BDI INNONATION

STELLUNGNAHME | DIGITALPOLITIK | CYBERSICHERHEIT

CRA-Durchführungsgesetz

Stellungnahme der deutschen Industrie zum Referentenentwurf des Bundesministeriums des Innern

13. April 2026

Executive Summary

Die Zunahme der Quantität und Intensität von Cybercrime erhöhen die Notwendigkeit, dass alle Produkte mit digitalen Elementen risikoadäquate Cybersicherheitsanforderungen erfüllen. Die deutsche Industrie unterstützt daher grundsätzlich das Ziel des Cyber Resilience Acts (Verordnung (EU) 2024/2847) (CRA), horizontal verpflichtende Anforderungen an die Cybersicherheit von Produkten mit digitalen Elementen einzuführen. Für die wirksame Umsetzung des CRA ist es zwingend erforderlich, dass jeder Mitgliedstaat mindestens eine Marktüberwachungsbehörde und eine notifizierende Behörde benennt. Den vorliegenden Referentenentwurf begrüßt die deutsche Industrie daher grundsätzlich, da er die Umsetzung des CRA konsequent vorantreibt.

Die deutsche Industrie implementiert heute bereits bei Produkten mit digitalen Elementen ein hohes Sicherheitsniveau durch risikoadäquate Cyberresilienzmaßnahmen. Für eine praxistaugliche Umsetzung des CRA empfehlen wir:

- **Marktaufsicht mit ausreichenden Kapazitäten:** Eine starke und fachkundige Marktüberwachung ist ein elementarer Bestandteil einer wirksamen Durchführung des CRA und wird somit vom BDI ausdrücklich unterstützt. Es gilt zu prüfen, inwiefern der vorgesehene Aufwuchs um 114 Planstellen hierfür ausreichend ist. Eine nur punktuelle oder selektive Marktüberwachung würde dazu führen, dass sich regelkonforme Hersteller einem Wettbewerbsnachteil gegenüber solchen Marktakteuren ausgesetzt sehen, die die regulatorischen Anforderungen nicht oder nur unzureichend erfüllen.
- **Funktionale Trennung und Governance im BSI sicherstellen:** Marktüberwachung, CSIRT-Aufgaben, Notifizierung, Unterstützungsmaßnahmen sowie Bewertung und Aufsicht von Konformitätsbewertungsstellen müssen klar voneinander getrennt sein.
- **Unterstützungsmaßnahmen für die Wirtschaft:** Ebenso erachten wir die im Referentenentwurf vorgesehenen Unterstützungsmaßnahmen für betroffene Wirtschaftsakteure – etwa durch Sensibilisierungs- und Schulungsangebote oder die Einführung eines Reallabors für Cyberresilienz – als sehr positiv. Insbesondere in der frühen Umsetzungsphase sowie auch über einen längeren Zeitraum für kleine und mittlere Unternehmen (KMU) können solche Maßnahmen die Implementierung der CRA-Anforderungen deutlich erleichtern.
- **Praxisorientierte Weiterentwicklung des CRA auf EU-Ebene:** Neben den vorgesehenen Unterstützungsmaßnahmen erachtet die deutsche Industrie jedoch eine praxisgerechte Ausgestaltung und Weiterentwicklung des Cyber Resilience Acts auf europäischer Ebene als darüberhinausgehenden notwendigen Schritt.

Bundesverband der Deutschen Industrie e.V.
Steven Heckler | Senior Referent Cybersicherheit und Digitale Unternehmensidentitäten | s.heckler@bdi.eu | www.bdi.eu

Inhaltsverzeichnis

Bewertung im Detail

Stärkung des Bundesamts für Sicherheit in der Informationstechnik

Der BDI unterstützt die personelle und finanzielle Stärkung des Bundesamts für Sicherheit in der Informationstechnik (BSI). Nur durch eine adäquate Ausstattung kann das BSI die zusätzlichen Aufgaben in angemessenem Maße implementieren.

Das BSI ist bereits heute institutionell und operativ in europäische Cybersecurity-Zertifizierungs- und Bewertungsstrukturen eingebunden. Sollten europäische Cybersicherheitszertifizierungsschemata wie EUCC künftig stärker für CRA-Konformitätsbewertungen und damit für den Marktzugang an Bedeutung gewinnen, steigen die Anforderungen an eine funktional saubere Trennung innerhalb des BSI. Je enger Aufsichts-, Notifizierungs-, Bewertungs- und Unterstützungsfunktionen zusammengeführt werden, desto wichtiger werden belastbare institutionelle Sicherungen. Aus Sicht der deutschen Industrie ist deshalb sicherzustellen, dass innerhalb des BSI eine wirksame organisatorische, personelle und verfahrensmäßige Trennung dieser Funktionen vorgesehen wird.

Marktüberwachung (§ 65)

Um sicherzustellen, dass alle Marktakteure die Anforderungen des CRA umsetzen, ist eine konsequente Marktüberwachung zwingend erforderlich. Als nationale Cybersicherheitsbehörde ist das BSI bestens geeignet, die Marktüberwachung im engen Zusammenspiel mit privatwirtschaftlichen Akteuren mit adäquater technischer Expertise umzusetzen. Nur durch eine wirksame Marktüberwachung können unlautere Praktiken von Wirtschaftsakteuren geahndet und damit ein fairer Wettbewerb gewährleistet werden.

Eine wirksame Marktüberwachung im Bereich des CRA erfordert ein EU-weites Level-Playing-Field. Die derzeitige Rechtslage ist durch ein komplexes Geflecht digitaler Rechtsvorschriften (CRA, NIS2, CSA, KI-Gesetz usw.) gekennzeichnet, was zu unterschiedlichen nationalen Umsetzungen und Auslegungen führt. Die unterschiedlichen Ressourcen und Kompetenzniveaus der nationalen Marktüberwachungsbehörden führen für Hersteller aktuell zu einer „Postleitzahlenlotterie“, da es je nach Mitgliedstaat uneinheitliche Aufsichten gibt. Diese ungleiche Durchsetzung untergräbt die Ziele des CRA. Eine Harmonisierung ist zwingend erforderlich.

Darüber hinaus sollte die Europäische Union ein Lead-Authority-Prinzip einführen, analog zur DSGVO. Die Marktüberwachung würde dabei durch eine einzige federführende Behörde erfolgen – basierend auf dem Sitz des Herstellers oder des EU-Bevollmächtigten. Dies würde die gegenwärtige Fragmentierung beseitigen, Mehrfachverfahren vermeiden und die regulatorische Belastung insbesondere für Unternehmen, die Produkte in mehreren Mitgliedstaaten vertreiben, erheblich reduzieren.

Die Beseitigung der derzeitigen Ungleichheiten bei der CRA-Marktüberwachung erfordert einen harmonisierten Ansatz. Erstens sind gemeinsame Auslegungsleitlinien und standardisierte Umsetzungsrahmen von entscheidender Bedeutung, um nationale Abweichungen im Bereich der Ratingagenturen und der damit überschneidenden digitalen Rechtsvorschriften zu minimieren. Zweitens muss die EU die notwendigen Initiativen zum Aufbau von Ressourcen und Kompetenzen fördern, möglicherweise durch eine zentrale EU-Stelle oder koordinierte nationale Bemühungen. Dazu gehören zweckgebundene Finanzmittel, grenzüberschreitende Schulungsprogramme sowie die Einrichtung gemeinsamer technischer Toolkits. Drittens würden regelmäßige Peer-Reviews der nationalen Überwachungsergebnisse eine einheitliche Durchsetzung gewährleisten und Regulierungsarbitrage verhindern, wodurch letztlich wirklich gleiche Wettbewerbsbedingungen für die Marktüberwachung von Ratingagenturen in der gesamten EU geschaffen würden. Um die Rechtssicherheit weiter zu erhöhen, sollte Herstellern zudem ermöglicht werden, innerhalb der EU frei eine zuständige Marktüberwachungsbehörde auszuwählen, sofern diese Funktion nicht bereits kraft EU Rechts aufgrund des Lead Authority Prinzips zugewiesen wurde. Das Bundesministerium des Innern sollte sich gegenüber der Europäischen

Kommission und der Europäischen Cybersicherheitsagentur ENISA für Maßnahmen zur stärkeren Harmonisierung der CRA-Marktüberwachung einsetzen. Gleiche Wettbewerbsbedingungen würden den europäischen Binnenmarkt nachhaltig fördern.

Notifizierung und Akkreditierung (§ 66)

Die deutsche Industrie unterstützt den Vorstoß des Bundesministeriums des Innern, dass das BSI als Deutschlands oberste Cybersicherheitsbehörde für die Notifizierung und Akkreditierung von Konformitätsbewertungsstellen fungiert.

Unterstützung der betroffenen Wirtschaftsakteure (§ 67)

Die deutsche Industrie begrüßt grundsätzlich die Bereitschaft des Gesetzgebers, Wirtschaftsakteure bei der Implementierung des CRA zu unterstützen. Gleichwohl erachten wir die vorgesehenen Maßnahmen sowie deren Fokussierung auf kleine und mittlere Unternehmen als nicht ausreichend.

Damit das Reallabor „Cyberresilienz“ die vom Gesetzgeber intendierte erleichternde Wirkung für Wirtschaftsakteure entfalten kann und Unternehmen eine Möglichkeit zum Testen innovativer Ansätze in einem geschützten Rahmen bietet, ist es zwingend erforderlich, dass das BMI und BSI unter enger Einbeziehung der Wirtschaft das Reallabor aufbauen.

Zudem ist sicherzustellen, dass Kriterien für den verpflichtenden oder freiwilligen Einsatz des Reallabors EU weit harmonisiert werden. Hersteller sollten frei ein Reallabor innerhalb der EU wählen oder selbst bereitstellen können, sofern es über eine europäische Akkreditierung verfügt oder von einem akkreditierten Test House akzeptiert wird, um Doppelprüfungen und nationale Sonderanforderungen zu vermeiden.

Neben dem in Paragraf 67 genannten Maßnahmen, würde die deutsche Industrie insbesondere eine Bereitschaft der Bundesregierung, sich für notwendige gesetzliche Anpassungen am CRA einzusetzen, begrüßen. Konkrete Vorschläge hierfür unterbreiten wir im untenstehenden Kapitel (Weiterentwicklung des CRA).

Weiterentwicklung des CRA

Der BDI würde es begrüßen, wenn sich die Bundesregierung neben der Umsetzung der rechtlichen Anforderungen des CRA im Rahmen des Digital-Omnibusses und des Digital Fitness Checks für eine praxisorientierte Ausgestaltung des CRA einsetzen würde. Insbesondere erachten wir als notwendig:

Übergangsfrist

Um eine wirksame und praxisnahe Umsetzung der CRA zu gewährleisten, ist es unerlässlich, dass sich die Bundesregierung gegenüber der Europäischen Kommission – in enger Zusammenarbeit mit den europäischen Normungsorganisationen (ESOs) sowie technischen Expertinnen und Experten aus der Industrie – für realistische und technisch fundierte Zeitpläne für die Entwicklung und Bereitstellung harmonisierter Normen im Rahmen der CRA einsetzt.

Dies gilt insbesondere für die vertikalen, produktspezifischen Normen, die die Konformitätsvermutung mit den grundlegenden Anforderungen der CRA ermöglichen. Diese Normen sind nicht einfach nur Umsetzungsinstrumente. Vielmehr bilden sie eine integrale Rechtsgrundlage für den Nachweis der Konformität, insbesondere für Produkte mit digitalen Elementen, die gemäß Anhang III (Klasse I) als „wichtig“ eingestuft sind, bei denen andernfalls eine Konformitätsbewertung durch Dritte vorgeschrieben wäre.

Daher muss sichergestellt werden, dass zwischen der formellen Veröffentlichung der relevanten harmonisierten Normen im Amtsblatt der Europäischen Union und dem Ende der Übergangsfrist für die

Umsetzung der CRA mindestens 36 Monate vergehen. Nur dieser Zeitrahmen bietet den Herstellern die notwendige Rechtssicherheit und operative Durchführbarkeit, um die Anforderungen der CRA sinnvoll in die Produktentwicklungs- und Produktionsprozesse zu integrieren.

Einführung und Ausschluss von „harmlosen digitalen Produkten mit digitalen Elementen" (Artikel 2 und 3)

Viele vernetzte Produkte – wie DAB-Radios, Fahrradcomputer, Radiowecker, Barcode-Scanner, Analog-Digital-Wandler oder integrierte Mikrochips – stellen kein nennenswertes Cybersicherheitsrisiko dar. Obwohl sie Daten übertragen und somit in den Geltungsbereich des CRA fallen, handelt es sich bei diesen Daten ausschließlich um unbedeutende Informationen, die oft innerhalb eines einzigen Geräts verarbeitet werden. Auch wenn die CRA aufgrund der praktisch nicht vorhandenen Cybersicherheitsrisiken keine zusätzlichen Cybersicherheitsmaßnahmen vorschreibt, müssen diese Produkte mit digitalen Elementen dennoch die formelle Konformitätsbewertung nach NLF durchlaufen, um die Einhaltung aller CRA-Anforderungen in Bezug auf Prozesse, Dokumente und Kennzeichnung nachzuweisen. Folglich entstehen ohne Untergrenzen für solche „harmlosen Produkte" Kosten, die keinen erkennbaren Nutzen für den Hersteller, den Kunden oder die Gesellschaft haben.

Um diesem Ungleichgewicht entgegenzuwirken, schlagen wir vor, im Rahmen der CRA eine spezifische Ausnahmeregelung für „von Natur aus unbedenkliche Produkte" einzuführen. Diese Kategorie würde für Produkte gelten, die aufgrund ihrer technischen Einfachheit kein Cybersicherheitsrisiko darstellen können (und bei denen zudem keine sinnvollen Cybersicherheitsmaßnahmen umgesetzt werden können). Beispiele hierfür sind einfache Sensoren, passive elektronische Bauteile oder einfache Schaltgeräte. Ein Präzedenzfall für einen solchen Ansatz findet sich in Erwägungsgrund 12 der EMV-Richtlinie (2014/30/EU), der sich auf Produkte bezieht, die „hinsichtlich der elektromagnetischen Verträglichkeit von Natur aus unbedenklich" sind. Eine ähnliche Formulierung – „hinsichtlich der Cybersicherheit von Natur aus unbedenklich" – wäre im Kontext der CRA angemessen und sinnvoll.

Darüber hinaus sollten Produkte, die unter diese Kategorie fallen, ausdrücklich von komplexen Dokumentations-, Kennzeichnungs- und Meldepflichten entlastet werden, um Ressourcen auf risikobehaftete Produktkategorien zu konzentrieren.

Um Rechtssicherheit zu gewährleisten und eine Umgehung der Verordnung zu verhindern, schlagen wir folgende Definition vor:

Artikel 3(4a): *"benign product" means a product which cannot cause a cybersecurity risk because it is technically too limited to do so.*

Weitere Klarstellungen zum Geltungsbereich und zur Anwendung dieser Kategorie könnten durch Durchführungsleitlinien oder delegierte Rechtsakte erfolgen. So würde eine einheitliche Auslegung und Durchsetzung gewährleistet werden. Die Einführung dieser Ausnahmeregelung würde die Verhältnismäßigkeit der Regulierung stärken und gleichzeitig die Ziele der Cybersicherheit wahren.

Unbegrenzte Überwachungs- und Berichtspflichten (Artikel 14, Artikel 69 Absatz 3)

Im Gegensatz zu den Verpflichtungen im Bereich des Schwachstellenmanagements, die spätestens mit Ablauf des letzten Supportzeitraums enden, gelten die Verpflichtungen zur Überwachung von Produkten und zur Meldung aktiv ausgenutzter Schwachstellen sowie schwerwiegender Vorfälle auf Dauer. Darüber hinaus gelten diese Überwachungs- und Meldepflichten auch für bestehende Produkte, die vor Inkrafttreten der CRA auf den Markt gebracht wurden (vgl. Art. 69 Abs. 3). Dies stellt eine unverhältnismäßige Belastung dar, insbesondere für langjährige Marktteilnehmer mit vielen neuen und vor allem vielen älteren Produkten.

Derzeit verpflichtet der CRA Hersteller dazu, jede aktiv ausgenutzte Schwachstelle oder jeden schwerwiegenden Vorfall zu melden, von dem sie Kenntnis erlangen, selbst wenn die Schwachstelle keine

Auswirkungen auf Produkte oder Dienste hat, die innerhalb der Union bereitgestellt werden. Dies kann zu unnötigen Meldungen von Problemen führen, die keine Auswirkungen auf Nutzerinnen und Nutzer in der EU haben.

Um den mit dem CRA verbundenen Verwaltungsaufwand zu verringern, sollte der Überwachungs- und Berichtszeitraum befristet sein und nach Ablauf des Unterstützungszeitraums enden.

Hersteller sollten nur dann verpflichtet sein, ausgenutzte Sicherheitslücken und schwerwiegende Vorfälle zu melden, wenn die Sicherheitslücke oder der Vorfall die Sicherheit oder Funktionalität von Produkten mit digitalen Elementen innerhalb der Union wesentlich beeinträchtigt. Dies würde die Verhältnismäßigkeit gewährleisten und den Verwaltungsaufwand verringern, während gleichzeitig ein starker Schutz für Verbraucher und Systeme in der Union gewahrt bleibt.

Artikel 14:

1. A manufacturer shall notify any actively exploited vulnerability contained in the product with digital elements *affecting users in the Union* that it becomes aware of simultaneously to the CSIRT designated as coordinator, in accordance with paragraph 7 of this Article, and to ENISA. The manufacturer shall notify that actively exploited vulnerability via the single reporting platform established pursuant to Article 16.

Anerkennung bestehender Industriestandards für Konformitätsbewertung

Die europäische Industrie hat mehrere weltweit anerkannte Sicherheitsstandards wie EMVCo und GSMA eSA etabliert. Gleichzeitig erteilt die Europäische Kommission im Rahmen des CRA Normungsaufträge. Etablierte Industriestandards müssen für Konformitätsbewertungen im Rahmen des CRA direkt anerkannt werden, ohne dass sie in europäische Normen umgewandelt werden müssen, um den bürokratischen Aufwand zu verringern und die Umsetzung des CRA zu beschleunigen.

Definition des Begriffs „Kenntniserlangung“ von einer aktiv ausgenutzten Sicherheitslücke und einem schwerwiegenden Vorfall (Artikel 14)

Derzeit verpflichtet der CRA Hersteller dazu, Meldung zu erstatten, sobald sie von einer aktiv ausgenutzten Sicherheitslücke und einem schwerwiegenden Vorfall „Kenntnis erlangen“, definiert jedoch nicht, was unter „Kenntniserlangung“ zu verstehen ist. Diese Unklarheit führt zu Rechtsunsicherheit und birgt das Risiko vorzeitiger oder uneinheitlicher Meldungen auf der Grundlage unbestätigter Vermutungen. Der NIS2-Durchführungsrechtsakt 2024/2690, Erwägungsgrund 31, enthält eine detaillierte Definition und einen Leitfaden für das „Kenntnis erlangen“ bei schwerwiegenden Vorfällen. Da die Mehrheit der europäischen Unternehmen im verarbeitenden Gewerbe beide Verpflichtungen erfüllen muss, sollte dieser bereits vereinbarte Leitfaden für die CRA-Verpflichtungen zur Meldung verschiedener Vorfälle und aktiv ausgenutzter Schwachstellen gefördert werden. Der Leitfaden sieht das „Kenntnis erlangen“ nach einer zeitnahen ersten Bewertung vor.

Darüber hinaus sollte der Begriff der „aktiv genutzten Schwachstelle“ präzisiert werden. Er sollte nur dann als erfüllt gelten, wenn hinreichend belastbare Hinweise aus Incident Reports, Threat-Intelligence oder CERT-Warnungen vorliegen, dass eine Schwachstelle tatsächlich ausgenutzt wird – nicht lediglich theoretisch ausnutzbar wäre.

Die Definition von „Kenntniserlangung“ als ein angemessenes Maß an Gewissheit des Herstellers auf der Grundlage ausreichender und zuverlässiger Informationen stellt sicher, dass Meldungen nur dann ausgelöst werden, wenn eine fundierte Grundlage vorliegt und nicht aufgrund bloßer vorläufiger Anzeichen. Der Prozess sollte eine zeitnahe Bewertung durch den Hersteller hinsichtlich Schweregrad, Art und Ausnutzung von Vorfällen und Schwachstellen vorsehen. Dieser Ansatz steht im Einklang mit dem Grundsatz der Verhältnismäßigkeit, unterstützt ein wirksames Vorfall- und Schwachstellen-

management und spiegelt die etablierte Regulierungspraxis in ähnlichen Kontexten wider, wodurch die Rechtssicherheit verbessert und unnötige Compliance-Belastungen verringert werden.

11. *With regard to the first paragraph, when a manufacturer has detected a suspicious event or vulnerability, or after a potential incident or vulnerability has been brought to its attention by a third party, such as an individual, a customer, an entity, an authority, a media organisation, or another source, the manufacturer should assess in a timely manner the suspicious event or vulnerability to determine whether it constitutes an incident or vulnerability and, if so, determine its nature and severity or exploitation. The relevant entity is therefore to be regarded as having become 'aware' of the severe incident or actively exploited vulnerability when, after such initial assessment, the manufacturer has a reasonable degree of certainty that a severe incident has occurred or a vulnerability is actively exploited.*

Berichtspflichten

Derzeit unterscheiden sich die Meldepflichten je nach Rechtsakt. Dies führt zu einem unnötigen Verwaltungsaufwand für die betroffenen Unternehmen.

Um doppelte Meldeprozesse zu vermeiden, sollten die Meldepflichten gemäß CRA, NIS-2, DORA und DSGVO vollständig harmonisiert werden. Folglich begrüßt die deutsche Wirtschaft den Vorschlag der Europäischen Kommission, ein Single Entry Point for Incident Reporting (SEP) im Rahmen von NIS-2, DORA, CER und eIDAS einzurichten, da dies den bürokratischen Aufwand aufgrund von Meldepflichten erheblich reduzieren wird. Wir unterstützen das Prinzip „Einmal melden, vielfach nutzen". Die Meldung von Vorfällen über ein SEP kann die Erstellung eines täglichen Lageberichts erleichtern, was privaten Einrichtungen und öffentlichen Institutionen helfen würde, Cyberangriffen entgegenzuwirken und damit die Widerstandsfähigkeit Europas zu stärken. Es ist jedoch ein noch ehrgeizigerer Ansatz erforderlich, der auch die CRA einbezieht und die Meldepflichten selbst harmonisiert.

Insbesondere sollte der SEP auch die Meldepflichten aus dem CRA vollständig integrieren. Die Plattform sollte Meldungen automatisch an die zuständigen Marktüberwachungsbehörden, ENISA und CSIRTs verteilen. Dies würde eine echte „Einmal melden, vielfach nutzen"-Struktur schaffen und Unternehmen vor redundanten Meldeprozessen in mehreren Mitgliedstaaten schützen.

Zur Verbesserung der Effizienz sollte das Meldeverfahren auf zwei Schritte gestrafft werden: eine Erstmeldung innerhalb von 72 Stunden mit den wesentlichen Informationen und ein umfassender Bericht innerhalb von 14 Tagen nach der Korrekturmaßnahme. Alle Berichte sollten nur einmal auf EU-Ebene eingereicht werden, idealerweise über die ENISA-Plattform, um parallele Prozesse zu vermeiden. Darüber hinaus sprechen wir uns dafür aus, die vereinfachten Dokumentationsanforderungen für KMU auf alle Hersteller anzuwenden.

Impressum

Bundesverband der Deutschen Industrie e.V. (BDI)
Breite Straße 29
10178 Berlin
www.bdi.eu
T: +49 30 2028-0

EU-Transparenzregister: 1771817758-48

Lobbyregister: R000534

Autor
Steven Heckler
Senior Referent Cybersicherheit und Digitale Unternehmensidentitäten
T: +49 30 2028-1523
s.heckler@bdi.eu

BDI-Dokumentennummer: D 2260