I

(Entschließungen, Empfehlungen und Stellungnahmen)

EMPFEHLUNGEN

EUROPÄISCHER AUSSCHUSS FÜR SYSTEMRISIKEN

EMPFEHLUNG DES EUROPÄISCHEN AUSSCHUSSES FÜR SYSTEMRISIKEN

vom 2. Dezember 2021

zu einem europaweiten Koordinierungsrahmen für betreffende Behörden in Bezug auf systemische Cybervorfälle

(ESRB/2021/17)

(2022/C 134/01)

DER VERWALTUNGSRAT DES EUROPÄISCHEN AUSSCHUSSES FÜR SYSTEMRISIKEN —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

gestützt auf das Abkommen über den Europäischen Wirtschaftsraum ([1]), insbesondere auf Anhang IX,

gestützt auf die Verordnung (EU) Nr. 1092/2010 des Europäischen Parlaments und des Rates vom 24. November 2010 über die Finanzaufsicht der Europäischen Union auf Makroebene und zur Errichtung eines Europäischen Ausschusses für Systemrisiken ([2]), insbesondere auf Artikel 3 Absatz 2 Buchstaben b und d und die Artikel 16 und 18,

gestützt auf den Beschluss ESRB/2011/1 des Europäischen Ausschusses für Systemrisiken vom 20. Januar 2011 zur Verabschiedung der Geschäftsordnung des Europäischen Ausschusses für Systemrisiken ([3]), insbesondere auf die Artikel 18 bis 20,

in Erwägung nachstehender Gründe:

(1) Wie in Erwägungsgrund 4 der Empfehlung ESRB/2013/1 des Europäischen Ausschusses für Systemrisiken ([4]) ausgeführt wird, besteht das Endziel makroprudenzieller Maßnahmen darin, zum Schutz der Stabilität des Finanzsystems in seiner Gesamtheit beizutragen, u. a. durch die Stärkung der Widerstandsfähigkeit des Finanzsystems und durch den Abbau der Anhäufung von Systemrisiken, wodurch ein nachhaltiger Beitrag des Finanzsektors zum Wirtschaftswachstum sichergestellt wird. Der Europäische Ausschuss für Systemrisiken (ESRB) ist für die makroprudenzielle Aufsicht über das Finanzsystem in der Union verantwortlich. Bei der Erfüllung seines Auftrags sollte der ESRB einen Beitrag zur Vermeidung und Minderung von Systemrisiken für die Finanzstabilität leisten, einschließlich Risiken im Zusammenhang mit Cybervorfällen, und Vorschläge zur Risikominderung machen.

(2) Schwerwiegende Cybervorfälle können ein systemisches Risiko für das Finanzsystem darstellen, da sie das Potenzial haben, kritische Finanzdienstleistungen und -geschäfte zu unterbrechen. Die Ausweitung eines anfänglichen Schocks kann entweder durch Ansteckung auf operativer oder finanzieller Ebene oder durch den Verlust des Vertrauens in das Finanzsystem erfolgen. Wenn das Finanzsystem nicht in der Lage ist, diese Schocks abzufedern, ist die Finanzstabilität in Gefahr, und diese Situation kann zu einer systemischen Cyberkrise ([5]) führen.

([1]) ABl. L 1 vom 3.1.1994, S. 3.
([2]) ABl. L 331 vom 15.12.2010, S. 1.
([3]) ABl. C 58 vom 24.2.2011, S. 4.
([4]) Empfehlung ESRB/2013/1 des Europäischen Ausschusses für Systemrisiken vom 4. April 2013 zu Zwischenzielen und Instrumenten für makroprudenzielle Maßnahmen (ABl. C 170 vom 15.6.2013, S. 1).
([5]) Siehe Systemic cyber risk, ESRB, Februar 2020, abrufbar auf der Website des ESRB unter www.esrb.europa.eu

(3) Die sich laufend verändernde Cyberbedrohungslage und die jüngste Zunahme schwerwiegender Cybervorfälle sind Indikatoren für eine stärkere Gefährdung der Finanzstabilität in der Union. Durch die Coronavirus-Pandemie ist deutlich geworden, welche Bedeutung die Technologie für den Betrieb des Finanzsystems hat. Die betreffenden Behörden und Institutionen mussten ihre technische Infrastruktur und ihre Risikosteuerungsrahmen an die plötzliche Zunahme von Telearbeitsplätzen anpassen, die insgesamt zu einer stärkeren Anfälligkeit des Finanzsystems für Cyberbedrohungen geführt hat und es Kriminellen ermöglicht hat, sowohl neue Methoden zu entwickeln als auch ihre bisherigen Methoden anzupassen, um die Lage auszunutzen ([6]). Vor diesem Hintergrund ist die Anzahl der Cybervorfälle, die der EZB-Bankenaufsicht im Jahr 2020 gemeldet wurde, gegenüber 2019 um 54 % gestiegen ([7]).

(4) Das mögliche große Ausmaß eines schwerwiegenden Cybervorfalls und die Geschwindigkeit, mit der ein schwerwiegender Cybervorfall auftritt und sich ausbreitet, erfordern eine wirksame Reaktion der betreffenden Behörden, damit mögliche negative Folgen für die Finanzstabilität abgeschwächt werden können. Eine rasche Koordinierung und Kommunikation zwischen den betreffenden Behörden auf Unionsebene kann dabei helfen, die Auswirkungen eines schwerwiegenden Cybervorfalls auf die Finanzstabilität frühzeitig zu bewerten, das Vertrauen in das Finanzsystem aufrechtzuerhalten und die Ansteckung anderer Finanzinstitute zu begrenzen, und so dazu beitragen, zu verhindern, dass ein schwerwiegender Cybervorfall zu einem Risiko für die Finanzstabilität wird.

(5) Der zugrundliegende Schock entsteht auf neuartige Weise im Vergleich zu den üblichen Finanz- und Liquiditätskrisen, mit denen die betreffenden Behörden meist konfrontiert werden. Abgesehen von finanziellen Aspekten muss eine Gesamtrisikobewertung das Ausmaß und die Auswirkungen von Betriebsstörungen umfassen, da diese die Wahl der makroprudenziellen Instrumente beeinflussen könnten. Ebenso könnte auch die Finanzstabilität die Wahl der operativen Abschwächungsmöglichkeiten durch Cyberexperten beeinflussen. Es ist also eine enge und rasche Koordinierung und eine offene Kommunikation gefragt, unter anderem, um das Lagebewusstsein zu stärken.

(6) Es besteht das Risiko eines Koordinierungsversagens seitens der Behörden, das angegangen werden muss. Die betreffenden Behörden in der Union werden sich untereinander und mit anderen Behörden, mit denen sie meist nicht zusammenarbeiten, wie etwa der Agentur der Europäischen Union für Cybersicherheit (ENISA), abstimmen müssen. Da eine wesentliche Anzahl von Finanzinstituten der Union global tätig ist, wird ein schwerwiegender Cybervorfall wahrscheinlich nicht auf die Union beschränkt sein, oder der Cybervorfall könnte außerhalb der Union ausgelöst werden, sodass eine koordinierte globale Reaktion erforderlich sein könnte.

(7) Die betreffenden Behörden müssen auf diese Zusammenarbeit vorbereitet sein. Andernfalls riskieren sie, abweichende Maßnahmen zu treffen, die der Reaktion anderer Behörden widersprechen oder deren Reaktion gefährden. Ein solches Koordinierungsversagen könnte den Schock für das Finanzsystem verstärken, indem es zu einem Verlust des Vertrauens in das Funktionieren des Finanzsystems führt. Dies wiederum würde im schlimmsten Fall ein Risiko für die Finanzstabilität darstellen ([8]). Daher sollten die erforderlichen Schritte ergriffen werden, um das Risiko für die Finanzstabilität anzugehen, das mit einem Koordinierungsversagen im Fall eines schwerwiegenden Cybervorfalls einhergeht.

(8) Im ESRB-Bericht zu „*Mitigating systemic cyber risk*“ (2021) ([9]) wird die Notwendigkeit festgestellt, einen europaweiten Koordinierungsrahmen für systemische Cybervorfälle (pan-European systemic cyber incident coordination framework – EU-SCICF) für die betreffenden Behörden in der Union einzurichten. Ziel des EU-SCICF wäre eine verbesserte Bereitschaft der betreffenden Behörden für eine koordinierte Reaktion auf einen möglichen schwerwiegenden Cybervorfall. Der ESRB-Bericht zu „*Mitigating systemic cyber risk*“ (2021) enthält eine Bewertung des ESRB zu den Rahmenmerkmalen, die dem ersten Anschein nach erforderlich wären, um dem Risiko eines Koordinierungsversagens zu begegnen.

(9) Das Hauptziel dieser Empfehlung besteht darin, auf einer der vorgesehenen Funktionen der Europäischen Aufsichtsbehörden (European Supervisory Authorities – ESA) im Rahmen des Vorschlags für eine Verordnung des Europäischen Parlaments und des Rates über die Betriebsstabilität digitaler Systeme des Finanzsektors ([10]) (nachfolgend „DORA“) aufzubauen, nämlich schrittweise eine wirksame koordinierte Reaktion auf Unionsebene zu ermöglichen, sofern es zu einem schwerwiegenden grenzüberschreitenden Vorfall im Zusammenhang mit Informations- und Kommunikationstechnologien (IKT) oder zu einer vergleichbaren Bedrohung kommt, die systemische Auswirkungen auf den gesamten Finanzsektor der Union mit sich bringen. Dieser Prozess wird zur Einrichtung des EU-SCICF für die betreffenden Behörden führen.

([6]) Siehe Internet Organised Crime Threat Assessment, Europol, 2020, abrufbar auf der Website von Europol unter www.europol.europa.eu

([7]) Siehe IT and cyber risk: a constant challenge, ECB, 2021, abrufbar auf der Website der EZB zur Bankenaufsicht unter www.bankingsupervision.europa.eu

([8]) Siehe Systemic cyber risk, ESRB, Februar 2020, abrufbar auf der Website des ESRB unter www.esrb.europa.eu

([9]) Siehe Mitigating systemic cyber risk, ESRB, 2021, (erscheint in Kürze).

([10]) COM/2020/595 final.

(10) Der EU-SCICF sollte nicht darauf abzielen, bestehende Rahmenwerke zu ersetzen, sondern alle Koordinierungs- und Kommunikationslücken zu schließen, die zwischen den betreffenden Behörden in der Union untereinander und zwischen diesen und anderen Behörden in der Union oder anderen wichtigen Akteuren auf internationaler Ebene bestehen. In diesem Zusammenhang sollte auch berücksichtigt werden, welche Stellung der EU-SCICF innerhalb des bestehenden Finanzkrisenrahmens und des Rahmens für den Umgang mit Cybervorfällen in der Union einnehmen soll. Was die Koordinierung zwischen den betreffenden Behörden untereinander betrifft, sollten unter anderem die Funktionen und Tätigkeiten der Kooperationsgruppe für Netz- und Informationssysteme (NIS-Kooperationsgruppe) für Finanzinstitute gemäß der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates ([11]) sowie die Koordinierungsmechanismen berücksichtigt werden, die im Rahmen der Einrichtung der Gemeinsamen Cyber-Einheit (Joint Cyber Unit) neben der Einbindung der ENISA vorgesehen sind.

(11) Insbesondere zielt der Vorschlag, die Vorbereitungen für den EU-SCICF einzuleiten, darauf ab, die gemäß dem DORA-Vorschlag vorgesehenen möglichen Funktionen der ESA zu bestätigen. DORA sieht Folgendes vor: „Die ESA können über den Gemeinsamen Ausschuss und in Zusammenarbeit mit den zuständigen Behörden, der EZB und dem ESRB Mechanismen für den Austausch wirksamer Verfahren zwischen Finanzsektoren einrichten, um das Lagebewusstsein zu verbessern und sektorübergreifend gemeinsame Cyberanfälligkeiten und -risiken zu ermitteln." „Ebenso können sie Krisenmanagement- und Notfallübungen mit Szenarien für Cyberangriffe konzipieren, um Kommunikationskanäle zu entwickeln und schrittweise eine wirksame koordinierte Reaktion auf EU-Ebene zu ermöglichen, sofern es zu einem schwerwiegenden grenzüberschreitenden IKT-bezogenen Vorfall oder einer vergleichbaren Bedrohung kommt, die systemische Auswirkungen auf den gesamten Finanzsektor der Union mit sich bringen." ([12]) Noch gibt es keinen europaweiten Rahmen wie den EU-SCICF; daher sollte dieser im Zusammenhang mit DORA eingerichtet und entwickelt werden.

(12) In Anbetracht des mit Cyberrisiken einhergehenden Risikos für die Finanzstabilität in der Union sollten die Vorarbeiten für die schrittweise Einrichtung des EU-SCICF möglichst schon beginnen, bevor der erforderliche rechtliche und politische Rahmen für die Einrichtung des EU-SCICF in vollem Umfang anwendbar ist. Der rechtliche und politische Rahmen würde dann vollständig aufgestellt und finalisiert, sobald die jeweiligen Bestimmungen von DORA und ihrer delegierten Rechtsakte anwendbar sind.

(13) Eine wirksame Kommunikation trägt zu einem Lagebewusstsein unter den betreffenden Behörden bei und ist somit eine unabdingbare Voraussetzung für eine unionsweite Koordinierung im Fall eines schwerwiegenden Cybervorfalls. Dahingehend sollte die Kommunikationsinfrastruktur festgelegt werden, die benötigt wird, um eine Reaktion auf einen schwerwiegenden Cybervorfall zu koordinieren. Dies würde bedeuten, dass die Art der auszutauschenden Informationen, die üblichen Kommunikationswege, über die solche Informationen ausgetauscht werden sollen, und die Kontaktstellen, mit denen die Informationen auszutauschen sind, festzulegen wären. Jeglicher Informationsaustausch hat die bestehenden rechtlichen Anforderungen zu erfüllen. Darüber hinaus müssen möglicherweise ein klarer Handlungsplan und Protokolle, die zu befolgen sind, von den betreffenden Behörden festgelegt werden, damit eine angemessene Koordinierung zwischen den Behörden gewährleistet ist, die an der Planung einer koordinierten Reaktion auf einen schwerwiegenden Cybervorfall beteiligt sind.

(14) Eine systemische Cyberkrise wird die Aufnahme einer uneingeschränkten Kooperation auf nationaler und Unionsebene erfordern. Aus diesem Grund könnten Kontaktstellen bei den ESA, bei der EZB und bei allen Mitgliedstaten – in letzterem Fall aus dem Kreis ihrer jeweiligen nationalen Behörden – benannt und den ESA mitgeteilt werden, um die zentralen Ansprechpartner im Koordinierungssystem des EU-SCICF festzulegen, die im Fall eines schwerwiegenden Cybervorfalls zu unterrichten sind. Die Notwendigkeit der Benennung von Kontaktstellen sollte bei der Entwicklung des EU-SCICF geprüft werden. Hierbei ist die in der Richtlinie (EU) 2016/1148 vorgesehene zentrale Anlaufstelle zu berücksichtigen, die von den Mitgliedstaaten im Zusammenhang mit der Sicherheit von Netz- und Informationssystemen benannt wurde, um eine grenzüberschreitende Zusammenarbeit mit anderen Mitgliedstaaten und mit der NIS-Kooperationsgruppe ([13]) zu gewährleisten.

(15) Die Durchführung von Krisenmanagement- und Notfallübungen könnte die Umsetzung des EU-SCICF erleichtern und den Behörden ermöglichen, ihre Abwehrbereitschaft und ihren Vorbereitungsstand im Hinblick auf eine systemische Cyberkrise auf Unionsebene zu bewerten. Aus solchen Übungen könnten die Behörden Erfahrungswerte ableiten, um eine kontinuierliche Verbesserung und Entwicklung des EU-SCICF herbeizuführen.

([11]) Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (ABl. L 194 vom 19.7.2016, S. 1).

([12]) Siehe Artikel 43 des DORA-Vorschlags.

([13]) Siehe Europäische Kommission, NIS-Kooperationsgruppe, abrufbar auf der Website der Europäischen Kommission unter www.ec.europa.eu

(16) Für die Entwicklung des EU-SCICF ist es unerlässlich, dass die ESA gemeinsam entsprechende Vorarbeiten leisten, um mögliche Schlüsselelemente des Rahmens sowie erforderliche Ressourcen und Anforderungen zu prüfen, die für die Weiterentwicklung des Rahmens notwendig sind. Anschließend könnten die ESA die Arbeit an einer vorläufigen Analyse aller Hindernisse aufnehmen, welche die ESA und die betreffenden Behörden in ihrer Fähigkeit, den EU-SCICF einzurichten und entsprechende Informationen über Kommunikationswege im Fall eines schwerwiegenden Cybervorfalls auszutauschen, einschränken könnten. Eine solche Analyse wäre ein wichtiger Schritt hin zu weiteren Maßnahmen, sei es legislativer Art oder in Form anderer unterstützender Initiativen, welche die Europäische Kommission in der Umsetzungsphase nach DORA ergreifen könnte —

HAT FOLGENDE EMPFEHLUNG ERLASSEN:

ABSCHNITT 1

EMPFEHLUNGEN

Empfehlung A – Einrichtung eines europaweiten Koordinierungsrahmens für systemische Cybervorfälle (EU-SCICF)

1. Entsprechend dem Vorschlag der Kommission für eine Verordnung des Europäischen Parlaments und des Rates über die Betriebsstabilität digitaler Systeme des Finanzsektors (nachfolgend „DORA“) wird empfohlen, dass die Europäischen Aufsichtsbehörden (ESA) gemeinsam im Rahmen des Gemeinsamen Ausschusses und zusammen mit der Europäischen Zentralbank (EZB), dem Europäischen Ausschuss für Systemrisiken (ESRB) und den jeweiligen nationalen Behörden mit den Vorbereitungen für die schrittweise Entwicklung einer wirksamen koordinierten Reaktion auf Unionsebene beginnen, für den Fall, dass es zu einem schwerwiegenden grenzüberschreitenden Vorfall im Zusammenhang mit Informations- und Kommunikationstechnologien (IKT) oder zu einer vergleichbaren Bedrohung kommt, die systemische Auswirkungen auf den Finanzsektor der Union mit sich bringen könnten. Die Vorarbeiten für eine koordinierte Reaktion auf Unionsebene sollten die schrittweise Entwicklung eines europaweiten Koordinierungsrahmens für systemische Cybervorfälle (EU-SCICF) für die ESA, die EZB, den ESRB und die jeweiligen nationalen Behörden umfassen. Zudem sollte im Rahmen der Vorarbeiten der für die wirksame Weiterentwicklung des Rahmens erforderliche Ressourcenbedarf geprüft werden.

2. Im Zusammenhang mit Empfehlung A Nummer 1 wird den ESA empfohlen, im Einvernehmen mit der EZB und dem ESRB eine Zuordnung und anschließende Analyse aller gegenwärtigen Hindernisse und rechtlichen oder anderen operativen Barrieren für die wirksame Entwicklung des EU-SCICF vorzunehmen.

Empfehlung B – Einrichtung von Kontaktstellen für den EU-SCICF

Es wird empfohlen, dass die ESA, die EZB und alle Mitgliedstaaten – in letzterem Fall aus dem Kreis ihrer jeweiligen nationalen Behörden – jeweils eine zentrale Kontaktstelle benennen, die den ESA mitgeteilt wird. Diese Kontaktliste wird die Entwicklung des EU-SCICF vereinfachen. Sobald der EU-SCICF eingerichtet worden ist, sollten die Kontaktstellen und der ESRB im Fall eines schwerwiegenden Cybervorfalls unterrichtet werden. Darüber hinaus sollte eine Koordinierung zwischen dem EU-SCICF und der in der Richtlinie (EU) 2016/1148 vorgesehenen zentralen Anlaufstelle, die von den Mitgliedstaaten im Zusammenhang mit der Sicherheit von Netz- und Informationssystemen benannt wurde, um eine grenzüberschreitende Zusammenarbeit mit anderen Mitgliedstaaten und mit der Kooperationsgruppe für Netz- und Informationssysteme (NIS-Kooperationsgruppe) zu gewährleisten, vorgesehen werden.

Empfehlung C – Geeignete Maßnahmen auf Unionsebene

Es wird empfohlen, dass die Kommission auf der Grundlage der Ergebnisse der gemäß Empfehlung A vorgenommenen Analysen prüft, welche Maßnahmen geeignet sind, um eine wirksame Koordinierung von Reaktionen auf systemische Cybervorfälle zu gewährleisten.

ABSCHNITT 2

UMSETZUNG

1. **Begriffsbestimmungen**

Für die Zwecke dieser Empfehlung gelten die folgenden Begriffsbestimmungen:

a) „cyber-“ oder „Cyber-“ betreffend, innerhalb oder durch das Medium der vernetzten Informationsinfrastruktur von Interaktionen zwischen Personen, Prozessen, Daten und Informationssystemen ([14]);

([14]) Siehe Cyber Lexicon, Financial Stability Board, 12. November 2018, abrufbar auf der Website des FSB unter www.fsb.org.

b) „schwerwiegender Cybervorfall“ ein IKT-Vorfall mit potenziell umfassenden nachteiligen Auswirkungen auf die Netz- und Informationssysteme, die kritische Funktionen des Finanzunternehmens unterstützen ([15]);

c) „systemische Cyberkrise“ ein schwerwiegender Cybervorfall, der eine Störung des Finanzsystems der Union verursacht, die mögliche schwerwiegende negative Folgen für das reibungslose Funktionieren des Binnenmarkts und das Funktionieren der Realwirtschaft hat. Eine solche Krise könnte von einem schwerwiegenden Cybervorfall ausgehen, der Schocks in mehreren Kanälen verursacht, etwa auf operativer oder finanzieller Ebene oder durch einen Vertrauensverlust;

d) „Europäische Aufsichtsbehörden“ oder „ESA“ die durch die Verordnung (EU) Nr. 1093/2010 des Europäischen Parlaments und des Rates ([16]) eingerichtete Europäische Aufsichtsbehörde (Europäische Bankenaufsichtsbehörde) zusammen mit der durch die Verordnung (EU) Nr. 1094/2010 des Europäischen Parlaments und des Rates ([17]) eingerichteten Europäischen Aufsichtsbehörde (Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung) und der durch die Verordnung (EU) Nr. 1095/2010 des Europäischen Parlaments und des Rates ([18]) eingerichteten Europäischen Aufsichtsbehörde (Europäische Wertpapier- und Marktaufsichtsbehörde);

e) „Gemeinsamer Ausschuss“ der gemäß Artikel 54 der Verordnung (EU) Nr. 1093/2010, der Verordnung (EU) Nr. 1094/2010 bzw. der Verordnung (EU) Nr. 1095/2010 eingerichtete Gemeinsame Ausschuss der Europäischen Aufsichtsbehörden;

f) „jeweilige nationale Behörde“

1. eine zuständige Behörde bzw. eine Aufsichtsbehörde eines Mitgliedstaats im Sinne der in Artikel 1 Absatz 2 der Verordnung (EU) Nr. 1093/2010, der Verordnung (EU) Nr. 1094/2010 und der Verordnung (EU) Nr. 1095/2010 genannten Rechtsakte der Union sowie jede andere, in den Rechtsakten der Union genannte nationale zuständige Behörde, die den ESA Aufgaben überträgt;

2. eine zuständige Behörde eines Mitgliedstaats, die gemäß einer der nachfolgenden Bestimmungen benannt worden ist:

i) Artikel 4 der Richtlinie 2013/36/EU des Europäischen Parlaments und des Rates ([19]), unbeschadet der besonderen Aufgaben, die der EZB durch die Verordnung (EU) Nr. 1024/2013 des Rates ([20]) übertragen wurden;

ii) Artikel 22 der Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates ([21]);

iii) Artikel 37 der Richtlinie 2009/110/EG des Europäischen Parlaments und des Rates ([22]);

iv) Artikel 4 der Richtlinie (EU) 2019/2034 des Europäischen Parlaments und des Rates ([23]);

([15]) Siehe Artikel 3 Nummer 7 des DORA-Vorschlags.

([16]) 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).

([17]) 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).

([18]) 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).

([19]) Richtlinie 2013/36/EU des Europäischen Parlaments und des Rates vom 26. Juni 2013 über den Zugang zur Tätigkeit von Kreditinstituten und die Beaufsichtigung von Kreditinstituten, zur Änderung der Richtlinie 2002/87/EG und zur Aufhebung der Richtlinien 2006/48/EG und 2006/49/EG (ABl. L 176 vom 27.6.2013, S. 338).

([20]) Verordnung (EU) Nr. 1024/2013 des Rates vom 15. Oktober 2013 zur Übertragung besonderer Aufgaben im Zusammenhang mit der Aufsicht über Kreditinstitute auf die Europäische Zentralbank (ABl. L 287 vom 29.10.2013, S. 63).

([21]) 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).

([22]) Richtlinie 2009/110/EG des Europäischen Parlaments und des Rates vom 16. September 2009 über die Aufnahme, Ausübung und Beaufsichtigung der Tätigkeit von E-Geld-Instituten, zur Änderung der Richtlinien 2005/60/EG und 2006/48/EG sowie zur Aufhebung der Richtlinie 2000/46/EG (ABl. L 267 vom 10.10.2009, S. 7).

([23]) Richtlinie (EU) 2019/2034 des Europäischen Parlaments und des Rates vom 27. November 2019 über die Beaufsichtigung von Wertpapierfirmen und zur Änderung der Richtlinien 2002/87/EG, 2009/65/EG, 2011/61/EU, 2013/36/EU, 2014/59/EU und 2014/65/EU (ABl. L 314 vom 5.12.2019, S. 64).

v) Artikel 3 Absatz 1 Buchstabe ee erster Gedankenstrich des Vorschlags für eine Verordnung des Europäischen Parlaments und des Rates über Märkte für Kryptowerte und zur Änderung der Richtlinie (EU) 2019/1937 ([24]);

vi) Artikel 11 der Verordnung (EU) Nr. 909/2014 des Europäischen Parlaments und des Rates ([25]);

vii) Artikel 22 der Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates ([26]);

viii) Artikel 67 der Richtlinie 2014/65/EU des Europäischen Parlaments und des Rates ([27]);

ix) Artikel 22 der Verordnung (EU) Nr. 648/2012;

x) Artikel 44 der Richtlinie 2011/61/EU des Europäischen Parlaments und des Rates ([28]);

xi) Artikel 97 der Richtlinie 2009/65/EG des Europäischen Parlaments und des Rates ([29]);

xii) Artikel 30 der Richtlinie 2009/138/EG des Europäischen Parlaments und des Rates ([30]);

xiii) Artikel 12 der Richtlinie (EU) 2016/97 des Europäischen Parlaments und des Rates ([31]);

xiv) Artikel 47 der Richtlinie (EU) 2016/2341 des Europäischen Parlaments und des Rates ([32]);

xv) Artikel 22 der Verordnung (EG) Nr. 1060/2009 des Europäischen Parlaments und des Rates ([33]);

xvi) Artikel 3 Absatz 2 und Artikel 32 der Richtlinie 2006/43/EG des Europäischen Parlaments und des Rates ([34]);

xvii) Artikel 40 der Verordnung (EU) Nr. 2016/1011 des Europäischen Parlaments und des Rates ([35]);

xviii) Artikel 29 der Verordnung (EU) Nr. 2020/1503 des Europäischen Parlaments und des Rates ([36]);

([24]) COM/2020/593 final.

([25]) Verordnung (EU) Nr. 909/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 zur Verbesserung der Wertpapierlieferungen und -abrechnungen in der Europäischen Union und über Zentralverwahrer sowie zur Änderung der Richtlinien 98/26/EG und 2014/65/EU und der Verordnung (EU) Nr. 236/2012 (ABl. L 257 vom 28.8.2014, S. 1).

([26]) Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates vom 4. Juli 2012 über OTC-Derivate, zentrale Gegenparteien und Transaktionsregister (ABl. L 201 vom 27.7.2012, S. 1).

([27]) Richtlinie 2014/65/EU des Europäischen Parlaments und des Rates vom 15. Mai 2014 über Märkte für Finanzinstrumente sowie zur Änderung der Richtlinien 2002/92/EG und 2011/61/EU (ABl. L 173 vom 12.6.2014, S. 349).

([28]) Richtlinie 2011/61/EU des Europäischen Parlaments und des Rates vom 8. Juni 2011 über die Verwalter alternativer Investmentfonds und zur Änderung der Richtlinien 2003/41/EG und 2009/65/EG und der Verordnungen (EG) Nr. 1060/2009 und (EU) Nr. 1095/2010 (ABl. L 174 vom 1.7.2011, S. 1).

([29]) Richtlinie 2009/65/EG des Europäischen Parlaments und des Rates vom 13. Juli 2009 zur Koordinierung der Rechts- und Verwaltungsvorschriften betreffend bestimmte Organismen für gemeinsame Anlagen in Wertpapieren (OGAW) (ABl. L 302 vom 17.11.2009, S. 32).

([30]) Richtlinie 2009/138/EG des Europäischen Parlaments und des Rates vom 25. November 2009 betreffend die Aufnahme und Ausübung der Versicherungs- und der Rückversicherungstätigkeit (Solvabilität II) (ABl. L 335 vom 17.12.2009, S. 1).

([31]) Richtlinie (EU) 2016/97 des Europäischen Parlaments und des Rates vom 20. Januar 2016 über Versicherungsvertrieb (ABl. L 26 vom 2.2.2016, S. 19).

([32]) Richtlinie (EU) 2016/2341 des Europäischen Parlaments und des Rates vom 14. Dezember 2016 über die Tätigkeiten und die Beaufsichtigung von Einrichtungen der betrieblichen Altersversorgung (EbAV) (ABl. L 354 vom 23.12.2016, S. 37).

([33]) Verordnung (EG) Nr. 1060/2009 des Europäischen Parlaments und des Rates vom 16. September 2009 über Ratingagenturen (ABl. L 302 vom 17.11.2009, S. 1).

([34]) Richtlinie 2006/43/EG des Europäischen Parlaments und des Rates vom 17. Mai 2006 über Abschlussprüfungen von Jahresabschlüssen und konsolidierten Abschlüssen, zur Änderung der Richtlinien 78/660/EWG und 83/349/EWG des Rates und zur Aufhebung der Richtlinie 84/253/EWG des Rates (ABl. L 157 vom 9.6.2006, S. 87).

([35]) Verordnung (EU) 2016/1011 des Europäischen Parlaments und des Rates vom 8. Juni 2016 über Indizes, die bei Finanzinstrumenten und Finanzkontrakten als Referenzwert oder zur Messung der Wertentwicklung eines Investmentfonds verwendet werden, und zur Änderung der Richtlinien 2008/48/EG und 2014/17/EU sowie der Verordnung (EU) Nr. 596/2014 (ABl. L 171 vom 29.6.2016, S. 1).

([36]) Verordnung (EU) 2020/1503 des Europäischen Parlaments und des Rates vom 7. Oktober 2020 über Europäische Schwarmfinanzierungsdienstleister für Unternehmen und zur Änderung der Verordnung (EU) 2017/1129 und der Richtlinie (EU) 2019/1937 (ABl. L 347 vom 20.10.2020, S. 1).

3. eine Behörde, die mit dem Erlass bzw. der Umsetzung makroprudenzieller Maßnahmen oder mit anderen Aufgaben im Bereich der Finanzstabilität, wie z. B. der Bereitstellung entsprechender ergänzender Analysen, betraut ist. Dieser Begriff umfasst insbesondere

   i) eine benannte Behörde gemäß Titel VII Kapitel 4 der Richtlinie 2013/36/EU oder Artikel 458 Absatz 1 der Verordnung (EU) Nr. 575/2013 des Europäischen Parlaments und des Rates ([37]);

   ii) eine makroprudenzielle Behörde mit den Zielen, Vorkehrungen, Aufgaben, Befugnissen, Instrumenten, Rechenschaftspflichten und anderen gemäß Empfehlung ESRB/2011/3 des Europäischen Ausschusses für Systemrisiken ([38]) festgelegten Merkmalen;

g) „betreffende Behörde"

   1. eine ESA;

   2. die EZB im Zusammenhang mit den ihr gemäß Artikel 4 Absätze 1 und 2 und Artikel 5 Absatz 2 der Verordnung (EU) Nr. 1024/2013 übertragenen Aufgaben;

   3. eine jeweilige nationale Behörde.

2. **Umsetzungskriterien**

Für die Umsetzung dieser Empfehlung gelten die folgenden Kriterien:

a) Dem Grundsatz des begründeten Bedarfs (need to know) und dem Verhältnismäßigkeitsgrundsatz sollte unter Berücksichtigung von Zweck und Inhalt jeder Empfehlung angemessen Rechnung getragen werden.

b) Die im Anhang gesondert für jede Empfehlung aufgeführten Befolgungskriterien sollten erfüllt werden.

3. **Zeitrahmen für die Nachverfolgung**

Gemäß Artikel 17 Absatz 1 der Verordnung (EU) Nr. 1092/2010 müssen die Adressaten dem Europäischen Parlament, dem Rat, der Kommission und dem ESRB mitteilen, welche Maßnahmen sie zur Umsetzung der Empfehlung ergriffen haben, oder ein eventuelles Nichthandeln begründen. Die Adressaten werden ersucht, Mitteilungen unter Berücksichtigung der folgenden Fristen einzureichen:

1. Empfehlung A

   a) Die ESA werden ersucht, dem Europäischen Parlament, dem Rat, der Kommission und dem ESRB bis zum 30. Juni 2023, frühestens jedoch sechs Monate nach Inkrafttreten von DORA, einen Zwischenbericht über die Umsetzung von Empfehlung A Nummer 1 vorzulegen.

   b) Die ESA werden ersucht, dem Europäischen Parlament, dem Rat, der Kommission und dem ESRB bis zum 30. Juni 2024, frühestens jedoch 18 Monate nach Inkrafttreten von DORA, einen Abschlussbericht über die Umsetzung von Empfehlung A Nummer 1 vorzulegen.

   c) Die ESA werden ersucht, dem Europäischen Parlament, dem Rat, der Kommission und dem ESRB bis zum 30. Juni 2025, frühestens jedoch 30 Monate nach Inkrafttreten von DORA, einen Bericht über die Umsetzung von Empfehlung A Nummer 2 vorzulegen.

2. Empfehlung B

   Die ESA, die EZB und die Mitgliedstaaten werden ersucht, dem Europäischen Parlament, dem Rat, der Kommission und dem ESRB bis zum 30. Juni 2023, frühestens jedoch sechs Monate nach Inkrafttreten von DORA, einen Bericht über die Umsetzung von Empfehlung B vorzulegen.

3. Empfehlung C

   a) Die Kommission wird ersucht, dem Europäischen Parlament, dem Rat und dem ESRB bis zum 31. Dezember 2023, frühestens jedoch zwölf Monate nach Inkrafttreten von DORA, einen Bericht über die Umsetzung von Empfehlung C vorzulegen, der dem gemäß Empfehlung A Nummer 1 vorgesehenen Zwischenbericht der ESA Rechnung trägt.

([37]) Verordnung (EU) Nr. 575/2013 des Europäischen Parlaments und des Rates vom 26. Juni 2013 über Aufsichtsanforderungen an Kreditinstitute und Wertpapierfirmen und zur Änderung der Verordnung (EU) Nr. 646/2012 (ABl. L 176 vom 27.6.2013, S. 1)

([38]) Empfehlung ESRB/2011/3 des Europäischen Ausschusses für Systemrisiken vom 22. Dezember 2011 zu dem makroprudenziellen Mandat der nationalen Behörden (ABl. C 41 vom 14.2.2012, S. 1).

b) Die Kommission wird ersucht, dem Europäischen Parlament, dem Rat und dem ESRB bis zum 31. Dezember 2025, frühestens jedoch 36 Monate nach Inkrafttreten von DORA, einen Bericht über die Umsetzung von Empfehlung C vorzulegen, der den gemäß Empfehlung A vorgesehenen Berichten der ESA Rechnung trägt.

4. **Überwachung und Bewertung**

1. Das Sekretariat des ESRB

a) unterstützt die Adressaten durch Gewährleistung der Koordination der Meldepflichten und Bereitstellung der maßgeblichen Meldebögen und gegebenenfalls detaillierter Angaben zum Verfahren und zum Zeitrahmen für die Nachverfolgung,

b) überprüft die Nachverfolgung durch die Adressaten, sorgt auf Verlangen für Unterstützung und erstattet dem Verwaltungsrat Bericht über die Nachverfolgung. Es werden Bewertungen wie folgt veranlasst:

i) Innerhalb von zwölf Monaten nach Inkrafttreten von DORA betreffend die Umsetzung der Empfehlungen A und B;

ii) innerhalb von 18 Monaten nach Inkrafttreten von DORA betreffend die Umsetzung von Empfehlung C;

iii) innerhalb von 24 Monaten nach Inkrafttreten von DORA betreffend die Umsetzung von Empfehlung A;

iv) innerhalb von 36 Monaten nach Inkrafttreten von DORA betreffend die Umsetzung von Empfehlung A;

v) innerhalb von 42 Monaten nach Inkrafttreten von DORA betreffend die Umsetzung von Empfehlung C.

2. Der Verwaltungsrat bewertet die von den Adressaten gemeldeten Maßnahmen und Rechtfertigungen und kann gegebenenfalls entscheiden, dass die Empfehlung nicht befolgt wurde und ein Adressat sein Nichthandeln nicht angemessen gerechtfertigt hat.

Geschehen zu Frankfurt am Main am 2. Dezember 2021.

Leiter des ESRB-Sekretariats,
im Auftrag des Verwaltungsrats des ESRB,
Francesco MAZZAFERRO

ANHANG

FESTLEGUNG DER FÜR DIE EMPFEHLUNGEN GELTENDEN BEFOLGUNGSKRITERIEN

Empfehlung A – Einrichtung eines europaweiten Koordinierungsrahmens für systemische Cybervorfälle (EU-SCICF)

Für Empfehlung A Nummer 1 werden folgende Befolgungskriterien festgelegt.

1. Bei den Vorarbeiten für eine wirksame koordinierte Reaktion auf Unionsebene, – die eine schrittweise Entwicklung des EU-SCICF durch Nutzung der in der künftigen Verordnung des Europäischen Parlaments und des Rates über die Betriebsstabilität digitaler Systeme des Finanzsektors (nachfolgend „DORA“) vorgesehenen Befugnisse umfassen sollten, – sollten die Europäischen Aufsichtsbehörden (ESA) im Rahmen des Gemeinsamen Ausschusses und zusammen mit der Europäischen Zentralbank (EZB), dem Europäischen Ausschuss für Systemrisiken (ESRB) und den jeweiligen nationalen Behörden sowie, sofern dies für erforderlich erachtet wird, im Einvernehmen mit der Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA) und der Kommission mindestens folgende Aspekte bei den Vorbereitungen für den EU-SCICF berücksichtigen:

   a) Analyse des für eine wirksame Entwicklung des EU-SCICF erforderlichen Ressourcenbedarfs;

   b) Konzeption von Krisenmanagement- und Notfallübungen mit Szenarien für Cyberangriffe, um Kommunikationskanäle zu entwickeln;

   c) Entwicklung einer gemeinsamen Terminologie;

   d) Entwicklung eines kohärenten Klassifizierungssystems für Cybervorfälle;

   e) Einrichtung sicherer und verlässlicher Kanäle für den Informationsaustausch, einschließlich Systemen für die Datensicherung (Backup);

   f) Einrichtung von Kontaktstellen;

   g) Umgang mit vertraulichen Daten im Rahmen des Informationsaustauschs;

   h) Initiativen für eine Zusammenarbeit und einen Informationsaustausch mit Cyber Intelligence im Finanzsektor;

   i) Entwicklung wirksamer Aktivierungs- und Eskalationsprozesse auf der Grundlage des Lagebewusstseins;

   j) Klarstellung der Zuständigkeiten der Teilnehmer des Rahmens;

   k) Entwicklung von Schnittstellen für eine sektorübergreifende Koordinierung und ggf. eine Koordinierung mit Drittstaaten;

   l) Sicherstellung einer kohärenten Kommunikation der betreffenden Behörden mit der Öffentlichkeit, um das Vertrauen zu wahren;

   m) Einrichtung vordefinierter Kommunikationswege, damit eine rechtzeitige Kommunikation gewährleistet ist;

   n) Durchführung angemessener Übungen, um den Rahmen zu testen, – einschließlich einer grenzüberschreitenden Testung und der Testung der Koordinierung mit Drittländern, – und Analysen, aus denen sich Erfahrungswerte ableiten lassen und durch die eine Weiterentwicklung des EU-SCICF herbeigeführt werden kann;

   o) Sicherstellung einer wirksamen Kommunikation sowie von Maßnahmen gegen Falschinformationen.

Empfehlung B – Einrichtung von Kontaktstellen für den EU-SCICF

Für Empfehlung B werden folgende Befolgungskriterien festgelegt.

1. Die ESA, die EZB und alle Mitgliedstaaten – wobei in letzterem Fall eine Einigung zwischen ihren jeweiligen nationalen Behörden zu erzielen ist – sollten sich auf eine gemeinsame Vorgehensweise für den Austausch und die Pflege der Liste der benannten Kontaktstellen des EU-SCICF einigen.

2. Bei der Benennung der Kontaktstelle ist die in der Richtlinie (EU) 2016/1148 vorgesehene zentrale Anlaufstelle zu berücksichtigen, die von den Mitgliedstaaten im Zusammenhang mit der Sicherheit von Netz- und Informationssystemen benannt wurde, um eine grenzüberschreitende Zusammenarbeit mit anderen Mitgliedstaaten und mit der Kooperationsgruppe für Netz- und Informationssysteme (NIS-Kooperationsgruppe) zu gewährleisten.

Empfehlung C – Änderungen des Rechtsrahmens der Union

Für Empfehlung C werden folgende Befolgungskriterien festgelegt.

Die Kommission sollte prüfen, ob aufgrund der Ergebnisse der gemäß Empfehlung A vorgenommenen Analysen Maßnahmen erforderlich sind, wie beispielsweise Änderungen der einschlägigen Rechtsvorschriften der Union, damit sichergestellt ist, dass einerseits die ESA im Rahmen des Gemeinsamen Ausschusses und zusammen mit der EZB, dem ESRB und den jeweiligen nationalen Behörden den EU-SCICF gemäß Empfehlung A Nummer 1 entwickeln können, und andererseits die ESA, die EZB, der ESRB, die jeweiligen nationalen Behörden und andere Behörden Koordinierungsmaßnahmen treffen und Informationen austauschen können, die ausreichend detailliert und kohärent sind, um einen wirksamen EU-SCICF zu fördern.