bitkom

Stellungnahme

Dezember 2024

Nationale Marktaufsichtsbehörde für den Cyber Resilience Act

Die Benennung der nationalen Marktaufsichtsbehörde für den Cyber Resilience Act (CRA) stellt einen zentralen Schritt für die effektive Umsetzung der Verordnung dar. Marktaufsichtsbehörden spielen im CRA eine tragende Rolle, indem sie die Sicherheit und Konformität von Produkten mit digitalen Elementen gewährleisten. Ihre Aufgaben umfassen nicht nur die Überwachung und Einhaltung der CRA-Anforderungen durch die Hersteller, Importeure, Distributoren o.ä., sondern auch die Koordination mit anderen Behörden auf nationaler und europäischer Ebene.

Der Bitkom spricht sich nachdrücklich für eine zentrale, nationale Aufsichtsbehörde aus. Eine sektorale Aufteilung der Zuständigkeiten würde das Risiko einer Fragmentierung schaffen, die sowohl für die Wirtschaft als auch für die Sicherheit der Verbraucher erhebliche Nachteile mit sich bringen könnte. Eine zentrale Stelle würde klare Zuständigkeiten und kohärente Standards für Unternehmen gewährleisten und die Effizienz der Marktüberwachung steigern. Die Behörde muss außerdem ausreichend mit Ressourcen ausgestattet sein sowie über ausreichend Erfahrung und Expertise verfügen, um ihre umfassenden Aufgaben wirksam erfüllen zu können. Dazu gehören unter anderem Leitlinienentwicklung, die jährliche Berichterstattung und die Durchführung von Kontrollmaßnahmen bei Verdacht auf Verstöße gegen den CRA. Zusätzlich ist die Harmonisierung von regulatorischen Vorgaben auf europäischer Ebene von entscheidender Bedeutung. Nur durch einheitliche Anforderungen und eine europäische Vernetzung kann gewährleistet werden, dass Unternehmen keine unnötigen Belastungen durch unterschiedliche Auslegungen erfahren und die Wettbewerbsbedingungen innerhalb der EU vergleichbar bleiben.

Aus unserer Sicht ist zudem eine klare Ablehnung der Schaffung einer neuen Behörde erforderlich, da dies zu zusätzlicher Bürokratie und unnötigen Kosten führen würde. Die Aufgaben der Aufsicht könnten mit Anpassungen und entsprechender Ressourcenstärkung von bestehenden Behörden übernommen werden. Insgesamt ist eine enge Zusammenarbeit der Aufsichtsbehörde mit anderen nationalen Behörden und Ministerien notwendig, um Überlappungen zu vermeiden und eine kohärente Umsetzung sicherzustellen. Dies ist besonders wichtig, da die regulatorische Landschaft bereits sehr komplex ist.

In Deutschland kommen dafür entweder das Bundesamt für Sicherheit in der Informationstechnik (BSI) oder die Bundesnetzagentur (BNetzA) in Frage, da beide über einschlägige Erfahrungen und Strukturen verfügen, die für die effektive Überwachung im Sinne des CRA genutzt werden können.

Bundesnetzagentur

Die BNetzA hat in den vergangenen Jahren als Marktüberwachungsbehörde in verschiedenen Bereichen ein hohes Maß an Kompetenz entwickelt. Hervorzuheben ist ihre Expertise in der Anwendung der Radio Equipment Directive (RED) und Regulierungen, wie etwa der Maschinenverordnung, wodurch umfassende Erfahrungen im Bereich der Produktaufsicht vorliegen. Mit der KI-Verordnung kommt nun die Aufsicht in einem weiteren Bereich hinzu, bei der eine Harmonisierung mit dem CRA von großer Bedeutung sein wird. Diese Tätigkeiten erlauben der BNetzA, die Einhaltung von Sicherheitsanforderungen auf Produktsicherheitsebene zu überwachen und gleichzeitig den Aufwand für regulierte Unternehmen gering zu halten.

Ein weiterer Vorteil der BNetzA liegt in ihrem starken Netzwerk innerhalb der Industrie, das durch langjährige Zusammenarbeit etabliert ist. Diese bestehenden Kontakte können insbesondere für die effektive Umsetzung des CRA von großer Bedeutung sein, da die BNetzA auf den offenen Dialog mit Herstellern und Importeuren setzt und bereits anerkannte Prozesse und Strukturen zur Kooperation mit der Wirtschaft vorweisen kann. Gerade im Hinblick auf die CRA-Vorgaben zur Produktkonformität ist eine solch enge und vertrauensvolle Zusammenarbeit mit der Wirtschaft ein wesentlicher Vorteil.

Allerdings gibt es bei der BNetzA auch Herausforderungen, die berücksichtigt werden sollten. Während die BNetzA als Marktüberwachungsbehörde über umfassende Kompetenzen und Erfahrungen verfügt, ist ihre spezifische Expertise im Bereich Cybersicherheit im Vergleich zum BSI weniger ausgeprägt. Die CRA-Umsetzung verlangt jedoch fundierte Kenntnisse in der Identifikation und Bewertung von Cybersicherheitsrisiken in digital vernetzten Produkten. In diesem Bereich könnte eine Aufstockung der entsprechenden Kapazitäten notwendig sein, damit die BNetzA die Cybersicherheitsanforderungen des CRA vollständig erfüllen kann.

Bundesamt für Sicherheit in der Informationstechnik

Das BSI ist die zentrale Cybersicherheitsbehörde in Deutschland und verfügt über umfassende Kompetenzen, die für die Aufsicht über den CRA relevant sind. Die Behörde ist bereits maßgeblich an der Ausgestaltung der Cybersicherheitsarchitektur in Deutschland beteiligt und verfügt über weitreichende Erfahrungen im Umgang mit Schwachstellenmanagement und der technischen Absicherung digitaler Produkte. Dazu zählen insbesondere bestehende Referate zum IT-Sicherheitskennzeichen und zur Marktaufsicht. Im Rahmen der NIS2-Richtlinie ist das BSI bereits als nationale Aufsichtsbehörde

tätig. Auch im Bereich der 5G-Zertifizierung wurden Strukturen und Fachkenntnisse aufgebaut, um ähnliche Anforderungen wie jene des CRA zu erfüllen.

Es ist positiv hervorzuheben, dass das BSI wiederholt betont hat, dass eine stärkere Integration von Maßnahmen zur Schwachstellenschließung erforderlich ist. Dies entspricht den Interessen der Wirtschaft, da Unternehmen auf klares, konsistentes und praxisorientiertes Vorgehen in der Cybersicherheit angewiesen sind. Die Kompetenz des BSI in der Schwachstellenanalyse und seine bereits bestehenden Kontakte zu Betreibern kritischer Infrastrukturen, die unter die NIS2-Regulierung fallen, sind daher relevante Argumente, die das BSI als geeignete nationale Aufsichtsbehörde für den CRA qualifizieren würden.

Neben seiner Rolle in der deutschen Sicherheitsarchitektur ist das BSI auch aktiv bei der Standardisierung von Cybersicherheitsmaßnahmen beteiligt. Auf nationaler Ebene entwickelt es eine Strategie zur Vorbereitung und Beteiligung von betroffenen Unternehmen. . Auf europäischer Ebene arbeitet das BSI in der Arbeitsgruppe von CEN-CENELEC, dem europäischen Standardisierungsgremium, mit. Dies stärkt einerseits die fachliche Expertise und ermöglicht eine starke Positionierung in Europa. Es muss allerdings auch bedacht werden, dass die doppelte Rolle aus Normungsgeber und Aufsichtsbehörde teils zu erheblichen Interessenskonflikten führen kann. Die exekutive Rolle des BSI als notifizierende Behörde im Rahmen von CRA, Cyber Security Act und EU Cybersecurity Certification Scheme on Common Criteria verschärft dies noch. Jegliche Bedenken sind hier durch klare Zuständigkeitstrennung auszuräumen.

Insgesamt ist für die erfolgreiche Umsetzung des CRA eine zentrale, leistungsfähige Marktaufsichtsbehörde erforderlich, die die Konformität und Sicherheit digitaler Produkte in Deutschland gewährleistet. Bitkom empfiehlt daher, das BSI oder die BNetzA zu beauftragen, da eine dieser bestehenden Behörden die CRA-Überwachung ohne die Schaffung übermäßiger Bürokratie übernehmen könnte. Beide bringen relevante Kompetenzen mit; die endgültige Entscheidung sollte sich jedoch an der Frage orientieren, welche Behörde am besten in der Lage ist, Cybersicherheitsanforderungen in Einklang mit den CRA-Zielen umzusetzen. Langfristige Unklarheit über die Zuständigkeit muss vermieden werden, da sie dazu führt, dass Deutschland nicht aktiv an der Ausgestaltung der Standards und Konformitätsanforderungen beteiligt ist. Da die Arbeiten an diesen Standards bereits in vollem Gange sind und nicht auf Entscheidungen warten, besteht die Gefahr, dass nationale Interessen unzureichend berücksichtigt werden.

Ein enger Dialog zwischen Aufsichtsbehörde, Wirtschaft, Ministerien und weiteren Behörden wird entscheidend sein, um die Umsetzung praxisnah und wirtschaftsfreundlich zu gestalten. Dazu gehört insbesondere eine enge Zusammenarbeit zwischen der BNetzA und dem BSI, unabhängig von der Benennung der nationalen Marktaufsichtsbehörde. Im Sinne der Hersteller muss eine ausgewogene Balance angestrebt werden, bei der Sicherheits-, Wirtschafts- und Gesellschaftsinteressen gleichermaßen berücksichtigt werden.

Sicherheitsanforderungen sollten so gestaltet sein, dass sie nicht nur den Schutz digitaler Produkte stärken, sondern auch die wirtschaftliche Wettbewerbsfähigkeit sichern. Dazu zählt die Vermeidung doppelter Prüfungen und Zertifizierungen entlang der Wertschöpfungskette. Auf EU-Ebene ist es entscheidend, einheitliche Wettbewerbsbedingungen zu schaffen, um zu verhindern, dass der Standort Deutschland durch übermäßig strenge Regelungen einen Wettbewerbsnachteil erleidet. Die zukünftige Aufsichtsbehörde muss regulatorischen Anforderungen mit wirtschaftlichen Interessen in Einklang bringen, um für den Erfolg des CRA zu sorgen.

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 | Referent Sicherheitspolitik

T 030 27576-279 | f.kuhlenkamp@bitkom.org

Verantwortliches Bitkom-Gremium

AK Sicherheitspolitik