bitkom

Stellungnahme

Januar 2026

Cyber Resilience Act: Umsetzung auf nationaler Ebene

Der Cyber Resilience Act (CRA) ist ein zentraler Baustein der europäischen Digitalgesetzgebung und markiert einen entscheidenden Schritt hin zu einem einheitlichen Cybersicherheitsniveau innerhalb des EU-Binnenmarkts. 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 zu stärken. Für Unternehmen in Deutschland und Europa bedeutet dies nicht nur eine Ausweitung regulatorischer Pflichten, sondern zugleich eine Chance, die Wettbewerbsfähigkeit durch nachweislich sichere Produkte zu steigern.

Eine praxisorientierte und innovationsfreundliche CRA-Umsetzung ist von zentraler Bedeutung, um die intendierte Wirkung des Gesetzes zu entfalten, ohne übermäßige bürokratische Belastungen zu erzeugen oder den Binnenmarkt zu fragmentieren. Voraussetzung hierfür ist auch eine ausgewogene und praktikable Umsetzung auf nationaler Ebene. In Hinblick auf das bevorstehende deutsche Umsetzungsgesetz und die laufenden Umsetzungsfristen möchten wir die Gelegenheit nutzen, um auf vier Punkte für eine erfolgreiche Umsetzung des CRA auf nationaler Ebene hinzuwirken:

1. Vermeidung von »Gold Plating« durch eine strikt europarechtskonforme, einheitliche Umsetzung ohne nationale Zusatzanforderungen.
2. Aufbau eines tragfähigen, wettbewerbsfähigen Prüfökosystems durch Nutzung etablierter IT-Sicherheitsprüfstellen, bewährter BSI-Strukturen und international anerkannter Standards.
3. Koordinierte Digitalregulierung durch ressortübergreifende Abstimmung, klare Federführung und eine EU-weit harmonisierte Aufsichtspraxis.
4. Stärkung der deutschen Digitalwirtschaft durch ein aktives Eintreten für konsistente europäische Regelungs- und Standardisierungsprozesse im CRA zur Stärkung des Binnenmarkts.

Die Forderungen werden im Folgenden im Detail dargestellt. Entscheidend ist ein ausgewogenes Maß an Regulierungstiefe zu wahren, das einerseits die notwendige Qualität und Unabhängigkeit sicherstellt, andererseits aber die

59%

der deutschen Unternehmen halten Cyberattacken für existenzbedrohend (Bitkom, 2025).

Umsetzungsgeschwindigkeit und Wettbewerbsfähigkeit europäischer Anbieter nicht behindert. Nur auf dieser Basis kann der CRA erfolgreich umgesetzt und Europas digitale Souveränität im Bereich der IT-Sicherheit langfristig gestärkt werden.

Vermeidung von »Gold Plating« zur Sicherung des Binnenmarkts

Ein zentrales Anliegen der Digitalwirtschaft ist, dass die nationale Umsetzung keine zusätzlichen oder ggf. abweichenden Anforderungen enthält, die über die europäischen Vorgaben hinausgehen. Solche nationalen Sonderregelungen – häufig als »Gold Plating« bezeichnet – würden den einheitlichen europäischen Rechtsrahmen unterlaufen und zu Wettbewerbsnachteilen für Unternehmen in Deutschland führen. Gerade im Bereich der Cybersicherheit, der von grenzüberschreitenden Lieferketten und internationalen Wertschöpfungsnetzwerken geprägt ist, ist ein konsistentes Regelwerk innerhalb der EU unverzichtbar. Nur durch eine enge Abstimmung der Mitgliedstaaten und ihrer Marktüberwachungsbehörden können faire Wettbewerbsbedingungen für alle Marktteilnehmenden entstehen. Unterschiede in der Auslegung und Durchsetzung zwischen der Marktüberwachungsbehörde in einzelnen Mitgliedsstaaten müssen daher unbedingt vermieden werden.

Aufbau eines tragfähigen Prüfökosystems auf Basis bestehender Strukturen und Standards

Eine reibungslose Umsetzung des CRA setzt die hinreichende Notifizierung von Stellen oder bei der Durchführung von Konformitätsprüfungen voraus. Verzögerungen können erhebliche Auswirkungen auf Innovationszyklen, Markteinführungen und Investitionsentscheidungen haben. Unternehmen benötigen verlässliche und zeitnahe Verfahren, um ihre Produkte zügig und zu wettbewerbsfähigen Kosten zertifizieren und in den Markt bringen zu können. Neben geeigneten Verfahren ist ebenso der Aufbau eines skalierbaren und tragfähigen Ökosystems entscheidend, das die praktische Durchführung der Konformitätsbewertungen gewährleistet und auf den bereits bestehenden Strukturen und Kompetenzen in Deutschland aufbaut. Eine angemessene Ressourcenausstattung und klare Zuständigkeiten sind daher unerlässlich, um sowohl regulatorische Sicherheit als auch Effizienz sicherzustellen.

Es ist klar, dass eine hohe Anzahl an Konformitätsbewertungen notwendig sein wird, um den Anforderungen des CRA gerecht werden zu können. Die hierfür notwendige Expertise ist bereits bei den etablierten IT-Prüfstellen und IT-Sicherheitsdienstleistern vorhanden. Prüfstellen und Dienstleister werden seit über einem Jahrzehnt durch das BSI mit Hilfe der ISO/IEC 17025 als anerkannten Qualifizierungsmaßstab anerkannt. Die Norm ist international anerkannt und bietet die Grundlage für etablierte Systeme wie Common Criteria und NESAS/5G. Auf der Basis von ISO/IEC 17025 konnten bislang über zwanzig Unternehmen unterschiedlicher Größe akkreditiert und in das nationale Sicherheitsökosystem eingebunden werden. Dieses Ökosystem bietet eine bewährte

Grundlage, auf der weiter aufgebaut werden sollte und die für den CRA nutzbar gemacht werden sollte.

Um die operative Handlungsfähigkeit zum Start des CRA sicherzustellen, dürfen bestehende Dienstleister nicht durch zusätzliche bürokratische Hürden belastet werden. Jedoch steht aktuell eine Umstellung auf die Norm ISO/IEC 17065 im Raum. Diese würde jedoch erhebliche praktische und inhaltliche Probleme mit sich bringen: Nach der ISO/IEC 17065 wäre eine Konformitätsbewertungsstelle nicht berechtigt, Beratungsleistungen anzubieten. Gerade im Bereich der Cybersicherheit ist jedoch die Kombination aus Prüfung und Beratung essenziell, um Sicherheitsniveaus kontinuierlich zu verbessern und Schwachstellen effektiv zu beheben. Die meisten Prüfstellen bieten seit Jahrzehnten sowohl Prüf- als auch Beratungsleistungen an, ohne dass die Unabhängigkeit der Bewertung jemals beeinträchtigt worden wäre. Ein Verbot der Beratung wäre in diesem Umfeld kontraproduktiv. Eine erzwungene Umstellung auf die ISO/IEC 17065 würde erhebliche Kosten und überbordende Bürokratie verursachen und die gesamtgesellschaftlich notwendige Skalierung der Prüfinfrastruktur behindern. Neue Anbieter würden vor hohen Eintrittshürden stehen, da ein zentraler Resilienzbaustein – die beratende Begleitung – wegfallen würde. Als Konsequenz würde ein Flaschenhals bei den Prüfkapazitäten entstehen, der die Umsetzung des CRA erheblich gefährden könnte.

Darüber hinaus würde eine verpflichtende 17065-Akkreditierung die europäische Kohärenz gefährden. Während die ISO/IEC 17025 weltweit als technischer Kompetenzstandard anerkannt ist, stellt die 17065 lediglich eine generische Produktzertifizierungsnorm dar – ohne spezifische Ausrichtung auf IT-Sicherheitsprüfungen. Eine solche Abkehr von der 17025 würde die Anschlussfähigkeit an bestehende europäische Systeme (z. B. RED, AI Act, Common Criteria) schwächen und unnötige Doppelstrukturen schaffen. Besonders die führenden EU-Staaten im Bereich der IT-Sicherheitsprüfung – namentlich Deutschland, Frankreich, Spanien und die Niederlande – müssen ihre bestehenden Systeme aktiv und koordiniert in den europäischen Gesamtprozess einbringen.

Der Bitkom spricht sich daher klar dafür aus, auf die etablierten Standards – konkret die ISO/IEC 17025 – zu setzen und diese als Grundlage für die Konformitätsbewertung nach dem CRA zu verankern.

Koordinierte Umsetzung der Digitalregulierung unter einheitlicher Führung

Für eine kohärente nationale Umsetzung ist eine enge Abstimmung aller beteiligten Behörden einschließlich der Zollbehörden zur Importkontrolle erforderlich. Die Vielzahl aktueller und sich überschneidender EU-Regulierungen – vom CRA über die KI-Verordnung bis hin zu NIS2 und DORA – erfordert eine koordinierte Steuerung, idealerweise unter der Federführung des BMDS. Nur durch ein abgestimmtes Vorgehen können Widersprüche und Doppelanforderungen vermieden sowie Synergien zwischen den Regelwerken genutzt werden. Dabei sollte das BSI als Marktaufsicht die europäische Harmonisierung in den Vordergrund stellen und eine über die EU-

Vorgaben hinausgehende Auslegung vermeiden. Stattdessen sollte es durch engen Austausch mit anderen europäischen Marktaufsichten wie ANSSI eine EU-weit einheitliche Auslegung und Durchsetzung sicherstellen.

Stärkung der deutschen Digitalwirtschaft durch aktive europäische Positionierung im CRA-Prozess

Die Bundesregierung sollte sich auf europäischer Ebene aktiv für die Interessen der deutschen Digitalwirtschaft im Rahmen des CRA einsetzen. Eine solche Positionierung ist entscheidend, um die europäische Wettbewerbsfähigkeit zu sichern und den digitalen Binnenmarkt nachhaltig zu stärken. Voraussetzung hierfür ist eine konsistente und kohärente Ausgestaltung der europäischen Prozesse sowohl im Rechtsrahmen als auch in der begleitenden Standardisierung. Nur wenn Regulierung und Normung zeitlich, inhaltlich und prozedural aufeinander abgestimmt sind, kann der CRA seine Wirkung entfalten, ohne Innovationshemmnisse zu erzeugen oder Rechtsunsicherheit zu schaffen. Dies gilt auch für die internationale Dimension der Cybersicherheit: Um globale Fragmentierung zu vermeiden, muss die Bundesregierung auf eine Harmonisierung mit Drittstaat-Regulierungen wie dem britischen PSTI Act oder dem US-amerikanischen CIRCIA hinwirken, falls diese jeweils landesweit Gültigkeit und Wirkung haben und sich für die gegenseitige Anerkennung von Konformitätsbewertungen starkmachen. Die Bundesregierung sollte sich daher für transparente, industriepraktikable und EU-weit einheitliche Verfahren einsetzen und diese Positionen aktiv in die europäischen Gremien einbringen.

Für weitere Herausforderungen und Lösungsansätze verweisen wir ergänzend auf unsere englischsprachige Stellungnahme zum CRA (Bitkom, 2026).

Bitkom vertritt mehr als 2.300 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 700 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 +49 30 27576-279 | f.kuhlenkamp@bitkom.org

Verantwortliches Bitkom-Gremium

AK Sicherheitspolitik