Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses zum „Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über horizontale Cybersicherheitsanforderungen an Produkte mit digitalen Bestandteilen und zur Änderung der Richtlinie EU/2019/1020“

(COM(2022) 454 final — 2022/0272 (COD))

(2023/C 100/15)

Berichterstatter: **Maurizio MENSI**

Ko-Berichterstatter: **Marinel Dănuț MUREȘAN**

Befassung	Europäisches Parlament, 9.11.2022
	Rat der Europäischen Union, 28.10.2022
Rechtsgrundlagen	Artikel 114 des Vertrags über die Arbeitsweise der Europäischen Union
Zuständige Fachgruppe	Fachgruppe Binnenmarkt, Produktion, Verbrauch
Annahme in der Fachgruppe	10.11.2022
Verabschiedung auf der Plenartagung	14.12.2022
Plenartagung Nr.	574
Ergebnis der Abstimmung	
(Ja-Stimmen/Nein-Stimmen/Enthaltungen)	177/0/0

1. **Schlussfolgerungen und Empfehlungen**

1.1. Der Europäische Wirtschafts- und Sozialausschuss (EWSA) begrüßt den Vorschlag der Kommission für einen Rechtsakt zur Cyberresilienz, mit dem höhere Standards für die Cybersicherheit festgelegt werden. Durch diesen Rechtsakt wird ein verlässliches System für Wirtschaftsakteure geschaffen und gleichzeitig gewährleistet, dass die EU-Bürger die auf dem Markt erhältlichen Produkte sicher verwenden können. Diese Initiative ist Teil der europäischen Datenstrategie, mit der die Sicherheit von Daten, einschließlich personenbezogener Daten, und die Grundrechte, die wesentliche Voraussetzungen für unsere digitale Gesellschaft sind, gestärkt werden.

1.2. Der EWSA hält es für unabdingbar, die kollektive Bekämpfung von Cyberangriffen zu verstärken und die Harmonisierung der Cybersicherheit auf nationaler Ebene in Bezug auf operative Vorschriften und Instrumente zu konsolidieren. Damit soll verhindert werden, dass unterschiedliche nationale Ansätze zu Rechtsunsicherheiten und rechtlichen Hindernissen führen.

1.3. Der EWSA begrüßt die Initiative der Kommission, die dazu beitragen kann, die erheblichen Kosten, die den Unternehmen durch Cyberangriffe entstehen, zu senken. Außerdem sorgt sie für einen besseren Schutz der Grundrechte wie beispielsweise der Privatsphäre der Bürger bzw. Verbraucher. Insbesondere zeigt die Kommission, dass sie bezüglich der Tätigkeiten der Zertifizierungsbehörden die spezifischen Bedürfnisse von KMU berücksichtigt. Nach Ansicht des EWSA jedoch müssen die Kriterien für die Anwendung des Rechtsakts zur Cyberresilienz präzisiert werden.

1.4. Der EWSA begrüßt zwar, dass der Rechtsakt erfreulicherweise nahezu alle digitalen Produkte abdeckt. Allerdings können aufgrund der damit verbundenen umfangreichen und komplexen Überprüfungs- und Kontrolltätigkeiten Probleme bei seiner praktischen Anwendung auftreten. Daher müssen die Überwachungs- und Kontrollinstrumente gestärkt werden.

1.5. Der EWSA stellt fest, dass der materielle Anwendungsbereich des Rechtsaktes genau geklärt werden muss, insbesondere in Bezug auf Produkte mit digitalen Elementen und auf Software.

1.6. Der EWSA stellt fest, dass die Hersteller verpflichtet werden, Schwachstellen ihrer Produkte sowie Sicherheitsvorfälle zu melden und die Europäische Agentur für Cybersicherheit (ENISA) darüber zu informieren. Daher muss die ENISA mit den erforderlichen Ressourcen ausgestattet werden, damit sie die ihr übertragenen wichtigen und sensiblen Aufgaben rechtzeitig und wirksam erfüllen kann.

1.7. Der EWSA schlägt der Kommission vor, spezielle Leitlinien zur Vermeidung von Unsicherheiten bei der Auslegung zu erarbeiten und damit Herstellern und Verbrauchern Orientierungshilfen für die anzuwendenden Vorschriften und Verfahren an die Hand zu geben. Denn eine Reihe von Produkten, die in den Anwendungsbereich des Vorschlags fallen, unterliegen offenbar auch anderen Rechtsvorschriften zur Cybersicherheit. In diesem Zusammenhang wäre es auch wichtig, dass insbesondere KMU und KKMU Zugang zu Unterstützung durch qualifizierte Experten haben, die in der Lage sind, spezifische berufliche Dienstleistungen zu erbringen.

1.8. Der EWSA stellt fest, dass die Beziehung zwischen Zertifizierungsbehörden im Sinne des Rechtsakts zur Cyberresilienz und anderen Stellen, die auf der Grundlage anderer Rechtsvorschriften zur Zertifizierung der Cybersicherheit befugt sind, nicht ganz klar ist. Das gleiche Problem bezüglich der operativen Koordinierung kann sich auch zwischen den in diesem Vorschlag vorgesehenen Aufsichtsbehörden und denjenigen Behörden ergeben, die bereits im Rahmen anderer, für dieselben Produkte geltender Rechtsvorschriften tätig sind.

1.9. Der EWSA stellt fest, dass der Vorschlag für die Zertifizierungsbehörden eine beträchtliche Zahl von Tätigkeiten und Zuständigkeiten vorsieht, deren praktische Durchführung sichergestellt werden muss. Damit soll auch verhindert werden, dass der Rechtsakt zur Cyberresilienz den bürokratischen Aufwand erhöht und damit Hersteller benachteiligt, die eine Reihe zusätzlicher Zertifizierungsanforderungen erfüllen müssen, um weiterhin auf dem Markt tätig sein zu können.

2. **Analyse des Vorschlags**

2.1. Mit dem Vorschlag für einen Rechtsakt zur Cyberresilienz beabsichtigt die Kommission, die geltenden Rechtsvorschriften zur Cybersicherheit umfassend und bereichsübergreifend zu straffen und neu zu regeln und sie gleichzeitig im Lichte der technologischen Innovationen zu aktualisieren.

2.2. Mit diesem Rechtsakt verfolgt die Kommission im Wesentlichen vier Ziele: sicherstellen, dass die Hersteller die Sicherheit ihrer Produkte mit digitalen Elementen bereits in der Konzeptions- und Entwicklungsphase und danach während des gesamten Lebenszyklus verbessern; einen kohärenten Rahmen von Rechtsvorschriften zur Cybersicherheit bieten, damit die Hardware- und Softwarehersteller die Vorschriften leichter einhalten können; die Transparenz der Sicherheitsmerkmale von Produkten mit digitalen Elementen verbessern, damit Unternehmen und Verbrauchern diese Produkte sicher nutzen können. Im Grunde genommen wird mit dem Vorschlag eine CE-Kennzeichnung für Cybersicherheit eingeführt, die auf allen Produkten angebracht werden muss, die unter den Rechtsakt zur Cyberresilienz fallen.

2.3. Mit dieser horizontalen Maßnahme möchte die Kommission die gesamte Problematik umfassend regeln, denn sie betrifft praktisch alle Produkte, die digitale Elemente enthalten. Davon ausgenommen sind nur medizinische Produkte und solche, die mit der Zivilluftfahrt in Zusammenhang stehen sowie Fahrzeuge und Rüstungsgüter. Der Vorschlag erstreckt sich auch nicht auf Software-as-a-Service (SaaS- bzw. Cloud-Dienste), es sei denn, sie werden zur Herstellung von Produkten mit digitalen Elementen verwendet.

2.4. Die Definition des Begriffs „Produkt mit digitalen Elementen“ ist sehr weit gefasst und bezieht sich auf alle Software- oder Hardwareprodukte einschließlich der Soft- und Hardware, die nicht Bestandteil des Produkts ist, aber gesondert auf den Markt gebracht wird.

2.5. Mit dem Rechtsakt werden verbindliche Cybersicherheitsanforderungen für Produkte eingeführt, die während ihres gesamten Lebenszyklus digitale Elemente enthalten. Er ersetzt jedoch nicht die bereits bestehenden Anforderungen. Vielmehr behalten diejenigen Produkte, deren Übereinstimmung mit bestehenden EU-Normen bereits zertifiziert wurde, ihre Zertifizierung auch im Rahmen der neuen Verordnung.

2.6. Das allgemeine Grundprinzip lautet, dass in Europa nur „sichere“ Produkte vermarktet werden. Die Hersteller sorgen dafür, dass ihre Produkte während des gesamten Lebenszyklus sicher bleiben.

2.7. Ein Produkt gilt als sicher, wenn es so konzipiert und hergestellt wird, dass es ein Sicherheitsniveau aufweist, das den mit seiner Verwendung verbundenen Cyberrisiken angemessen ist, wenn es zum Zeitpunkt seines Verkaufs keine bekannten Sicherheitslücken hat, eine sichere Standardkonfiguration aufweist und vor unrechtmäßigen Verbindungen geschützt ist, wenn die von ihm erfassten Daten geschützt werden und sich die Datenspeicherung auf die für seinen Betrieb erforderlichen Daten beschränkt.

2.8. Ein Hersteller gilt als geeignet, seine Produkte auf den Markt zu bringen, wenn er die Liste der verschiedenen Softwarekomponenten seiner Produkte offenlegt, im Falle neuer Sicherheitslücken rasch und kostenlos Abhilfe schafft, die von ihm festgestellten und beseitigten Sicherheitslücken veröffentlicht und die von ihm vermarkteten Produkte regelmäßig auf ihre Unbedenklichkeit hin überprüft. Diese und andere durch den Rechtsakt zur Cyberresilienz vorgeschriebene Tätigkeiten müssen während der gesamten Lebensdauer eines Produkts oder mindestens fünf Jahre nach dessen Inverkehrbringen durchgeführt werden. Der Hersteller muss sicherstellen, dass Sicherheitslücken durch regelmäßige Softwareupdates beseitigt werden.

2.9. Nach einem allgemeinen, in verschiedenen Sektoren angewandten Grundsatz gelten diese Verpflichtungen auch für Importeure und Händler.

2.10. Der Rechtsakt zur Cyberresilienz sieht eine Makrokategorie sogenannter „normaler" Produkte und Softwareprodukte vor, bei denen man sich auf die Selbstbewertung durch den Hersteller verlassen kann, wie dies bereits bei anderen Arten der CE-Kennzeichnung der Fall ist. Nach Angaben der Kommission fallen 90 % der auf dem Markt erhältlichen Produkte in diese Kategorie.

2.11. Diese Produkte dürfen in Verkehr gebracht werden, nachdem der Hersteller eine Selbstbewertung ihrer Cybersicherheit vorgenommen und die in den Leitlinien der Rechtsvorschriften festgelegten Unterlagen vorlegt hat. Derselbe Hersteller muss die Bewertung wiederholen, wenn das Produkt geändert wird.

2.12. Die übrigen 10 % der Produkte sind in zwei weitere Kategorien unterteilt (Klasse I: weniger gefährlich, und Klasse II: gefährlicher), deren Inverkehrbringen größere Sorgfalt erfordert. Dabei handelt es sich um sogenannte „kritische Produkte mit digitalen Elementen", deren Defekt zu anderen gefährlichen und weitreichenderen Sicherheitsverletzungen führen kann.

2.13. Für Produkte dieser beiden Klassen sind grundlegende Selbstbewertungen nur dann zulässig, wenn der Hersteller nachweist, dass er bestimmte Marktstandards und Sicherheitsspezifikationen erfüllt oder über die von der EU bereits vorgesehenen Cybersicherheitszertifikationen verfügt. Ist dies nicht der Fall, kann das Produkt eine Zertifizierung von einer akkreditierten Zertifizierungsstelle erhalten. Eine derartige Zertifizierung ist für Produkte der Klasse II obligatorisch.

2.14. Das System zur Einstufung von Produkten in Risikokategorien ist auch in der vorgeschlagenen Verordnung zur künstlichen Intelligenz (KI) enthalten. Um Zweifel an den anzuwendenden Bestimmungen zu vermeiden, berücksichtigt der Rechtsakt zur Cyberresilienz Produkte mit digitalen Elementen, die gleichzeitig gemäß dem KI-Vorschlag als „Hochrisiko-KI-Systeme" eingestuft werden. Solche Produkte müssen in der Regel dem in der KI-Verordnung festgelegten Konformitätsbewertungsverfahren entsprechen. Davon ausgenommen sind „kritische digitale Produkte", für die zusätzlich zu den „grundlegenden Anforderungen des Rechtsakts zur Cyberresilienz" die Konformitätsbewertungsvorschriften des Rechtsakts gelten.

2.15. Um die Einhaltung des Rechtsakts zur Cyberresilienz zu gewährleisten, wird in jedem Mitgliedstaat die Aufsichtstätigkeit einer nationalen Behörde übertragen. Stellt eine nationale Behörde fest, dass die Cybersicherheitsmerkmale eines Produkts unzureichend sind, kann das Inverkehrbringen dieses Produkts im Einklang mit den Rechtsvorschriften über die Sicherheit anderer Produkte in dem betreffenden Staat ausgesetzt werden. ENISA ist dafür zuständig, ein gemeldetes Produkt eingehend zu bewerten. Wird ein Produkt für unsicher befunden, kann dies zur Aussetzung des Inverkehrbringens des betreffenden Produkts in der EU führen.

2.16. Das Sanktionssystem des Rechtsakts zur Cyberresilienz umfasst eine Reihe von Sanktionen, die sich nach der Schwere des Verstoßes richten und im Falle einer Verletzung der grundlegenden Cybersicherheitsanforderungen bis zu 15 Mio. EUR oder 2,5 % des Umsatzes des vorangegangenen Geschäftsjahres betragen können.

3. **Bemerkungen**

3.1. Der EWSA begrüßt die Initiative der Kommission, das großangelegte Vorhaben der Cybersicherheitsgesetzgebung um einen wichtigen Baustein zu ergänzen und damit die Richtlinie zur Netz- und Informationssicherheit (NIS) ([1]) sowie den Rechtsakt zur Cybersicherheit ([2]) zu koordinieren und weiter auszubauen. Hohe Cybersicherheitsstandards spielen bei der Schaffung eines robusten EU-Cybersicherheitssystems für alle Wirtschaftsakteure eine bedeutende Rolle und tragen dazu bei, dass die EU-Bürger alle Produkte auf dem Markt sicher nutzen können und ihr Vertrauen in die digitale Welt gestärkt wird.

3.2. In der Verordnung geht es daher um zwei Probleme: die mangelnde Cybersicherheit vieler Produkte und vor allem die Tatsache, dass viele Hersteller keine Updates bereitstellen, um Sicherheitslücken zu schließen. Die Hersteller von Produkten mit digitalen Elementen müssen zwar mitunter einen Imageschaden hinnehmen, wenn ihre Produkte nicht sicher sind, doch die durch die Sicherheitslücken entstehenden Kosten werden hauptsächlich von gewerblichen Nutzern und Verbrauchern getragen. Dies schränkt die Anreize für die Hersteller ein, in die Konzeption und Entwicklung sicherer Produkte zu investieren und Sicherheitsupdates bereitzustellen. Darüber hinaus mangelt es Unternehmen und Verbrauchern

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

([2]) Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit) (ABl. L 151 vom 7.6.2019, S. 15).

häufig an ausreichenden und genauen Informationen, um sichere Produkte auswählen zu können. Sie wissen oft nicht, wie sie sichergehen können, dass die von ihnen erworbenen Produkte sicher konfiguriert wurden. Auf diese beiden Aspekte gehen die neuen Vorschriften ein: Es geht um die Frage der Updates und die Bereitstellung aktueller Informationen für die Kunden. Der EWSA ist der Auffassung, dass die vorgeschlagene Verordnung bei ordnungsgemäßer Anwendung zu einem internationalen Maßstab und einem Modell für die Cybersicherheit werden könnte.

3.3. Der EWSA begrüßt den Vorschlag, Cybersicherheitsanforderungen für Produkte mit digitalen Elementen einzuführen. Es wird jedoch wichtig sein, Überschneidungen mit anderen bestehenden Rechtsvorschriften in diesem Bereich, z. B. mit der neuen NIS-2-Richtlinie ([3]) und der KI-Verordnung, zu vermeiden.

3.4. Der EWSA begrüßt zwar, dass der Rechtsakt erfreulicherweise nahezu alle digitalen Produkte abdeckt. Allerdings können aufgrund der damit verbundenen umfangreichen und komplexen Überprüfungs- und Kontrolltätigkeiten Probleme bei seiner praktischen Anwendung auftreten.

3.5. Der materielle Anwendungsbereich des Rechtsakts ist weit gefasst und erstreckt sich auf alle Produkte mit digitalen Elementen. Gemäß der vorgeschlagenen Definition fallen darunter alle Software- und Hardwareprodukte sowie die damit zusammenhängenden Datenverarbeitungsvorgänge. Der EWSA schlägt der Kommission vor klarzustellen, ob jegliche Software in den Anwendungsbereich des Verordnungsvorschlags fällt.

3.6. Die Hersteller werden verpflichtet, aktiv ausgenutzte Schwachstellen und Sicherheitsvorfälle zu melden. Sie werden verpflichtet, die ENISA innerhalb von 24 Stunden, nachdem sie davon Kenntnis erlangt haben, über alle aktiv ausgenutzten Schwachstellen des Produkts und (gesondert) über jeden Vorfall, der sich auf die Sicherheit des Produkts auswirkt, zu informieren. In diesem Zusammenhang weist der EWSA darauf hin, dass die ENISA personell und fachlich angemessen ausgestattet werden muss, um die ihr im Rahmen der Verordnung übertragenen einschlägigen und sensiblen Aufgaben wirksam erfüllen zu können.

3.7. Die Tatsache, dass eine Reihe von Produkten, die in den Anwendungsbereich des Vorschlags fallen, auch anderen Rechtsvorschriften zur Cybersicherheit unterliegt, könnte zu Unsicherheiten darüber führen, welche Rechtsvorschriften anzuwenden sind. Obwohl der Rechtsakt zur Cyberresilienz voraussichtlich mit dem derzeitigen EU-Regulierungsrahmen für Produkte und anderen derzeit im Rahmen der digitalen Strategie der EU anhängigen Vorschlägen im Einklang stehen wird, überschneiden sich Vorschriften, wie sie z. B. für Hochrisiko-KI-Produkte vorgesehen sind, mit denen der Verordnung über die Verarbeitung personenbezogener Daten. In diesem Zusammenhang schlägt der EWSA der Kommission vor, für Hersteller und Verbraucher einschlägige Leitlinien zur korrekten Anwendung des Rechtsakts zur Cyberresilienz zu erarbeiten.

3.8. Der EWSA stellt fest, dass die Beziehung zwischen Zertifizierungsbehörden im Rahmen des Rechtsakts zur Cyberresilienz und anderen Stellen, die auf der Grundlage anderer, gleichermaßen anwendbarer Rechtsvorschriften zur Zertifizierung der Cybersicherheit befugt sind, nicht ganz klar ist.

3.9. Da den Zertifizierungsbehörden zudem ein erheblicher Teil des Aufwands und der Verantwortung zufällt, muss überprüft und gewährleistet werden, dass sie in der Praxis funktionieren. Auf diese Weise soll verhindert werden, dass der Rechtsakt zur Cyberresilienz zu einer Zunahme des Verwaltungsaufwands führt, den die Hersteller tragen müssen, um auf dem Markt tätig zu sein. In diesem Zusammenhang wäre es auch wichtig, dass insbesondere KMU und KKMU Zugang zu Unterstützung durch qualifizierte Experten haben, die in der Lage sind, spezifische berufliche Dienstleistungen zu erbringen.

3.10. Gemäß dem Rechtsakt zur Cyberresilienz müssen die Zertifizierungsbehörden bei ihrer Tätigkeit die besonderen Bedürfnisse von KMU berücksichtigen. Der EWSA weist jedoch darauf hin, dass die Kriterien für die Anwendung des Rechtsakts präzisiert werden müssen.

3.11. Ein Koordinierungsproblem kann sich auch zwischen den in der Verordnung vorgesehenen Aufsichtsbehörden und denjenigen ergeben, die bereits im Rahmen anderer, für dieselben Produkte geltender Rechtsvorschriften tätig sind. Der EWSA schlägt der Kommission daher vor, die Mitgliedstaaten zur Wachsamkeit aufzufordern und gegebenenfalls entsprechende Abhilfemaßnahmen zu ergreifen.

Brüssel, den 14. Dezember 2022

Die Präsidentin
des Europäischen Wirtschafts- und Sozialausschusses
Christa SCHWENG

([3]) 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) (ABl. L 333 vom 27.12.2022, S. 80).