliteit moeten de classificatiecriteria en de materialiteitsdrempels de omvang en het algemene risicoprofiel en de aard, schaal en complexiteit van de diensten van alle financiële entiteiten weerspiegelen. Bovendien moeten de criteria en materialiteitsdrempels zodanig worden opgesteld dat zij consequent van toepassing zijn op alle financiële entiteiten, ongeacht omvang en risicoprofiel van die entiteiten, en geen disproportionele rapportagelast vormen voor kleinere financiële entiteiten. Om situaties aan te pakken waarin een aanzienlijk aantal cliënten wordt getroffen door een incident dat als zodanig de toepasselijke drempel niet overschrijdt, moet echter een absolute drempel worden vastgesteld die voornamelijk gericht is op grotere financiële entiteiten.

(3) Met betrekking tot kaders voor het melden van incidenten, die bestonden vóór de inwerkingtreding van Verordening (EU) 2022/2554, moet de continuïteit voor financiële entiteiten worden gewaarborgd. Daarom moeten de classificatiecriteria en materialiteitsdrempels worden afgestemd en geïnspireerd op de EBA-richtsnoeren inzake de rapportage van ernstige incidenten uit hoofde van Richtlijn (EU) 2015/2366 van het Europees Parlement en de Raad ([2]), de richtsnoeren voor de informatie en kennisgeving van materiële wijzigingen die transactieregisters periodiek aan de ESMA moeten meedelen, het ECB-/GTM-rapportagekader voor cyberincidenten en andere relevante richtsnoeren. De classificatiecriteria en drempels moeten ook geschikt zijn voor de financiële entiteiten die vóór Verordening (EU) 2022/2554 niet onderworpen waren aan vereisten inzake het melden van incidenten.

(4) Wat het indelingscriterium "hoeveelheid en aantal getroffen transacties" betreft, is het begrip "transacties" ruim en omvat het verschillende activiteiten en diensten in de sectorale handelingen die van toepassing zijn op financiële entiteiten. Voor de toepassing van dat classificatiecriterium moeten betalingstransacties en alle vormen van uitwisseling van financiële instrumenten, cryptoactiva, grondstoffen of andere activa, ook in de vorm van margin, zekerheid of verpanding, zowel tegen contanten als tegen enig ander activum, worden bestreken. Alle transacties waarbij activa betrokken zijn waarvan de waarde in een geldbedrag kan worden uitgedrukt, moeten voor classificatiedoeleinden in aanmerking worden genomen.

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

([2]) Richtlijn (EU) 2015/2366 van het Europees Parlement en de Raad van 25 november 2015 betreffende betalingsdiensten in de interne markt, houdende wijziging van de Richtlijnen 2002/65/EG, 2009/110/EG en 2013/36/EU en Verordening (EU) nr. 1093/2010 en houdende intrekking van Richtlijn 2007/64/EG (PB L 337 van 23.12.2015, blz. 35, ELI: http://data.europa.eu/eli/dir/2015/2366/oj).

(5) De classificatiecriteria moeten ervoor zorgen dat alle relevante soorten ernstige incidenten in kaart worden gebracht. Cyberaanvallen in verband met indringing in netwerk- of informatiesystemen vallen mogelijk niet noodzakelijkerwijs onder heel wat van de classificatiecriteria. Zij zijn echter belangrijk omdat elke inmenging in netwerk- en informatiesystemen schade kan toebrengen aan de financiële entiteit. Daarom moeten de classificatiecriteria "getroffen kritieke diensten" en "gegevensverliezen" op zodanige wijze worden gespecificeerd dat rekening wordt gehouden met deze soorten ernstige incidenten, met name ongeoorloofde inbreuken die, ook al zijn de effecten niet onmiddellijk bekend, tot ernstige gevolgen kunnen leiden, met name inbreuken in verband met gegevens en gegevenslekken.

(6) Aangezien kredietinstellingen onderworpen zijn aan zowel het kader voor de classificatie van incidenten op grond van artikel 18 van Verordening (EU) 2022/2554 als het kader voor operationeel risico van Gedelegeerde Verordening (EU) 2018/959 van de Commissie ([3]), moet de aanpak voor de beoordeling van de economische gevolgen van een incident op basis van de berekening van de kosten en verliezen zo consistent mogelijk zijn tussen beide kaders om onverenigbare of tegenstrijdige vereisten te voorkomen.

(7) Het in artikel 18, lid 1, punt c), van Verordening (EU) 2022/2554 vastgestelde criterium met betrekking tot de geografische spreiding van een incident moet gericht zijn op de grensoverschrijdende gevolgen van het incident, aangezien de gevolgen van een incident voor de activiteiten van een financiële entiteit binnen één rechtsgebied onder de andere criteria van dat artikel zullen vallen.

(8) Aangezien de classificatiecriteria onderling afhankelijk en verbonden zijn, moet de aanpak voor het identificeren van ernstige incidenten die overeenkomstig artikel 19, lid 1, van Verordening (EU) 2022/2554 moeten worden gemeld, worden gebaseerd op een combinatie van criteria, waarbij sommige criteria die nauw verband houden met de definities van een ICT-gerelateerd incident en een ernstig ICT-gerelateerd incident als bedoeld in artikel 3, leden 8 en 10, van Verordening (EU) 2022/2554, meer moeten doorwegen bij de classificatie van ernstige incidenten dan andere criteria.

(9) Om ervoor te zorgen dat de door de bevoegde autoriteiten uit hoofde van artikel 19, lid 1, van Verordening (EU) 2022/2554 ontvangen meldingen van ernstige incidenten zowel dienen voor toezichtdoeleinden als ter voorkoming van besmetting in de financiële sector, moeten de materialiteitsdrempels het mogelijk maken om ernstige incidenten in kaart te brengen, door zich onder meer te richten op de gevolgen voor entiteitspecifieke kritieke diensten, de specifieke absolute en relatieve drempels van cliënten of financiële tegenpartijen, transacties die wijzen op een materieel effect op de financiële entiteit, en het belang van de impact in andere lidstaten.

(10) Incidenten die gevolgen hebben voor ICT-diensten of netwerk- en informatiesystemen die kritieke of belangrijke functies of financiële diensten waarvoor een vergunning nodig is, ondersteunen, of kwaadwillige ongeoorloofde toegang tot netwerk- en informatiesystemen die kritieke of belangrijke functies ondersteunen, moeten worden beschouwd als incidenten die kritieke diensten van de financiële entiteiten treffen. Kwaadwillige, ongeoorloofde toegang tot netwerk- en informatiesystemen die kritieke of belangrijke functies van financiële entiteiten ondersteunen, brengt ernstige risico's met zich mee voor de financiële entiteit en moet, gezien de mogelijke gevolgen voor andere financiële entiteiten, altijd worden beschouwd als ernstige incident dat moeten worden gemeld.

(11) Terugkerende incidenten die verband houden met een kennelijk soortgelijke onderliggende oorzaak, die afzonderlijk geen ernstige incidenten zijn, kunnen wijzen op significante tekortkomingen en zwakke punten in de procedures voor incidenten- en risicobeheer van de financiële entiteit. Daarom moeten terugkerende incidenten collectief als ernstige incidenten worden beschouwd wanneer zij zich gedurende een bepaalde periode herhaaldelijk voordoen.

(12) Aangezien cyberdreigingen negatieve gevolgen kunnen hebben voor de financiële entiteit en de sector, moeten de significante cyberdreigingen die financiële entiteiten kunnen indienen, aangeven hoe waarschijnlijk het is dat de dreiging werkelijkheid wordt en hoe kritiek de potentiële impact is. Om een duidelijke en consistente beoordeling van het belang van cyberdreigingen te waarborgen, moet de classificatie van een cyberdreiging als significant dan ook afhangen van de waarschijnlijkheid dat aan de classificatiecriteria voor ernstige incidenten en de drempel daarvoor zou worden voldaan indien de dreiging werkelijkheid was geworden, van het soort cyberdreiging en van de informatie waarover de financiële entiteit beschikt.

([3]) Gedelegeerde Verordening (EU) 2018/959 van de Commissie van 14 maart 2018 tot aanvulling van Verordening (EU) nr. 575/2013 van het Europees Parlement en de Raad ten aanzien van technische reguleringsnormen voor de specificatie van de beoordelingsmethode volgens welke de bevoegde autoriteiten instellingen toestaan geavanceerde meetbenaderingen voor operationeel risico te gebruiken (PB L 169 van 6.7.2018, blz. 1, ELI: http://data.europa.eu/eli/reg_del/2018/959/oj).

(13) Aangezien bevoegde autoriteiten in andere lidstaten in kennis moeten worden gesteld van incidenten die gevolgen hebben voor financiële entiteiten en cliënten in hun rechtsgebied, moet de beoordeling van de gevolgen in een ander rechtsgebied overeenkomstig artikel 19, lid 7, van Verordening (EU) 2022/2554 worden gebaseerd op de onderliggende oorzaak van het incident, op mogelijke besmetting via derde aanbieders en op financiëlemarktinfrastructuren, alsook op de gevolgen van het incident voor significante groepen cliënten of financiële tegenpartijen.

(14) De in artikel 19, leden 6 en 7, van Verordening (EU) 2022/2554 bedoelde procedures voor kennisgeving en verslaglegging moeten de respectieve ontvangers in staat stellen de gevolgen van de incidenten te beoordelen. Daarom moet de doorgegeven informatie betrekking hebben op alle details in de incidentverslagen die de financiële entiteit bij de bevoegde autoriteit indient.

(15) Wanneer een incident een inbreuk in verband met persoonsgegevens vormt overeenkomstig Verordening (EU) 2016/679 van het Europees Parlement en de Raad ([4]) en Richtlijn 2002/58/EG van het Europees Parlement en de Raad ([5]), mag deze verordening geen afbreuk doen aan de in die Uniewetgeving vastgestelde registratie- en meldingsverplichtingen voor inbreuken in verband met persoonsgegevens. De bevoegde autoriteiten moeten samenwerken en informatie uitwisselen over alle relevante aangelegenheden met de in Verordening (EU) 2016/679 en Richtlijn 2002/58/EG bedoelde autoriteiten.

(16) Deze verordening is gebaseerd op de ontwerpen van technische reguleringsnormen die door de Europese toezichthoudende autoriteiten, in overleg met het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa) en de Europese Centrale Bank (ECB), bij de Commissie zijn ingediend.

(17) Het Gemengd Comité van de Europese toezichthoudende autoriteiten als bedoeld in artikel 54 van Verordening (EU) nr. 1093/2010 van het Europees Parlement en de Raad ([6]), in artikel 54 van Verordening (EU) nr. 1094/2010 van het Europees Parlement en de Raad ([7]) en in artikel 54 van Verordening (EU) nr. 1095/2010 van het Europees Parlement en de Raad ([8]) heeft open publiek consultaties gehouden over de ontwerpen van technische reguleringsnormen waarop deze verordening is gebaseerd, heeft de mogelijke kosten en baten van die voorgestelde normen geanalyseerd en heeft het advies ingewonnen van de overeenkomstig artikel 37 van Verordening (EU) nr. 1093/2010 opgerichte Stakeholdergroep bankwezen, de overeenkomstig artikel 37 van Verordening (EU) nr. 1094/2010 opgerichte Stakeholdergroep verzekeringen en herverzekeringen en de overeenkomstig artikel 37 van Verordening (EU) nr. 1095/2010 opgerichte Stakeholdergroep effecten en markten.

([4]) Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PB L 119 van 4.5.2016, blz. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([5]) Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie) (PB L 201 van 31.7.2002, blz. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([6]) Verordening (EU) nr. 1093/2010 van het Europees Parlement en de Raad van 24 november 2010 tot oprichting van een Europese toezichthoudende autoriteit (Europese Bankautoriteit), tot wijziging van Besluit nr. 716/2009/EG en tot intrekking van Besluit 2009/78/EG van de Commissie (PB L 331 van 15.12.2010, blz. 12, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([7]) Verordening (EU) nr. 1094/2010 van het Europees Parlement en de Raad van 24 november 2010 tot oprichting van een Europese toezichthoudende autoriteit (Europese Autoriteit voor verzekeringen en bedrijfspensioenen), tot wijziging van Besluit nr. 716/2009/EG en tot intrekking van Besluit 2009/79/EG van de Commissie (PB L 331 van 15.12.2010, blz. 48, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([8]) Verordening (EU) nr. 1095/2010 van het Europees Parlement en de Raad van 24 november 2010 tot oprichting van een Europese toezichthoudende autoriteit (Europese Autoriteit voor effecten en markten), tot wijziging van Besluit nr. 716/2009/EG en tot intrekking van Besluit 2009/77/EG van de Commissie (PB L 331 van 15.12.2010, blz. 84), ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

(18) De Europese Toezichthouder voor gegevensbescherming is geraadpleegd overeenkomstig artikel 42, lid 1, van Verordening (EU) 2018/1725 van het Europees Parlement en de Raad ([9]) en heeft op 24 januari 2024 een advies uitgebracht,

HEEFT DE VOLGENDE VERORDENING VASTGESTELD:

HOOFDSTUK I

CLASSIFICATIECRITERIA

Artikel 1

Cliënten, financiële tegenpartijen en transacties

1. Het aantal cliënten dat is getroffen door het incident als bedoeld in artikel 18, lid 1, punt a), van Verordening (EU) 2022/2554, is het totale aantal getroffen cliënten, ongeacht of het natuurlijke of rechtspersonen betreft, die tijdens het incident gebruikmaken van de door de financiële entiteit verleende dienst of die door het incident negatief zijn beïnvloed. Dit aantal omvat ook derde partijen die uitdrukkelijk vallen onder de contractuele overeenkomst tussen de financiële entiteit en de cliënt als begunstigden van de betrokken dienst.

2. Het aantal door het incident getroffen financiële tegenpartijen als bedoeld in artikel 18, lid 1, punt a), van Verordening (EU) 2022/2554, is het totale aantal getroffen financiële tegenpartijen die een contractuele overeenkomst met de financiële entiteit hebben gesloten.

3. Met betrekking tot de relevantie van cliënten en financiële tegenpartijen die getroffen zijn door het incident als bedoeld in artikel 18, lid 1, punt a), van Verordening (EU) 2022/2554, houdt de financiële entiteit rekening met de mate waarin de gevolgen voor een cliënt of een financiële tegenpartij van invloed zullen zijn op de verwezenlijking van de bedrijfsdoelstellingen van de financiële entiteit, alsook met de mogelijke gevolgen van het incident voor de marktefficiëntie.

4. Met betrekking tot de hoeveelheid of het aantal door het incident als bedoeld in artikel 18, lid 1, punt a), van Verordening (EU) 2022/2554 getroffen transacties, houdt de financiële entiteit rekening met alle getroffen transacties waarbij een geldbedrag betrokken is waarbij ten minste één deel van de transactie in de Unie wordt uitgevoerd.

5. Indien het werkelijke aantal getroffen cliënten of financiële tegenpartijen of het werkelijke aantal of de werkelijke hoeveelheid getroffen transacties niet kan worden bepaald, raamt de financiële entiteit die aantallen of hoeveelheden op basis van beschikbare gegevens van vergelijkbare referentieperioden.

Artikel 2

Reputatieschade

1. Voor het bepalen van de reputatieschade door het incident als bedoeld in artikel 18, lid 1, punt a), van Verordening (EU) 2022/2554, gaan financiële entiteiten ervan uit dat zich een reputatieschade heeft voorgedaan wanneer aan ten minste een van de volgende criteria is voldaan:

a) over het incident is bericht in de media;

b) het incident heeft geleid tot herhaalde klachten van verschillende cliënten of financiële tegenpartijen over diensten of kritieke zakelijke relaties;

c) de financiële entiteit zal als gevolg van het incident niet of wellicht niet in staat zijn aan de wettelijke vereisten te voldoen;

d) de financiële entiteit zal als gevolg van het incident cliënten of financiële tegenpartijen met een wezenlijke impact op haar bedrijfsactiviteiten verliezen of wellicht verliezen.

([9]) Verordening (EU) 2018/1725 van het Europees Parlement en de Raad van 23 oktober 2018 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de instellingen, organen en instanties van de Unie en betreffende het vrije verkeer van die gegevens, en tot intrekking van Verordening (EG) nr. 45/2001 en Besluit nr. 1247/2002/EG (PB L 295 van 21.11.2018, blz. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

2. Bij het beoordelen van de reputatieschade door het incident houden financiële entiteiten rekening met de mate van zichtbaarheid die het incident heeft of wellicht zal hebben met betrekking tot elk in lid 1 vermeld criterium.

Artikel 3

Duur en uitvaltijd van de dienst

1. Financiële entiteiten meten de duur van een incident als bedoeld in artikel 18, lid 1, punt b), van Verordening (EU) 2022/2554, vanaf het moment waarop het incident zich voordoet tot het moment waarop het is opgelost.

Wanneer financiële entiteiten niet in staat zijn het tijdstip te bepalen waarop het incident zich heeft voorgedaan, meten zij de duur van het incident vanaf het moment waarop het is ontdekt. Wanneer financiële entiteiten zich ervan bewust worden dat het incident zich heeft voorgedaan voordat het werd ontdekt, meten zij de duur vanaf het moment waarop het incident is geregistreerd in netwerk- of systeemlogbestanden of andere gegevensbronnen.

Wanneer financiële entiteiten nog niet weten wanneer het incident zal worden opgelost of niet in staat zijn gegevens in logbestanden of andere gegevensbronnen te verifiëren, gebruiken zij ramingen.

2. Financiële entiteiten meten de uitvaltijd van de dienst door een incident als bedoeld in artikel 18, lid 1, punt b), van Verordening (EU) 2022/2554, vanaf het moment dat de dienst geheel of gedeeltelijk niet beschikbaar is voor cliënten, financiële tegenpartijen of andere interne of externe gebruikers tot het moment waarop de reguliere activiteiten of verrichtingen zijn hersteld tot het niveau van dienstverlening dat vóór het incident werd verleend. Wanneer de uitvaltijd van de dienst een vertraging in de dienstverlening veroorzaakt nadat de geregelde activiteiten of activiteiten zijn hersteld, wordt de uitvaltijd gemeten vanaf het begin van het incident tot het moment waarop die vertraagde dienst volledig wordt verleend.

Wanneer financiële entiteiten niet in staat zijn het tijdstip te bepalen waarop de dienst uitviel, meten zij de uitvaltijd van de dienst vanaf het moment dat deze werd ontdekt.

Artikel 4

Geografische spreiding

Om de geografische spreiding te bepalen met betrekking tot de gebieden die worden getroffen door het incident als bedoeld in artikel 18, lid 1, punt c), van Verordening (EU) 2022/2554, beoordelen financiële entiteiten of het incident gevolgen heeft of heeft gehad in andere lidstaten, en met name of het effect aanzienlijk is in verband met:

a) cliënten en financiële tegenpartijen in andere lidstaten;

b) bijkantoren of andere financiële entiteiten binnen de groep die activiteiten verrichten in andere lidstaten;

c) financiëlemarktinfrastructuren of derde aanbieders, die gevolgen kunnen hebben voor financiële entiteiten in andere lidstaten waaraan zij diensten verlenen, voor zover dergelijke informatie beschikbaar is.

Artikel 5

Gegevensverliezen

Voor het bepalen van de gegevensverliezen die het incident met zich meebrengt als bedoeld in artikel 18, lid 1, punt d), van Verordening (EU) 2022/2554, houden financiële entiteiten rekening met het volgende:

a) met betrekking tot de beschikbaarheid van gegevens, of het incident de gegevens waar de financiële entiteit, haar cliënten of haar tegenpartijen om verzoeken, tijdelijk of permanent ontoegankelijk of onbruikbaar heeft gemaakt;

b) met betrekking tot de authenticiteit van gegevens, of het incident de betrouwbaarheid van de gegevensbron in het gedrang heeft gebracht;

c) met betrekking tot de integriteit van gegevens, of het incident heeft geleid tot niet-toegestane wijzigingen van gegevens waardoor die onjuist of onvolledig zijn geworden;

d) met betrekking tot de vertrouwelijkheid van gegevens, de vraag of het incident ertoe heeft geleid dat gegevens zijn geraadpleegd door of vrijgegeven aan een niet-gemachtigde partij of systeem.

Artikel 6

Mate waarin getroffen diensten als cruciaal kunnen worden aangemerkt

Om te bepalen in welke mate de getroffen diensten als cruciaal kunnen worden aangemerkt als bedoeld in artikel 18, lid 1, punt e), van Verordening (EU) 2022/2554, beoordelen financiële entiteiten of het incident:

a) gevolgen heeft of heeft gehad voor ICT-diensten of netwerk- en informatiesystemen die kritieke of belangrijke functies van de financiële entiteit ondersteunen;

b) gevolgen heeft of heeft gehad voor financiële diensten die worden verleend door de financiële entiteit waarvoor een vergunning of registratie vereist is of die onder toezicht staan van bevoegde autoriteiten;

c) een succesvolle, kwaadwillige en ongeoorloofde toegang tot de netwerk- en informatiesystemen van de financiële entiteit vormt of heeft gevormd.

Artikel 7

Economische effecten

1. Voor het bepalen van de economische effecten van het incident als bedoeld in artikel 18, lid 1, punt f), van Verordening (EU) 2022/2554, houden financiële entiteiten, zonder rekening te houden met financiële terugvorderingen, rekening met de volgende soorten directe en indirecte kosten en verliezen die zij als gevolg van het incident hebben gemaakt:

a) onteigende gelden of financiële activa waarvoor zij aansprakelijk zijn, met inbegrip van door diefstal verloren gegane activa;

b) kosten voor de vervanging of verplaatsing van software, hardware of infrastructuur;

c) personeelskosten, met inbegrip van kosten in verband met de vervanging of verhuizing van personeel, de aanwerving van extra personeel, de bezoldiging voor overuren en het terugverdienen van verloren of verminderde vaardigheden;

d) vergoedingen wegens niet-naleving van contractuele verplichtingen;

e) kosten voor verhaal en compensatie voor klanten;

f) verliezen als gevolg van gederfde inkomsten;

g) kosten voor interne en externe communicatie;

h) advieskosten, met inbegrip van kosten in verband met juridisch advies, forensische diensten en saneringsdiensten.

2. Kosten en verliezen als bedoeld in lid 1 omvatten geen kosten die nodig zijn voor de dagelijkse bedrijfsvoering van het bedrijf, met name geen:

a) kosten voor algemeen onderhoud van infrastructuur, uitrusting, hardware en software, en kosten voor het up-to-date houden van de vaardigheden van het personeel;

b) interne of externe kosten om het bedrijf na het incident te verbeteren, met inbegrip van upgrades, verbeteringen en risicobeoordelingsinitiatieven;

c) verzekeringspremies.

3. Financiële entiteiten berekenen de bedragen van de kosten en verliezen op basis van gegevens die ten tijde van de rapportage beschikbaar zijn. Indien de werkelijke bedragen van de kosten en verliezen niet kunnen worden bepaald, ramen financiële entiteiten die bedragen.

4. Bij de beoordeling van de economische gevolgen van het incident tellen financiële entiteiten de in lid 1 bedoelde kosten en verliezen samen.

HOOFDSTUK II

ERNSTIGE INCIDENTEN EN MATERIALITEITSDREMPELS

Artikel 8

Ernstige incidenten

1. Een incident wordt voor de toepassing van artikel 19, lid 1, van Verordening (EU) 2022/2554 als een ernstig incident beschouwd wanneer het gevolgen heeft gehad voor kritieke diensten als bedoeld in artikel 6 en indien aan een van de volgende voorwaarden is voldaan:

a) de in artikel 9, lid 5, punt b), bedoelde materialiteitsdrempel wordt bereikt;

b) twee of meer van de andere in de artikelen 9, leden 1 tot en met 6, genoemde materialiteitsdrempels worden bereikt.

2. Terugkerende incidenten die afzonderlijk niet als een ernstig incident overeenkomstig lid 1 worden beschouwd, worden als één ernstig incident beschouwd indien zij aan alle volgende voorwaarden voldoen:

a) zij hebben zich ten minste tweemaal binnen zes maanden voorgedaan;

b) zij hebben dezelfde kennelijk onderliggende oorzaak als bedoeld in artikel 20, eerste alinea, punt b), van Verordening (EU) 2022/2554;

c) zij voldoen gezamenlijk aan de in artikel 1 genoemde criteria om als een ernstig incident te worden beschouwd.

Financiële entiteiten beoordelen maandelijks of er sprake is van terugkerende incidenten.

Dit lid is niet van toepassing op micro-ondernemingen en financiële entiteiten die zijn vermeld in artikel 16, lid 1, van Verordening (EU) 2022/2554.

Artikel 9

Materialiteitsdrempels voor het bepalen van ernstige incidenten

1. De materialiteitsdrempel voor het criterium “cliënten, financiële tegenpartijen en transacties” wordt bereikt wanneer aan een van de volgende voorwaarden is voldaan:

a) het aantal cliënten dat wordt getroffen, bedraagt meer dan 10 % van alle cliënten die van de betrokken dienst gebruikmaken;

b) het aantal getroffen cliënten dat van de getroffen dienst gebruikmaakt, bedraagt meer dan 100 000;

c) het aantal getroffen financiële tegenpartijen bedraagt meer dan 30 % van alle financiële tegenpartijen die activiteiten verrichten in verband met de verlening van de getroffen dienst;

d) het aantal getroffen transacties ligt hoger dan 10 % van het gemiddelde dagelijkse aantal transacties dat is uitgevoerd door de financiële entiteit die verband houdt met de getroffen dienst;

e) de hoeveelheid getroffen transacties ligt hoger dan 10 % van de dagelijkse gemiddelde waarde van de transacties die zijn uitgevoerd door de financiële entiteit die verband houdt met de getroffen dienst;

f) cliënten of financiële tegenpartijen die overeenkomstig artikel 1, lid 3, als relevant zijn aangemerkt, zijn getroffen.

Indien het werkelijke aantal getroffen cliënten of financiële tegenpartijen of het werkelijke aantal of de werkelijke hoeveelheid getroffen transacties niet kan worden bepaald, raamt de financiële entiteit die aantallen of hoeveelheden op basis van beschikbare gegevens van vergelijkbare referentieperioden.

2. De materialiteitsdrempel voor het criterium “reputatieschade” wordt bereikt wanneer aan een van de voorwaarden van artikel 2, punten a) tot en met d), is voldaan.

3. De materialiteitsdrempel voor het criterium “duur en uitvaltijd van de dienst” wordt bereikt wanneer aan een van de volgende voorwaarden is voldaan:

a) de duur van het incident is langer dan 24 uur;

b) de uitvaltijd van de dienst is langer dan twee uur voor ICT-diensten die kritieke of belangrijke functies ondersteunen.

4. De materialiteitsdrempel voor het criterium "geografische spreiding" wordt bereikt wanneer het incident gevolgen heeft in twee of meer lidstaten overeenkomstig artikel 4.

5. De materialiteitsdrempel voor het criterium "gegevensverliezen" wordt bereikt wanneer aan een van de volgende voorwaarden is voldaan:

a) een effect als bedoeld in artikel 5 op de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van gegevens heeft een negatief effect of zal een negatief effect hebben op de verwezenlijking van de bedrijfsdoelstellingen van de financiële entiteit of op haar vermogen om aan de regelgevingsvereisten te voldoen;

b) er is sprake van een niet onder punt a) vallende succesvolle, kwaadwillige en ongeoorloofde toegang tot netwerk- en informatiesystemen waarbij die toegang tot gegevensverliezen kan leiden.

6. De materialiteitsdrempel voor het criterium "economische effecten" wordt bereikt wanneer de kosten en verliezen die de financiële entiteit als gevolg van het incident heeft gemaakt, 100 000 EUR hebben overschreden of waarschijnlijk zullen overschrijden.

HOOFDSTUK III

SIGNIFICANTE CYBERDREIGINGEN

Artikel 10

Hoge materialiteitsdrempels voor het bepalen van significante cyberdreigingen

Voor de toepassing van artikel 18, lid 2, van Verordening (EU) 2022/2554 wordt een cyberdreiging als significant beschouwd wanneer aan alle volgende voorwaarden is voldaan:

a) de cyberdreiging, indien deze werkelijkheid wordt, kan gevolgen hebben of zou gevolgen kunnen hebben voor kritieke of belangrijke functies van de financiële entiteit, of voor andere financiële entiteiten, derde aanbieders, cliënten of financiële tegenpartijen, op basis van informatie waarover de financiële entiteit beschikt;

b) de cyberdreiging heeft een grote kans om werkelijkheid te worden bij de financiële entiteit of bij andere financiële entiteiten, rekening houdend met ten minste de volgende elementen:

   i) toepasselijke risico's in verband met de in punt a) bedoelde cyberdreiging, met inbegrip van potentiële kwetsbaarheden van de systemen van de financiële entiteit die kunnen worden uitgebuit;

   ii) de capaciteiten en intentie van dreigingsactoren voor zover bekend bij de financiële entiteit;

   iii) de aanhoudende dreiging en alle verworven kennis over incidenten die gevolgen hebben gehad voor de financiële entiteit of haar derde aanbieder, cliënten of financiële tegenpartijen;

c) de cyberdreiging kan, als zij werkelijkheid wordt, aan een van de volgende situaties voldoen:

   i) het in artikel 18, lid 1, punt e), van Verordening (EU) 2022/2554 vastgestelde criterium inzake de mate waarin diensten als cruciaal kunnen worden aangemerkt, zoals gespecificeerd in artikel 6 van deze verordening;

   ii) de in artikel 9, lid 1, vastgestelde materialiteitsdrempel;

   iii) de in artikel 9, lid 4, vastgestelde materialiteitsdrempel.

Wanneer de financiële entiteit, afhankelijk van het soort cyberdreiging en de beschikbare informatie, concludeert dat de in artikel 9, leden 2, 3, 5 en 6, vastgestelde materialiteitsdrempels kunnen worden bereikt, kunnen die drempels ook in aanmerking worden genomen.

HOOFDSTUK IV

RELEVANTIE VAN ERNSTIGE INCIDENTEN VOOR BEVOEGDE AUTORITEITEN VAN ANDERE LIDSTATEN EN NADERE INFORMATIE VAN VERSLAGEN DIE AAN ANDERE BEVOEGDE AUTORITEITEN MOETEN WORDEN MEEGEDEELD

Artikel 11

Relevantie van ernstige incidenten voor bevoegde autoriteiten in andere lidstaten

De beoordeling van de relevantie van het ernstige incident voor bevoegde autoriteiten in andere lidstaten als bedoeld in artikel 19, lid 7, van Verordening (EU) 2022/2554, wordt gebaseerd op de vraag of het incident een onderliggende oorzaak heeft die afkomstig is van een andere lidstaat, dan wel of het incident aanzienlijke gevolgen heeft of heeft gehad in een andere lidstaat met betrekking tot:

a) cliënten of financiële tegenpartijen;

b) een bijkantoor van de financiële entiteit of een andere financiële entiteit binnen de groep;

c) een financiëlemarktinfrastructuur of een derde aanbieder die gevolgen kunnen hebben voor de financiële entiteiten waaraan zij diensten verlenen.

Artikel 12

Nadere bijzonderheden over ernstige incidenten die met andere bevoegde autoriteiten moet worden gedeeld

Nadere bijzonderheden over ernstige incidenten die de bevoegde autoriteiten overeenkomstig artikel 19, lid 6, van Verordening (EU) 2022/2554 aan andere bevoegde autoriteiten moeten verstrekken en de kennisgevingen die de EBA, de ESMA of de Eiopa en de ECB overeenkomstig artikel 19, lid 7, van die verordening bij de relevante bevoegde autoriteiten in andere lidstaten moeten indienen, bevatten hetzelfde niveau van informatie, zonder enige anonimisering, als de kennisgevingen van en verslagen over ernstige incidenten die overeenkomstig artikel 19, lid 4, van Verordening (EU) 2022/2554 van financiële entiteiten zijn ontvangen.

HOOFDSTUK V

SLOTBEPALINGEN

Artikel 13

Inwerkingtreding

Deze verordening treedt in werking op de twintigste dag na die van de bekendmaking ervan in het *Publicatieblad van de Europese Unie*.

Deze verordening is verbindend in al haar onderdelen en is rechtstreeks toepasselijk in elke lidstaat.

Gedaan te Brussel, 13 maart 2024.

Voor de Commissie
De voorzitter
Ursula VON DER LEYEN