Europäischer Wirtschafts- und Sozialausschuss

TEN/730
Cybersicherheit und Resilienz kritischer Einrichtungen

STELLUNGNAHME

Europäischer Wirtschafts- und Sozialausschuss

Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148 und **Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Resilienz kritischer Einrichtungen**

[COM(2020) 823 final – 2020/0359 (COD), COM(2020) 829 final – 2020/0365 (COD)]

Berichterstatter: **Maurizio MENSI**

Befassung	Europäisches Parlament, 21/01/2021 – 11/02/2021 Rat, 26/01/2021 – 19/02/2021
Rechtsgrundlage	Artikel 114 des Vertrags über die Arbeitsweise der Europäischen Union
Zuständige Fachgruppe	Fachgruppe Verkehr, Energie, Infrastrukturen, Informationsgesellschaft
Annahme in der Fachgruppe	14/04/2021
Verabschiedung auf der Plenartagung	27/04/2021
Plenartagung Nr.	560
Ergebnis der Abstimmung (Ja-Stimmen/Nein-Stimmen/Enthaltungen)	243/0/5

1. **Schlussfolgerungen und Empfehlungen**

1.1 Der Europäische Wirtschafts- und Sozialausschuss (EWSA) begrüßt die Bemühungen der Kommission, die Resilienz öffentlicher und privater Einrichtungen gegen Vorfälle, Cyberbedrohungen und physische Bedrohungen zu erhöhen. Er hält es auch für notwendig, die Industrie und die Innovationskapazitäten der EU auf integrative Weise und auf der Grundlage einer auf vier Säulen beruhenden Strategie zu stärken: Datenschutz, Grundrechte, Sicherheit und Cybersicherheit.

1.2 Der EWSA verweist jedoch darauf, dass angesichts der Relevanz und Sensibilität der mit den beiden Vorschlägen verfolgten Ziele eine Verordnung einer Richtlinie vorzuziehen gewesen wäre. Weshalb die Kommission eine solche Option nicht einmal in Erwägung gezogen hat, wird jedoch nicht erläutert.

1.3 Der EWSA stellt fest, dass sich einige Bestimmungen der beiden Richtlinienvorschläge überschneiden. Im ersten Vorschlag betreffen sie in erster Linie die Cybersicherheit und im zweiten die physische Sicherheit. Sie sind aber eng miteinander verbunden und komplementär. Deshalb fordert der EWSA, aus Gründen der funktionalen Vereinfachung und Straffung zu prüfen, ob die beiden Vorschläge nicht in einem Text zusammengefasst werden können.

1.4 Der EWSA begrüßt den Ansatz, die in der ursprünglichen NIS-Richtlinie vorgenommene Unterscheidung zwischen Betreibern wesentlicher Dienste und Anbietern digitaler Dienste aufzuheben. Gleichzeitig verweist er auf die Möglichkeit präziserer und klarerer Leitlinien für die Ermittlung der Einrichtungen, die in den Anwendungsbereich der Richtlinie fallen und an sie gebunden sind. Insbesondere sollten die Kriterien für die Unterteilung in „wesentliche“ und „wichtige“ Einrichtungen sowie die zu erfüllenden Anforderungen genauer definiert werden, um zu vermeiden, dass infolge unterschiedlicher einzelstaatlicher Ansätze Hindernisse beim Wettbewerb und beim freien Waren- und Dienstleistungsverkehr entstehen, die die Unternehmen benachteiligen und den Handel beeinträchtigen können.

1.5 Nach Ansicht des EWSA ist es angesichts der zu erwarteten Komplexität des in den beiden Vorschlägen dargelegten Systems wichtig, dass die Kommission den Geltungsbereich der zwei miteinander verflochtenen Rechtsakte genau präzisiert, insbesondere für Bereiche, in denen unterschiedliche Bestimmungen denselben Sachverhalt bzw. dieselbe Einrichtung regeln.

1.6 Der EWSA verweist darauf, dass neben dem Abbau von Bürokratie und Fragmentierung durch die Vereinfachung von Prozessen, Sicherheitsanforderungen und Verpflichtungen zur Meldung von Vorfällen das unumstößliche Ziel einer jeden gesetzlichen Regelung in ihrer klaren Formulierung bestehen muss. Auch zu diesem Zweck könnte es sich als zweckmäßig erweisen, im Interesse der Bürger und Unternehmen die beiden Richtlinienvorschläge in einem Text zusammenzuführen, um eine komplizierte Auslegung und Anwendung zu vermeiden.

1.7 Der EWSA erkennt die im Richtlinienvorschlag hervorgehobene wesentliche Rolle der Leitungsorgane der „wesentlichen“ und „wichtigen“ Einrichtungen an. Deren Mitglieder müssen regelmäßig spezielle Schulungen absolvieren, um ausreichende Kenntnisse und Fähigkeiten für den Umgang mit den verschiedenen Cyberrisiken und für die Bewertung ihrer

Auswirkungen zu erwerben. In diesem Zusammenhang sollte im Richtlinienvorschlag der Mindestumfang solcher Kenntnisse und Fertigkeiten angegeben werden, um im Rahmen europäischer Leitlinien Vorgaben für geeignete Schulungskompetenzen zu geben und dadurch zu vermeiden, dass sich die Schulungen von Mitgliedstaat zu Mitgliedstaat inhaltlich unterscheiden.

1.8 Der EWSA stimmt zu, dass der Agentur der Europäischen Union für Cybersicherheit (ENISA) im gesamten institutionellen und operativen Rahmen der Cybersicherheit auf europäischer Ebene eine wichtige Rolle zukommt. Er vertritt in diesem Zusammenhang die Auffassung, dass diese Agentur neben ihrem zweijährlichen Bericht über den Stand der Cybersichereit in der Union auch regelmäßig aktuelle Informationen über die Cybersicherheitsvorfälle sowie sektorspezifische Bekanntmachungen im Internet veröffentlichen muss, um den von der NIS-2-Richtlinie betroffenen Akteuren mit diesem zusätzlichen nützlichen Instrument die Möglichkeit zu geben, ihre Unternehmen besser zu schützen.

1.9 Der EWSA stimmt dem Vorschlag zu, die ENISA mit der Einrichtung eines europäischen Schwachstellenregisters zu betrauen. Er ist der Auffassung, dass die Bereitstellung von Informationen über die wichtigsten Schwachstellen und Vorfälle nicht freiwillig, sondern verpflichtend gemacht werden muss, damit auch Auftraggeber der zahlreichen Vergabeverfahren auf europäischer Ebene von diesen Informationen profitieren können (auch für 5G-Produkte und -Technologien).

2. Allgemeine Bemerkungen

2.1 Am 16. Dezember 2020 wurden die neue Cybersicherheitsstrategie der EU vorgestellt und dazu zwei Legislativvorschläge vorgelegt: Die überarbeitete Richtlinie (EU) 2016/1148[1] über die Sicherheit von Netz- und Informationssystemen (NIS 2) und eine neue Richtlinie über die Resilienz kritischer Einrichtungen. Die Strategie – Schlüsselelement der Mitteilung „Gestaltung der digitalen Zukunft Europas“[2], des europäischen Aufbauplans und der EU-Strategie für eine Sicherheitsunion – zielt darauf ab, die kollektive Resilienz Europas gegen Cyberbedrohungen zu stärken und verlässliche und sichere Online-Dienste und -Instrumente für alle Bürger und Unternehmen zu gewährleisten.

2.2 Die auf EU-Ebene bestehenden Maßnahmen zum Schutz kritischer Dienste und Infrastrukturen vor Cybergefahren und physischen Bedrohungen müssen auf den neuesten Stand gebracht werden. Die mit der Cybersicherheit zusammenhängenden Risiken entwickeln sich mit der zunehmenden Digitalisierung und Konnektivität weiter. Deshalb ist es notwendig, den geltenden Rechtsrahmen im Sinne der EU-Sicherheitsstrategie zu überarbeiten und von der Dichotomie zwischen Online und Offline und einem Ansatz mit undurchlässigen Teilbereichen wegzukommen.

---

1 ABl. L 194 vom 19.7.2016, S. 1.

2 COM(2020) 67 final.

2.3 Die beiden Richtlinienvorschläge betreffen ein breites Spektrum von Sektoren und gehen auf jetzige und künftige Online- und Offline-Risiken im Zusammenhang mit Cyberangriffen, kriminellen Anschlägen, Naturkatastrophen und anderen Vorfällen ein. Dabei werden auch Lehren aus der jetzigen Pandemie gezogen. Diese hat die Anfälligkeit der zunehmend von digitalen Lösungen abhängigen Gesellschaft und Wirtschaft offenbart, die wachsenden und sich rasant weiterentwickelnden Cyberbedrohungen ausgesetzt sind. Betroffen sind hier insbesondere von sozialer Ausgrenzung bedrohte Gruppen, wie Menschen mit Behinderungen. Dies hat die EU veranlasst, eine Strategie zum Schutz eines globalen und offenen Cyberraums vorzuschlagen, der auf soliden Sicherheitsgarantien sowie technologischer Souveränität und Führung beruht. Dabei sollen operative Fähigkeiten ausgebaut werden, um im Rahmen einer stärkeren Zusammenarbeit potenzielle Gefahren zu verhindern, abzuwenden und darauf zu reagieren, wobei die Vorrechte der Mitgliedstaaten im Bereich der nationalen Sicherheit zu achten sind.

3. Vorschlag für eine Überarbeitung der Richtlinie über die Sicherheit von Netz- und Informationssystemen

3.1 Die Richtlinie über die Sicherheit von Netz- und Informationssystemen (NIS) (EU) 2016/1148 war das erste „horizontale“ Rechtsinstrument der EU im Bereich der Cybersicherheit und hatte zum Ziel, die Resilienz der Netz- und Informationssysteme der Union gegen Cyberrisiken zu verbessern. Ungeachtet der guten Ergebnisse stieß die NIS-Richtlinie auch an einige Grenzen, da mit dem zunehmenden digitalen Wandel der Gesellschaft, der durch die COVID-19-Krise noch an Tempo gewonnen hat, auch die Bedrohungen zugenommen haben. Dabei wurde die Anfälligkeit unserer Gesellschaften offenbart, die angesichts der erheblichen unvorhergesehenen Risiken immer stärker voneinander abhängen. Neue Herausforderungen sind zu Tage getreten, die angemessene und innovative Antworten erfordern. In einer breit angelegten Konsultation der Interessenträger wurde Folgendes ermittelt: unzureichendes Cybersicherheitsniveau in den europäischen Unternehmen, uneinheitliche nationale Anwendung der Vorschriften in den verschiedenen Sektoren und fehlende Kenntnis der wichtigsten Bedrohungen und Herausforderungen.

3.2 Der NIS-2-Vorschlag hängt eng mit zwei anderen Initiativen zusammen: Vorschlag für eine Verordnung über die Betriebsstabilität digitaler Systeme im Finanzsektor (Digital Operational Resilience Act, DORA) und Vorschlag für eine Richtlinie über kritische Einrichtungen (Resilienzrichtlinie), der den Anwendungsbereich der Richtlinie 2008/114/EG[3] über Energie und Verkehr auf weitere Sektoren wie beispielsweise das Gesundheitswesen sowie Einrichtungen ausweitet, die im Bereich Arzneimittelforschung und -entwicklung tätig sind. Der Schwerpunkt der Resilienzrichtlinie, deren sektoraler Geltungsbereich in Bezug auf die wesentlichen Einrichtungen jenem der NIS-2-Richtlinie entspricht (Anhang 1 der NIS-2-Richtlinie), verlagert sich vom Schutz wirtschaftlicher Güter auf die Resilienz der Einrichtungen, die diese verwalten, und geht von der Ermittlung kritischer europäischer Infrastrukturen mit grenzüberschreitender Dimension zur Ermittlung kritischer Infrastrukturen auf nationaler Ebene über. Darüber hinaus steht der NIS-2-Vorschlag in Kohärenz und Komplementarität zu anderen geltenden Rechtsinstrumenten, so zu dem europäischen Kodex für

3 ABl. L 345 vom 23.12.2008, S. 75.

elektronischen Kommunikation, zur Datenschutz-Grundverordnung und zur eIDAS-Verordnung über elektronische Identifizierung und Vertrauensdienste.

3.3 Mit dem Vorschlag für eine NIS-2-Richtlinie, der in den Rahmen des Programms zur Gewährleistung der Effizienz und Leistungsfähigkeit der Rechtsetzung (REFIT) fällt, sollen der Regelungsaufwand für die zuständigen Behörden verringert, die Befolgungskosten für öffentliche und private Einrichtungen gesenkt und der rechtliche Bezugsrahmen modernisiert werden. Darüber hinaus werden damit die Sicherheitsanforderungen an die Unternehmen gestärkt, die Frage der Sicherheit der Lieferketten angegangen, die Meldepflichten angeglichen, strengere Aufsichtsmaßnahmen für die nationalen Behörden eingeführt und eine Harmonisierung der Sanktionsregelungen in den Mitgliedstaaten angestrebt.

3.4 Außerdem trägt die NIS-2-Richtlinie dazu bei, den Informationsaustausch und die Zusammenarbeit beim Cyber-Krisenmanagement auf nationaler und europäischer Ebene zu verbessern. Die Unterscheidung zwischen Betreibern wesentlicher Dienste und Anbietern digitaler Dienste aus der NIS-Richtlinie wird aufgehoben. Der Anwendungsbereich erstreckt sich nunmehr auf mittlere bis große Unternehmen in Branchen, die auf der Grundlage ihrer Bedeutung für Wirtschaft und Gesellschaft ermittelt wurden. Solche öffentlichen bzw. privaten Einrichtungen werden in „wesentliche“ und „wichtige“ Einrichtungen unterteilt und unterliegen unterschiedlichen Aufsichtsregelungen. Die Mitgliedstaaten können jedoch gegebenenfalls auch kleinere Einrichtungen in Erwägung ziehen, die ein hohes Risikoprofil aufweisen.

3.5 Vorgesehen ist auch ein neues Netz von durch künstliche Intelligenz (KI) geleiteten unionsweiten Sicherheitseinsatzzentren, die als regelrechter Cybersicherheits-Schutzschild fungieren sollen. Diese Zentren sollen die Anzeichen eines Cyberangriffs so weit im Voraus erkennen, dass noch vor Schadenseintritt eingegriffen werden kann. Die Bedeutung der künstlichen Intelligenz für die Cybersicherheit wird auch im Bericht der National Security Commission on Artificial Intelligence der Vereinigten Staaten vom 1. März 2021 hervorgehoben. Folglich werden die Mitgliedstaaten und die Betreiber kritischer Infrastrukturen im Rahmen eines europäischen Sicherheitsnetzes einen direkten Zugang zu den Informationen über Bedrohungen („Threat Intelligence“) haben.

3.6 Darüber hinaus geht die Kommission auch auf das Problem der Sicherheit von Lieferketten und der Beziehungen mit Anbietern ein: Die Mitgliedstaaten können in Zusammenarbeit mit der Kommission und der ENISA koordinierte Risikobewertungen kritischer Lieferketten durchführen und sich dabei am bereits erfolgreichen Konzept für die 5G-Netze gemäß der einschlägigen Empfehlung vom 26. März 2019[4] orientieren.

3.7 Mit dem Vorschlag werden die für Unternehmen geltenden Sicherheitsmaßnahmen und Meldepflichten vereinheitlicht und gestrafft. Gleichzeitig wird ein gemeinsamer Ansatz für das Risikomanagement mit einem Mindestumfang durchzuführender grundlegender Sicherheitsmaßnahmen festgelegt. Es sind präzisere Bestimmungen zum Verfahren zur Meldung von Sicherheitsvorfällen, zum Inhalt der Beziehungen und zu den Fristen vorgesehen. In diesem Zusammenhang wird mit dem Vorschlag ein zweistufiger Ansatz festgelegt: Die

4 ABl. L 88 vom 29.3.2019, S. 42.

Unternehmen müssen innerhalb von 24 Stunden eine erste Meldung übermitteln und spätestens einen Monat danach einen Abschlussbericht vorlegen.

3.8 Die Mitgliedstaaten sollen die für das Krisenmanagement zuständigen nationalen Behörden benennen. Zu diesem Zweck wird auf spezifische Pläne und ein neues Netzwerk der Verbindungsorganisationen für Cyberkrisen (Cyber Crisis Liaison Organisation Network, EU-CyCLONe) verwiesen. Die Rolle der Kooperationsgruppe bei der strategischen Entscheidungsfindung wird gestärkt. Die in der EU ermittelten Schwachstellen sollen in ein von der ENISA verwaltetes Register aufgenommen werden. Darüber hinaus wird der Informationsaustausch und die Zusammenarbeit zwischen den Mitgliedstaaten intensiviert, darunter auch die operative Zusammenarbeit bei der Bewältigung von Cyberkrisen.

3.9 Es werden strengere Aufsichtsmaßnahmen für die nationalen Behörden und strengere Durchführungsanforderungen festgelegt. Außerdem wird eine Vereinheitlichung der Sanktionsregelungen in allen Mitgliedstaaten angestrebt.

3.10 In diesem Zusammenhang wird in dem Vorschlag überdies ein Mindestumfang von Verwaltungssanktionen bei Verstößen gegen die Verpflichtungen im Bereich des Cybersicherheitsrisikomanagements und die Meldepflichten festgelegt. Es werden Bestimmungen bezüglich der Zuständigkeiten von natürlichen Personen festgelegt, die in den von der Richtlinie abgedeckten Unternehmen eine repräsentative bzw. leitende Position haben. Die EU-Maßnahmen zur Vorbeugung und zum Management von Cybersicherheitsvorfällen und -krisen größeren Ausmaßes sowie zur Reaktion darauf werden im Rahmen des Vorschlags mit der Festlegung klarer Zuständigkeiten, einer angemessenen Planung und einer gestärkten Zusammenarbeit auf EU-Ebene verbessert.

3.11 Die Mitgliedstaaten werden in die Lage versetzt, gemeinsam über die Durchführung der EU-Vorschriften zu wachen. Sie können sich bei grenzüberschreitenden Problemen gegenseitig unterstützen, einen stärker strukturierten Dialog mit dem Privatsektor einleiten, die Offenlegung von Schwachstellen in auf dem Binnenmarkt verfügbaren Soft- und Hardwareprodukten koordinieren und die Risiken im Zusammenhang mit der Sicherheit und den Bedrohungen rund um die neuen Technologien koordiniert bewerten (wie bereits im Falle der 5G-Netze).

4. Vorschlag für eine Richtlinie zur Resilienz kritischer Einrichtungen

4.1 Die EU hat im Jahr 2006 das Europäische Programm zum Schutz der kritischen Infrastrukturen (EPSKI) aufgestellt und 2008 die Richtlinie über europäische kritische Infrastrukturen (EKI) für die Sektoren Energie und Verkehr verabschiedet. Sowohl in der von der Europäischen Kommission angenommenen EU-Strategie für eine Sicherheitsunion 2020–2025[5] als auch in der unlängst angenommenen Agenda zur Terrorismusbekämpfung wird hervorgehoben, wie wichtig es ist, die Resilienz kritischer Infrastrukturen gegen physische und digitale Risiken zu gewährleisten. Sowohl die 2019 durchgeführte Bewertung der Durchführung der EKI-Richtlinie als auch die Ergebnisse der Folgenabschätzung des vorgenannten Vorschlags haben jedoch ergeben, dass die geltenden europäischen und einzelstaatlichen Maßnahmen eine

5 COM(2020) 605 final.

angemessene Bewältigung der aktuellen Risiken durch die Betreiber nicht in ausreichendem Maße sicherstellen. Deshalb haben der Rat und das Europäische Parlament die Kommission wiederholt ermahnt, den jetzigen Ansatz zum Schutz der kritischen Infrastrukturen zu überarbeiten.

4.2 In der von der Kommission am 24. Juli 2020 angenommen EU-Strategie für eine Sicherheitsunion werden die zunehmenden Verflechtungen und gegenseitigen Abhängigkeiten zwischen physischen und digitalen Infrastrukturen anerkannt. Es wird betont, dass ein kohärenter und einheitlicher Ansatz zwischen der EKI-Richtlinie und der NIS-Richtlinie notwendig ist. In diesem Sinne wird der ursprünglich auf die Sektoren Energie und Verkehr begrenzte Anwendungsbereich der Richtlinie 2008/114/EG mit dem Vorschlag für eine Richtlinie zur Resilienz kritischer Einrichtungen (Resilienzrichtlinie), dessen Geltungsbereich der NIS-2-Richtlinie über wesentliche Einrichtungen entspricht, auf folgende Bereiche ausgeweitet: Bankwesen, Finanzmarktinfrastruktur, Gesundheitswesen, Trinkwasser, Abwasser, digitale Infrastruktur sowie öffentliche Verwaltung und Weltraum. Es werden klare Zuständigkeiten, eine angemessene Planung und eine umfassendere Zusammenarbeit festgelegt. In diesem Zusammenhang ist es notwendig, einen Bezugsrahmen für alle Risiken zu schaffen und die Mitgliedstaaten dabei zu unterstützen, die kritischen Einrichtungen in die Lage zu versetzen, Sicherheitsvorfälle zu vermeiden, ihnen standzuhalten und deren Folgen abzufedern, unabhängig davon, ob es sich um Risiken im Zusammenhang mit Naturgefahren, Vorfällen, Terrorismus, internen Bedrohungen oder – wie derzeit – um Notfallsituationen im Bereich der öffentlichen Gesundheit handelt.

4.3 Jeder Mitgliedstaat ist gehalten, eine nationale Strategie zur Gewährleistung der Resilienz kritischer Einrichtungen anzunehmen, regelmäßige Risikobewertungen durchzuführen und auf dieser Grundlage die kritischen Einrichtungen zu ermitteln. Die kritischen Einrichtungen wiederum müssen ebenfalls Risikobewertungen durchführen, angemessene technische und organisatorische Maßnahmen zur Stärkung der Resilienz ergreifen und die Vorfälle den nationalen Behörden melden. Einrichtungen, die für bzw. in mindestens ein(em) Drittel der Mitgliedstaaten Dienste erbringen, unterliegen einer spezifischen Überwachung. Diese umfasst spezielle, auf sie zugeschnittene Unterstützungsmaßnahmen der Kommission.

4.4 Der Vorschlag für die Resilienzrichtlinie sieht unterschiedliche Formen der Unterstützung von Mitgliedstaaten und kritischen Einrichtungen vor, enthält eine Übersicht der Risiken auf EU-Ebene, listet die besten Vorgehensweisen und Methoden auf und umfasst auch Vorschläge für Schulungsmaßnahmen und Maßnahmen zur Erprobung der Resilienz kritischer Einrichtungen. Das System der grenzüberschreitenden Zusammenarbeit umfasst auch eine Ad-hoc-Sachverständigengruppe, eine Gruppe für die Resilienz kritischer Einrichtungen, das Forum für die strategische Zusammenarbeit und den Informationsaustausch zwischen den Mitgliedstaaten.

5. Vorschläge zur Änderung des betreffenden Legislativvorschlags

5.1 Der EWSA begrüßt die Bemühungen der Kommission um eine Stärkung der Resilienz öffentlicher und privater Einrichtungen gegen Bedrohungen durch Cyberangriffe und physische Angriffe. Dies ist vor allem angesichts des raschen digitalen Wandels infolge des COVID-19-Ausbruchs besonders relevant. Er teilt auch die in der Mitteilung „Gestaltung der digitalen Zukunft Europas“ zum Ausdruck gebrachte Auffassung, dass Europa von den Vorteilen des digitalen Zeitalters profitieren und seine Wirtschaft (insbesondere die kleinen und mittleren Unternehmen) und seine Innovationskapazität in inklusiver Weise und auf der Grundlage einer auf vier Säulen beruhenden Strategie stärken muss: Datenschutz, Grundrechte, Sicherheit und Cybersicherheit sind die wesentlichen Voraussetzungen für eine Gesellschaft, die sich auf die Macht von Daten stützt.

5.2 Angesichts der Erkenntnisse aus der Folgenabschätzung und der Konsultation im Vorfeld des NIS-2-Vorschlags sowie des mehrfach hervorgehobenen Ziels, eine Fragmentierung der auf nationaler Ebene erlassenen Bestimmungen zu vermeiden (was auch in der Mitteilung vom 4. Oktober 2017 über die Umsetzung der NIS-Richtlinie[6] gefordert wurde), erschließt sich dem EWSA jedoch nicht, wieso die Kommission keine Verordnung, sondern eine Richtlinie vorgeschlagen hat. Eine solche Option wurde nicht einmal in Erwägung gezogen.

5.3 Der EWSA stellt fest, dass sich einige Bestimmungen der beiden Richtlinienvorschläge überschneiden. Im ersten Vorschlag betreffen sie in erster Linie die Cybersicherheit und im zweiten die physische Sicherheit. Sie sind aber eng miteinander verbunden und komplementär. Darüber hinaus decken die kritischen Einrichtungen im Sinne der Resilienzrichtlinie dieselben Sektoren ab wie die NIS-2-Richtlinie[7] und stimmen mit den darin genannten „wesentlichen“ Einrichtungen überein. Außerdem unterliegen alle kritischen Einrichtungen, die in den Anwendungsbereich der Resilienzrichtlinie fallen, den selben Verpflichtungen im Bereich der Cybersicherheit wie in der NIS-2-Richtlinie vorgesehen. Die beiden Vorschläge sehen auch eine Reihe von Überbrückungsklauseln vor, um die Verbindung zu gewährleisten: Bestimmungen über eine verstärkte Zusammenarbeit zwischen den Behörden, Informationsaustausch über Überwachungsmaßnahmen, Meldung von im Sinne der Resilienzrichtlinie kritischen Einrichtungen an die NIS-2-Behörden sowie regelmäßige Sitzungen der jeweiligen Kooperationsgruppen (mindestens einmal jährlich). Beide Vorschläge basieren außerdem auf derselben Rechtsgrundlage: Artikel 114 AEUV, in dem es um das Funktionieren des Binnenmarkts durch die Angleichung der Rechts- und Verwaltungsvorschriften geht. Dies entspricht u. a. auch der Auslegung durch den Gerichtshof in der Rechtssache C-58/08 Vodafone und andere. Deshalb fordert der EWSA, die Möglichkeit der Zusammenfassung der beiden Vorschläge in einem Text aus Gründen der funktionalen Vereinfachung und Straffung zu prüfen.

---

6 COM(2017) 476 final.

7 Anhang 1: ABl. L 194 vom 19.7.2016, S. 1.

5.4 Der EWSA begrüßt den Ansatz, die in der ursprünglichen NIS-Richtlinie vorgenommene Unterscheidung zwischen Betreibern wesentlicher Dienste und Anbietern digitaler Dienste aufzuheben. Gleichzeitig verweist er auf die Möglichkeit präziserer und klarerer Leitlinien für die Ermittlung der Einrichtungen, die in den Anwendungsbereich der Richtlinie fallen und an sie gebunden sind. Neben der Auflistung in den Anhängen I und II enthält NIS 2 eine Reihe von uneinheitlichen Kriterien, die schwierige qualitative und quantitative Bewertungen voraussetzen, deren Durchführung auf nationaler Ebene zudem unterschiedlich ablaufen kann. Dadurch kann es erneut zur Fragmentierung kommen, die mit dem vorgeschlagenen Rechtsakt eigentlich vermieden werden sollte. Es ist wichtig zu vermeiden, dass infolge unterschiedlicher einzelstaatlicher Ansätze Hindernisse beim Wettbewerb und beim freien Waren- und Dienstleistungsverkehr entstehen, die die Unternehmen benachteiligen und den Handel beeinträchtigen können.

5.5 Gemäß der NIS-2-Richtlinie gelten für kritische Betreiber in den Sektoren, die nach dem vorliegenden Vorschlag als „wesentlich“ eingestuft werden, allgemeine resilienzfördernde Verpflichtungen mit besonderem Schwerpunkt auf nicht cyberbezogenen Risiken im Sinne der Resilienzrichtlinie. In der Resilienzrichtlinie heißt es allerdings ausdrücklich, dass sie sich nicht auf Bereiche bezieht, die von der NIS-2-Richtlinie abgedeckt werden. So wird laut der Resilienzrichtlinie in der NIS-2-Richtlinie in ausreichendem Maße auf die Cybersicherheit eingegangen, weshalb die von NIS 2 abgedeckten Bereiche aus dem Anwendungsbereich der Resilienzrichtlinie ausgenommen werden sollen. Eine Ausnahme bilden hierbei die besonderen Bestimmungen für Einrichtungen auf dem Gebiet der digitalen Infrastrukturen. In der Resilienzrichtlinie heißt es weiter, dass Einrichtungen, die Teil des Sektors der digitalen Infrastrukturen sind, im Wesentlichen auf Netz- und Informationssystemen beruhen und in den Anwendungsbereich der NIS-2-Richtlinie fallen. Diese regelt auch die physische Sicherheit dieser Systeme als Teil ihrer Risikomanagement-Verpflichtungen in Bezug auf die Cybersicherheit und Meldung von Vorfällen. Gleichzeitig wird in der Resilienzrichtlinie explizit nicht ausgeschlossen, dass sich einige ihrer spezifischen Bestimmungen auch auf die Netz- und Informationssysteme beziehen können.

5.6 Vor diesem komplexen Hintergrund ist es nach Ansicht des EWSA unerlässlich, dass die Kommission den Geltungsbereich der zwei miteinander verflochtenen Rechtsakte genau präzisiert, insbesondere für Bereiche, in denen die jeweiligen Bestimmungen denselben Sachverhalt bzw. dieselbe Einrichtung regeln.

5.7 Neben dem Abbau von Bürokratie und Fragmentierung durch die Vereinfachung von Prozessen, Sicherheitsanforderungen und Verpflichtungen zur Meldung von Vorfällen muss das auf allen Ebenen geltende unumstößliche Ziel einer jeden gesetzlichen Regelung in ihrer klaren Formulierung bestehen. Dies gilt umso mehr, wenn sie Gegenstand solch umfangreicher und komplexer Texte wie der beiden vorliegenden Richtlinienvorschläge ist. Darüber hinaus gilt es sicherzustellen, dass es bei der Fülle an Stellen, die mit spezifischen Aufgaben betraut sind, nicht unmöglich wird, ihre jeweiligen Zuständigkeiten zu ermitteln. Dies würde die angestrebten Ziele untergraben. Auch zu diesem Zweck könnte es sich als zweckmäßig erweisen, im Interesse der Bürger und Unternehmen die beiden Richtlinienvorschläge in einem Text zusammenzuführen, um eine komplizierte Auslegung und Anwendung zu vermeiden.

5.8 In der NIS-2-Richtlinie wird an mehreren Stellen auf die Bestimmungen anderer Rechtsinstrumente verwiesen, wie z. B. auf die Richtlinie (EU) 2018/1972 über den europäischen Kodex für die elektronische Kommunikation, deren Anwendung sich nach dem Grundsatz der Spezialität richtet. Einige Bestimmungen der Richtlinie (EU) 2018/1972 werden ausdrücklich aufgehoben (Artikel 41 und 42), während andere im Einklang mit dem vorgenannten Grundsatz angewandt werden müssen, ohne dass darauf jedoch präziser eingegangen wird. In diesem Zusammenhang müssen nach Auffassung des EWSA jegliche Zweifel ausgeräumt werden, um Probleme bei der Auslegung zu vermeiden. Der EWSA unterstützt auch das Ziel der Kommission, das Sanktionssystem für Verstöße im Rahmen des Risikomanagements zwecks besseren Informationsaustauschs und einer besseren Zusammenarbeit auf EU-Ebene zu harmonisieren.

5.9 Der EWSA anerkennt die im Richtlinienvorschlag hervorgehobene wichtige Rolle der Lenkungsorgane der „wesentlichen“ und der „wichtigen“ Einrichtungen bei der Cybersicherheitsstrategie und beim Risikomanagement, die Risikomaßnahmen genehmigen, deren Umsetzung überwachen und auf Verstöße reagieren müssen. In diesem Zusammenhang ist vorgesehen, dass die Mitglieder dieser Einrichtungen regelmäßig spezielle Schulungen absolvieren müssen, um ausreichende Kenntnisse und Fähigkeiten für den Umgang mit den verschiedenen Cyberrisiken und die Einschätzung ihrer Auswirkungen zu erwerben. Allerdings sollte im Richtlinienvorschlag der Umfang solcher Kenntnisse und Fertigkeiten angegeben werden, um im Rahmen europäischer Leitlinien vorzugeben, welche Kompetenzen im Rahmen von Schulungsmaßnahmen erworben werden sollten, um den im Vorschlag genannten Anforderungen zu entsprechen. Dadurch ließe sich auch vermeiden, dass sich die Schulungen von Mitgliedstaat zu Mitgliedstaat inhaltlich unterscheiden.

5.10 Der EWSA stimmt zu, dass der Agentur der Europäischen Union für Cybersicherheit (ENISA) im gesamten institutionellen und operativen Rahmen der Cybersicherheit auf europäischer Ebene eine wichtige Rolle zukommt. Er vertritt in diesem Zusammenhang die Auffassung, dass diese Agentur neben ihrem Bericht über den Stand der Cybersicherheit in der Union im Internet auch aktuelle Informationen über die Cybersicherheitsvorfälle sowie sektorspezifische Bekanntmachungen veröffentlichen muss, um den von der NIS-2-Richtlinie betroffenen Akteuren mit diesem zusätzlichen nützlichen Instrument die Möglichkeit zu geben, ihre Unternehmen besser zu schützen.

5.11 Der EWSA teilt die Auffassung, dass der rechtzeitige Zugang zu korrekten Informationen über Schwachstellen, die IKT-Produkte und -Dienste betreffen, zu einem besseren Cybersicherheitsrisikomanagement beiträgt. In dieser Hinsicht sind öffentlich zugängliche Informationen über Schwachstellen ein wichtiges Instrument für die zuständigen nationalen Behörden, die Soforteinsatzteams für IT-Sicherheitsvorfälle (CSIRTs), die Unternehmen und die Nutzer. Aus diesem Grund stimmt der EWSA dem Vorschlag zu, die ENISA mit der Einrichtung eines europäischen Schwachstellenregisters zu betrauen, in dem wesentliche und wichtige Einrichtungen und deren Anbieter Informationen bereitstellen, die es den Nutzern ermöglichen, geeignete Abhilfemaßnahmen zu ergreifen. Nach Ansicht des EWSA muss die Bereitstellung dieser Informationen über die wichtigsten Schwachstellen und Vorfälle nicht freiwillig, sondern verpflichtend sein, damit auch die Auftraggeber der zahlreichen Vergabeverfahren auf europäischer Ebene von diesen Informationen profitieren können (auch für 5G-Produkte und -Technologien). Ein solches Register würde dann auch Inhalte umfassen, die bei der Bewertung der Angebote verwendbar wären, und zwar sowohl bei der Prüfung ihrer Qualität als auch der Zuverlässigkeit der europäischen und außereuropäischen Auftragnehmer in Bezug auf die Sicherheit der Produkte und Dienstleistungen, die Gegenstand der Auftragsvergabe sind – im Einklang mit der Empfehlung zur Cybersicherheit der 5G-Netze vom 26. März 2019. Bezüglich des Registers sollte auch sichergestellt werden, dass die darin enthaltenen Informationen ohne jedwede Diskriminierung zugänglich sind.

Brüssel, den 27. April 2021

Christa SCHWENG
Präsidentin des Europäischen Wirtschafts- und Sozialausschusses