Berlin, 27. März 2026

Deutsche Industrie- und Handelskammer

Stellungnahme

Referentenentwurf des Bundesministeriums des Innern
Entwurf eines Gesetzes zur Durchführung der Verordnung (EU) 2024/2847 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen (Cyberresilienz-Verordnung)

Der Cyber Resilience Act (CRA) führt erstmals EU-weit verbindliche Cybersicherheitsanforderungen für vernetzte Produkte ein. Produkte dürfen künftig nur dann im Binnenmarkt bereitgestellt werden, wenn sie die festgelegten Sicherheitsstandards erfüllen. Auch neue Meldepflichten werden eingeführt für aktiv ausgenutzte Schwachstellen und für Cybersicherheitsvorfälle. Die Pflichten gelten unmittelbar für Hersteller, Importeure und Händler und erweitern das CE-Kennzeichen um den Aspekt der Cybersicherheit. Der Referentenentwurf zur nationalen Umsetzung des CRA sieht dafür insbesondere Änderungen im BSI-Gesetz vor. Wir bedanken uns für die Möglichkeit zur Stellungnahme.

Das Wichtigste in Kürze

Die DIHK unterstützt das zentrale Ziel des Cyber Resilience Acts, die Cybersicherheit vernetzter Produkte europaweit zu erhöhen und einheitliche Mindeststandards für Hersteller zu schaffen. Eine hohe Cyberresilienz stärkt Vertrauen, Wettbewerbsfähigkeit und Produktsicherheit im digitalen Binnenmarkt.

Gleichzeitig bedeutet die Umsetzung des CRA – insbesondere für kleine und mittlere Unternehmen – erheblichen organisatorischen, technischen und finanziellen Aufwand. Die DIHK weist nachdrücklich darauf hin, dass in Deutschland viele tausende kleine Unternehmen tätig sind, die maßgeblich zur Innovationskraft und Wettbewerbsfähigkeit des Standorts beitragen. Je nach Auslegung und praktischer Umsetzung des CRA droht für viele dieser Betriebe jedoch eine existenzielle Überforderung.

Insbesondere kleine Betriebe verfügen häufig nicht über spezialisierte Compliance-Ressourcen und wären von neuen Dokumentations-, Melde- und Konformitätsanforderungen besonders stark betroffen. Ohne eine praxisnahe, verhältnismäßige und unterstützende Ausgestaltung der Vorgaben droht hier ein strukturelles Risiko für einen zentralen Teil der mittelständischen Wirtschaft. Die Belange kleiner Unternehmen sollten bei der Umsetzung des CRA ausdrücklich

DIHK | Deutsche Industrie- und Handelskammer
Besucheranschrift: Breite Straße 29 | 10178 Berlin-Mitte | Postanschrift: DIHK | 11052 Berlin
Tel. 030-20308-0 | Internet: www.dihk.de

berücksichtigt und mögliche Fehlanreize oder überzogene Belastungen frühzeitig vermieden werden.

Damit Unternehmen – vor allem KMU – keine Wettbewerbsnachteile erfahren, müssen die nationalen Regeln praxisgerecht, transparent und wirtschaftsfreundlich ausgestaltet werden. Der DIHK ist bewusst, dass die Spielräume dafür begrenzt sind, da viele Vorgaben bereits auf europäischer Ebene fest verankert sind. Auch viele harmonisierte Normen sind noch nicht verabschiedet. Deshalb ist es umso wichtiger, dass sich das BSI auf eine ermöglichende, unterstützende Umsetzung fokussiert.

Der Referentenentwurf setzt die europäischen Vorgaben weitgehend 1:1 um. Die schlanke Ausgestaltung des Gesetzentwurfs zur Durchführung des CRA befürwortet die DIHK ausdrücklich. Insbesondere vor dem Hintergrund, dass sehr viele Unternehmen aktuell Anforderungen aus mehreren Digitalrechtsakten parallel umsetzen müssen, ist eine Begrenzung rechtlicher Vorgaben auf das Allernötigste sinnvoll, um nicht durch noch mehr Komplexität unnötig weitere Kapazitäten in den Unternehmen zu binden.

Dem BSI wird die Rolle der zentralen Marktüberwachungs- und notifizierenden Behörde zugewiesen. Dies ist sinnvoll, da so Fachkompetenz gebündelt und eine Zersplitterung von Zuständigkeiten vermieden wird.

Entscheidend ist eine frühzeitige, verlässliche und adressatengerechte Information der Wirtschaft. Ohne praxisnahe Leitfäden entsteht eine beträchtliche Orientierungslücke. Dem BSI kommt richtiger Weise explizit die Aufgabe zu, die betroffenen Wirtschaftsakteure zu unterstützen. Die IHK-Organisation ist gern bereit, gemeinsam mit dem BSI Informations- und Unterstützungsstrukturen für Unternehmen weiter auszubauen und in die Fläche zu bringen.

Bewertung im Einzelnen

Erfüllungsaufwand

In der Begründung wird festgestellt, dass für die Wirtschaft kein zusätzlicher Erfüllungsaufwand entstehe, da die Pflichten unmittelbar aus der Verordnung (EU) 2024/2847 (CRA) hervorgehen.

Diese Einschätzung ist formal korrekt, aber in der Praxis irreführend. Unternehmen müssen sich auf Meldewege und neue Prozesse im Umgang mit der Beschwerdestelle beim BSI einstellen sowie das Konformitätsbewertungsverfahren nach deutschem Recht durchlaufen. Die damit verbundenen Aufwände sollten realistisch dargestellt werden.

Marktüberwachung (§ 65 BSI-G)

Das BSI wird zur zentralen Marktüberwachungsbehörde für den CRA und arbeitet dabei eng mit anderen Bundes- und Landesbehörden zusammen. Es richtet eine Beschwerdestelle für

Verbraucher ein und leitet Hinweise bei Bedarf an zuständige Stellen weiter. Entscheidungen des BSI gelten sofort, da Widerspruch und Klage keine aufschiebende Wirkung haben.

Nur ein praktikabel ausgestalteter Vollzug stellt sicher, dass Unternehmen – gerade KMU – den CRA umsetzen können, ohne durch unnötige Bürokratie oder unverhältnismäßige Eingriffe belastet zu werden. Die Vielzahl der EU-Digital-Regulierungen, vom CRA über die KI-Verordnung bis hin zu NIS2 und DORA, macht ein koordiniertes Vorgehen der jeweiligen Überwachungsbehörden dringend erforderlich. Die enge Abstimmung aller beteiligten Behörden bis hin zu den Zollbehörden im Rahmen der Importkontrolle sollte effektiv gesteuert werden. Durch geeignete Governance-Prozesse lassen sich Widersprüche und Doppelanforderungen vermeiden. Für die Unternehmen reduziert dies bürokratische Belastungen.

Vor dem Hintergrund der zahlreichen Anforderungen aus verschiedenen Digitalrechtsakten sollte die Vollzugspraxis ganz besonders auf Verhältnismäßigkeit, Transparenz und Praxistauglichkeit setzen. Kritisch ist, dass § 65 Abs 4 BSI-G zur Marktüberwachung eine sofortige Vollziehbarkeit von Maßnahmen vorsieht. Für Unternehmen birgt das erhebliche Risiken, da Entscheidungen sofort wirksam wären – auch wenn Sachverhalte noch ungeklärt sind.

Im Gesetz sollte zumindest eine klare Verhältnismäßigkeitsprüfung vorgesehen werden. Diese muss sicherstellen, dass behördliche Maßnahmen im Rahmen des CRA nicht zu unverhältnismäßigen Eingriffen führen – insbesondere nicht zu Beeinträchtigungen der Versorgung der Bevölkerung mit wichtigen digitalen Diensten und Produkten. Darüber hinaus sollten keine Sofortmaßnahmen ohne vorherige Anhörung ergriffen werden (außer bei klaren Gefährdungslagen).

Insgesamt ist eine kooperative, risikobasierte Vollzugspraxis erforderlich, um unverhältnismäßige Belastungen und Rechtsunsicherheit zu vermeiden. Dazu gehören beispielsweise Beratungen, bevor Sanktionen erfolgen, insbesondere bei Erstverstößen während der Einführungsphase.

Notifizierung und Akkreditierung (§ 66 BSI-G)

Das BSI erhält die Befugnis, als notifizierende Behörde Konformitätsbewertungsstellen – gemeinsam mit der Deutschen Akkreditierungsstelle – zu prüfen und zu notifizieren.

Für die Wirtschaft ist entscheidend, dass der Vollzug realistisch, verhältnismäßig und planbar erfolgt. Ein überfordertes System würde zu Verzögerungen, Unsicherheiten und Wettbewerbsnachteilen beim Marktzugang führen. Unternehmen benötigen verlässliche, effiziente und zeitnahe Verfahren, um ihre Produkte zügig und zu wettbewerbsfähigen Kosten zertifizieren und in den Markt bringen zu können.

Entscheidend ist nicht nur die Verfügbarkeit harmonisierter Standards, sondern ebenso der Aufbau eines skalierbaren und tragfähigen Prüfökosystems, das eine praktikable Umsetzung ermöglicht. Die Verfügbarkeit ausreichend vieler Konformitätsbewertungsstellen wird ein entscheidender Faktor sein, damit die notwendige Zahl an Produkten rechtzeitig CE-zertifiziert

werden kann. BMI und BSI sollten gemeinsam darauf hinwirken, dass rechtzeitig ausreichend Kapazitäten bei den Konformitätsbewertungsstellen verfügbar sind.

Die Bundesregierung sollte sich auf europäischer Ebene aktiv für die Mitgestaltung harmonisierter Standards einsetzen. Sie sind Voraussetzung dafür, dass der CRA seine intendierte Wirkung entfalten kann, ohne Innovationshemmnisse zu erzeugen oder Rechtsunsicherheiten für Unternehmen zu schaffen.

Auch die internationale Dimension der Cybersicherheit sollte berücksichtigt werden. Um globale Fragmentierung zu vermeiden, sollte die Bundesregierung aktiv auf Harmonisierung mit Drittstaaten-Regulierungen hinwirken und sich für eine gegenseitige Anerkennung von Konformitätsbewertungen einzusetzen.

Unterstützung der betroffenen Wirtschaftsakteure (§ 67 BSI-G)

§ 67 BSIG-E sieht Unterstützungsmaßnahmen insbesondere für kleine und mittlere Unternehmen vor. Gleichzeitig stellt die Begründung klar, dass daraus kein Anspruch auf eine individuelle Beratung abgeleitet werden kann. Sensibilisierungs- und Schulungsmaßnahmen sowie ein „Reallabor für Cyberresilienz“ sollen Unternehmen bei der praktischen Umsetzung unterstützen.

Der CRA hat weitreichende Folgen für nahezu alle Unternehmen, die digitale Produkte entwickeln, importieren oder vertreiben. Die neuen Pflichten führen zu erheblichen organisatorischen, technischen und finanziellen Aufwänden in den Unternehmen. Gleichzeitig unterstützen sie eine notwendige Professionalisierung der Sicherheitsprozesse entlang des gesamten Produktlebenszyklus. Dabei sehen sich besonders kleine und mittlere Unternehmen vor große Herausforderungen gestellt, die Anforderungen aus dem CRA fristgerecht umzusetzen. Betroffen sind aber nicht nur sogenannte KMU, sondern beispielsweise auch kommunale Unternehmen oder Stadtwerke, die eigene Apps und digitale Dienste entwickeln und betreiben. Aus der Wirtschaft erreichen die DIHK vermehrt Hinweise, dass vielen Unternehmen noch nicht ausreichend bekannt ist, welche Anforderungen konkret auf sie zukommen, oder sogar erwägen, einzelne Produkte vom Markt zu nehmen, statt den erheblichen Aufwand der Umsetzung zu tragen. Das zeigt deutlich: Ohne umfassende und frühzeitige Informations- und Qualifizierungsangebote werden zentrale Teile der digitalen Wertschöpfungsketten in Deutschland unnötig belastet. Auch größere Unternehmen haben – trotz bestehender Compliance-Strukturen – häufig spezifische Fragestellungen, zu denen gezielte Informationen des BSI helfen würden.

BMI und BSI sollten daher Schulungs-, Beratungs- und Unterstützungsmaßnahmen so zur Verfügung stellen, dass Unternehmen tatsächlich in die Lage versetzt werden, die CRA-Vorgaben fristgerecht und verlässlich zu erfüllen.

Für viele kleine und mittlere Unternehmen ist bereits die Betroffenheitsprüfung die erste große Hürde – ähnlich wie bei der Umsetzung von NIS2. Bevor Unternehmen überhaupt Maßnahmen planen können, müssen sie klären, ob und in welchem Umfang sie unter den CRA

fallen. Damit diese Einstiegsbarriere nicht zur unnötigen Belastung wird, sollte das BSI niedrigschwellige Self-Assessment-Tools bereitstellen. Solche einfach nutzbaren Online-Selbsttests würden KMU ermöglichen, schnell und rechtssicher einzuschätzen, ob der CRA auf ihre Produkte zutrifft und welche Pflichten konkret entstehen.

Auch wenn in Artikel 33 Abs 3 CRA die Bereitstellung von Leitlinien für Kleinstunternehmen sowie kleine und mittlere Unternehmen durch die EU-Kommission vorsieht, sollte § 67 BSIG-E um eine klare Verpflichtung ergänzt werden, spätestens sechs Monate vor Vollwirksamkeit der Verordnung – also bis zum 11. Juni 2027 – branchenspezifische Umsetzungsleitfäden zu veröffentlichen. Diese Leitfäden sollten gemeinsam mit den betroffenen Wirtschaftsverbänden erarbeitet werden, um Praxistauglichkeit, Verständlichkeit und sektorspezifische Relevanz sicherzustellen. Ebenso deutlich vor Inkrafttreten der CRA-Pflichten sollten Muster, FAQs und Praxisbeispiele bereitgestellt werden. Die Kommunikation sollte jeweils adressatengerecht gestaltet und die Angebote allen Wirtschaftsakteuren zugänglich gemacht werden. Auch kommunale Unternehmen und Unternehmen der öffentlichen Daseinsvorsorge sollten explizit adressiert werden.

Die DIHK weist an dieser Stelle auf den deutlichen Kumulationseffekt von NIS2 und CRA hin. Viele Unternehmen stehen derzeit vor der anspruchsvollen Umsetzung von NIS2. Parallel dazu tritt der CRA mit eigenen Meldepflichten und umfangreichen Dokumentationsanforderungen hinzu. Diese parallelen Regime führen zu erheblichen Mehrbelastungen und bergen das Risiko doppelter Prozesse, wenn sie nicht sauber aufeinander abgestimmt werden. Unterstützungsangebote sollten auch adressieren, wie NIS2-Maßnahmen und CRA-Pflichten in den Unternehmen so verzahnt werden können, dass Synergien genutzt und Doppelaufwände vermieden werden.

Es fehlt eine klare Regelung, ab wann das Reallabor zur Verfügung stehen wird und wie der Zugang konkret gestaltet sein soll. Damit Unternehmen den CRA rechtzeitig umsetzen können, muss diese Infrastruktur frühzeitig und vollständig funktionsfähig bereitstehen – und nicht erst dann, wenn die gesetzlichen Pflichten bereits greifen. Dazu gehört auch, dass der Zugang zum Reallabor sowie zu Test- und Prüfkapazitäten zu angemessenen Kosten möglich ist. Unklar bleibt zudem, wie die in Artikel 33 Abs 2 CRA vorgesehene Abgrenzung, welche Unternehmen Zugang erhalten sollen, praktisch umgesetzt wird (genannt werden dort innovative Produkte sowie insbesondere Kleinst- und Kleinunternehmen einschließlich Start-ups). Die DIHK empfiehlt, den Zugang möglichst breit zu öffnen, sodass viele Unternehmen von der Unterstützung profitieren können.

Die in Artikel 33 Abs 1b) CRA vorgesehene Möglichkeit, einen speziellen Kommunikationskanal für Kleinst- und Kleinunternehmen einzurichten, wurde im BSI-G nicht genutzt. Ein solcher Kanal könnte dazu beitragen, den besonders hohen Informations- und Beratungsbedarf dieser Unternehmensgruppen zu decken – insbesondere, um Verständnisfragen zur praktischen Umsetzung der Verordnung frühzeitig zu klären. Insofern stellt sich die Frage, ob das BMI keinen Bedarf für ein solches Angebot sieht oder ob davon ausgegangen wird, dass bereits

ausreichende Unterstützungsstrukturen bestehen. Aus Sicht der Wirtschaft wäre ein klar definierter, niedrigschwelliger Kommunikationsweg jedoch sinnvoll, um Kleinst- und Kleinunternehmen gezielt zu entlasten und ihre Umsetzungsfähigkeit im CRA-Regime sicherzustellen.

Die IHK-Organisation bietet an, gemeinsam mit dem BSI die Unternehmen bei der Umsetzung des CRA zu unterstützen.

Übergangs- und Fristenregelungen (Artikel 4 BSI-G)

Die Anforderungen greifen bereits gestaffelt ab dem 11. Juni 2026, weitere Pflichten ab dem 11. September 2026 und vollständig ab dem 11. Dezember 2027.

Die im CRA vorgesehenen Übergangsfristen sind sehr knapp bemessen und stellen viele Unternehmen – besonders kleine und mittlere Betriebe – vor große Herausforderungen. Technische Anpassungen, neue Dokumentationspflichten und mögliche Konformitätsbewertungen erfordern einen erheblichen organisatorischen und finanziellen Vorlauf. Für viele Unternehmen sind die Fristen kaum einzuhalten, vor allem wenn Leitfäden, Prüfstrukturen und Meldeprozesse nicht frühzeitig bereitstehen. Umso wichtiger ist es, die ambitionierten Zeitvorgaben des CRA durch frühzeitige und wirkungsvolle Unterstützungsangebote zu flankieren. Darauf sollten BMI und BSI ein besonderes Augenmerk legen.

Meldepflichten aus Cybersecurity-/Digital-Gesetzen

Unternehmen stehen gleichzeitig vor zahlreichen neuen rechtlichen Vorgaben – vom CRA über NIS2, den EU-Cybersecurity-Act und die DSGVO bis hin zum AI-Act und der Produkthaftungsreform. Viele dieser Regelwerke enthalten Meldepflichten, die sich inhaltlich überschneiden. Aktuell müssen Unternehmen identische Informationen häufig mehrfach und an unterschiedliche Stellen übermitteln. Auf europäischer Ebene wird mit dem Digital-Omnibus eine einheitliche Meldestelle angestrebt.

Gemäß Artikel 14 Abs 1 und 2 CRA müssen Hersteller sowohl aktiv ausgenutzte Schwachstellen als auch schwerwiegende Sicherheitsvorfälle melden. Der deutsche Referentenentwurf benennt hierfür das BSI als zuständige Stelle. Für die Wirtschaft ist entscheidend, dass die vielfältigen Meldepflichten harmonisiert werden, damit kein paralleler Melde-Wildwuchs entsteht und Unternehmen nicht mit unnötiger Bürokratie belastet werden.

Ein einheitlicher, digitaler Meldekanal für CRA, NIS2 und weitere Meldepflichten würde Unternehmen erheblich entlasten. National könnte dies über bestehende Lösungen wie das BSI-Portal erfolgen, das bereits für NIS2-Meldungen genutzt wird. Eine solche gebündelte Meldestruktur würde Mehrfachmeldungen vermeiden, Prozesse vereinfachen und Rechtsklarheit schaffen. Eine Bündelung der Meldungen auf europäischer Ebene hält die DIHK aus Sicherheits- und Praktikabilitätsgründen nicht für zielführend.

Verwalter quelloffener Software („Open-Source-Software-Stewards“)

Der CRA führt mit Artikel 24 erstmals spezifische Pflichten für sogenannte „Verwalter quelloffener Software“ („Open-Source-Software-Stewards“) ein. Damit sind juristische Personen gemeint, die Open-Source-Projekte dauerhaft unterstützen, wenn diese für kommerzielle Zwecke genutzt werden – ohne selbst Hersteller zu sein. Diese Organisationen arbeiten neutral, nicht produktorientiert, und leisten einen entscheidenden Beitrag zur Sicherheit, Stabilität und Weiterentwicklung der jeweiligen Open-Source-Software. Sie tragen maßgeblich dazu bei, dass digitale Wertschöpfungsketten zuverlässig funktionieren.

Ein starkes europäisches Open-Source-Ökosystem ist wesentlich für digitale Souveränität und Unabhängigkeit. In Europa gibt es bereits wichtige Einrichtungen wie die Open Source Business Alliance, das Open Source Automation Development Lab in Stuttgart oder die TYPO3 Association. Gleichzeitig wird ein großer Teil zentraler Open-Source-Projekte von außereuropäischen Institutionen getragen, etwa von der Linux Foundation oder der WordPress Foundation.

Der Referentenentwurf enthält bislang keine näheren Ausführungen zu Artikel 24, offenbar in der Annahme, dass die EU-Regelung hinreichend konkret ist. Aus Sicht der DIHK ist jedoch entscheidend, dass die klare Trennung zwischen Verwaltern quelloffener Software und Herstellern konsequent umgesetzt wird. Verwalter quelloffener Software übernehmen eine strategisch wichtige Rolle für die Sicherheit und Resilienz der digitalen Infrastruktur in Europa. Der CRA erkennt diese Bedeutung an und schafft bewusst einen leichtgewichtigen, eigenen Pflichtenkatalog, der deren Besonderheiten berücksichtigt. Ihre Arbeit ist elementar für die digitale Souveränität Europas, denn Open-Source-Software bildet einen großen Teil der technologischen Basis moderner Produkte.

Deutsche Verwalter quelloffener Software sollten gezielt unterstützt werden, um ihre strategische Bedeutung für die digitale Souveränität Deutschlands und der EU zu sichern. Sie benötigen, gerade im Zusammenhang mit dem CRA, klare Leitlinien, Ressourcen und Unterstützung, damit sie ihre Sicherheits- und Meldepflichten erfüllen können und das europäische Open-Source-Ökosystem als unabhängige, resiliente technologische Basis langfristig gestärkt wird.

Ansprechpartnerin

Dr. Katrin Sobania, Bereich Digitalisierung, Infrastruktur, Regionalpolitik (DIR), Leiterin des Referats Informations- und Kommunikationstechnologie, E-Government, Postdienste, Daten- und Informationssicherheit, sobania.katrin@dihk.de

Wer wir sind:

Unter dem Dach der Deutschen Industrie- und Handelskammer (DIHK) sind die 79 Industrie- und Handelskammern (IHKs) zusammengeschlossen. Unser gemeinsames Ziel: Beste Bedingungen für erfolgreiches Wirtschaften.

Auf Bundes- und Europaebene setzt sich die DIHK für die Interessen der gesamten gewerblichen Wirtschaft gegenüber Politik, Verwaltung und Öffentlichkeit ein. Denn mehrere Millionen Unternehmen aus Handel, Industrie und Dienstleistung sind gesetzliche Mitglieder einer IHK - vom Kiosk-Besitzer bis zum Dax-Konzern. So sind DIHK und IHKs eine Plattform für die vielfältigen Belange der Unternehmen. Diese bündeln wir in einem verfassten Verfahren auf gesetzlicher Grundlage zum Gesamtinteresse der gewerblichen Wirtschaft und tragen so zum wirtschaftspolitischen Meinungsbildungsprozess bei.

Grundlage unserer Stellungnahmen sind die wirtschaftspolitischen Positionen und beschlossenen Positionspapiere der DIHK unter Berücksichtigung der der DIHK bis zur Abgabe der Stellungnahme zugegangenen Äußerungen der IHKs und ihrer Mitgliedsunternehmen.

Darüber hinaus koordiniert die DIHK das Netzwerk der 150 Auslandshandelskammern, Delegationen und Repräsentanzen der Deutschen Wirtschaft in 93 Ländern.