Amtsblatt
der Europäischen Union

DE
Reihe L

2024/1772

25.6.2024

DELEGIERTE VERORDNUNG (EU) 2024/1772 DER KOMMISSION

vom 13. März 2024

zur Ergänzung der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards zur Festlegung der Kriterien für die Klassifizierung von IKT-bezogenen Vorfällen und Cyberbedrohungen, der Wesentlichkeitsschwellen und der Einzelheiten von Meldungen schwerwiegender Vorfälle

(Text von Bedeutung für den EWR)

DIE EUROPÄISCHE KOMMISSION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

gestützt auf die Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011 ([1]), insbesondere auf Artikel 18 Absatz 4 Unterabsatz 3,

in Erwägung nachstehender Gründe:

(1) Die Verordnung (EU) 2022/2554 zielt darauf ab, die Anforderungen für die Meldung von IKT-bezogenen Vorfällen und von zahlungsbezogenen Betriebs- oder Sicherheitsvorfällen, die Kreditinstitute, Zahlungsinstitute, Kontoinformationsdienstleister und E-Geld-Institute betreffen, (im Folgenden „Vorfälle“) zu harmonisieren und zu straffen. Da die Meldeanforderungen für 20 unterschiedliche Arten von Finanzunternehmen gelten, sollten die Klassifizierungskriterien und Wesentlichkeitsschwellen für die Bestimmung schwerwiegender Vorfälle und erheblicher Cyberbedrohungen auf eine einfache, harmonisierte und kohärente Weise festgelegt werden, die den Besonderheiten der Dienstleistungen und Tätigkeiten aller relevanten Finanzunternehmen Rechnung trägt.

(2) Um Verhältnismäßigkeit sicherzustellen, sollten die Klassifizierungskriterien und Wesentlichkeitsschwellen die Größe und das Gesamtrisikoprofil sowie die Art, den Umfang und die Komplexität der Dienstleistungen aller Finanzunternehmen widerspiegeln. Darüber hinaus sollten die Kriterien und Wesentlichkeitsschwellen so konzipiert sein, dass sie für alle Finanzunternehmen unabhängig von deren Größe und Risikoprofil in kohärenter Weise gelten und kleineren Finanzunternehmen keinen unverhältnismäßigen Meldeaufwand auferlegen. Jedoch sollte für Fälle, in denen eine erhebliche Zahl von Kunden von einem Vorfall betroffen ist, der den geltenden Schwellenwert für sich genommen nicht überschreitet, ein absoluter Schwellenwert festgelegt werden, der hauptsächlich auf größere Finanzunternehmen abstellt.

(3) Im Falle bereits vor Inkrafttreten der Verordnung (EU) 2022/2554 bestehender Rahmenwerke für die Meldung von Vorfällen sollte den Finanzunternehmen Kontinuität gewährleistet werden. Deshalb sollten die Klassifizierungskriterien und Wesentlichkeitsschwellen auf die EBA-Leitlinien für die Meldung schwerwiegender Vorfälle gemäß der Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates ([2]), auf die Leitlinien für die regelmäßige Unterrichtung und die Meldung wesentlicher Änderungen an die ESMA durch Transaktionsregister, auf den EZB/SSM-Rahmen für die Meldung von Cybervorfällen und auf andere einschlägige Leitlinien abgestimmt sein und sich daran orientieren. Die Klassifizierungskriterien und Schwellenwerte sollten auch für Finanzunternehmen geeignet sein, die vor der Verordnung (EU) 2022/2554 noch keinen Anforderungen für die Meldung von Vorfällen unterlagen.

(4) Was das Klassifizierungskriterium „Wert und Anzahl der betroffenen Transaktionen“ betrifft, so ist der Begriff der Transaktion weit gefasst und beinhaltet verschiedene Tätigkeiten und Dienstleistungen aus den für Finanzunternehmen geltenden sektorspezifischen Rechtsakten. Für die Zwecke dieses Klassifizierungskriteriums sollten Zahlungsvorgänge und alle Formen des Austauschs von Finanzinstrumenten, Kryptowerten, Waren oder anderen Vermögenswerten, auch in Form von Einschüssen, Sicherheiten oder Pfandrechten, sowohl gegen Bargeld als auch gegen jeden anderen Vermögenswert, abgedeckt werden. Alle Transaktionen mit Vermögenswerten, deren Wert als Geldbetrag ausgedrückt werden kann, sollten für die Zwecke der Klassifizierung berücksichtigt werden.

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

([2]) Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25. November 2015 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 2002/65/EG, 2009/110/EG und 2013/36/EU und der Verordnung (EU) Nr. 1093/2010 sowie zur Aufhebung der Richtlinie 2007/64/EG (ABl. L 337 vom 23.12.2015, S. 35. ELI: http://data.europa.eu/eli/dir/2015/2366/oj).

(5) Die Klassifizierungskriterien sollten sicherstellen, dass alle relevanten Arten von schwerwiegenden Vorfällen erfasst werden. Cyberangriffe, die mit dem Eindringen in Netzwerk- oder Informationssysteme zusammenhängen, werden von vielen Klassifizierungskriterien möglicherweise nicht unbedingt erfasst. Jedoch sind sie bedeutsam, da jedes Eindringen in Netzwerk- und Informationssysteme dem Finanzunternehmen schaden kann. Dementsprechend sollten die Klassifizierungskriterien „betroffene kritische Dienstleistungen" und „Verluste von Daten" so festgelegt werden, dass diese Arten von schwerwiegenden Vorfällen erfasst werden, insbesondere auch unbefugtes Eindringen, das, auch wenn die Auswirkungen nicht unmittelbar bekannt sind, gravierende Folgen haben kann, vor allem Datenschutzverletzungen und Datenlecks.

(6) Da die Kreditinstitute sowohl dem Rahmen für die Klassifizierung von Vorfällen nach Artikel 18 der Verordnung (EU) 2022/2554 als auch dem Rahmen für operationelle Risiken gemäß der Delegierten Verordnung (EU) 2018/959 der Kommission ([3]) unterliegen, sollte der Ansatz für die Bewertung der wirtschaftlichen Auswirkungen eines Vorfalls auf Basis der Kosten- und Verlustkalkulation so weit wie möglich bei beiden Rahmen konsistent sein, damit keine unvereinbaren oder widersprüchlicher Anforderungen eingeführt werden.

(7) Das in Artikel 18 Absatz 1 Buchstabe c der Verordnung (EU) 2022/2554 festgelegte Kriterium der geografischen Ausbreitung eines Vorfalls sollte die grenzüberschreitenden Auswirkungen des Vorfalls in den Fokus nehmen, da die Auswirkungen eines Vorfalls auf die Tätigkeiten eines Finanzunternehmens innerhalb eines einzelnen Rechtsraums durch die anderen im genannten Artikel festgelegten Kriterien erfasst werden.

(8) Da die Klassifizierungskriterien voneinander abhängen und miteinander verknüpft sind, sollte der Ansatz für die Ermittlung schwerwiegender Vorfälle, die nach Artikel 19 Absatz 1 der Verordnung (EU) 2022/2554 gemeldet werden müssen, auf einer Kriterienkombination beruhen, wobei bestimmte Kriterien, die eng mit den in Artikel 3 Absätze 8 und 10 der Verordnung (EU) 2022/2554 enthaltenen Begriffsbestimmungen eines IKT-bezogenen Vorfalls bzw. schwerwiegender IKT-bezogener Vorfälle zusammenhängen, bei der Klassifizierung stärker im Vordergrund stehen sollten als andere Kriterien.

(9) Um sicherzustellen, dass die Meldungen über schwerwiegende Vorfälle, die die zuständigen Behörden nach Artikel 19 Absatz 1 der Verordnung (EU) 2022/2554 erhalten, sowohl Aufsichtszwecken als auch der Verhinderung einer finanzsektorweiten Ansteckung dienen, sollten es die Wesentlichkeitsschwellen ermöglichen, schwerwiegende Vorfälle zu erfassen, indem sie unter anderem die Auswirkungen auf unternehmensspezifische kritische Dienstleistungen, die spezifischen absoluten und relativen Schwellenwerte für Kunden oder finanzielle Gegenparteien, auf wesentliche Auswirkungen auf das Finanzunternehmen hinweisende Transaktionen und die Signifikanz der Auswirkungen in anderen Mitgliedstaaten in den Fokus nehmen.

(10) Vorfälle, die IKT-Dienstleistungen oder Netzwerk- und Informationssysteme zur Unterstützung kritischer oder wichtiger Funktionen oder zulassungspflichtige Finanzdienstleistungen betreffen, oder ein böswilliger unbefugter Zugriff auf Netzwerk- und Informationssysteme zur Unterstützung kritischer oder wichtiger Funktionen sollten als Vorfälle angesehen werden, die kritische Dienstleistungen der Finanzunternehmen betreffen. Ein böswilliger, unbefugter Zugriff auf Netzwerk- und Informationssysteme zur Unterstützung kritischer oder wichtiger Funktionen von Finanzunternehmen birgt ernsthafte Risiken für das Finanzunternehmen und sollte, da auch andere Finanzunternehmen davon betroffen sein könnten, stets als schwerwiegender Vorfall betrachtet werden, der gemeldet werden muss.

(11) Wiederholte Vorfälle mit offensichtlich ähnlicher Ursache, die einzeln betrachtet keine schwerwiegenden Vorfälle sind, können auf erhebliche Mängel und Schwächen in den Verfahren des Finanzunternehmens für das Management von Vorfällen und Risiken hinweisen. Deswegen sollten wiederholte Vorfälle insgesamt als schwerwiegend betrachtet werden, wenn sie über einen gewissen Zeitraum mehrfach auftreten.

(12) Da Cyberbedrohungen negative Auswirkungen auf das Finanzunternehmen und den Finanzsektor haben können, sollte bei etwaigen von den Finanzunternehmen gemeldeten erheblichen Cyberbedrohungen auf die Eintrittswahrscheinlichkeit und die Kritikalität der potenziellen Auswirkungen hingewiesen werden. Um eine eindeutige und konsistente Bewertung der Signifikanz von Cyberbedrohungen sicherzustellen, sollte die Klassifizierung einer Cyberbedrohung als erheblich von der Wahrscheinlichkeit, dass die Klassifizierungskriterien für schwerwiegende Vorfälle und die zugehörigen Schwellenwerte bei Eintritt der Bedrohung erfüllt würden, sowie von der Art der Cyberbedrohung und den verfügbaren Informationen des Finanzunternehmens abhängen.

([3]) Delegierte Verordnung (EU) 2018/959 der Kommission vom 14. März 2018 zur Ergänzung der Verordnung (EU) Nr. 575/2013 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards zur Festlegung der Beurteilungsmethode, nach der die zuständigen Behörden Instituten die Verwendung fortgeschrittener Messansätze für operationelle Risiken gestatten (ABl. L 169 vom 6.7.2018, S. 1. ELI: http://data.europa.eu/eli/reg_del/2018/959/oj).

(13) Da die zuständigen Behörden in anderen Mitgliedstaaten über Vorfälle, die sich auf Finanzunternehmen und Kunden in ihrem Hoheitsgebiet auswirken, benachrichtigt werden müssen, sollte die in Artikel 19 Absatz 7 der Verordnung (EU) 2022/2554 vorgesehene Bewertung der Auswirkungen in einem anderen Hoheitsgebiet auf den Ursachen des Vorfalls, dem Ansteckungspotenzial über Drittdienstleister und Finanzmarktinfrastrukturen sowie den Auswirkungen des Vorfalls auf bedeutende Gruppen von Kunden oder finanziellen Gegenparteien beruhen.

(14) Die in Artikel 19 Absätze 6 und 7 der Verordnung (EU) 2022/2554 genannten Melde- und Benachrichtigungsverfahren sollten es den jeweiligen Empfängern ermöglichen, die Auswirkungen der Vorfälle zu bewerten. Deswegen sollten die übermittelten Informationen alle Einzelheiten beinhalten, die in den Vorfallmeldungen des Finanzunternehmens an die zuständige Behörde enthalten sind.

(15) Stellt ein Vorfall eine Verletzung des Schutzes personenbezogener Daten im Sinne der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates ([4]) und der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates ([5]) dar, so sollte die vorliegende Verordnung die in den genannten Rechtsvorschriften der Union festgelegten Aufzeichnungs- und Benachrichtigungspflichten bei Verletzungen des Schutzes personenbezogener Daten unberührt lassen. Die zuständigen Behörden sollten mit den in der Verordnung (EU) 2016/679 und der Richtlinie 2002/58/EG genannten Behörden zusammenarbeiten und Informationen über alle relevanten Angelegenheiten austauschen.

(16) Diese Verordnung beruht auf dem Entwurf technischer Regulierungsstandards, den die Europäischen Aufsichtsbehörden der Kommission in Abstimmung mit der Agentur der Europäischen Union für Cybersicherheit (ENISA) und der Europäischen Zentralbank (EZB) vorgelegt haben.

(17) Der in Artikel 54 der Verordnung (EU) Nr. 1093/2010 des Europäischen Parlaments und des Rates ([6]), in Artikel 54 der Verordnung (EU) Nr. 1094/2010 des Europäischen Parlaments und des Rates ([7]) und in Artikel 54 der Verordnung (EU) Nr. 1095/2010 des Europäischen Parlaments und des Rates ([8]) genannte Gemeinsame Ausschuss der Europäischen Aufsichtsbehörden hat zu diesem Entwurf technischer Regulierungsstandards, auf dem die vorliegende Verordnung beruht, öffentliche Konsultationen durchgeführt, die damit verbundenen Kosten- und Nutzeneffekte analysiert und die Stellungnahme der nach Artikel 37 der Verordnung (EU) Nr. 1093/2010 eingesetzten Interessengruppe Bankensektor, der nach Artikel 37 der Verordnung (EU) Nr. 1094/2010 eingesetzten Interessengruppe Versicherung und Rückversicherung und der nach Artikel 37 der Verordnung (EU) Nr. 1095/2010 eingesetzten Interessengruppe Wertpapiere und Wertpapiermärkte eingeholt.

([4]) Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([5]) Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) (ABl. L 201 vom 31.7.2002, S. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([6]) Verordnung (EU) Nr. 1093/2010 des Europäischen Parlaments und des Rates vom 24. November 2010 zur Errichtung einer Europäischen Aufsichtsbehörde (Europäische Bankenaufsichtsbehörde), zur Änderung des Beschlusses Nr. 716/2009/EG und zur Aufhebung des Beschlusses 2009/78/EG der Kommission (ABl. L 331 vom 15.12.2010, S. 12. ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([7]) Verordnung (EU) Nr. 1094/2010 des Europäischen Parlaments und des Rates vom 24. November 2010 zur Errichtung einer Europäischen Aufsichtsbehörde (Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung), zur Änderung des Beschlusses Nr. 716/2009/EG und zur Aufhebung des Beschlusses 2009/79/EG der Kommission (ABl. L 331 vom 15.12.2010, S. 48. ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([8]) Verordnung (EU) Nr. 1095/2010 des Europäischen Parlaments und des Rates vom 24. November 2010 zur Errichtung einer Europäischen Aufsichtsbehörde (Europäische Wertpapier- und Marktaufsichtsbehörde), zur Änderung des Beschlusses Nr. 716/2009/EG und zur Aufhebung des Beschlusses 2009/77/EG der Kommission (ABl. L 331 vom 15.12.2010, S. 84. ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

(18) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates ([9]) angehört und hat am 24. Januar 2024 eine Stellungnahme abgegeben —

HAT FOLGENDE VERORDNUNG ERLASSEN:

KAPITEL I

KLASSIFIZIERUNGSKRITERIEN

Artikel 1

Kunden, finanzielle Gegenparteien und Transaktionen

(1) Die in Artikel 18 Absatz 1 Buchstabe a der Verordnung (EU) 2022/2554 genannte Anzahl der von dem Vorfall betroffenen Kunden spiegelt die Anzahl aller betroffenen Kunden unabhängig davon, ob es sich um natürliche oder juristische Personen handelt, wider, die den vom Finanzunternehmen bereitgestellten Dienst während des Vorfalls nicht nutzen können bzw. konnten oder die durch den Vorfall beeinträchtigt wurden. Diese Anzahl umfasst auch Dritte, die als Nutznießer der betroffenen Dienste ausdrücklich unter die vertragliche Vereinbarung zwischen dem Finanzunternehmen und dem Kunden fallen.

(2) Die in Artikel 18 Absatz 1 Buchstabe a der Verordnung (EU) 2022/2554 genannte Anzahl der von dem Vorfall betroffenen finanziellen Gegenparteien spiegelt die Anzahl aller betroffenen finanziellen Gegenparteien wider, die eine vertragliche Vereinbarung mit dem Finanzunternehmen geschlossen haben.

(3) In Bezug auf die in Artikel 18 Absatz 1 Buchstabe a der Verordnung (EU) 2022/2554 genannte Relevanz der von dem Vorfall betroffenen Kunden und finanziellen Gegenparteien berücksichtigt das Finanzunternehmen, in welchem Maße sich die Auswirkungen auf einen Kunden oder eine finanzielle Gegenpartei auf die Verwirklichung der Geschäftsziele des Finanzunternehmens auswirken werden und wie sich der Vorfall auf die Markteffizienz auswirken könnte.

(4) In Bezug auf den Wert oder die Anzahl der von dem Vorfall betroffenen Transaktionen im Sinne von Artikel 18 Absatz 1 Buchstabe a der Verordnung (EU) 2022/2554 berücksichtigt das Finanzunternehmen alle betroffenen Transaktionen über einen Geldbetrag, sofern mindestens ein Teil der Transaktion in der Union durchgeführt wird.

(5) Lässt sich die tatsächliche Anzahl der betroffenen Kunden oder finanziellen Gegenparteien oder die tatsächliche Anzahl oder der tatsächliche Wert der betroffenen Transaktionen nicht bestimmen, so schätzt das Finanzunternehmen diese Zahlen oder Werte auf der Grundlage verfügbarer Daten aus vergleichbaren Referenzzeiträumen.

Artikel 2

Reputationsschaden

(1) Zur Bestimmung des in Artikel 18 Absatz 1 Buchstabe a der Verordnung (EU) 2022/2554 genannten Reputationsschadens betrachten die Finanzunternehmen einen Reputationsschaden als eingetreten, wenn mindestens eines der folgenden Kriterien erfüllt ist:

a) über den Vorfall wurde in den Medien berichtet;

b) der Vorfall hat zu wiederholten Beschwerden verschiedener Kunden oder finanzieller Gegenparteien über kundenorientierte Dienstleistungen oder kritische Geschäftsbeziehungen geführt;

c) das Finanzunternehmen wird aufgrund des Vorfalls nicht oder wahrscheinlich nicht in der Lage sein, regulatorische Anforderungen zu erfüllen;

d) das Finanzunternehmen wird infolge des Vorfalls Kunden oder finanzielle Gegenparteien verlieren oder wahrscheinlich verlieren, was wesentliche Auswirkungen auf seine Geschäftstätigkeit haben wird.

([9]) Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG (ABl. L 295 vom 21.11.2018, S. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

(2) Bei der Bewertung der Reputationswirkung des Vorfalls berücksichtigen die Finanzunternehmen die Sichtbarkeit, die der Vorfall in Bezug auf jedes in Absatz 1 aufgeführte Kriterium erlangt hat oder wahrscheinlich erlangen wird.

Artikel 3

Dauer und Ausfallzeiten

(1) Die Finanzunternehmen messen die in Artikel 18 Absatz 1 Buchstabe b der Verordnung (EU) 2022/2554 genannte Dauer eines Vorfalls ab dem Zeitpunkt des Eintritts des Vorfalls bis zum Zeitpunkt der Behebung des Vorfalls.

Können die Finanzunternehmen den Eintrittszeitpunkt des Vorfalls nicht bestimmen, messen sie die Dauer des Vorfalls ab dem Zeitpunkt seiner Feststellung. Wissen Finanzunternehmen schon um den Vorfall, bevor er festgestellt wurde, messen sie die Dauer ab dem Zeitpunkt, zu dem der Vorfall in den Netzwerk- oder Systemprotokollen oder anderen Datenquellen aufgezeichnet wurde.

Wissen Finanzunternehmen noch nicht, wann der Vorfall behoben sein wird, oder können sie Aufzeichnungen in Protokollen oder anderen Datenquellen nicht verifizieren, so ziehen sie Schätzungen heran.

(2) Finanzunternehmen messen die in Artikel 18 Absatz 1 Buchstabe b der Verordnung (EU) 2022/2554 genannten Ausfallzeiten bei einem Vorfall ab dem Zeitpunkt, zu dem der Dienst für Kunden, finanzielle Gegenparteien oder andere interne oder externe Nutzer ganz oder teilweise nicht mehr verfügbar ist, bis zu dem Zeitpunkt, zu dem die regulären Tätigkeiten oder Vorgänge in dem vor dem Vorfall herrschenden Umfang wiederhergestellt sind. Führen die Ausfallzeiten nach der Wiederherstellung der regulären Tätigkeiten oder Vorgänge zu einer Verzögerung bei der Bereitstellung von Dienstleistungen, so werden die Ausfallzeiten vom Beginn des Vorfalls bis zu dem Zeitpunkt gemessen, zu dem die verzögerte Dienstleistung in vollem Umfang erbracht ist.

Können die Finanzunternehmen den Beginn der Ausfallzeiten nicht bestimmen, messen sie die Dauer der Ausfallzeiten ab dem Zeitpunkt ihrer Feststellung.

Artikel 4

Geografische Ausbreitung

Um die in Artikel 18 Absatz 1 Buchstabe c der Verordnung (EU) 2022/2554 genannte geografische Ausbreitung im Hinblick auf die von dem Vorfall betroffenen Gebiete zu bestimmen, bewerten Finanzunternehmen, ob der Vorfall Auswirkungen in anderen Mitgliedstaaten hat oder hatte, und insbesondere, wie erheblich die Auswirkungen in Bezug auf eines von Folgendem sind:

a) Kunden und finanzielle Gegenparteien in anderen Mitgliedstaaten;

b) Zweigniederlassungen oder andere Finanzunternehmen innerhalb der Gruppe, die in anderen Mitgliedstaaten tätig sind;

c) Finanzmarktinfrastrukturen oder Drittdienstleister mit möglichen Auswirkungen auf Finanzunternehmen in anderen Mitgliedstaaten, für die sie Dienstleistungen erbringen, soweit diese Informationen verfügbar sind.

Artikel 5

Verluste von Daten

Um die in Artikel 18 Absatz 1 Buchstabe d der Verordnung (EU) 2022/2554 genannten Verluste von Daten, die durch den Vorfall verursacht werden, zu bestimmen, berücksichtigen die Finanzunternehmen Folgendes:

a) in Bezug auf die Verfügbarkeit von Daten, ob der Vorfall die vom Finanzunternehmen, seinen Kunden oder seinen Gegenparteien nachgefragten Daten vorübergehend oder dauerhaft unzugänglich oder unbrauchbar gemacht hat;

b) in Bezug auf die Authentizität der Daten, ob der Vorfall die Vertrauenswürdigkeit der Datenquelle kompromittiert hat;

c) in Bezug auf die Integrität der Daten, ob der Vorfall zu einer nicht autorisierten Veränderung der Daten geführt hat, wodurch diese unrichtig oder unvollständig geworden sind;

d) in Bezug auf die Vertraulichkeit der Daten, ob der Vorfall dazu geführt hat, dass eine unbefugte Partei oder ein unbefugtes System Zugang zu oder Kenntnis von den Daten erhalten hat.

Artikel 6

Kritikalität der betroffenen Dienste

Um die in Artikel 18 Absatz 1 Buchstabe e der Verordnung (EU) 2022/2554 genannte Kritikalität der betroffenen Dienste zu bestimmen, bewerten die Finanzunternehmen, ob der Vorfall

a) IKT-Dienste oder Netzwerk- und Informationssysteme zur Unterstützung kritischer oder wichtiger Funktionen des Finanzunternehmens beeinträchtigt oder beeinträchtigt hat;

b) von dem Finanzunternehmen erbrachte Finanzdienstleistungen beeinträchtigt oder beeinträchtigt hat, die einer Zulassung oder Registrierung bedürfen oder von den zuständigen Behörden beaufsichtigt werden;

c) einen erfolgreichen, böswilligen und unbefugten Zugriff auf die Netzwerk- und Informationssysteme des Finanzunternehmens darstellt oder dargestellt hat.

Artikel 7

Wirtschaftliche Auswirkungen

(1) Zur Bestimmung der in Artikel 18 Absatz 1 Buchstabe f der Verordnung (EU) 2022/2554 genannten wirtschaftlichen Auswirkungen des Vorfalls berücksichtigen die Finanzunternehmen, ohne Einrechnung von finanziellen Wiedereinziehungen, die folgenden Arten von direkten und indirekten Kosten und Verlusten, die ihnen infolge des Vorfalls entstanden sind:

a) enteignete Mittel oder finanzielle Vermögenswerte, für die sie haften, einschließlich gestohlener Vermögenswerte;

b) Kosten für die Ersetzung oder Verlegung von Software, Hardware oder Infrastruktur;

c) Personalkosten, einschließlich Kosten im Zusammenhang mit der Ersetzung oder Verlegung von Personal, der Einstellung zusätzlichen Personals, der Vergütung von Überstunden und der Wiederherstellung verloren gegangener oder beeinträchtigter Kompetenzen;

d) Gebühren wegen Nichteinhaltung vertraglicher Verpflichtungen;

e) Kosten für Ausgleichs- und Entschädigungszahlungen an Kunden;

f) Verluste wegen entgangener Einnahmen;

g) Kosten für die interne und externe Kommunikation;

h) Beratungskosten, einschließlich Kosten für Rechtsberatung, forensische Dienstleistungen und Behebungsdienstleistungen.

(2) Die in Absatz 1 genannten Kosten und Verluste schließen keine Kosten ein, die für den alltäglichen Geschäftsbetrieb notwendig sind, insbesondere

a) keine Kosten für die allgemeine Instandhaltung von Infrastruktur, Ausrüstung, Hardware und Software und keine Kosten für die laufende Fortbildung des Personals, um dessen Kompetenzen auf Stand zu halten;

b) keine internen oder externen Kosten für die Verstärkung des Geschäftsbetriebs nach dem Vorfall, insbesondere auch keine Kosten für Upgrades, Verbesserungen und Initiativen zur Risikobewertung;

c) keine Versicherungsprämien.

(3) Die Finanzunternehmen berechnen die Höhe der Kosten und Verluste auf der Grundlage der zum Meldezeitpunkt verfügbaren Daten. Kann die tatsächliche Höhe der Kosten und Verluste nicht bestimmt werden, so schätzen die Finanzunternehmen die entsprechenden Beträge.

(4) Bei der Bewertung der wirtschaftlichen Auswirkungen des Vorfalls summieren die Finanzunternehmen die in Absatz 1 genannten Kosten und Verluste.

KAPITEL II

SCHWERWIEGENDE VORFÄLLE UND WESENTLICHKEITSSCHWELLEN

Artikel 8

Schwerwiegende Vorfälle

(1) Ein Vorfall wird für die Zwecke von Artikel 19 Absatz 1 der Verordnung (EU) 2022/2554 als schwerwiegender Vorfall angesehen, wenn die in Artikel 6 genannten kritischen Dienste beeinträchtigt und eine der folgenden beiden Bedingungen erfüllt ist:

a) Die in Artikel 9 Absatz 5 Buchstabe b genannte Wesentlichkeitsschwelle ist erreicht;

b) zwei oder mehr der in Artikel 9 Absätze 1 bis 6 genannten anderen Wesentlichkeitsschwellen sind erreicht.

(2) Wiederholte Vorfälle, die nach Absatz 1 einzeln betrachtet keine schwerwiegenden Vorfälle sind, werden zusammengenommen als schwerwiegender Vorfall betrachtet, wenn sie alle folgenden Bedingungen erfüllen:

a) Sie sind innerhalb von sechs Monaten mindestens zwei Mal aufgetreten;

b) sie haben dieselbe offensichtliche Ursache im Sinne von Artikel 20 Absatz 1 Buchstabe b der Verordnung (EU) 2022/2554;

c) sie erfüllen zusammengenommen die in Absatz 1 festgelegten Kriterien für die Betrachtung als schwerwiegender Vorfall.

Die Finanzunternehmen bewerten das Vorliegen wiederholter Vorfälle monatlich.

Dieser Absatz gilt nicht für Kleinstunternehmen und die in Artikel 16 Absatz 1 der Verordnung (EU) 2022/2554 genannten Finanzunternehmen.

Artikel 9

Wesentlichkeitsschwellen für die Bestimmung schwerwiegender Vorfälle

(1) Die Wesentlichkeitsschwelle für das Kriterium „Kunden, finanzielle Gegenparteien und Transaktionen“ ist erreicht, wenn eine der folgenden Bedingungen erfüllt ist:

a) Die Zahl der betroffenen Kunden beläuft sich auf mehr als 10 % aller Kunden, die die betroffene Dienstleistung nutzen;

b) die Zahl der betroffenen Kunden, die die betroffene Dienstleistung nutzen, liegt bei mehr als 100 000;

c) die Zahl der betroffenen finanziellen Gegenparteien beläuft sich auf mehr als 30 % aller finanziellen Gegenparteien, die Tätigkeiten im Zusammenhang mit der Bereitstellung der betroffenen Dienstleistung ausüben;

d) die Zahl der betroffenen Transaktionen beläuft sich auf mehr als 10 % der täglichen durchschnittlichen Zahl von Transaktionen, die das Finanzunternehmen im Zusammenhang mit der betroffenen Dienstleistung durchführt;

e) der Wert der betroffenen Transaktionen beträgt mehr als 10 % des täglichen Durchschnittswerts der Transaktionen, die das Finanzunternehmen im Zusammenhang mit der betroffenen Dienstleistung durchführt;

f) betroffen sind Kunden oder finanzielle Gegenparteien, die nach Artikel 1 Absatz 3 als relevant eingestuft wurden.

Lässt sich die tatsächliche Anzahl der betroffenen Kunden oder finanziellen Gegenparteien oder die tatsächliche Anzahl oder der tatsächliche Wert der betroffenen Transaktionen nicht bestimmen, so schätzt das Finanzunternehmen diese Zahlen oder Werte auf der Grundlage verfügbarer Daten aus vergleichbaren Referenzzeiträumen.

(2) Die Wesentlichkeitsschwelle für das Kriterium „Reputationsschaden“ ist erreicht, wenn eine der in Artikel 2 Buchstaben a bis d genannten Bedingungen erfüllt ist.

(3) Die Wesentlichkeitsschwelle für das Kriterium „Dauer und Ausfallzeiten“ ist erreicht, wenn eine der folgenden Bedingungen erfüllt ist:

a) Der Vorfall dauert mehr als 24 Stunden;

b) die Ausfallzeiten bei IKT-Diensten zur Unterstützung kritischer oder wichtiger Funktionen betragen mehr als zwei Stunden.

(4) Die Wesentlichkeitsschwelle für das Kriterium „geografische Ausbreitung“ ist erreicht, wenn der Vorfall im Sinne von Artikel 4 Auswirkungen in zwei oder mehr Mitgliedstaaten hat.

(5) Die Wesentlichkeitsschwelle für das Kriterium „Verluste von Daten“ ist erreicht, wenn eine der folgenden Bedingungen erfüllt ist:

a) Eine in Artikel 5 genannte Auswirkung auf die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von Daten hat negative Auswirkungen auf die Verwirklichung der Geschäftsziele des Finanzunternehmens oder auf dessen Fähigkeit, regulatorische Anforderungen zu erfüllen, oder wird solche negativen Auswirkungen haben;

b) es findet ein nicht unter Buchstabe a fallender erfolgreicher böswilliger und unbefugter Zugriff auf Netzwerk- und Informationssysteme statt, sofern dieser Zugriff zu Verlusten von Daten führen kann.

(6) Die Wesentlichkeitsschwelle für das Kriterium „wirtschaftliche Auswirkungen“ ist erreicht, wenn die Kosten und Verluste, die dem Finanzunternehmen durch den Vorfall entstanden sind, 100 000 EUR übersteigen oder wahrscheinlich übersteigen werden.

KAPITEL III

ERHEBLICHE CYBERBEDROHUNGEN

Artikel 10

Hohe Wesentlichkeitsschwellen für die Bestimmung erheblicher Cyberbedrohungen

Für die Zwecke von Artikel 18 Absatz 2 der Verordnung (EU) 2022/2554 wird eine Cyberbedrohung als erheblich angesehen, wenn alle folgenden Bedingungen erfüllt sind:

a) Die Cyberbedrohung könnte nach den verfügbaren Informationen des Finanzunternehmens bei Eintritt kritische oder wichtige Funktionen des Finanzunternehmens beeinträchtigen oder beeinträchtigt haben oder könnte andere Finanzunternehmen, Drittdienstleister, Kunden oder finanzielle Gegenparteien beeinträchtigen.

b) Die Cyberbedrohung hat eine hohe Eintrittswahrscheinlichkeit bei dem Finanzunternehmen oder bei anderen Finanzunternehmen, wenn mindestens die folgenden Elemente berücksichtigt werden:

   i) die mit der unter Buchstabe a genannten Cyberbedrohung zusammenhängenden einschlägigen Risiken, insbesondere auch potenzielle Schwachstellen der Systeme des Finanzunternehmens, die ausgenutzt werden können;

   ii) die Fähigkeiten und Absichten der Angreifer, soweit dem Finanzunternehmen bekannt;

   iii) das Anhalten der Bedrohung und etwaige Kenntnisse über bisherige Vorfälle, die sich auf das Finanzunternehmen oder dessen Drittdienstleister, Kunden oder finanzielle Gegenparteien ausgewirkt haben.

c) Die Cyberbedrohung könnte bei Eintritt das folgende Kriterium oder einen der folgenden Schwellenwerte erfüllen:

   i) das in Artikel 18 Absatz 1 Buchstabe e der Verordnung (EU) 2022/2554 genannte Kriterium der Kritikalität der Dienste, wie in Artikel 6 der vorliegenden Verordnung ausgeführt;

   ii) die in Artikel 9 Absatz 1 ausgeführte Wesentlichkeitsschwelle;

   iii) die in Artikel 9 Absatz 4 ausgeführte Wesentlichkeitsschwelle.

Kommt das Finanzunternehmen je nach Art der Cyberbedrohung und den verfügbaren Informationen zu dem Schluss, dass die in Artikel 9 Absätze 2, 3, 5 und 6 genannten Wesentlichkeitsschwellen erreicht werden könnten, so können diese Schwellenwerte ebenfalls berücksichtigt werden.

KAPITEL IV

RELEVANZ SCHWERWIEGENDER VORFÄLLE FÜR DIE ZUSTÄNDIGEN BEHÖRDEN IN ANDEREN MITGLIEDSTAATEN UND EINZELHEITEN DER MELDUNGEN AN ANDERE ZUSTÄNDIGE BEHÖRDEN

Artikel 11

Relevanz schwerwiegender Vorfälle für die zuständigen Behörden in anderen Mitgliedstaaten

Die in Artikel 19 Absatz 7 der Verordnung (EU) 2022/2554 genannte Bewertung, ob der schwerwiegende Vorfall für die zuständigen Behörden in anderen Mitgliedstaaten von Belang ist, stützt sich darauf, ob der Vorfall eine von einem anderen Mitgliedstaat ausgehende Ursache oder in einem anderen Mitgliedstaat erhebliche Auswirkungen in Bezug auf eines von Folgendem hat:

a) Kunden oder finanzielle Gegenparteien;

b) eine Zweigniederlassung des Finanzunternehmens oder ein anderes Finanzunternehmen innerhalb der Gruppe;

c) eine Finanzmarktinfrastruktur oder einen Drittdienstleister mit potenziellen Auswirkungen auf die Finanzunternehmen, für die Dienstleistungen erbracht werden.

Artikel 12

An andere zuständige Behörden zu übermittelnde Einzelheiten zu schwerwiegenden Vorfällen

Die Einzelheiten schwerwiegender Vorfälle, die von den zuständigen Behörden nach Artikel 19 Absatz 6 der Verordnung (EU) 2022/2554 an andere zuständige Behörden zu übermitteln sind, und die Benachrichtigungen, die die EBA, die ESMA oder die EIOPA und die EZB nach Artikel 19 Absatz 7 der genannten Verordnung an die jeweils zuständigen Behörden in anderen Mitgliedstaaten zu übermitteln haben, weisen denselben Umfang an Informationen — ohne Anonymisierung — auf wie die Meldungen schwerwiegender Vorfälle, die nach Artikel 19 Absatz 4 der Verordnung (EU) 2022/2554 von Finanzunternehmen vorzulegen sind.

KAPITEL V

SCHLUSSBESTIMMUNGEN

Artikel 13

Inkrafttreten

Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.

Brüssel, den 13. März 2024

Für die Kommission
Die Präsidentin
Ursula VON DER LEYEN