Auf einen Blick

Cyber Resilience Act (CRA)

Ausgangslage

Der CRA zielt als Ergänzung zum Cybersecurity Act (CSA) darauf ab, den Marktbedürfnissen gerecht zu werden und digitale Produkte sicherer zu machenindem horizontale Cybersicherheitsregeln für Wirtschaftsakteure, insbesondere Hersteller von materiellen und immateriellen digitalen Produkten und Zusatzdiensten, eingeführt werden. Vor diesem Hintergrund steht eine wegweisende Regulierung auf EU-Ebene bevor, die uns als Digitalwirtschaft unmittelbar betrifft.

Bitkom-Bewertung

Geht in die richtige Richtung: Die Schaffung eines effizienteren Rechtsrahmens zur Verbesserung der Cybersicherheit wird von uns begrüßt. Der CRA bietet die Chance einen kohärenten Ansatz auf europäischer Ebene zu verfolgen, um regulatorische Lücken, die zu Sicherheitslücken in der digitalen Wertschöpfungskette führen, zu schließen und widersprüchliche bzw. sich überschneidende Vorschriften abzuschaffen.

Das Wichtigste

Aus Sicht des Bitkom sollte der CRA daher vorrangig die folgenden Ziele verfolgen:

- **Ausweitung des Geltungsbereiches der Sicherheitspflichten auf den Lebenszyklus digitaler Produkte**

  Digitale Produkte – Hardware, Software sowie die Kombination daraus – werden zu teils in hochgradig komplexen Systemen integriert. Folglich bedarf es in der Regulierung der Beachtung von Wechselwirkungen, um für digitale Infrastrukturen ein hohes Sicherheitsniveau über den gesamten Produktlebenszyklus gewährleisten zu können. Verpflichtungen müssen dort liegen, wo Gegenmaßnahmen am effizientesten greifen – im Zusammenspiel von Hersteller und Anwender. Dabei gilt es, sowohl Marktakteuren als auch Überwachungsbehörden gleichermaßen die notwendige Rechtssicherheit zu bieten.

- **Verbesserung der Konsistenz des rechtlichen Rahmens für Cybersicherheit nach den Grundsätzen des NLF**

  Eine Reduzierung der Komplexität zwischen verschiedenen, oft sektoralen Regulierungsansätzen durch die politische Option einer horizontalen Regulierung nach den Grundsätzen des NLF wird unterstützt. Die Verwendung harmonisierter Normen hat dabei eine lange und erfolgreiche Geschichte in der EU-Produktgesetzgebung im Rahmen des NLF.

- **Konsistenz der Anforderungen mit bestehenden Rechtsakten**

  Der CRA bietet die Möglichkeit, der Reduzierung der Komplexität zwischen verschiedenen, oft sektoralen, Regulierungsansätzen zur Cybersicherheit von Produkten und der Harmonisierung der Regulierungslandschaft unter einem zentralen, horizontalen, konsistenten und kohärenten Bezugspunkt.

- **Angleichung an internationale Anforderungen**

  Sollten nationale Normen bestehen, sollten diese an internationale Normen angeglichen werden, da diese umfassend validiert wurden und auf Konsens basierende Informationen und Anleitungen für die Definition und Umsetzung wirksamer Sicherheitsmethoden beruhen. Da die IKT-Normung bereits global angelegt ist, kann hier auf eine bestehende, bereits wirksame Normungsinfrastruktur zurückgegriffen werden.

Position des Bitkom

Durch die Ausweitung der Dienstleistungen im digitalen Bereich und die zunehmende Abhängigkeit von digitalen Produkten hat das Cyber-Risiko erheblich zugenommen. Auch wenn die Sicherheitsmaßnahmen an diese neuen Herausforderungen stetig angepasst werden, erfolgen die kriminellen Bemühungen immer raffinierter und zunehmend digital. Cybersicherheit ist daher eine zentrale Voraussetzung für eine erfolgreiche digitale Wirtschaft und Gesellschaft. Hieraus resultiert, dass Cybersicherheitsanforderungen durch eine wachsende Zahl bestehender oder vorgeschlagener Rechtsakte zur Regulierung von Produkten oder Organisationen schrittweise eingeführt wurden (z.B. Cyber Security Act, Funkanlagen-Richtlinie RED 2014/53/EU, Richtlinie über die Sicherheit von Netz- und Informationssystemen (*NIS-Richtlinie*) Richtlinie (EU) 2016/1148, Europäische Verordnung für Medizinprodukte MDR Verordnung (EU) 2017/745). Trotz dieser Bemühungen sehen wir, dass der Rechtsrahmen für den europäischen digitalen Markt weiterhin fragmentiert bleibt. Auch sehen sich die verschiedenen Wirtschaftsakteure einer unterschiedlichen Regulierung ausgesetzt. Die Bekämpfung der Cybersicherheit unter verschiedenen Voraussetzungen über mehrere Rechtsinstrumente hinweg führt unweigerlich zu Rechtsunsicherheiten und einer hohen, unnötigen Belastung für die Unternehmen. Folglich werden sich so weiterhin erhebliche Sicherheitslücken in der digitalen Wertschöpfungskette ergeben.

Angelina Marko
Fachreferentin
Industrie4.0 &
Technische Regulierung

T +49 30 27576-133
a.marko@bitkom.org

Bitkom e.V.
Albrechtstraße 10
10117 Berlin

Bitkom begrüßt daher die Initiative der EU-Kommission zur Schaffung eines effizienteren Rechtsrahmens für Cybersicherheit durch die Einführung von Rechtsvorschriften zu horizontalen Anforderungen. Aus unserer Sicht bietet der bevorstehende Cyber Resilience Act (CRA) der Europäischen Union die Gelegenheit, einen kohärenten Ansatz zu verfolgen. Bei diesem gilt es, klare, harmonisierte Regeln, die einem risikobasierten Ansatz folgen, zu definieren. Der CRA-Gesetzgebungsprozess bietet die Möglichkeit, die gesetzlichen Regelungen zu straffen und ihre Umsetzung effizienter zu gestalten. Deswegen sollte nicht nur die Verabschiedung einer zusätzlichen Regulierungsebene angestrebt werden, sondern auch widersprüchliche oder sich überschneidende Vorschriften in einem einzigen Rechtsakt zusammengeführt werden. Dabei sollte sich an international anerkannten Standards orientiert werden und übermäßig präskriptive Anforderungen und Unstimmigkeiten mit anderen EU-Rechtsvorschriften vermieden werden. Für den digitalen Binnenmarkt der EU, seine Unternehmen und Verbraucher bietet das derzeitige Gesetzgebungsverfahren die Gelegenheit, ein höheres Sicherheitsniveau zu erreichen, indem die regulatorischen Lücken in der Wertschöpfungskette geschlossen werden und die Regulierung effizienter und leichter anwendbar wird. Die Etablierung eines einzigen horizontalen CRA bietet darüber hinaus die Möglichkeit einer klaren und effektiven Marktüberwachung, welche für das Durchsetzen von Anforderungen der Cybersicherheit essentiell ist.

Die Verordnung muss mit großer Sorgfalt erarbeitet werden, da sie massive Auswirkungen auf den europäischen Binnenmarkt und seine Wettbewerbsfähigkeit haben wird.

Aus Sicht des Bitkom sollte der CRA daher vorrangig die folgenden Ziele verfolgen:

Ausweitung des Geltungsbereiches der Sicherheitspflichten auf den Lebenszyklus digitaler Produkte

Die Grundvoraussetzung für das störungsfreie Funktionieren von in hohem Maße digitalisierten Prozessen, vernetzen Produkten und Dienstleistungen ist ein hoher Grad an Cyber-Resilienz. Insbesondere gilt es zu beachten, dass Produkte – Hardware, Software sowie Kombination daraus – zu teils hochgradig komplexen Systemen integriert werden. Dies stellt eine rechtliche Herausforderung dar, da all diese Elemente in einem One-Fits-All-Ansatz sehr schwer abzudecken sein werden. Folglich bedarf es auch der Beachtung von Wechselwirkungen in der Regulierung. Ziel muss es sein, ein hohes Sicherheitsniveau für digitale Infrastrukturen für Verbraucher und Unternehmen zu gewährleisten. Dabei gilt es, sowohl Marktakteuren als auch Überwachungsbehörden gleichermaßen die notwendige Rechtssicherheit zu bieten. So sollte aus Sicht des Bitkom, ein einheitliches Paket von Cybersicherheitsvorschriften für alle Produkte bereitgestellt werden ohne dabei den Freiraum für eine effiziente und wirtschaftlich sinnvolle Umsetzung unangemessen einzuschränken, die derzeit der EU-Produktregulierung unterliegen. Dieser Ansatz sollte sämtliche IoT-Geräte umfassen, die für einer cybersichere Gesellschaft relevant sind. Insbesondere sollte sich der CRA in seinem Geltungsbereich daher ausschließlich auf vernetzte digitale Produkte fokussieren.

Bitkom ist der Auffassung, dass Hersteller von Hard- und Software schon heute prinzipiell verantwortungsvoll „Security-by-Design“ umsetzen. Jedoch können in einer dynamischen Bedrohungslandschaft Fixed-Point-in-Time Testbedingungen am Produkt die Sicherheit nur bedingt gewährleisten. Um den CRA zukunftssicher zu gestalten, muss der CRA grundlegende Sicherheitsziele festlegen, die auch über das Produkt selbst hinausgehen. Während der zu erwartenden Lebensdauer eines Produkts muss daher sichergestellt werden, dass regelmäßig Sicherheitsupdates zur Verfügung gestellt und vom Verwender installiert werden. Die Dauer des Lebenszyklus muss jedoch unbedingt vom Hersteller definiert werden und transparent an die Nutzer kommuniziert werden.

Die Stärkung des Bewusstseins und der Best Practices in Bezug auf Produktentwicklung, Schwachstellenmanagement und Transparenz über Sicherheitssoftware-Updates kann aus unserer Sicht große Sicherheitsrisiken reduzieren.

Verbesserung der Konsistenz des rechtlichen Rahmens für Cybersicherheit nach den Grundsätzen des NLF

Bitkom unterstützt die Option einer horizontalen Regulierung nach den Grundsätzen des New Legislative Framework (NLF) als wichtigen Schritt in Richtung eines harmonisierten und höheren Sicherheitsniveaus, mehr Rechtssicherheit sowie der Konsistenz auf dem gesamten digitalen Markt. Hierbei ist es erforderlich, die Kritikalität einer Komponente, eines digitalen Produkts sowie ihren Anwendungsbereich und den Grad ihrer Markteinführung zu bewerten. Aufbauend auf dem Verwendungszweck des Produkts und einer Risikobewertung können spezifischere Anforderungen oder anspruchsvollere Konformitätsbewertungsverfahren eingesetzt werden.

Die Auswahl oder Zuweisung von Konformitätsbewertungsverfahren für Produkte, die unter eine solche Verordnung fallen, muss daher sorgfältig geprüft werden. Der Beschluss 768/2008/EG bietet hierfür eine Vielzahl von unterschiedlichen Verfahren, aus denen der Gesetzgeber die geeigneten auswählen soll. Bitkom präferiert die Selbstbewertung durch den Hersteller, solange es keinen triftigen Grund für die verpflichtende Einschaltung einer Drittsteller (Hochrisiko) gibt. Bei Sicherheitsvorschriften in Form von harmonisierten Normen für Produkte hat sich gezeigt, dass es sich hierbei nachweislich um einen effizienten und risikobasierten Ansatz handelt, mit dem die Sicherheit für Verbraucher und andere Endnutzer gewährleistet werden kann. Die Verwendung harmonisierter Normen hat dabei eine lange und erfolgreiche Geschichte in der EU-Produktgesetzgebung im Rahmen des NLF. Der wesentliche Vorteil besteht darin, dass allgemeine rechtliche Anforderungen auf technischer Ebene detailliert beschrieben werden können, wodurch eine effektive Einbeziehung sektorspezifischer Bedürfnisse, zusätzlich zu den von der CRA festgelegten horizontalen Anforderungen, ermöglicht wird. Begründet auf dem breiten Spektrum des Anwendungsbereichs des CRA, empfiehlt Bitkom diesen Ansatz zu nutzen. Die Selbstbewertung unterstreicht dabei den Grundsatz, dass Hersteller die Sicherheit – in diesem Fall die Cybersicherheit – ihrer Produkte bestätigen und dafür verantwortlich sein müssen. Unternehmen, die sich dafür entscheiden, Dritte zur Konformitätsbewertung einzubeziehen, sollten ebenfalls die Möglichkeit dazu haben. Hierbei gilt es im CRA zu beachten, dass ein flexibler Mechanismus vorgesehen werden muss, um Doppelarbeit zu vermeiden und einen modularen Ansatz zur Nutzung von Konformitätsbewertungsverfahren zu gewährleisten. Dies gilt ebenso für Produkte und Anwendungsumgebungen, bei denen ergänzende oder höhere Anforderungen verlangt werden.

Wichtig ist es aus unserer Sicht somit auch, dass der CRA neben den grundlegenden Anforderungen an Produkte auch Verpflichtungen für Hersteller festlegen kann, die über die reine Produktfertigung hinausgehen. Dieser Ansatz steht im Einklang mit der Produktregulierung im Rahmen des New Legislative Framework (NLF) und trägt dem Konformitätsbedarf vor und nach dem Zeitpunkt des Inverkehrbringens oder der Inbetriebnahme von Produkten Rechnung.

Die Konformitätsbewertung – sowohl in selbstbestimmter Form als auch durch Dritte – kann aus unserer Sicht jedoch nur dann eine Zunahme der Cybersicherheit bewirken, wenn sie durch eine wirksame Marktüberwachung unterstützt wird. Die Reduzierung der Anzahl der unrechtmäßig handelnden Marktteilnehmer, welche sich durch ungenügende Konformitätsaufwendungen Wettbewerbsvorteile schaffen, ist von entscheidender Bedeutung zur Erreichung der Ziele. Sanktionen gegen nicht gesetzeskonform handelnde Marktteilnehmer müssen empfindlich sein und damit eine Abschreckungswirkung erzielen. Dies gilt auch für die beteiligten unabhängigen Konformitätsbewertungsstellen.

Konsistenz der Anforderungen mit bestehenden Rechtsakten

Es wird für die EU von entscheidender Bedeutung sein, die Kohärenz mit bestehenden, bevorstehenden und überarbeiteten sektoralen Rechtsvorschriften sicherzustellen. Derzeit ist die Gesetzeslandschaft durch eine Fragmentierung und das parallele Nebeneinander von nationalen und europäischen Cybersicherheitsgesetzen gekennzeichnet. Die Komplexität des Regulierungsumfelds wird noch dadurch erhöht, dass es keine klare Unterscheidung zwischen den Aufgaben und Pflichten der Hersteller, Verkäufer und Betreiber, der Definition von

Produkten und Diensten und ihren jeweiligen Verantwortlichkeiten in der Wertschöpfungskette gibt.

Bitkom sieht das Ziel in der Reduzierung der Komplexität zwischen verschiedenen, oft sektoralen, Regulierungsansätzen zur Cybersicherheit von Produkten und der Harmonisierung der Regulierungslandschaft unter einem zentralen, konsistenten und kohärenten Bezugspunkt. Cybersicherheitsanforderungen in anderen EU-Produktvorschriften müssen vermieden werden und bereits verabschiedete Rechtsvorschriften oder relevante Bestimmungen sollten ersetzt oder aufgehoben werden, als Beispiel sei hier der delegierte Rechtsakt zur Aktivierung der Artikel 3.3 d, e und f (Cybersecurity) der RED erwähnt.

Angleichung an internationale Anforderungen

Eine angemessene politische Option sehen wir in künftigen Vorschriften, die harmonisierte europäische Normen beinhalten. Dabei gilt es, eine Selbstbewertung als Standard-Konformitätsbewertungsverfahren festzulegen. Dies sollte durch die Möglichkeit ergänzt werden, für eine bestimmte Kategorie von Hochrisikoprodukten Bewertungen durch Dritte durchführen lassen zu müssen. Sollte es nationale Normen geben, sollten diese an internationale Normen angeglichen werden, da diese umfassend validiert wurden und auf Konsens basierende Informationen und Anleitungen für die Definition und Umsetzung wirksamer Sicherheitsmethoden beruhen. So kann sichergestellt werden, dass ein gemeinschaftlicher Ansatz für gemeinsame Herausforderungen genutzt wird, wodurch sich die globale Zusammenarbeit und Interoperabilität ermöglichen lässt.

Da die IKT-Normung bereits global angelegt ist und die Einbeziehung aller Beteiligten enorm wichtig ist, kann hier auf eine bestehende, bereits wirksame Normungsinfrastruktur mit ISO/IEC JTC1, CEN/CLC/JTC 13, ETSI TC CYBER und weiteren Gremien zurückgegriffen werden.

Bitkom vertritt mehr als 2.000 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie erzielen allein mit IT- und Telekommunikationsleistungen jährlich Umsätze von 190 Milliarden Euro, darunter Exporte in Höhe von 50 Milliarden Euro. Die Bitkom-Mitglieder beschäftigen in Deutschland mehr als 2 Millionen Mitarbeiterinnen und Mitarbeiter. 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 oder in anderer Weise Teil der digitalen Wirtschaft. 80 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils 8 Prozent kommen aus Europa und den USA, 4 Prozent aus anderen Regionen. 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 weltweit führenden Digitalstandort zu machen.

Bitkom e. V.

Albrechtstraße 10
10117 Berlin
T 030 27576-0
bitkom@bitkom.org

bitkom.org

bitkom