bitkom

Stellungnahme

März 2026

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

Zusammenfassung

Der Cyber Resilience Act (CRA) ist ein zentraler Baustein der europäischen Digitalgesetzgebung und markiert einen entscheidenden Schritt hin zu einem einheitlichen Cybersicherheitsniveau im EU-Binnenmarkt. Ziel der Verordnung ist es, die Sicherheit digitaler und vernetzter Produkte über ihren gesamten Lebenszyklus hinweg zu gewährleisten und damit das Vertrauen in digitale Technologien nachhaltig zu stärken. Für Unternehmen in Deutschland und Europa bedeutet der CRA nicht nur zusätzliche regulatorische Anforderungen, sondern zugleich die Chance, ihre Wettbewerbsfähigkeit durch nachweislich sichere Produkte zu stärken.

Für den Erfolg des CRA kommt es entscheidend auf eine praxisnahe und innovationsfreundliche nationale Umsetzung an. Vor diesem Hintergrund ist es ausdrücklich zu begrüßen, dass der Entwurf zur CRA-Durchführung schlank ausgestaltet ist. Dieser Ansatz sollte im weiteren Verfahren konsequent beibehalten werden. Maßgeblich ist dabei, auf zusätzliche nationale Anforderungen zu verzichten und eine strikt europarechtskonforme Ausgestaltung sicherzustellen. Dies gilt insbesondere für nationale Erwartungshaltungen an die praktische Umsetzung, etwa mit Blick auf Inhalte und Tiefe von Software Bill of Materials (SBOM). Solche Anforderungen sollten sich eng an der CRA-Baseline sowie an EU-weit abgestimmten Leitlinien und Standards orientieren, um Fragmentierung und zusätzliche Lasten durch

divergierende nationale Auslegungen zu vermeiden. Nur so lassen sich Gold Plating und die damit verbundenen Wettbewerbsnachteile im Binnenmarkt vermeiden.

Ebenso wichtig ist der zügige Aufbau eines tragfähigen und wettbewerbsfähigen Prüfökosystems. Dieses sollte gezielt auf bestehenden IT-Sicherheitsprüfstellen, bewährten BSI-Strukturen und international anerkannten Standards aufsetzen, um effiziente und skalierbare Konformitätsbewertungen zu ermöglichen. Zugleich müssen die zuständigen Akteure die Digitalregulierung koordiniert ausgestalten, ressortübergreifend zusammenarbeiten, klare Zuständigkeiten festlegen und zu einer EU-weit harmonisierten Aufsichtspraxis beitragen. Nur so lassen sich Widersprüche, Doppelstrukturen und unnötige Belastungen für die Wirtschaft vermeiden. Für weiterführende Details wird auf die Bitkom-Position zur nationalen Umsetzung des CRA verwiesen.

Insgesamt ist jedoch anzuerkennen, dass die wesentlichen Hebel für eine praxistaugliche CRA-Umsetzung auf europäischer Ebene liegen. Die Bundesregierung sollte sich daher auf europäischer Ebene aktiv für die Interessen der deutschen Digitalwirtschaft einsetzen und auf konsistente Regelungs- und Standardisierungsprozesse im Rahmen des CRA hinwirken. Das ist eine wesentliche Voraussetzung, um ein höheres Sicherheitsniveau für Produkte mit digitalen Elementen in der Breite zu erreichen und zugleich die Wettbewerbsfähigkeit der Unternehmen sowie die Stabilität des digitalen Binnenmarkts langfristig zu sichern. Ergänzend wird hier auf die Bitkom-Position zur europäischen Umsetzung des CRA verwiesen.

Für weiterführende Details und konkrete Ausführungen wird im Folgenden auf einzelne Punkte aus dem vorliegenden Referentenentwurf eingegangen, bei denen noch Anpassungsbedarf besteht:

Erfüllungsaufwand für die Wirtschaft

Beim Erfüllungsaufwand für die Wirtschaft wird auf die geltende Verordnung (EU) 2024/2847 verwiesen. Es ist zutreffend, dass durch das deutsche Umsetzungsgesetz selbst keine zusätzlichen Kosten entstehen. Gleichwohl sollte berücksichtigt werden, dass bereits durch Zertifizierungen über Drittstellen, zu deren Kosten pro Produkt bislang keine Angaben vorliegen, sowie durch die Umstellung von Prozessen, Entwicklung und Herstellung erhebliche Aufwände entstehen. Für einzelne Bestandsprodukte und Produktportfolios kann die Umstellung im verbleibenden Zeitraum äußerst herausfordernd sein. Um Planbarkeit sicherzustellen, sind frühzeitige Klarheit durch EU-Leitlinien und -Standards, verlässliche Auslegung sowie ausreichende Prüf- und Konformitätsbewertungskapazitäten zentral.

§ 5 BSIG-E: Allgemeine Meldestelle für die Sicherheit in der Informationstechnik

Für eine sichere und effiziente Umsetzung der CRA Meldepflichten sollte die nationale Anbindung an die EU Meldeplattform praxistauglich und resilient ausgestaltet werden. Digitale Einreichwege (z. B. Web Portale) sollten ausdrücklich möglich sein, um die Meldestrecke gegen Spam /DoS Risiken abzusichern und eine skalierbare Bearbeitung bei hoher Fallzahl zu unterstützen.

§ 65 BSIG-E: Marktüberwachung

Der Gesetzentwurf lässt offen, wie das BSI mit Verbrauchermeldungen nach § 65 Abs. 3 umgeht. Betroffene Unternehmen sollten über solche Meldungen informiert werden, soweit die Beschwerde nicht offensichtlich unbegründet ist.

Dass Widerspruch und Klage nach § 65 Abs. 4 keine aufschiebende Wirkung entfalten, ist besonders eingriffsintensiv. Da einzelne Maßnahmen erhebliche bis existenzbedrohliche wirtschaftliche Folgen haben können, sollte das BSI verpflichtet werden, diese Folgen bei der Wahl seiner Maßnahmen angemessen zu berücksichtigen.

§ 66 BSIG-E: Notifizierung und Akkreditierung

Die Anzahl der Konformitätsbewertungsstellen bis Mitte 2027, besser noch bis Ende 2026, wird ein kritischer Faktor dafür sein, die erforderliche Zahl von Produkten CE-zertifizieren zu können. Vor diesem Hintergrund sollte das BMI im Zusammenspiel mit dem BSI als Marktaufsichtsbehörde einen klaren Schwerpunkt auf die ausreichende Verfügbarkeit von Konformitätsbewertungsstellen legen.

Wir sprechen uns daher gegen eine verpflichtende Akkreditierung notifizierter Prüfstellen unter dem CRA in Deutschland aus. Nationale Sonderregelungen sollten vermieden werden, um einheitliche Marktbedingungen und internationale Anschlussfähigkeit sicherzustellen. Hinzu kommt, dass eine verpflichtende Akkreditierung das Risiko von Engpässen bei der Notifizierung von Konformitätsbewertungsstellen birgt, insbesondere solange die Finanzierung der Deutschen Akkreditierungsstelle (DAkkS) und damit auch ihre personellen Ressourcen nicht nachhaltig gesichert sind.

§ 67 BSIG-E: Unterstützung der betroffenen Wirtschaftsakteure

§ 67 verweist ausdrücklich auf kleine und mittlere Unternehmen. Es ist nachvollziehbar und richtig, dass diese Unterstützung benötigen; dies gilt entsprechend auch für Vorgabe 4.3.6. Gleichwohl sollte das BSI seine Unterstützungsangebote an alle Wirtschaftsakteure richten. Gerade größere

Unternehmen entwickeln häufig eine breite Palette an Produkten, vielfach in mehreren Kategorien, und sind ebenfalls auf entsprechende Unterstützung angewiesen. Zugleich ist der hierfür angesetzte Aufwand von 17.600 Stunden für kleine und mittlere Unternehmen relativ hoch. Grundsätzlich sollte gelten: Wo Unterstützung und Vereinfachung verfügbar sind, sollten möglichst viele Akteure davon profitieren können, ohne dass das angestrebte Sicherheitsniveau darunter leidet. So kann die Bundesregierung ihrem Ziel nachkommen und „unsere Unternehmen bei der Umsetzung des Cyber Resilience Act zu unterstützen“ (Koalitionsvertrag, Seite 10).

Zwar wird klargestellt, dass kein Anspruch auf Individualberatung besteht. Angesichts des Aufwands insbesondere für Produkte mit erhöhtem Risiko wäre es jedoch sinnvoll, gezielte und priorisierte Unterstützungsangebote vorzusehen. Solche Unterstützungsangebote würden effizienteres Arbeiten ermöglichen und zugleich dem Ziel des Gesetzes dienen, Produkte möglichst zügig CRA konform zu machen und innerhalb der vorgesehenen Fristen auf den Markt zu bringen. Alternativ sollten hierfür skalierbare Unterstützungsformate (z. B. strukturierte Leitfäden, FAQ, regelmäßige Sprechstunden sowie ein transparenter Q&A Prozess) etabliert werden, um Interpretationsfragen effizient und einheitlich zu klären.

§ 67 sieht zudem die Einrichtung und den Betrieb eines Reallabors vor. Es sollte klarer definiert werden, wie und ab wann dieses von der Wirtschaft genutzt werden kann. Insbesondere sollten Zugangsvoraussetzungen, Antrags /Bewilligungsprozess, Kapazitäten sowie erwartbare Ergebnisse (z. B. Testberichte oder Orientierungshilfen) transparent beschrieben werden.

§ 70 BSIG-E: Behörden

Der Ausschluss von Geldbußen gegen Behörden und sonstige öffentliche Stellen birgt die Gefahr von Marktverzerrungen. Sofern diese Stellen Software selbst auf den Markt bringen, birgt dieses geringere Risiko jedenfalls die Gefahr, dass hergestellte Software eine geringere Cybersicherheit aufweist als gewünscht.

Bitkom vertritt mehr als 2.200 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie generieren in Deutschland gut 200 Milliarden Euro Umsatz mit digitalen Technologien und Lösungen und beschäftigen mehr als 2 Millionen Menschen. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig, kreieren Content, bieten Plattformen an oder sind in anderer Weise Teil der digitalen Wirtschaft. 82 Prozent der im Bitkom engagierten Unternehmen haben ihren Hauptsitz in Deutschland, weitere 8 Prozent kommen aus dem restlichen Europa und 7 Prozent aus den USA. 3 Prozent stammen aus anderen Regionen der Welt. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem leistungsfähigen und souveränen Digitalstandort zu machen.

Herausgeber

Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Ansprechpartner

Felix Kuhlenkamp | Leiter Sicherheit
T 030 27576-279 | f.kuhlenkamp@bitkom.org

Verantwortliches Bitkom-Gremium

AK Sicherheitspolitik