Compliance Berater Schriftenreihe

Stephan Schmidt (Hrsg.)

Cybersicherheitsrecht (Textsammlung)

NIS-2-Richtlinie
CER-Richtlinie
Digital Operational Resilience Act
eIDAS-Verordnung
BSI Gesetz
und viele weitere Texte

dfv Mediengruppe
R&W Fachmedien Recht und Wirtschaft

Compliance Berater

Cybersicherheitsrecht (Textsammlung)

NIS-2-Richtlinie
CER-Richtlinie
Digital Operational Resilience Act
eIDAS-Verordnung
BSI Gesetz
und viele weitere Texte

Stephan Schmidt (Hrsg.)

Fachmedien Recht und Wirtschaft | dfv Mediengruppe | Frankfurt am Main

Bibliografische Information Der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.de abrufbar.

ISBN 978-3-8005-1893-7

dfv Mediengruppe

www.ruw.de

Druck: WIRmachenDRUCK GmbH, Backnang

Printed in Germany

Inhaltsverzeichnis

I. Einleitung des Herausgebers

A. Einführung

Nur wenige Rechtsgebiete haben in den letzten Jahren eine so dynamische Entwicklung erlebt wie das Cybersicherheitsrecht. Die Geschichte der Gesetze und Regelungen zur Cybersicherheit ist eng mit dem Aufstieg der digitalen Ära verbunden. In den Anfangsjahren des Internets und der digitalen Kommunikation war die Bedrohungslage noch vergleichsweise gering. Es dauerte jedoch nicht lange, bis Cyberkriminelle und andere Akteure die Schwachstellen in digitalen Systemen ausnutzten. Dies führte zur Entstehung der ersten Cybersicherheitsgesetze – das erste deutsche IT-Sicherheitsgesetz (IT-SiG) stammt aus dem Jahr 2015. In den letzten Jahren hat sich das Cybersicherheitsrecht rasant weiterentwickelt. Getrieben von einer stetig steigenden Zahl von Cyberangriffen und den daraus resultierenden Schäden in Wirtschaft und öffentlicher Verwaltung, haben der nationale Gesetzgeber und auch die Europäische Union mittlerweile eine Vielzahl an Normen und Regelungen geschaffen. Cybersicherheit, etwas internationaler auch Cybersecurity genannt, bildet dabei den Oberbegriff für eine Vielzahl von Themen und damit auch gesetzlichen Regelungen. Cybersicherheit umfasst die IT-Sicherheit, die Informationssicherheit und auch die Datensicherheit, wobei man unter Cybersicherheit aus technischer Sicht die Technologien, Dienste, Strategien, Praktiken und Richtlinien versteht, die geeignet sind, Computersysteme, Netzwerke, Softwareanwendungen und digitale Daten und damit auch Menschen vor Cyberangriffen zu schützen. Die Gewährleistung dieses Schutzes stellt die moderne Informationsgesellschaft vor immer neue Herausforderungen.

Unter IT-Sicherheit versteht man die Sicherheit eines IT-Systems, unabhängig davon, ob es sich um ein vernetztes System handelt oder nicht. Der Begriff beinhaltet nicht nur eine infrastrukturell-technische Perspektive, sondern insbesondere auch eine organisatorisch-personelle Komponente. IT-Sicherheit findet sich als Begriff z. B. im BSI Gesetz, in § 5 Onlinezugangsgesetz (OZG) oder im IT-Justizgesetz. Unter Informationssicherheit versteht man die Aufrechterhaltung der Vertraulichkeit, Integrität und Verfügbarkeit von personenbezogenen und nicht-personenbezogenen Daten und Informationen (Schutzziele der IT-Sicherheit).

Vertraulichkeit ist die Anforderung, dass nur berechtigte Personen auf ein System und die darin gespeicherten Informationen zugreifen können. Integrität bezeichnet die Korrektheit der Daten und die Sicherstellung der Funktionsfähigkeit. Verfügbarkeit bezeichnet die jederzeitige Zugriffsmöglichkeit auf Systeme und deren Daten. Ergänzend wird häufig das Schutzziel der Verbindlichkeit betrachtet, dass die Authentizität, also die Sicherstellung der Identität von Personen, IT-Komponenten oder Anwendungen, sowie die Nichtabstreitbarkeit umfasst.

Unter Datensicherheit werden allgemein die technischen und organisatorischen Maßnahmen, also Sicherheitsmaßnahmen, verstanden, die zum Schutz von personenbezogenen Daten zum Beispiel nach Art. 32 DSGVO erforderlich sind und getroffen werden. Zudem finden sich bereichsspezifische Vorschriften zur Datensicherheit z. B. für den Bereich der Telekommunikation in §§ 165, 167, 169 TKG.

Die Pflicht zur Ergreifung von Cybersicherheitsmaßnahmen, ergibt sich heute sowohl aus nationalem als auch aus europäischem Recht, aus dem sich Rahmenvorschriften und spezialgesetzliche bereichsspezifische Regelungen ergeben können. Die bereichsspezifischen Cybersicherheits-Regelungen sind heute, je nach Sektor und Branche in dem ein Unternehmen tätig ist, sehr vielfältig.

Grundsätzlich gilt, dass sich aus allen Regelungen, die Maßnahmen der Qualitätssicherung, Organisations- oder Verarbeitungsvorgängen von Daten oder zur Nutzung informationstechnischer Systeme enthalten auch Verpflichtungen zur Cybersicherheit ergeben können.

Beginnend mit dem deutschen IT-SiG (2015) haben nationaler und europäischer Gesetzgeber eine Vielzahl an Cybersicherheitsgesetzen geschaffen, zu denen insbesondere die Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV – 2016/17), die EU-Richtlinie 2016/1148 „über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union" (NIS-RL, 2016) auf europäischer Ebene inklusive des dazugehörigen nationalen Umsetzungsgesetzes (2017), der EU Cybersecurity Act (CSA – 2019), der Vorschlag einer Verordnung über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen („Cyber Resilience Act") sowie die NIS-2-Richtlinie und die Richtlinie über die Resilienz kritischer Einrichtungen („CER-Richtlinie") (Dezember 2022) gehören. CER-Richtlinie und NIS-2-Richtlinie wurden beide Ende 2022 verabschiedet und müssen bis zum 17. 10.2024 in den Mitgliedstaaten umgesetzt sein. Die CER-Richtlinie wird voraussichtlich durch das Gesetz zur Umsetzung der CER-Richtlinie und zur Stärkung der Resilienz kritischer Anlagen (KRITIS-Dachgesetz), die NIS-2-Richtlinie durch das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) in nationales Recht umgesetzt. Beide Gesetze liegen noch nicht in finalen Fassungen vor, und sind daher in dieser Auflage der Textsammlung noch nicht enthalten.

Die Textsammlung Cybersicherheit bietet einen vertieften Einblick in die Gesetzeslage zu einem Thema, das für Unternehmen und die Gesellschaft als Ganzes zunehmend von entscheidender Bedeutung ist. Die Zukunft der Cybersicherheit-Gesetzgebung wird eng mit der Entwicklung der Technologie und der Bedrohungslage verknüpft sein, und Unternehmen müssen sich auf eine ständige Anpassung einstellen. Die vorliegende Textsammlung soll den Anwendern helfen, ein umfassendes Verständnis für die Bedeutung der Gesetze zur Cybersicherheit zu entwickeln.

B. Inhalt

Ziel der **NIS-2-Richtline** ist, ausweislich ErwG 5, die großen Unterschiede zwischen den Mitgliedstaaten hinsichtlich der auferlegten Anforderungen an die Cybersicherheit von solchen Einrichtungen, die Dienste erbringen oder wirtschaftlich signifikante Tätigkeiten ausüben, zu beseitigen. Dies soll insbesondere durch Mindestvorschriften für einen funktionierenden und koordinierten Rechtsrahmen und Mechanismen für die wirksame Zusammenarbeit zwischen den zuständigen Behörden in den einzelnen Mitgliedstaaten erreicht werden. Die Liste der Sektoren und Tätigkeiten, für welche Pflichten im Hinblick auf die Cybersicherheit gelten, wird im Vergleich zur NIS-RL aktualisiert und es werden Abhilfe- und Durchsetzungsmaßnahmen eingeführt. Neben den inzwischen üblichen Bußgeldern bei Verstößen, ist insbesondere auch eine direkte Haftung der Geschäftsleitung vorgesehen.

Die **CER-Richtlinie** (Critical Entities Resilience) zielt darauf ab, die Widerstandsfähigkeit kritischer Einrichtungen zu stärken. Sie verpflichtet die Mitgliedstaaten, solche Einrichtungen zu identifizieren und Maßnahmen zu ergreifen, um ihre physische Widerstandsfähigkeit gegenüber verschiedenen Bedrohungen wie Naturgefahren, Terroranschlägen oder Sabotage zu verbessern. Die Richtlinie legt den Rahmen für den Schutz kritischer Infrastrukturen auf EU-Ebene fest. Es liegt jedoch in der Verantwortung der einzelnen Mitgliedstaaten, spezifische nationale Maßnahmen zur Umsetzung dieser Richtlinie zu erarbeiten und durchzuführen.

Der **Digital Operational Resilience Act (DORA)** ist eine Verordnung, die am 17. Januar 2023 in Kraft getreten ist und darauf abzielt, die IT-Sicherheit von Finanzinstituten wie

Banken, Versicherungsunternehmen und Investmentfirmen zu stärken und sicherzustellen, dass der Finanzsektor in Europa im Falle einer schweren betrieblichen Störung widerstandsfähig bleibt. DORA schafft einen verbindlichen, umfassenden Rahmen für das Risikomanagement im Bereich der Informations- und Kommunikationstechnologie (IKT) und soll die die digitale operationale Resilienz des gesamten europäischen Finanzsektors stärken.

Der **Rechtsakt zur Cybersicherheit** hat als Verordnung zwei Hauptziele. Zum einen die Stärkung des Mandats der zum 27. Juni 2019 errichteten Agentur der Europäischen Union für Cybersicherheit (ENISA) und zum anderen die Einführung eines EU-Rahmens für die freiwillige IT-Sicherheitszertifizierung. Aufgabe der ENISA ist es, die Cybersicherheitskapazitäten in der EU zu erhöhen und die Abwehrbereitschaft zu fördern. Sie fungiert auch als unabhängiges Kompetenzzentrum, das EU-Organe und Mitgliedstaaten bei der Entwicklung und Umsetzung von politischen Rahmenbedingungen im Bereich der Cybersicherheit unterstützt. Sie erhält durch die Verordnung ein dauerhaftes Mandat und wird mit den erforderlichen Ressourcen ausgestattet. Der Rechtsakt zur Cybersicherheit etabliert zudem einen EU-weiten Rahmen für die IT-Sicherheitszertifizierung von Produkten, Dienstleistungen und Prozessen zur Verwirklichung verschiedener Sicherheitsziele, wie z. B. den Schutz gespeicherter, übermittelter und verarbeiteter Daten. Die Schemata für die freiwillige Cybersicherheitszertifizierung können dabei Produkte, Dienste und Prozesse die Vertrauenswürdigkeitsstufen „niedrig“, „mittel“ oder „hoch“ angeben und müssen bestimmte Elemente wie z. B. eine eindeutige Beschreibung des Zwecks des Schemas, den Gegenstand und Umfang des Schemas sowie die Bewertungskriterien und -methoden enthalten.

Die **eIDAS-Verordnung** enthält verbindliche Regelungen in den Bereichen “Elektronische Identifizierung” und „Elektronische Vertrauensdienste“. Sie schafft einheitliche Rahmenbedingungen für die grenzüberschreitende Nutzung elektronischer Identifizierungsmittel und Vertrauensdienste.

Die **Funkanlagenrichtlinie**, auch bekannt als Radio Equipment Directive (RED), ist ein wichtiges Regelungsinstrument für das Inverkehrbringen elektronischer Produkte in der Europäischen Union. Sie hat das Ziel, ein hohes Maß an Schutz in den Bereichen Gesundheit und Sicherheit zu gewährleisten, sowie ein angemessenes Niveau an elektromagnetischer Verträglichkeit und eine effiziente Nutzung von Funkfrequenzen zur Vermeidung von Störungen sicherzustellen. Sie gilt, mit Ausnahme von Amateurfunkanlagen, Schiffsanlagen, Anlagen an Bord von Luftfahrzeugen und zu reinen Forschungs- oder Entwicklungszwecken betriebenen Erprobungsmodulen, für alle Funkanlagen. Sie soll dabei auch den freien Warenverkehr zu ermöglichen. In Deutschland wurde die Richtlinie durch das Gesetz über die Bereitstellung von Funkanlagen auf dem Markt (Funkanlagengesetz) vom 27. Juni 2017 umgesetzt.

Die **Richtlinie über Angriffe auf Informationssysteme** hat das Ziel eine Angleichung des Strafrechts der Mitgliedstaaten im Bereich Angriffe auf Informationssysteme zu erreichen, indem Mindestvorschriften zur Festlegung von Straftaten und einschlägigen Strafen festgelegt werden. Zudem soll die Verbesserung der Zusammenarbeit zwischen den zuständigen Behörden einschließlich der Polizei und anderer spezialisierter Strafverfolgungsbehörden der Mitgliedstaaten sowie der zuständigen Agenturen und Einrichtungen der Union wie Eurojust, Europol und dessen Europäisches Zentrum zur Bekämpfung der Cyberkriminalität und der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) erreicht werden.

Auch die weiteren in der Testsammlung auszugsweise enthaltenen Verordnungen und Richtlinien enthalten für die Cybersicherheit relevante Vorschriften.

Der nationale Gesetzgeber hat sich im europäischen Vergleich bereits sehr früh, und nicht erst im Jahr 2015 mit dem ersten deutschen IT-Sicherheitsgesetz, mit den Bedrohungen aus dem Cyberraum befasst. Seit der 2011 beschlossenen nationalen Cyber-Sicherheitsstrategie hat der Gesetzgeber diverse Gesetze angepasst und um Cybersicherheitsvorschriften ergänzt. Dies passierte nicht zuletzt durch das IT-Sicherheitsgesetz, welches als Artikelgesetz verschiedene Einzelgesetzte betrifft. Zu den geänderten Einzelgesetzen gehören unter anderem das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG), das Telekommunikationsgesetz (TKG) sowie das Bundeskriminalamtgesetz (BKAG). Auch das das Telemediengesetz (TMG) wurde durch das IT-Sicherheitsgesetz geändert, die Regelungen sind durch die TMG-Novelle jedoch inzwischen nicht mehr im TMG enthalten. Mit der BSI-Kritisverordnung wurden ergänzend zum IT-Sicherheitsgesetz bzw. dem BSI-Gesetz dann Sektoren festgelegt, die als kritische Infrastruktur gelten. Zuletzt wurden die Sektoren Anfang 2023 um LNG-Anlagen und Seekabelanlandestationen ergänzt.

Die übrigen in der Textsammlung auszugsweise enthalten Gesetze enthalte jeweils spezifische Regelungen zur Cybersicherheit.

November 2023 Stephan Schmidt

II. RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie)

(Text von Bedeutung für den EWR)

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION –

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 114,

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

nach Stellungnahme der Europäischen Zentralbank([1]),

nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses([2]),

nach Anhörung des Ausschusses der Regionen,

gemäß dem ordentlichen Gesetzgebungsverfahren([3]),

in Erwägung nachstehender Gründe:

(1) Ziel der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates([4]) war der unionsweite Aufbau von Cybersicherheitskapazitäten, die Eindämmung von Bedrohungen für Netz- und Informationssysteme, die zur Erbringung wesentlicher Dienste in Schlüsselsektoren verwendet werden, und die Sicherstellung der Kontinuität solcher Dienste bei Vorfällen, um so zur Sicherheit der Union und zum reibungslosen Funktionieren ihrer Wirtschaft und Gesellschaft beizutragen.

(2) Seit Inkrafttreten der Richtlinie (EU) 2016/1148 sind erhebliche Fortschritte bei der Stärkung der Cyberresilienz der Union erzielt worden. Die Überprüfung jener Richtlinie hat gezeigt, dass sie als Katalysator für das institutionelle und regulatorische Cybersicherheitskonzept in der Union gedient und ein erhebliches Umdenken bewirkt hat. Durch die Einrichtung nationaler Strategien für die Sicherheit von Netz- und Informationssystemen, die Schaffung nationaler Kapazitäten und die Umsetzung von Regulierungsmaßnahmen für Infrastrukturen und Akteure, die von den einzelnen Mitgliedstaaten als wesentlich eingestuft wurden, wurde mit jener Richtlinie die Vervollständigung der nationalen Rechtsrahmen über die Sicherheit von Netz- und Informationssystemen sichergestellt. Darüber hinaus hat die Richtlinie (EU) 2016/1148 durch die Einrichtung der Kooperationsgruppe und des Netzwerks nationaler Computer-Notfallteams zur Zusammenarbeit auf Unionsebene beigetragen. Ungeachtet dieser Erfolge hat die Überprüfung der Richtlinie (EU) 2016/1148 inhärente Mängel ergeben, die ein wirksames Vorgehen gegen aktuelle und neue Herausforderungen im Bereich Cybersicherheit verhindern.

(3) Netz- und Informationssysteme sind durch den schnellen digitalen Wandel und die Vernetzung der Gesellschaft zu einem zentralen Bestandteil des Alltags und für den

grenzüberschreitenden Austausch geworden. Diese Entwicklung hat zu einer Ausweitung der Cyberbedrohungslage geführt und neue Herausforderungen mit sich gebracht, die in allen Mitgliedstaaten entsprechende koordinierte und innovative Reaktionen erfordern. Die Anzahl, Tragweite, Komplexität, Häufigkeit und Auswirkungen von Vorfällen nehmen zu und stellen eine erhebliche Bedrohung für den störungsfreien Betrieb von Netz- und Informationssystemen dar. Im Ergebnis können Vorfälle die Ausübung wirtschaftlicher Tätigkeiten im Binnenmarkt beeinträchtigen, finanziellen Verlust verursachen, das Vertrauen der Nutzer untergraben und der Wirtschaft und Gesellschaft der Union großen Schaden zufügen. Heute sind daher im Bereich Cybersicherheit Vorsorge und Wirksamkeit wichtiger denn je für das reibungslose Funktionieren des Binnenmarkts. Darüber hinaus ist die Cybersicherheit für viele kritische Sektoren eine entscheidende Voraussetzung, um den digitalen Wandel erfolgreich zu bewältigen und die wirtschaftlichen, sozialen und dauerhaften Vorteile der Digitalisierung voll zu nutzen.

(4) Rechtsgrundlage der Richtlinie (EU) 2016/1148 war Artikel 114 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV), der verstärkte Maßnahmen zur Angleichung der einzelstaatlichen Vorschriften vorsieht, die die Errichtung und das Funktionieren des Binnenmarkts zum Gegenstand haben. Die Anforderungen an die Cybersicherheit, die Einrichtungen, die Dienste erbringen oder wirtschaftlich signifikante Tätigkeiten ausüben, auferlegt werden, unterscheiden sich von Mitgliedstaat zu Mitgliedstaat erheblich in Bezug auf die Art der Anforderungen, ihre Detailliertheit und die Art der Aufsicht. Diese Unterschiede verursachen zusätzliche Kosten und führen zu Schwierigkeiten für Einrichtungen, die Waren oder Dienste grenzüberschreitend anbieten. Anforderungen, die von einem Mitgliedstaat auferlegt werden und sich von denen eines anderen Mitgliedstaats unterscheiden oder sogar im Widerspruch zu ihnen stehen, können derartige grenzüberschreitenden Tätigkeiten wesentlich beeinträchtigen. Darüber hinaus dürfte, insbesondere angesichts der Intensität des grenzüberschreitenden Austauschs, eine etwaige unangemessene Gestaltung oder Umsetzung von Cybersicherheitsanforderungen in einem Mitgliedstaat Auswirkungen auf das Cybersicherheitsniveau anderer Mitgliedstaaten haben. Die Überprüfung der Richtlinie (EU) 2016/1148 hat gezeigt, dass die Mitgliedstaaten die Richtlinie sehr unterschiedlich umsetzen, unter anderem in Bezug auf ihren Anwendungsbereich, dessen Abgrenzung weitgehend im Ermessen der Mitgliedstaaten lag. In der Richtlinie (EU) 2016/1148 wurde den Mitgliedstaaten auch ein sehr großer Ermessensspielraum bei der Umsetzung der in der Richtlinie festgelegten Verpflichtungen in Bezug auf die Sicherheit und die Meldung von Sicherheitsvorfällen eingeräumt. Diese Verpflichtungen wurden daher auf nationaler Ebene auf sehr unterschiedliche Weise umgesetzt. Ähnliche Unterschiede gibt es bei der Umsetzung der in der Richtlinie (EU) 2016/1148 enthaltenen Bestimmungen zu Aufsicht und Durchsetzung.

(5) All diese Unterschiede führen zu einer Fragmentierung des Binnenmarkts und können sich nachteilig auf dessen Funktionieren auswirken und aufgrund der Anwendung einer Vielzahl von Maßnahmen insbesondere die grenzüberschreitende Erbringung von Diensten und das Niveau der Cyberresilienz beeinträchtigen. Letztendlich könnten diese Unterschiede zu einer höheren Anfälligkeit einiger Mitgliedstaaten gegenüber Cyberbedrohungen führen, deren Auswirkungen auf die gesamte Union übergreifen könnten. Ziel der vorliegenden Richtlinie ist, diese großen Unterschiede zwischen den Mitgliedstaaten zu beseitigen, indem insbesondere Mindestvorschriften für einen funktionierenden und koordinierten Rechtsrahmen festgelegt werden, Mechanismen für die wirksame Zusammenarbeit zwischen den zuständigen Behörden

in den einzelnen Mitgliedstaaten vorgesehen werden, die Liste der Sektoren und Tätigkeiten, die Pflichten im Hinblick auf die Cybersicherheit unterliegen, aktualisiert wird und wirksame Abhilfemaßnahmen und Durchsetzungsmaßnahmen, die für die wirksame Durchsetzung dieser Verpflichtungen von entscheidender Bedeutung sind, eingeführt werden. Daher sollte die Richtlinie (EU) 2016/1148 aufgehoben und durch die vorliegende Richtlinie ersetzt werden.

(6) Mit der Aufhebung der Richtlinie (EU) 2016/1148 sollte der Anwendungsbereich nach Sektoren auf einen größeren Teil der Wirtschaft ausgeweitet werden, um eine umfassende Abdeckung der Sektoren und Dienste zu gewährleisten, die im Binnenmarkt für grundlegende gesellschaftliche und wirtschaftliche Tätigkeiten von entscheidender Bedeutung sind. Diese Richtlinie zielt darauf insbesondere darauf ab, die Mängel bei der Differenzierung zwischen Betreibern wesentlicher Dienste und Anbietern digitaler Dienste zu beheben, die sich als überholt erwiesen hat, da sie nicht die tatsächliche Bedeutung der Sektoren oder Dienste für die gesellschaftlichen und wirtschaftlichen Tätigkeiten im Binnenmarkt widerspiegelt.

(7) Gemäß der Richtlinie (EU) 2016/1148 waren die Mitgliedstaaten dafür zuständig zu ermitteln, welche Einrichtungen die Kriterien für die Einstufung als Betreiber wesentlicher Dienste erfüllen. Um die diesbezüglichen großen Unterschiede zwischen den Mitgliedstaaten zu beheben und für alle relevanten Einrichtungen Rechtssicherheit hinsichtlich der Risikomanagementmaßnahmen im Bereich der Cybersicherheit und der Berichtspflichten zu gewährleisten, sollte ein einheitliches Kriterium dafür festgelegt werden, welche Einrichtungen in den Anwendungsbereich der vorliegenden Richtlinie fallen. Dieses Kriterium sollte in der Anwendung des Schwellenwerts für die Größe bestehen, nach der alle Einrichtungen, die nach Artikel 2 des Anhangs der Empfehlung 2003/361/EG der Kommission([5]) als mittlere Unternehmen gelten oder die Schwellenwerte für mittlere Unternehmen nach Absatz 1 jenes Artikels überschreiten und die in den Sektoren tätig sind und die Art von Diensten erbringen, die unter die vorliegende Richtlinie fallen, in den Anwendungsbereich der Richtlinie fallen. Die Mitgliedstaaten sollten auch vorsehen, dass bestimmte Kleinunternehmen und Kleinstunternehmen im Sinne von Artikel 2 Absätze 2 und 3 jenes Anhangs, die bestimmte Kriterien erfüllen, die auf eine Schlüsselrolle für die Gesellschaft, die Wirtschaft oder für bestimmte Sektoren oder Arten von Diensten hindeuten, in den Anwendungsbereich dieser Richtlinie fallen.

(8) Der Ausschluss von Einrichtungen der öffentlichen Verwaltung aus dem Anwendungsbereich dieser Richtlinie sollte für Einrichtungen gelten, deren Tätigkeiten überwiegend in den Bereichen nationale Sicherheit, öffentliche Sicherheit, Verteidigung oder Strafverfolgung, einschließlich der Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten, ausgeübt werden. Einrichtungen der öffentlichen Verwaltung, deren Tätigkeiten nur geringfügig mit diesen Bereichen zusammenhängen, sollten jedoch nicht vom Anwendungsbereich dieser Richtlinie ausgenommen werden. Für die Zwecke dieser Richtlinie gelten Einrichtungen mit Regulierungskompetenzen nicht als Einrichtungen, die Tätigkeiten im Bereich der Strafverfolgung ausüben, und sind demnach nicht aus diesem Grunde vom Anwendungsbereich dieser Richtlinie ausgenommen. Einrichtungen der öffentlichen Verwaltung, die gemäß einer internationalen Übereinkunft gemeinsam mit einem Drittland gegründet wurden, sind vom Anwendungsbereich dieser Richtlinie ausgenommen. Diese Richtlinie gilt nicht für diplomatische und konsularische Vertretungen der Mitgliedstaaten in Drittländern oder für deren Netz- und Informationssysteme, sofern sich diese Systeme in

den Räumlichkeiten der Mission befinden oder für Nutzer in einem Drittland betrieben werden.

(9) Die Mitgliedstaaten sollten die Möglichkeit haben, die für die Wahrung ihrer wesentlichen Interessen der nationalen Sicherheit und den Schutz der öffentlichen Ordnung und der öffentlichen Sicherheit erforderlichen Maßnahmen zu ergreifen und die Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten zu ermöglichen. Zu diesem Zweck sollten die Mitgliedstaaten bestimmte Einrichtungen, die in den Bereichen nationale Sicherheit, öffentliche Sicherheit, Verteidigung oder Strafverfolgung tätig sind, einschließlich der Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten, von bestimmten in dieser Richtlinie festgelegten Verpflichtungen in Bezug auf diese Tätigkeiten ausnehmen können. Erbringt eine Einrichtung Dienste ausschließlich für eine Einrichtung der öffentlichen Verwaltung, die vom Anwendungsbereich dieser Richtlinie ausgenommen ist, so sollten die Mitgliedstaaten diese Einrichtung nicht von bestimmten in dieser Richtlinie festgelegten Verpflichtungen in Bezug auf diese Dienste ausnehmen können. Darüber hinaus sollte kein Mitgliedstaat verpflichtet sein, Auskünfte zu erteilen, deren Preisgabe seinen wesentlichen Interessen der nationalen Sicherheit, der öffentlichen Sicherheit oder der Verteidigung widerspräche. Unionsvorschriften und nationale Vorschriften zum Schutz von Verschlusssachen, Geheimhaltungsvereinbarungen und informelle Geheimhaltungsvereinbarungen wie das sogenannte Traffic Light Protocol sollten in diesem Zusammenhang berücksichtigt werden. Das Traffic Light Protocol ist als eine Mittel zu verstehen, um Informationen über etwaige Einschränkungen im Hinblick auf die weitere Verbreitung von Informationen bereitzustellen. Es wird in fast allen Computer-Notfallteams (computer security incident response teams – CSIRTs) und in einigen Zentren für Informationsanalyse und -weitergabe eingesetzt.

(10) Diese Richtlinie gilt zwar für Einrichtungen, die Tätigkeiten zur Erzeugung von Strom aus Kernkraftwerken ausüben, einige dieser Tätigkeiten können jedoch mit der nationalen Sicherheit in Verbindung stehen. Ist dies der Fall, so sollte ein Mitgliedstaat seine Verantwortung für den Schutz der nationalen Sicherheit in Bezug auf diese Tätigkeiten, einschließlich Tätigkeiten innerhalb der nuklearen Wertschöpfungskette, im Einklang mit den Verträgen wahrnehmen können.

(11) Einige Einrichtungen üben Tätigkeiten in den Bereichen nationale Sicherheit, öffentliche Sicherheit, Verteidigung oder Strafverfolgung, einschließlich der Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten, aus und erbringen gleichzeitig Vertrauensdienste. Vertrauensdiensteanbieter, die in den Anwendungsbereich der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates([6]) fallen, sollten in den Anwendungsbereich dieser Richtlinie fallen, um das gleiche Niveau der Sicherheitsanforderungen und der Aufsicht zu gewährleisten, wie es zuvor in der genannten Verordnung für Vertrauensdiensteanbieter festgelegt war. Entsprechend dem Ausschluss bestimmter besonderer Dienste von der Verordnung (EU) Nr. 910/2014 findet diese Richtlinie keine Anwendung auf die Erbringung von Vertrauensdiensten, die ausschließlich innerhalb geschlossener Systeme aufgrund von nationalem Recht oder von Vereinbarungen zwischen einem bestimmten Kreis von Beteiligten verwendet werden.

(12) Anbieter von Postdiensten im Sinne der Richtlinie 97/67/EG des Europäischen Parlaments und des Rates([7]), einschließlich Anbieter von Kurierdiensten sollten der vorliegenden Richtlinie unterliegen, wenn sie mindestens einen der Schritte in der Postzustellkette und insbesondere Abholung, Sortierung, Transport oder Zustellung von Postsendungen, einschließlich Abholung durch den Empfänger, anbieten, wobei das

Ausmaß ihrer Abhängigkeit von Netz- und Informationssystemen zu berücksichtigen ist. Transportdienste, die nicht in Verbindung mit einem dieser Schritte erbracht werden, sollten nicht unter Postdienste fallen.

(13) Angesichts der Verschärfung und der zunehmenden Komplexität von Cyberbedrohungen sollten die Mitgliedstaaten bestrebt sein, dafür zu sorgen, dass Einrichtungen, die vom Anwendungsbereich dieser Richtlinie ausgenommen sind, ein hohes Maß an Cybersicherheit erreichen, und die Umsetzung gleichwertiger Maßnahmen für das Risikomanagement im Bereich der Cybersicherheit unterstützen, die dem sensiblen Charakter dieser Einrichtungen Rechnung tragen.

(14) Jede Verarbeitung personenbezogener Daten im Rahmen dieser Richtlinie unterliegt dem Unionsrecht zum Datenschutz und zum Schutz der Privatsphäre. Diese Richtlinie lässt insbesondere die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates([8]) und die Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates([9]) unberührt. Diese Richtlinie sollte daher unter anderem nicht die Aufgaben und Befugnisse der Behörden berühren, die für die Überwachung der Einhaltung des geltenden Unionsrechts zum Datenschutz und zum Schutz der Privatsphäre zuständig sind.

(15) Bei Einrichtungen, die für die Zwecke der Einhaltung von Risikomanagementmaßnahmen und der Meldepflichten im Bereich der Cybersicherheit in den Geltungsbereich dieser Richtlinie fallen, sollten zwei Kategorien unterschieden werden: wesentliche Einrichtungen und wichtige Einrichtungen; zu berücksichtigen ist dabei der Grad ihrer Kritikalität in Bezug auf ihren Sektor oder die Art der von ihnen erbrachten Dienste sowie ihre Größe. In diesem Zusammenhang sollten gegebenenfalls einschlägige sektorspezifische Risikobewertungen oder Leitlinien der zuständigen Behörden gebührend berücksichtigt werden. Bei den Aufsichts- und Durchsetzungsregelungen sollte bei diesen beiden Kategorien von Einrichtungen differenziert werden, um ein ausgewogenes Verhältnis zwischen risikobasierten Anforderungen und Pflichten einerseits und dem Verwaltungsaufwand, der sich andererseits aus der Überwachung der Einhaltung ergibt, zu gewährleisten.

(16) Um zu vermeiden, dass Einrichtungen, die Partnerunternehmen haben oder verbundene Unternehmen sind, als wesentliche oder wichtige Einrichtungen betrachtet werden, wenn dies unverhältnismäßig wäre, können die Mitgliedstaaten bei der Anwendung von Artikel 6 Absatz 2 des Anhangs der Empfehlung 2003/361/EG den Grad der Unabhängigkeit einer Einrichtung gegenüber ihren Partnerunternehmen und verbundenen Unternehmen berücksichtigen. Insbesondere können die Mitgliedstaaten berücksichtigen, dass eine Einrichtung in Bezug auf die Netz- und Informationssysteme, die sie bei der Erbringung ihrer Dienste nutzt, und in Bezug auf die von ihr erbrachten Dienste unabhängig von ihren Partnerunternehmen oder verbundenen Unternehmen ist. Auf dieser Grundlage können die Mitgliedstaaten gegebenenfalls davon ausgehen, dass eine solche Einrichtung nicht nach Artikel 2 des Anhangs der Empfehlung 2003/361/EG als mittleres Unternehmen gilt oder die Schwellenwerte für mittlere Unternehmen nach Absatz 1 jenes Artikels nicht überschreitet, wenn nach Berücksichtigung des Grades der Unabhängigkeit dieser Einrichtung davon ausgegangen worden wäre, dass sie nicht als mittleres Unternehmen gilt oder diese Schwellenwerte nicht überschreitet, falls nur ihre eigenen Daten berücksichtigt worden wären. Die in dieser Richtlinie festgelegten Verpflichtungen von Partnerunternehmen und verbundenen Unternehmen, die in den Anwendungsbereich dieser Richtlinie fallen, bleiben davon unberührt.

(17) Die Mitgliedstaaten sollten beschließen können, dass Einrichtungen, die vor Inkrafttreten dieser Richtlinie gemäß der Richtlinie (EU) 2016/1148 als Betreiber wesentlicher Dienste ermittelt wurden, als wesentliche Einrichtungen gelten.

(18) Um für einen klaren Überblick über die in den Anwendungsbereich dieser Richtlinie fallenden Einrichtungen zu sorgen, sollten die Mitgliedstaaten eine Liste von wesentlichen und wichtigen Einrichtungen und von Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, erstellen. Zu diesem Zweck sollten die Mitgliedstaaten die Einrichtungen dazu verpflichten, den zuständigen Behörden mindestens die folgenden Informationen zu übermitteln, nämlich Name, Anschrift und aktuelle Kontaktdaten, einschließlich E-Mail-Adressen, IP-Adressbereiche und Telefonnummern der Einrichtung, und gegebenenfalls betreffender Sektor und Teilsektor gemäß den Anhängen, sowie gegebenenfalls eine Liste der Mitgliedstaaten, in denen sie in den Anwendungsbereich dieser Richtlinie fallende Dienste erbringen. Zu diesem Zweck sollte die Kommission mit Unterstützung der Agentur der Europäischen Union für Cybersicherheit (ENISA) unverzüglich Leitlinien und Vorlagen für die Verpflichtungen zur Übermittlung von Informationen bereitstellen. Um die Erstellung und Aktualisierung der Liste von wesentlichen und wichtigen Einrichtungen und von Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, zu erleichtern, sollten die Mitgliedstaaten die Möglichkeit haben, nationale Mechanismen für die Registrierung von Einrichtungen einzurichten. Bestehen Register auf nationaler Ebene, können die Mitgliedstaaten geeignete Mechanismen beschließen, die die Identifizierung von Einrichtungen ermöglichen, die in den Anwendungsbereich dieser Richtlinie fallen.

(19) Die Mitgliedstaaten sollten dafür verantwortlich sein, der Kommission mindestens die Zahl der wesentlichen und wichtigen Einrichtungen für jeden in den Anhängen genannten Sektor und Teilsektor sowie relevante Informationen über die Zahl der ermittelten Einrichtungen und die Bestimmungen dieser Richtlinie, auf deren Grundlage sie ermittelt wurden, und die Art der von ihnen erbrachten Dienste zu übermitteln. Die Mitgliedstaaten werden aufgefordert, mit der Kommission Informationen über wesentliche und wichtige Einrichtungen und – im Falle eines Cybersicherheitsvorfalls großen Ausmaßes – relevante Informationen wie den Namen der betreffenden Einrichtung auszutauschen.

(20) Die Kommission sollte in Zusammenarbeit mit der Kooperationsgruppe und nach Konsultation der einschlägigen Interessenträger Leitlinien für die Anwendung der für Kleinstunternehmen und kleine Unternehmen geltenden Kriterien bereitstellen, um zu bewerten, ob sie in den Anwendungsbereich dieser Richtlinie fallen. Die Kommission sollte auch dafür sorgen, dass Kleinstunternehmen und Kleinunternehmen, die in den Anwendungsbereich dieser Richtlinie fallen, eine angemessene Anleitung erhalten. Die Kommission sollte mit Unterstützung der Mitgliedstaaten den Kleinstunternehmen und Kleinunternehmen diesbezügliche Informationen zur Verfügung stellen.

(21) Die Kommission könnte Leitlinien herausgeben, um die Mitgliedstaaten bei der Umsetzung der Bestimmungen dieser Richtlinie über den Anwendungsbereich und bei der Bewertung der Verhältnismäßigkeit der im Rahmen dieser Richtlinie zu treffenden Maßnahmen zu unterstützen, insbesondere in Bezug auf Einrichtungen mit komplexen Geschäftsmodellen oder Betriebsumgebungen, wobei eine Einrichtung gleichzeitig die Kriterien für wesentliche und für wichtige Einrichtungen erfüllen kann oder gleichzeitig Tätigkeiten, die in den Anwendungsbereich dieser Richtlinie fallen, und andere Tätigkeiten, die nicht in den Anwendungsbereich dieser Richtlinie fallen, ausführen kann.

(22) In dieser Richtlinie wird das Grundniveau für Risikomanagementmaßnahmen und Berichtspflichten im Bereich der Cybersicherheit für die in den Anwendungsbereich der Richtlinie fallenden Sektoren festgelegt. Wenn zusätzliche sektorspezifische Rechtsakte der Union über Maßnahmen zum Cybersicherheitsrisikomanagement und Berichtspflichten für notwendig erachtet werden, um in der gesamten Union ein hohes Maß an Cybersicherheit zu gewährleisten, sollte die Kommission – zur Vermeidung einer Fragmentierung der Cybersicherheitsbestimmungen von Rechtsakten der Union – prüfen, ob diese weiteren Bestimmungen im Rahmen eines Durchführungsrechtsakts gemäß dieser Richtlinie festgelegt werden könnten. Sollte sich ein solcher Durchführungsrechtsakt zu diesem Zweck nicht eignen, so könnten sektorspezifische Rechtsakte der Union dazu beitragen, dass in der gesamten Union ein hohes Maß an Cybersicherheit gewährleistet ist und gleichzeitig den Besonderheiten und Komplexitäten der betreffenden Sektoren in vollem Umfang Rechnung getragen wird. Daher schließt die vorliegende Richtlinie nicht aus, dass zusätzliche sektorspezifische Rechtsakte der Union zu Risikomanagementmaßnahmen und Berichtspflichten im Bereich der Cybersicherheit, die der Notwendigkeit eines umfassenden und kohärenten Cybersicherheitsrahmens gebührend Rechnung tragen, erlassen werden. Die vorliegende Richtlinie berührt nicht die bestehenden Durchführungsbefugnisse, die der Kommission in einer Reihe von Sektoren, darunter Verkehr und Energie, übertragen wurden.

(23) Wenn wesentliche oder wichtige Einrichtungen gemäß den Bestimmungen eines sektorspezifischen Rechtsakts der Union entweder Risikomanagementmaßnahmen im Bereich der Cybersicherheit ergreifen oder erhebliche Sicherheitsvorfälle melden müssen und wenn die entsprechenden Anforderungen in ihrer Wirkung den in dieser Richtlinie festgelegten Verpflichtungen zumindest gleichwertig sind, sollten diese Bestimmungen, einschließlich der Bestimmungen über Aufsicht und Durchsetzung, keine Anwendung auf solche Einrichtungen finden. Wenn ein sektorspezifischer Rechtsakt der Union nicht für alle in den Anwendungsbereich dieser Richtlinie fallenden Einrichtungen eines bestimmten Sektors gilt, sollten die einschlägigen Bestimmungen dieser Richtlinie weiterhin im Falle der Einrichtungen zur Anwendung kommen, die nicht unter diesen Rechtsakt fallen.

(24) Wenn wesentliche oder wichtige Einrichtungen nach den Bestimmungen eines sektorspezifischen Rechtsakts der Union verpflichtet sind, Berichtspflichten zu erfüllen, die mindestens die gleiche Wirkung wie die in dieser Richtlinie festgelegten Berichtspflichten haben, sollte dafür gesorgt werden, dass Meldungen von Sicherheitsvorfällen kohärent und wirksam bearbeitet werden. Zu diesem Zweck sollten die Bestimmungen über die Meldung von Sicherheitsvorfällen des sektorspezifischen Rechtsakts der Union den CSIRTs, den zuständigen Behörden oder den zentralen Anlaufstellen für Cybersicherheit (zentrale Anlaufstelle) gemäß dieser Richtlinie einen sofortigen Zugang zu den gemäß dem sektorspezifischen Rechtsakt der Union übermittelten Meldungen von Sicherheitsvorfällen ermöglichen. Ein solcher sofortiger Zugang kann insbesondere gewährt werden, wenn Meldungen von Sicherheitsvorfällen unverzüglich an das CSIRT, die zuständige Behörde oder die zentrale Anlaufstelle gemäß dieser Richtlinie weitergeleitet werden. Gegebenenfalls sollten die Mitgliedstaaten einen automatischen und direkten Meldemechanismus einrichten, der einen systematischen und sofortigen Informationsaustausch mit den CSIRTs, den zuständigen Behörden oder den zentralen Anlaufstellen für die Bearbeitung solcher Meldungen von Sicherheitsvorfällen sicherstellt. Um die Berichterstattung zu vereinfachen und den Mechanismus der automatischen und direkten Berichterstattung umzusetzen,

könnten die Mitgliedstaaten im Einklang mit dem sektorspezifischen Rechtsakt der Union eine zentrale Anlaufstelle nutzen.

(25) In sektorspezifischen Rechtsakten der Union, in denen Risikomanagementmaßnahmen oder Berichtspflichten im Bereich der Cybersicherheit vorgesehen sind, die in ihrer Wirkung den in dieser Richtlinie festgelegten entsprechenden Maßnahmen und Pflichten mindestens gleichwertig sind, könnte vorgesehen werden, dass die gemäß dieser Rechtsakte zuständigen Behörden ihre Aufsichts- und Durchsetzungsbefugnisse in Bezug auf solche Maßnahmen oder Pflichten mit Unterstützung der zuständigen Behörden gemäß der vorliegenden Richtlinie ausüben. Die betreffenden zuständigen Behörden könnten zu diesem Zweck Kooperationsvereinbarungen schließen. In solchen Kooperationsvereinbarungen könnten unter anderem die Verfahren für die Koordinierung der Aufsichtstätigkeiten festgelegt werden, einschließlich der Verfahren für im Einklang mit nationalem Recht durchzuführende Untersuchungen und Prüfungen vor Ort und eines Mechanismus für den Austausch einschlägiger Informationen zwischen den zuständigen Behörden über Aufsicht und Durchsetzung, wozu auch der Zugang zu Cyberinformationen gehört, der von den zuständigen Behörden gemäß dieser Richtlinie beantragt wird.

(26) Wenn sektorspezifische Rechtsakte der Union Einrichtungen zur Meldung erheblicher Cyberbedrohungen verpflichten oder ihnen entsprechende Anreize bieten, sollten die Mitgliedstaaten auch fördern, dass erhebliche Cyberbedrohungen den CSIRTs, den zuständigen Behörden oder den zentralen Anlaufstellen gemäß dieser Richtlinie gemeldet werden, um dafür zu sorgen, dass diesen Stellen die Cyberbedrohungslage besser bewusst ist, und sie in die Lage zu versetzen, wirksam und rechtzeitig zu reagieren, falls die erheblichen Cyberbedrohungen eintreten sollten.

(27) In künftigen sektorspezifischen Rechtsakten der Union sollte den in dieser Richtlinie festgelegten Begriffsbestimmungen und dem Aufsichts- und Durchsetzungsrahmen gebührend Rechnung getragen werden.

(28) Die Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates([10]) sollte im Zusammenhang mit der vorliegenden Richtlinie als sektorspezifischer Rechtsakt der Union in Bezug auf Finanzunternehmen betrachtet werden. Anstelle der Bestimmungen in der vorliegenden Richtlinie sollten die Bestimmungen der Verordnung (EU) 2022/2554 gelten, die sich auf Risikomanagement im Bereich der Informations- und Kommunikationstechnologien (IKT), das Management von IKT-bezogenen Vorfällen und insbesondere die Meldung von schwerwiegenden IKT-bezogenen Vorfällen sowie die Prüfung der digitalen Betriebsstabilität, Vereinbarungen über den Informationsaustausch und Risiken durch IKT-Drittanbieter beziehen. Die Mitgliedstaaten sollten daher die Bestimmungen der vorliegenden Richtlinie, die sich auf Cybersicherheitsrisikomanagement und Berichtspflichten sowie Aufsicht und Durchsetzung beziehen, nicht auf Finanzunternehmen anwenden, die unter jene Verordnung fallen. Gleichzeitig ist es wichtig, im Rahmen der vorliegenden Richtlinie eine enge Beziehung zum und den Informationsaustausch mit dem Finanzsektor aufrechtzuerhalten. Zu diesem Zweck ist es gemäß der Verordnung (EU) 2022/2554 zulässig, dass die Europäischen Aufsichtsbehörden und die gemäß der Verordnung (EU) 2022/2554 zuständigen nationalen Behörden sich an der Tätigkeit der Kooperationsgruppe beteiligen und mit den zentralen Anlaufstellen sowie den nationalen CSIRTs und den zuständigen Behörden gemäß dieser Richtlinie Informationen austauschen und zusammenarbeiten Die gemäß der Verordnung (EU) 2022/2554 zuständigen Behörden sollten auch Einzelheiten über schwerwiegende IKT-bezogenen Vorfällen und, gegebenenfalls, erhebliche Cyberbedrohungen auch an die CSIRTs, die zuständigen

Behörden oder an die gemäß der vorliegenden Richtlinie benannten zentralen Anlaufstellen übermitteln. Dies lässt sich erreichen, indem ein unmittelbarer Zugang zu Meldungen von Vorfällen und ihre direkte Weiterleitung oder über eine zentrale Anlaufstelle für die Meldung von Vorfällen ermöglicht wird. Darüber hinaus sollten die Mitgliedstaaten den Finanzsektor weiterhin in ihre Cybersicherheitsstrategien einbeziehen, und die CSIRTs können den Finanzsektor bei ihren Tätigkeiten einbeziehen.

(29) Um Lücken und Überschneidungen bei Luftverkehrseinrichtungen auferlegten Cybersicherheitsverpflichtungen zu vermeiden, sollten die gemäß den Verordnungen (EG) Nr. 300/2008([11]) und (EU) 2018/1139([12]) des Europäischen Parlaments und des Rates benannten nationalen Behörden und die gemäß dieser Richtlinie zuständigen Behörden bei der Umsetzung von Maßnahmen zum Cybersicherheitsrisikomanagement und der Aufsicht über die Einhaltung dieser Maßnahmen auf nationaler Ebene zusammenarbeiten. Die Einhaltung der Sicherheitsanforderungen durch eine Einrichtung, die in den Verordnungen (EG) Nr. 300/2008 und (EU) 2018/1139 sowie in den gemäß diesen Verordnungen erlassenen einschlägigen delegierten Rechtsakten und Durchführungsrechtsakten festgelegt sind, könnte von den gemäß dieser Richtlinie zuständigen Behörden als Einhaltung der entsprechenden Anforderungen dieser Richtlinie erachtet werden.

(30) Angesichts der Zusammenhänge zwischen der Cybersicherheit und der physischen Sicherheit von Einrichtungen sollte dafür gesorgt werden, dass der Ansatz der Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates([13]) und der Ansatz der vorliegenden Richtlinie kohärent sind. Um dies zu erreichen, sollten Einrichtungen, die gemäß der Richtlinie (EU) 2022/2557 als kritische Einrichtungen eingestuft wurden als wesentliche Einrichtungen im Sinne der vorliegenden Richtlinie gelten. Darüber hinaus sollte jeder Mitgliedstaat sicherstellen, dass seine nationale Cybersicherheitsstrategie einen politischen Rahmen für eine verstärkte Koordinierung innerhalb dieses Mitgliedstaaten zwischen seinen gemäß der vorliegenden Richtlinie zuständigen Behörden und denen gemäß Richtlinie (EU) 2022/2557 beim Informationsaustausch über Risiken, Cyberbedrohungen und Sicherheitsvorfälle sowie über nicht cyberbezogene Risiken, Bedrohungen und Sicherheitsvorfälle sowie bei der Wahrnehmung von Aufsichtsaufgaben vorsieht. Die gemäß der vorliegenden Richtlinie zuständigen Behörden und denen gemäß Richtlinie (EU) 2022/2557 sollten zusammenarbeiten und unverzüglich Informationen austauschen, insbesondere in Bezug auf die Ermittlung kritischer Einrichtungen, Cyberbedrohungen, Cybersicherheitsrisiken und Sicherheitsvorfälle sowie nicht cyberbezogene Risiken, Bedrohungen und Sicherheitsvorfälle, die kritische Einrichtungen beeinträchtigen, einschließlich der von kritischen Einrichtungen ergriffenen Cybersicherheitsmaßnahmen und physischen Maßnahmen sowie der Ergebnisse der bezüglich dieser Einrichtungen durchgeführten Aufsichtstätigkeiten.

Um die Aufsichtstätigkeiten zwischen den nach der vorliegenden Richtlinie zuständigen Behörden und denen gemäß Richtlinie (EU) 2022/2557 zu straffen und den Verwaltungsaufwand für die betreffenden Einrichtungen so gering wie möglich zu halten, sollten diese zuständigen Behörden zudem bestrebt sein, die Vorlagen für die Meldung von Sicherheitsvorfällen und die Aufsichtsverfahren zu harmonisieren. Gegebenenfalls sollten die gemäß der Richtlinie (EU) 2022/2557 zuständigen Behörden die gemäß der vorliegenden Richtlinie zuständigen Behörden ersuchen können, ihre Aufsichts- und Durchsetzungsbefugnisse in Bezug auf eine Einrichtung, die gemäß der Richtlinie (EU) 2022/2557 als kritische Einrichtung eingestuft wird, auszuüben. Die gemäß der vorliegenden Richtlinie zuständigen Behörden und denen gemäß

Richtlinie (EU) 2022/2557 sollten zu diesem Zweck nach Möglichkeit in Echtzeit zusammenarbeiten und Informationen austauschen.

(31) Einrichtungen im Bereich digitale Infrastruktur beruhen im Wesentlichen auf Netz- und Informationssystemen; aus diesem Grund sollte in den Verpflichtungen, die diesen Einrichtungen gemäß dieser Richtlinie im Rahmen ihrer Risikomanagementmaßnahmen und Berichtspflichten im Bereich Cybersicherheit auferlegt werden, umfassend auf die physische Sicherheit dieser Systeme eingegangen werden. Da diese Angelegenheiten Gegenstand der vorliegenden Richtlinie sind, gelten die in den Kapiteln III, IV und VI der Richtlinie (EU) 2022/2557 festgelegten Verpflichtungen nicht für solche Einrichtungen.

(32) Die Aufrechterhaltung und Beibehaltung eines zuverlässigen, resilienten und sicheren Domänennamensystems (domain name system – DNS) ist ein Schlüsselfaktor für die Wahrung der Integrität des Internets und von entscheidender Bedeutung für dessen kontinuierlichen und stabilen Betrieb, von dem die digitale Wirtschaft und Gesellschaft abhängig ist. Daher sollte die vorliegende Richtlinie für Namenregister der Domäne oberster Stufe (top-level-domain – TLD) und DNS-Diensteanbieter gelten, die als Einrichtungen zu verstehen sind, die öffentlich zugängliche rekursive Dienste zur Auflösung von Domänennamen für Internet-Endnutzer oder autoritative Dienste zur Auflösung von Domänennamen erbringen. Diese Richtlinie sollte nicht für Root-Namenserver gelten.

(33) Cloud-Computing-Dienste sollten digitale Dienste umfassen, die auf Abruf die Verwaltung und den umfassenden Fernzugang zu einem skalierbaren und elastischen Pool gemeinsam nutzbarer Rechenressourcen ermöglichen, auch wenn diese Ressourcen auf mehrere Standorte verteilt sind. Zu Rechenressourcen zählen Ressourcen wie Netze, Server oder sonstige Infrastruktur, Betriebssysteme, Software, Speicher, Anwendungen und Dienste. Zu den Dienstmodellen des Cloud-Computing gehören unter anderem IaaS (Infrastructure as a Service, PaaS (Platform as a Service), SaaS (Software as a Service) und NaaS (Network as a Service). Die Bereitstellungsmodelle für Cloud-Computing sollten die private, die gemeinschaftliche, die öffentliche und die hybride Cloud umfassen. Die Cloud-Computing-Dienst- und Bereitstellungsmodelle haben dieselbe Bedeutung wie die in der Norm ISO/IEC 17788:2014 definierten Dienst- und Bereitstellungsmodelle. Dass sich der Cloud-Computing-Nutzer selbst ohne Interaktion mit dem Anbieter von Cloud-Computing-Diensten Rechenkapazitäten wie Serverzeit oder Netzwerkspeicherplatz zuweisen kann, könnte als Verwaltung auf Abruf beschrieben werden.

Der Begriff „umfassender Fernzugang“ wird verwendet, um zu beschreiben, dass die Cloud-Kapazitäten über das Netz bereitgestellt und über Mechanismen zugänglich gemacht werden, die den Einsatz heterogener Thin- oder Thick-Client-Plattformen (einschließlich Mobiltelefonen, Tablets, Laptops und Arbeitsplatzrechnern) fördern. Der Begriff „skalierbar“ bezeichnet Rechenressourcen, die unabhängig von ihrem geografischen Standort vom Anbieter des Cloud-Dienstes flexibel zugeteilt werden, damit Nachfrageschwankungen bewältigt werden können. Der Begriff „elastischer Pool“ wird verwendet, um Rechenressourcen zu beschreiben, die entsprechend der Nachfrage bereitgestellt und freigegeben werden, damit die Menge der verfügbaren Ressourcen je nach Arbeitsaufkommen rasch erhöht oder reduziert werden kann. Der Begriff „gemeinsam nutzbar“ wird verwendet, um Rechenressourcen zu beschreiben, die einer Vielzahl von Nutzern bereitgestellt werden, die über einen gemeinsamen Zugang auf den Dienst zugreifen, wobei jedoch die Verarbeitung für jeden Nutzer separat erfolgt, obwohl der Dienst über dieselbe elektronische Ausrüstung erbracht

wird. Der Begriff „verteilt“ wird verwendet, um Rechenressourcen zu beschreiben, die sich auf verschiedenen vernetzten Computern oder Geräten befinden und die untereinander durch Nachrichtenaustausch kommunizieren und koordinieren.

(34) Angesichts des Aufkommens innovativer Technologien und neuer Geschäftsmodelle dürften auf dem Binnenmarkt neue Dienst- und Bereitstellungsmodelle für Cloud-Computing entstehen, um den sich wandelnden Kundenbedürfnissen gerecht zu werden. In diesem Zusammenhang können Cloud-Computing-Dienste in hochgradig verteilter Form, noch näher am Ort der Datengenerierung oder -sammlung, erbracht werden, wodurch vom traditionellen Modell zu einem hochgradig verteilten Modell („Edge-Computing“) übergegangen wird.

(35) Dienste, die von Anbietern von Rechenzentrumsdiensten angeboten werden, werden möglicherweise nicht immer in Form eines Cloud-Computing-Diensts erbracht. Dementsprechend sind Rechenzentren möglicherweise nicht immer Teil einer Cloud-Computing-Infrastruktur. Um allen Risiken für die Sicherheit von Netz- und Informationssystemen zu begegnen, sollte die vorliegende Richtlinie daher für Anbieter von Rechenzentrumsdiensten gelten, bei denen es sich nicht um Cloud-Computing-Dienste handelt. Für die Zwecke der vorliegenden Richtlinie sollte der Begriff „Rechenzentrumsdienst“ Dienste umfassen, mit denen Strukturen oder Gruppen von Strukturen für die zentrale Unterbringung, die Verbindung und den Betrieb von Informationstechnologie (IT) und Netzausrüstungen zur Erbringung von Datenspeicher-, Datenverarbeitungs- und Datentransportdiensten sowie alle Anlagen und Infrastrukturen für die Leistungsverteilung und die Umgebungskontrolle bereitgestellt werden. Der Begriff „Rechenzentrumsdienst“ sollte nicht für interne Rechenzentren, die sich im Besitz der betreffenden Einrichtung befinden und von der betreffenden Einrichtung für eigene Zwecke betrieben werden.

(36) Forschungstätigkeiten spielen eine Schlüsselrolle bei der Entwicklung neuer Produkte und Prozesse. Viele dieser Tätigkeiten werden von Einrichtungen durchgeführt, die ihre Forschungsergebnisse zu kommerziellen Zwecken teilen, verbreiten oder nutzen. Diese Einrichtungen können daher wichtige Akteure in Wertschöpfungsketten sein, was die Sicherheit ihrer Netz- und Informationssysteme zu einem integralen Bestandteil der allgemeinen Cybersicherheit des Binnenmarkts macht. Unter Forschungseinrichtungen sind unter anderem Einrichtungen zu verstehen, die sich im Wesentlichen auf die Durchführung von angewandter Forschung oder experimenteller Entwicklung im Sinne des Frascati-Handbuchs der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung von 2015 (Leitlinien zur Erfassung von Daten zu Forschung und experimenteller Entwicklung sowie zur entsprechenden Berichterstattung) konzentrieren, um ihre Ergebnisse für kommerzielle Zwecke wie die Herstellung oder Entwicklung eines Produkts oder eines Verfahrens, die Erbringung eines Dienstes, oder dessen Vermarktung zu nutzen.

(37) Die wachsenden gegenseitigen Abhängigkeiten sind das Ergebnis eines sich über immer mehr Grenzen hinweg erstreckenden und zunehmend interdependenten Dienstleistungsnetzes, das zentrale Infrastrukturen in der gesamten Union nutzt, und zwar in Sektoren wie z. B. Energie, Verkehr, digitale Infrastruktur, Trinkwasser und Abwasser, Gesundheit, bestimmten Bereichen der öffentlichen Verwaltung sowie im Weltraumsektor, soweit es um die Erbringung bestimmter Dienste geht, die von Bodeninfrastrukturen abhängig sind, die sich im Eigentum von Mitgliedstaaten oder privaten Parteien befinden und von diesen verwaltet und betrieben werden; damit sind Infrastrukturen ausgenommen, die sich im Eigentum der Union befinden oder von der Union oder in ihrem Namen im Rahmen ihres Weltraumprogramms verwaltet oder

betrieben werden. Wegen dieser gegenseitigen Abhängigkeiten kann jede Störung, auch wenn sie anfänglich auf eine Einrichtung oder einen Sektor beschränkt ist, zu breiteren Kaskadeneffekten führen, die weitreichende und lang anhaltende negative Auswirkungen auf die Erbringung von Diensten im gesamten Binnenmarkt haben können. Die verstärkten Cyberangriffe während der COVID-19-Pandemie haben gezeigt, wie anfällig zunehmend interdependente Gesellschaften für Risiken mit geringer Eintrittswahrscheinlichkeit sind.

(38) Angesichts der unterschiedlichen nationalen Governancestrukturen und zwecks Beibehaltung von bereits bestehenden sektorbezogenen Vereinbarungen und Aufsichts- oder Regulierungsstellen der Union sollten die Mitgliedstaaten befugt sein, eine oder mehr als eine nationale Behörde zu benennen oder einzurichten, die für die Cybersicherheit und die Aufsichtsaufgaben gemäß der vorliegenden Richtlinie zuständig sind.

(39) Zur Erleichterung der grenzüberschreitenden Zusammenarbeit und Kommunikation zwischen Behörden und um die wirksame Umsetzung der vorliegenden Richtlinie zu ermöglichen, ist es notwendig, dass jeder Mitgliedstaat eine zentrale Anlaufstelle benennt, die für die Koordinierung im Zusammenhang mit der Sicherheit von Netz- und Informationssystemen und für die grenzüberschreitende Zusammenarbeit auf Unionsebene zuständig ist.

(40) Die zentralen Anlaufstellen sollten für eine wirksame grenzüberschreitende Zusammenarbeit mit den zuständigen Behörden anderer Mitgliedstaaten und gegebenenfalls mit der Kommission und der ENISA sorgen. Die zentralen Anlaufstellen sollten daher beauftragt werden, Meldungen über erhebliche Sicherheitsvorfälle mit grenzüberschreitenden Auswirkungen auf Ersuchen des CSIRT oder der zuständigen Behörde an die zentralen Anlaufstellen anderer betroffener Mitgliedstaaten weiterzuleiten. Auf nationaler Ebene sollten die zentralen Anlaufstellen eine reibungslose sektorübergreifende Zusammenarbeit mit anderen zuständigen Behörden ermöglichen. Die zentralen Anlaufstellen könnten auch relevante Informationen über Vorfälle, die Finanzeinrichtungen betreffen, von den gemäß der Verordnung (EU) 2022/2554 zuständigen Behörden entgegennehmen, die sie gegebenenfalls gemäß der vorliegenden Richtlinie an die CSIRTs oder die zuständigen Behörden weiterleiten können sollten.

(41) Die Mitgliedstaaten sollten über angemessene technische und organisatorische Kapazitäten verfügen, um Sicherheitsvorfälle und Risiken zu verhüten und zu erkennen, darauf zu reagieren und um ihre Auswirkungen abzuschwächen. Die Mitgliedstaaten sollten daher ein oder mehrere CSIRTs gemäß dieser Richtlinie benennen und sicherstellen, dass sie über angemessene Ressourcen und technische Kapazitäten verfügen. Die CSIRTs sollten die Anforderungen im Sinne dieser Richtlinie erfüllen, damit wirksame und kompatible Kapazitäten zur Bewältigung von Sicherheitsvorfällen und Risiken und eine effiziente Zusammenarbeit auf Unionsebene gewährleistet sind. Die Mitgliedstaaten sollten auch bestehende Computer-Notfallteams (CERTs) als CSIRTs benennen können. Um das Vertrauensverhältnis zwischen den Einrichtungen und den CSIRTs zu stärken, sollten die Mitgliedstaaten in Fällen, in denen ein CSIRT Teil einer zuständigen Behörde ist, eine funktionale Trennung zwischen den operativen Aufgaben der CSIRTs, insbesondere in Bezug auf den Informationsaustausch und die den Einrichtungen gewährten Unterstützung, und den Aufsichtstätigkeiten der zuständigen Behörden in Erwägung ziehen können.

(42) Die CSIRTs sind mit der Bewältigung von Sicherheitsvorfällen betraut. Das umfasst die Verarbeitung großer Mengen in einigen Fällen sensibler Daten. Die Mitgliedstaaten sollten dafür sorgen, dass die CSIRTs über eine Infrastruktur für den Informa-

tionsaustausch und die Verarbeitung von Informationen sowie über gut ausgestattetes Personal verfügen, womit die Vertraulichkeit und Vertrauenswürdigkeit ihrer Tätigkeiten gewährleistet wird. Die CSIRTs könnten in diesem Zusammenhang auch Verhaltenskodizes annehmen.

(43) In Bezug auf personenbezogene Daten sollten die CSIRTs in der Lage sein, im Einklang mit der Verordnung (EU) 2016/679 im Namen und auf Ersuchen einer wesentlichen oder wichtigen Einrichtung eine proaktive Überprüfung der für die Bereitstellung der Dienste der Einrichtungen verwendeten Netz- und Informationssysteme auf Schwachstellen vorzunehmen. Die Mitgliedstaaten sollten gegebenenfalls für alle sektorbezogenen CSIRTs ein vergleichbares Niveau an technischen Kapazitäten anstreben. Die Mitgliedstaaten sollten die ENISA um Unterstützung bei der Einsetzung ihrer CSIRTs ersuchen können.

(44) Die CSIRTs sollten in der Lage sein, auf Ersuchen einer wesentlichen oder wichtigen Einrichtung die mit dem Internet verbundenen Anlagen innerhalb und außerhalb der Geschäftsräume zu überwachen, um das organisatorische Gesamtrisiko der Einrichtung für neu ermittelte Sicherheitslücken in der Lieferkette oder kritische Schwachstellen zu ermitteln, zu verstehen und zu verwalten. Die Einrichtung sollte dazu angehalten werden, dem CSIRT mitzuteilen, ob es eine privilegierte Verwaltungsschnittstelle betreibt, da dies die Geschwindigkeit der Durchführung von Abhilfemaßnahmen beeinträchtigen könnte.

(45) Wegen der Bedeutung der internationalen Zusammenarbeit im Bereich Cybersicherheit sollten die CSIRTs sich zusätzlich zum durch die vorliegende Richtlinie geschaffenen CSIRTs-Netzwerk an internationalen Kooperationsnetzen beteiligen können. Zur Erfüllung ihrer Aufgaben sollten die CSIRTs und die zuständigen Behörden daher in der Lage sein, Informationen, einschließlich personenbezogener Daten, mit nationalen Computer-Notfallteams oder zuständigen Behörden von Drittländern auszutauschen, sofern die Bedingungen des Datenschutzrechts der Union für die Übermittlung personenbezogener Daten an Drittländer, unter anderem gemäß Artikel 49 der Verordnung (EU) 2016/679, erfüllt sind.

(46) Es ist von wesentlicher Bedeutung, dass angemessene Ressourcen bereitgestellt werden, um die Ziele dieser Richtlinie zu erreichen und es den zuständigen Behörden und den CSIRTs zu ermöglichen, die dort festgelegten Aufgaben zu erfüllen. Die Mitgliedstaaten können auf nationaler Ebene einen Finanzierungsmechanismus zur Deckung der Ausgaben einführen, die im Zusammenhang mit der Wahrnehmung der Aufgaben der in dem Mitgliedstaat gemäß dieser Richtlinie für Cybersicherheit zuständigen öffentlichen Einrichtungen erforderlich sind. Ein solcher Mechanismus sollte im Einklang mit dem Unionsrecht stehen, verhältnismäßig und diskriminierungsfrei sein und den unterschiedlichen Ansätzen für die Bereitstellung sicherer Dienste Rechnung tragen.

(47) Das CSIRTs-Netzwerk sollte weiterhin zur Stärkung des Vertrauens beitragen und eine rasche und wirksame operative Zusammenarbeit zwischen den Mitgliedstaaten fördern. Um die operative Zusammenarbeit auf Unionsebene zu verbessern, sollte das CSIRTs-Netzwerk in Erwägung ziehen, mit Cybersicherheitspolitik befasste Einrichtungen und Agenturen der Union, etwa Europol, zur Teilnahme an seiner Arbeit einzuladen.

(48) Um ein hohes Cybersicherheitsniveau zu erreichen und aufrechtzuerhalten, sollten die gemäß dieser Richtlinie erforderlichen nationalen Cybersicherheitsstrategien aus kohärenten Rahmen bestehen, in denen strategische Ziele und Prioritäten im Bereich

der Cybersicherheit und die zu ihrer Verwirklichung erforderliche Governance festgelegt werden. Diese Strategien können aus einem oder mehreren legislativen oder nichtlegislativen Instrumenten bestehen.

(49) Maßnahmen für die Cyberhygiene bilden die Grundlage für den Schutz von Netz- und Informationssysteminfrastrukturen, Hardware, Software und Online-Anwendungssicherheit sowie von Geschäfts- oder Endnutzerdaten, derer sich Einrichtungen bedienen. Maßnahmen für die Cyberhygiene, die eine Reihe von grundlegenden Verfahren umfassen, wie z. B. Software- und Hardware-Updates, Passwortänderungen, die Verwaltung neuer Installationen, die Einschränkung von Zugriffskonten auf Administratorenebene und die Sicherung von Daten, ermöglichen einen proaktiven Rahmen für die Bereitschaft und die allgemeine Sicherheit im Falle von Sicherheitsvorfällen oder Cyberbedrohungen. Die ENISA sollte die Cyberhygienemaßnahmen der Mitgliedstaaten überwachen und analysieren.

(50) Sensibilisierung für Cybersicherheit und Cyberhygiene sind von entscheidender Bedeutung, um das Cybersicherheitsniveau in der Union zu erhöhen, insbesondere angesichts der wachsenden Zahl vernetzter Geräte, die zunehmend bei Cyberangriffen eingesetzt werden. Es sollten Anstrengungen unternommen werden, um das allgemeine Bewusstsein für die Risiken im Zusammenhang mit derartigen Produkten zu schärfen, wobei Bewertungen auf Unionsebene dazu beitragen könnten, für ein gemeinsames Verständnis dieser Risiken im Binnenmarkt zu sorgen.

(51) Die Mitgliedstaaten sollten den Einsatz innovativer Technologien, einschließlich künstlicher Intelligenz, fördern, deren Einsatz die Aufdeckung und Verhütung von Cyberangriffen verbessern könnte, sodass Ressourcen wirksamer gegen Cyberangriffe genutzt werden können. Die Mitgliedstaaten sollten daher im Rahmen ihrer nationalen Cybersicherheitsstrategie Tätigkeiten im Bereich Forschung und Entwicklung fördern, um die Nutzung derartiger Technologien, insbesondere solcher, die sich auf automatisierte oder halbautomatisierte Instrumente für die Cybersicherheit beziehen, und gegebenenfalls den Austausch von Daten zu erleichtern, die für die Schulung und Verbesserung dieser Technologien erforderlich sind. Der Einsatz innovativer Technologien, einschließlich künstlicher Intelligenz, sollte in Einklang mit dem Datenschutzrecht der Union stehen, einschließlich der Datenschutzgrundsätze der Datengenauigkeit, Datenminimierung, Fairness und Transparenz sowie Datensicherheit, wie z. B. modernste Verschlüsselung. Die in der Verordnung (EU) 2016/679 festgelegten Anforderungen des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen sollten voll ausgeschöpft werden.

(52) Open-Source-Cybersicherheitswerkzeuge und -Anwendungen können zu einem höheren Maß an Offenheit beitragen und sich positiv auf die Effizienz industrieller Innovationen auswirken. Offene Standards erleichtern die Interoperabilität zwischen Sicherheitstools, was der Sicherheit der Interessenträger aus der Industrie zugutekommt. Open-Source-Cybersicherheitswerkzeuge und -anwendungen können die breitere Entwicklergemeinschaft nutzen und damit eine Diversifizierung der Anbieter ermöglichen. Open-Source kann zu einem transparenteren Verfahren für die Überprüfung von Werkzeugen für die Cybersicherheit und zu einem von der Gemeinschaft gesteuerten Prozess der Aufdeckung von Schwachstellen führen. Die Mitgliedstaaten sollten daher den Einsatz von Open-Source-Software und offenen Standards fördern können, indem sie Maßnahmen zur Nutzung offener Daten und Open-Source als Teil der Sicherheit durch Transparenz verfolgen. Maßnahmen zur Förderung der Einführung und nachhaltigen Nutzung von Open-Source-Cybersicherheitswerkzeugen sind besonders für kleine und mittlere Unternehmen wichtig, bei denen erhebliche Imple-

mentierungskosten anfallen, die durch die Reduzierung des Bedarfs an spezifischen Anwendungen oder Werkzeugen minimiert werden könnten.

(53) Versorgungsunternehmen sind zunehmend an digitale Netze in Städten angeschlossen, um die städtischen Verkehrsnetze zu verbessern, die Wasserversorgungs- und Abfallentsorgungseinrichtungen zu verbessern und die Effizienz der Beleuchtung und der Beheizung von Gebäuden zu erhöhen. Diese digitalisierten Versorgungsunternehmen sind anfällig für Cyberangriffe und es besteht aufgrund ihrer Vernetzung die Gefahr, dass den Bürgern im Falle eines erfolgreichen Cyberangriffs schwerwiegend geschadet wird. Die Mitgliedstaaten sollten im Rahmen ihrer nationalen Cybersicherheitsstrategie eine Strategie entwickeln, die sich mit der Entwicklung solcher vernetzten oder intelligenten Städte und deren potenziellen Auswirkungen auf die Gesellschaft befasst.

(54) In den letzten Jahren war die Union mit einem exponentiellen Anstieg von Ransomware-Angriffen konfrontiert, bei denen Daten und Systeme durch Malware verschlüsselt werden und eine Lösegeldzahlung für die Freigabe verlangt wird. Die zunehmende Häufigkeit und Schwere von Ransomware-Angriffen kann auf verschiedene Faktoren zurückgeführt werden, wie z. B. unterschiedliche Angriffsmuster, kriminelle Geschäftsmodelle im Zusammenhang mit „Ransomware als Dienst“ und Kryptowährungen, die Forderung nach Lösegeld und die Zunahme von Angriffen auf die Lieferkette. Die Mitgliedstaaten sollten eine Strategie zum Vorgehen gegen die zunehmende Häufigkeit von Ransomware-Angriffen als Teil ihrer nationalen Cybersicherheitsstrategie ergreifen.

(55) Öffentlich-private Partnerschaften (ÖPP) im Bereich der Cybersicherheit können einen angemessenen Rahmen für den Wissensaustausch, die Weitergabe von bewährten Verfahren und die Schaffung einer gemeinsamen Verständnisebene zwischen den Beteiligten bieten. Die Mitgliedstaaten sollten Maßnahmen fördern, die die Einrichtung von cybersicherheitsspezifischen ÖPP unterstützen. Diese Maßnahmen sollten unter anderem den Anwendungsbereich und die beteiligten Akteure, das Verwaltungsmodell, die verfügbaren Finanzierungsoptionen und das Zusammenspiel der beteiligten Akteure in Bezug auf ÖPP präzisieren. ÖPP können das Fachwissen privatwirtschaftlicher Einrichtungen nutzen, um die zuständigen Behörden bei der Entwicklung modernster Dienste und Prozesse zu unterstützen, unter anderem in den Bereichen Informationsaustausch, Frühwarnungen, Übungen zu Cyberbedrohungen und -vorfällen, Krisenmanagement und Resilienzplanung.

(56) Die Mitgliedstaaten sollten in ihren nationalen Cybersicherheitsstrategien auf die besonderen Cybersicherheitsbedürfnisse von kleinen und mittleren Unternehmen eingehen. Kleine und mittlere Unternehmen stellen in der gesamten Union einen großen Prozentsatz des Industrie-/Geschäftsmarktes und haben damit zu kämpfen, sich an ein neues Geschäftsgebaren in einer stärker vernetzten Welt anzupassen und sich in der digitalen Umgebung zurechtzufinden, in der Mitarbeiter von zu Hause aus arbeiten und Geschäfte zunehmend online getätigt werden. Einige kleine und mittlere Unternehmen stehen vor besonderen Herausforderungen im Bereich der Cybersicherheit, wie z. B. geringes Cyberbewusstsein, fehlende IT-Sicherheit aus der Ferne, hohe Kosten für Cybersicherheitslösungen und ein erhöhtes Maß an Bedrohungen, wie z. B. Ransomware, für die sie Anleitung und Unterstützung erhalten sollten. Kleine und mittlere Unternehmen werden aufgrund ihrer weniger strengen Risikomanagementmaßnahmen im Bereich der Cybersicherheit und ihres geringer ausgeprägten Angriffsmanagements sowie der Tatsache, dass sie über eingeschränkte Sicherheitsressourcen verfügen, zunehmend zum Ziel von Angriffen auf die Lieferkette. Diese

Angriffe auf die Lieferkette wirken sich nicht nur auf kleine und mittlere Unternehmen und deren eigene Geschäftstätigkeit aus, sondern können im Rahmen größerer Angriffe auch eine Kaskadenwirkung auf die von ihnen belieferten Einrichtungen haben. Die Mitgliedstaaten sollten mittels ihrer nationalen Cybersicherheitsstrategien kleine und mittlere Unternehmen dabei unterstützen, die Herausforderungen in ihren Lieferketten zu bewältigen. Die Mitgliedstaaten sollten über eine Kontaktstelle für kleine und mittlere Unternehmen auf nationaler oder regionaler Ebene verfügen, die kleinen und mittleren Unternehmen entweder Leitlinien und Unterstützung bietet oder sie an die geeigneten Stellen für Leitlinien und Unterstützung in Fragen im Zusammenhang mit der Cybersicherheit weiterleitet. Die Mitgliedstaaten werden außerdem angehalten, auch Kleinstunternehmen und kleinen Unternehmen, die nicht über diese Fähigkeiten verfügen, Dienste wie die Konfiguration von Websites und die Aktivierung der Protokollierung anzubieten.

(57) Im Rahmen ihrer nationalen Cybersicherheitsstrategien sollten die Mitgliedstaaten Maßnahmen zur Förderung eines aktiven Cyberschutzes ergreifen. Anstatt nur zu reagieren, besteht aktiver Cyberschutz in der aktiven Verhütung, Erkennung, Überwachung, Analyse und Abschwächung von Sicherheitsverletzungen im Netzwerk, kombiniert mit der Nutzung von Kapazitäten, die innerhalb und außerhalb des Opfernetzwerks eingesetzt werden. Dies könnte auch die Bereitstellung kostenfreier Dienste oder Instrumente für bestimmte Einrichtungen, einschließlich Selbstbedienungskontrollen (self-service checks), Detektionswerkzeugen und Bereinigungsdiensten, durch die Mitgliedstaaten einschließen. Die Fähigkeit, Bedrohungsinformationen und -analysen, Warnungen zu Cyberaktivitäten und Reaktionsmaßnahmen schnell und automatisch auszutauschen und zu verstehen, ist entscheidend, um eine einheitliche Vorgehensweise bei der erfolgreichen Verhütung, Erkennung, Bekämpfung und Blockierung von Angriffen gegen Netz- und Informationssysteme zu ermöglichen. Der aktive Cyberschutz beruht auf einer defensiven Strategie, die offensive Maßnahmen ausschließt.

(58) Da durch die Ausnutzung von Schwachstellen in Netz- und Informationssystemen erhebliche Störungen und Schäden verursacht werden können, ist die rasche Erkennung und Behebung dieser Schwachstellen ein wichtiger Faktor bei der Verringerung des Risikos. Einrichtungen, die Netz- und Informationssysteme entwickeln oder verwalten, sollten daher geeignete Verfahren für die Behandlung von entdeckten Schwachstellen festlegen. Da Schwachstellen häufig von Dritten oder meldenden Einrichtungen entdeckt und offengelegt werden, sollte der Hersteller oder Anbieter von IKT-Produkten oder -Diensten auch Verfahren einführen, damit er von Dritten Informationen über Schwachstellen entgegennehmen kann. Diesbezüglich enthalten die internationalen Normen ISO/IEC 30111 und ISO/IEC 29147 Leitlinien für die Behandlung von Schwachstellen und die Offenlegung von Schwachstellen. Eine stärkere Koordinierung zwischen meldenden natürlichen und juristischen Personen und Herstellern oder Anbietern von IKT-Produkten oder -Diensten ist besonders wichtig, um den freiwilligen Rahmen für die Offenlegung von Schwachstellen attraktiver zu machen. Die koordinierte Offenlegung von Schwachstellen erfolgt in einem strukturierten Prozess, in dem dem Hersteller oder Anbieter der potenziell gefährdeten IKT-Produkte oder -Dienste Schwachstellen in einer Weise gemeldet werden, die ihm die Diagnose und Behebung der Schwachstelle ermöglicht, bevor detaillierte Informationen über die Schwachstelle an Dritte oder die Öffentlichkeit weitergegeben werden. Die koordinierte Offenlegung von Schwachstellen sollte auch die Koordinierung zwischen der meldenden natürlichen oder juristischen Person und dem Herstel-

ler oder Anbieter der potenziell gefährdeten IKT-Produkte oder -Dienste in Bezug auf den Zeitplan für die Behebung und Veröffentlichung von Schwachstellen umfassen.

(59) Die Kommission, die ENISA und die Mitgliedstaaten sollten die Anpassung an internationale Normen und vorliegende bewährte Verfahren der Branche beim Risikomanagement im Bereich der Cybersicherheit weiterhin fördern, beispielsweise in den Bereichen Bewertungen der Sicherheit der Lieferkette, Informationsaustausch und Offenlegung von Schwachstellen.

(60) Die Mitgliedstaaten sollten in Zusammenarbeit mit der ENISA Maßnahmen ergreifen, um eine koordinierte Offenlegung von Schwachstellen zu erleichtern, indem sie eine einschlägige nationale Strategie festlegen. Die Mitgliedstaaten sollten im Rahmen ihrer nationalen Strategien im Einklang mit den nationalen Rechtsvorschriften so weit wie möglich die Herausforderungen angehen, mit denen Forscher, die sich mit Schwachstellen befassen, konfrontiert sind, wozu auch deren potenzielle strafrechtliche Haftung gehört. Da natürliche und juristische Personen, die Schwachstellen erforschen, in einigen Mitgliedstaaten der strafrechtlichen und zivilrechtlichen Haftung unterliegen könnten, werden die Mitgliedstaaten aufgefordert, Leitlinien für die Nichtverfolgung von Forschern im Bereich der Informationssicherheit zu verabschieden und eine Ausnahme von der zivilrechtlichen Haftung für ihre Tätigkeiten zu erlassen.

(61) Die Mitgliedstaaten sollten eines ihrer CSIRTs als Koordinator benennen, der gegebenenfalls als vertrauenswürdiger Vermittler zwischen den meldenden natürlichen oder juristischen Personen und den Herstellern oder Anbietern von IKT-Produkten oder -Diensten, die wahrscheinlich von der Schwachstelle betroffen sind, fungiert. Zu den Aufgaben des als Koordinator benannten CSIRT sollte insbesondere gehören, betreffende Einrichtungen zu ermitteln und zu kontaktieren, die natürlichen oder juristischen Personen, die eine Schwachstelle melden, zu unterstützen, Zeitpläne für die Offenlegung auszuhandeln und das Vorgehen bei Schwachstellen zu koordinieren, die mehrere Einrichtungen betreffen (koordinierte Offenlegung von Schwachstellen, die mehrere Parteien betreffen). Könnte die gemeldete Schwachstelle in mehr als einem Mitgliedstaat erhebliche Auswirkungen auf Einrichtungen haben, sollten die als Koordinator benannten CSIRTs gegebenenfalls im Rahmen des CSIRTs-Netzwerks zusammenarbeiten.

(62) Der rechtzeitige Zugang zu korrekten Informationen über Schwachstellen, die IKT-Produkte und -Dienste beeinträchtigen, trägt zu einem besseren Cybersicherheitsrisikomanagement bei. Öffentlich zugängliche Informationen über Schwachstellen sind nicht nur für die Einrichtungen und die Nutzer ihrer Dienste, sondern auch für die zuständigen Behörden und die CSIRTs ein wichtiges Instrument. Aus diesem Grund sollte die ENISA eine europäische Schwachstellendatenbank einrichten, in der Einrichtungen, unabhängig davon, ob sie in den Anwendungsbereich dieser Richtlinie fallen, und deren Anbieter von Netz- und Informationssystemen sowie die zuständigen Behörden und CSIRTs auf freiwilliger Basis öffentlich bekannte Schwachstellen offenlegen und registrieren können, die es den Nutzern ermöglichen, geeignete Abhilfemaßnahmen zu ergreifen. Das Ziel dieser Datenbank besteht darin, die einzigartigen Herausforderungen zu bewältigen, die sich aus den Risiken für Einrichtungen der Union ergeben. Darüber hinaus sollte die ENISA ein geeignetes Verfahren für den Veröffentlichungsprozess einführen, um den Einrichtungen Zeit zu geben, Maßnahmen zur Behebung ihrer Schwachstellen zu ergreifen und moderne Risikomanagementmaßnahmen im Bereich der Cybersicherheit sowie maschinenlesbare Datensätze und entsprechende Schnittstellen einzusetzen. Zur Förderung einer

Kultur der Offenlegung von Schwachstellen sollte eine Offenlegung ohne nachteilige Folgen für die meldende natürliche oder juristische Person erfolgen.

(63) Es gibt zwar bereits ähnliche Register oder Datenbanken für Schwachstellen, aber diese werden von Einrichtungen betrieben und gepflegt, die nicht in der Union niedergelassen sind. Eine von der ENISA gepflegte europäische Schwachstellendatenbank würde für mehr Transparenz in Bezug auf den Prozess der Veröffentlichung vor der öffentlichen Offenlegung der Schwachstelle sorgen und die Resilienz im Falle von einer Störung oder Unterbrechung bei der Erbringung ähnlicher Dienste verbessern. Um Doppelarbeit so weit wie möglich zu vermeiden und im Interesse der größtmöglichen Komplementarität, sollte die ENISA die Möglichkeit prüfen, Vereinbarungen über eine strukturierte Zusammenarbeit mit ähnlichen Registern oder Datenbanken zu schließen, die unter die Gerichtsbarkeit von Drittländern fallen. Insbesondere sollte die ENISA die Möglichkeit einer engen Zusammenarbeit mit den Betreibern des Systems für bekannte Schwachstellen und Anfälligkeiten (CVE) prüfen.

(64) Die Kooperationsgruppe sollte die strategische Zusammenarbeit und den Informationsaustausch unterstützen und erleichtern und das Vertrauen zwischen den Mitgliedstaaten stärken. Die Kooperationsgruppe sollte alle zwei Jahre ein Arbeitsprogramm aufstellen. In dem Arbeitsprogramm sollten die Maßnahmen aufgeführt sein, die die Kooperationsgruppe zur Umsetzung ihrer Ziele und Aufgaben zu ergreifen hat. Der Zeitrahmen für die Aufstellung des Arbeitsprogramms gemäß der vorliegenden Richtlinie sollte an den Zeitrahmen des letzten gemäß der Richtlinie (EU) 2016/1148 aufgestellten Arbeitsprogramms angepasst werden, um etwaige Unterbrechungen der Arbeit der Kooperationsgruppe zu vermeiden.

(65) Bei der Ausarbeitung von Leitfäden sollte die Kooperationsgruppe konsequent nationale Lösungen und Erfahrungen erfassen, die Auswirkungen ihrer Vorgaben auf nationale Ansätze bewerten, Herausforderungen bei der Umsetzung erörtern und spezifische Empfehlungen für eine bessere Umsetzung bestehender Vorschriften formulieren, insbesondere hinsichtlich der Erleichterung der Angleichung bei der Umsetzung dieser Richtlinie zwischen den Mitgliedstaaten. Die Kooperationsgruppe könnte auch eine Bestandsaufnahme der nationalen Lösungen vornehmen, um die Kompatibilität von Cybersicherheitslösungen zu fördern, die für jeden einzelnen Sektor in der gesamten Union angewandt werden. Dies gilt insbesondere für Sektoren mit internationalem oder grenzüberschreitendem Charakter.

(66) Die Kooperationsgruppe sollte ein flexibles Forum bleiben und in der Lage sein, unter Berücksichtigung der verfügbaren Ressourcen auf sich ändernde und neue politische Prioritäten und Herausforderungen zu reagieren. Sie könnte regelmäßige gemeinsame Sitzungen mit einschlägigen privaten Interessenträgern aus der gesamten Union organisieren, um die Tätigkeiten der Kooperationsgruppe zu erörtern und Daten und Beiträge zu neuen politischen Herausforderungen einzuholen. Darüber hinaus sollte die Kooperationsgruppe regelmäßig den aktuellen Stand in Bezug auf Cyberbedrohungen oder -vorfälle wie Ransomware bewerten. Um die Zusammenarbeit auf Unionsebene zu verbessern, sollte die Kooperationsgruppe in Erwägung ziehen, mit Cybersicherheitspolitik befasste einschlägige Organe, Einrichtungen und Agenturen der Union, etwa das Europäische Parlament, Europol, den Europäischen Datenschutzausschuss, die Agentur der Europäischen Union für Flugsicherheit, die mit der Verordnung (EU) 2018/1139 eingerichtet wurde, und die Agentur der Europäischen Union für das Weltraumprogramm, die mit der Verordnung (EU) 2021/696 des Europäischen Parlaments und des Rates([14]) eingeführt wurde, zur Teilnahme an ihrer Arbeit einzuladen.

(67) Die zuständigen Behörden und die CSIRTs sollten die Möglichkeit haben, innerhalb eines spezifischen Rahmens und gegebenenfalls vorbehaltlich der erforderlichen Sicherheitsüberprüfung der an solchen Austauschprogrammen teilnehmenden Beamten an Austauschprogrammen für Bedienstete aus anderen Mitgliedstaaten teilzunehmen, um die Zusammenarbeit zu verbessern und das Vertrauen unter den Mitgliedstaaten zu stärken. Die zuständigen Behörden sollten Maßnahmen ergreifen, damit die Bediensteten aus anderen Mitgliedstaaten bei den Tätigkeiten der aufnehmenden zuständigen Behörde oder des aufnehmenden CSIRT konstruktiv mitwirken können.

(68) Die Mitgliedstaaten sollten über die bestehenden Kooperationsnetzwerke – insbesondere dem Europäischen Netzwerk der Verbindungsorganisationen für Cyberkrisen (EU-CyCLONe), das CSIRTs-Netzwerk und die Kooperationsgruppe – zur Schaffung des EU-Rahmens für die Reaktion auf Cybersicherheitskrisen gemäß der Empfehlung (EU) 2017/1584 der Kommission([15]) beitragen. EU-CyCLONe und das CSIRTs-Netzwerk sollten auf der Grundlage von verfahrenstechnischen Vereinbarungen zusammenarbeiten, in denen die Einzelheiten dieser Zusammenarbeit festgelegt werden, und jegliche Doppelarbeit vermeiden. In der Geschäftsordnung von EU-CyCLONe sollten die Regelungen für das Funktionieren des Netzwerks genauer festgelegt werden, einschließlich der Funktion und Aufgaben des Netzwerks, Formen der Zusammenarbeit, Interaktionen mit anderen relevanten Akteuren und Vorlagen für den Informationsaustausch sowie Kommunikationsmittel. Für das Krisenmanagement auf Unionsebene sollten sich die relevanten Parteien auf die Integrierte Regelung für die politische Reaktion auf Krisen gemäß dem Durchführungsbeschluss (EU) 2018/1993 des Rates([16]) (IPCR-Regelung) stützen. Die Kommission sollte zu diesem Zweck auf den sektorübergreifenden Krisenkoordinierungsprozess auf hoher Ebene, ARGUS, zurückgreifen. Berührt die Krise eine wichtige externe Dimension oder eine Dimension der Gemeinsamen Sicherheits- und Verteidigungspolitik, so sollte der Krisenreaktionsmechanismus des Europäischen Auswärtigen Dienstes ausgelöst werden.

(69) Im Einklang mit dem Anhang der Empfehlung (EU) 2017/1584 sollte der Begriff „Cybersicherheitsvorfall großen Ausmaßes“ einen Sicherheitsvorfall bezeichnen, der der eine Störung verursacht, deren Ausmaß die Reaktionsfähigkeit eines Mitgliedstaats übersteigt oder der beträchtliche Auswirkungen auf mindestens zwei Mitgliedstaaten hat. Je nach Ursache und Auswirkung können sich Cybersicherheitsvorfälle großen Ausmaßes verschärfen und zu echten Krisen entwickeln, die das reibungslose Funktionieren des Binnenmarkts verhindern oder ernsthafte, die öffentliche Sicherheit betreffende Risiken für Einrichtungen und Bürger in mehreren Mitgliedstaaten oder in der gesamten Union darstellen. Angesichts der großen Tragweite und des, in den meisten Fällen, grenzübergreifenden Charakters solcher Sicherheitsvorfälle sollten die Mitgliedstaaten und die einschlägigen Organe, Einrichtungen und sonstigen Stellen der Union auf technischer, operativer und politischer Ebene zusammenarbeiten, um die Reaktion unionsweit angemessen zu koordinieren.

(70) Cybersicherheitsvorfälle großen Ausmaßes und Krisen auf Unionsebene erfordern aufgrund der starken Interdependenz zwischen Sektoren und Mitgliedstaaten ein koordiniertes Vorgehen, um eine schnelle und wirksame Reaktion zu gewährleisten. Die Verfügbarkeit von gegen Cyberangriffe widerstandsfähigen Netz- und Informationssystemen sowie die Verfügbarkeit, Vertraulichkeit und Integrität von Daten sind von entscheidender Bedeutung für die Sicherheit der Union und den Schutz ihrer Bürger, Unternehmen und Institutionen vor Sicherheitsvorfällen und Cyberbedrohungen sowie für die Stärkung des Vertrauens von Einzelpersonen und Organisationen in die

Fähigkeit der Union, einen globalen, offenen, freien, stabilen und sicheren Cyberraum zu fördern und zu schützen, der auf Menschenrechten, Grundfreiheiten, Demokratie und Rechtsstaatlichkeit beruht.

(71) Das EU-CyCLONe sollte im Fall von Cybersicherheitsvorfällen großen Ausmaßes und Krisen als Vermittler zwischen der technischen und politischen Ebene fungieren und die Zusammenarbeit auf operativer Ebene verbessern und die Entscheidungsfindung auf politischer Ebene unterstützen. In Zusammenarbeit mit der Kommission und unter Berücksichtigung der Zuständigkeiten der Kommission im Bereich des Krisenmanagements sollte das EU-CyCLONe auf den Erkenntnissen des CSIRTs-Netzwerks aufbauen und seine eigenen Fähigkeiten nutzen, um Folgenabschätzungen für Cybersicherheitsvorfälle großen Ausmaßes und Krisen zu erstellen.

(72) Cyberangriffe sind grenzüberschreitender Natur, und ein erheblicher Sicherheitsvorfall kann kritische Informationsinfrastrukturen, von denen das reibungslose Funktionieren des Binnenmarkts abhängt, stören und schädigen. In der Empfehlung (EU) 2017/1584 wird auf die Rolle aller relevanten Akteure eingegangen. Darüber hinaus ist die Kommission im Rahmen des durch den Beschluss Nr. 1313/2013/EU des Europäischen Parlaments und des Rates([17]) eingerichteten Katastrophenschutzverfahrens der Union für allgemeine Vorsorgemaßnahmen zuständig, einschließlich der Verwaltung des Zentrums für die Koordination von Notfallmaßnahmen und des Gemeinsamen Kommunikations- und Informationssystems für Notfälle, der Aufrechterhaltung und Weiterentwicklung der Fähigkeit zur Lageerfassung und -analyse sowie des Aufbaus und der Verwaltung der Fähigkeit zur Mobilisierung und Entsendung von Expertenteams im Falle eines Hilfeersuchens eines Mitgliedstaats oder eines Drittstaats. Die Kommission ist auch für die Erstellung von Analyseberichten für die IPCR-Regelung gemäß dem Durchführungsbeschluss (EU) 2018/1993 zuständig, unter anderem in Bezug auf die Lageerfassung und -vorsorge im Bereich der Cybersicherheit sowie für die Lageerfassung und Krisenreaktion in den Bereichen Landwirtschaft, widrige Witterungsbedingungen, Konfliktkartierung und -vorhersagen, Frühwarnsysteme für Naturkatastrophen, gesundheitliche Notlagen, Überwachung von Infektionskrankheiten, Pflanzengesundheit, chemische Zwischenfälle, Lebensmittel- und Futtermittelsicherheit, Tiergesundheit, Migration, Zoll, Notlagen im Bereich Kernenergie und Strahlenforschung, und Energie.

(73) Die Union kann gegebenenfalls internationale Übereinkünfte mit Drittländern oder internationalen Organisationen im Einklang mit Artikel 218 AEUV schließen, in denen deren Beteiligung an bestimmten Tätigkeiten der Kooperationsgruppe, dem CSIRTs-Netzwerk und EU-CyCLONe ermöglicht und geregelt wird. Solche Übereinkünfte sollten die Interessen der Union wahren und einen angemessenen Datenschutz gewährleisten. Das sollte nicht das Recht der Mitgliedstaaten ausschließen, mit Drittländern bei der Verwaltung von Schwachstellen und von Cybersicherheitsrisiken zusammenzuarbeiten und die Berichterstattung und den allgemeinen Informationsaustausch im Einklang mit dem Recht der Union zu erleichtern.

(74) Um die wirksame Umsetzung der Bestimmungen dieser Richtlinie, etwa zum Umgang mit Schwachstellen, zu Risikomanagementmaßnahmen im Bereich der Cybersicherheit, zu Berichtspflichten und zu Vereinbarungen über den Austausch cyberbezogener Informationen, zu fördern, können die Mitgliedstaaten mit Drittländern zusammenarbeiten und Tätigkeiten durchführen, die für diesen Zweck als angemessen erachtet werden, wozu auch der Informationsaustausch über Cyberbedrohungen, Vorfälle, Schwachstellen, Instrumente und Methoden, Taktiken, Techniken und Verfahren, die Vorsorge und Übungen im Hinblick auf das Krisenmanagement im Cyber-