zvei
electrifying ideas

Cyber Resilience Act

Cybersicherheit stärken, Lieferketten und Innovationskraft sichern

Mit dem Cyber Resilience Act (CRA) schafft die EU einen horizontalen Rechtsrahmen für die Cybersicherheit von vernetzten Produkten – sog. Produkten mit digitalen Elementen. Die Elektro- und Digitalindustrie unterstützt dieses Ziel ausdrücklich. Der CRA ist mit seinem Fundament auf dem New Legislative Framework (NLF) und seinem risikobasierten Ansatz grundsätzlich ein guter Schritt hin zu einem cyberresilienten und vertrauenswürdigen Wirtschaftsstandort. Ab Dezember 2027 muss jedes einzelne Produkt – auch bereits vertriebener Modelle – CRA-konform in Verkehr gebracht werden.

Allerdings schießt der CRA mit seinem sehr weiten Anwendungsbereich und seinen umfassenden Design-, Dokumentations-, Melde- und Schutzvorgaben teilweise über das Regelungsziel hinaus. Ein umfassendes Re-Design des gesamten einschlägigen Produktportfolios bis zu diesem Datum ist für viele Hersteller technisch und wirtschaftlich nicht realisierbar. Bleibt der Rechtsrahmen unverändert, drohen gravierende Lieferkettenstörungen – insbesondere im Bereich der Mikroelektronik. Produktionsunterbrechungen, Produktabkündigungen und eine potenzielle Verlagerung von Produktionsstätten wären die Folge.

Unsere Positionen

Ausnahme von „unkritischen Produkten“ ohne Cybersicherheitsrisiko aus dem CRA

Viele vernetzte Produkte – etwa DAB-Radios, Fahrradtachos, Funkuhren, Barcode-Scanner, Analog-Digital-Wandler oder integrierte Mikrochips – weisen kein relevantes Cybersicherheitsrisiko auf. Zwar übertragen sie Daten und fallen demnach pauschal unter den CRA, allerdings geht es dabei ausschließlich um triviale Datentypen, oft verarbeitet innerhalb eines Geräts. Wenn bspw. lediglich Audiodaten, sowie einfache Bedien- und Statusinformationen übertragen werden, ohne dass darüber ein Zugriff auf andere IT-Systeme oder sicherheitsrelevante Funktionen möglich ist, entsteht dadurch keine relevante Angriffsfläche im Cyberraum. Gleiches gilt für die meisten Mikroelektronik-Komponenten. Viele integrierte Mikrochips übertragen ausschließlich Steuer- und Statusinformationen innerhalb eines Geräts (z. B. Ein/Aus, Drehzahl, Temperatur, Füllstand) und das in der Regel über einfache interne Schnittstellen. Ihnen wohnt aufgrund der Einbausituation und der beschränkten Fähigkeiten schlicht kein Cybersicherheitsrisiko inne.

Hersteller haben diese unkritischen Produkte bzw. Komponenten bislang ohne Berücksichtigung des CRA entwickelt und müssten nun ihr gesamtes Portfolio anpassen. Ein komplettes Re-Design bis 2027 ist für viele Unternehmen praktisch unmöglich. Produktabkündigungen, insbesondere in der Halbleiterindustrie, wären die Folge – mit gravierenden Auswirkungen auf die Lieferketten.

Praxisbeispiel: Ein großer internationaler Halbleiterhersteller gibt an, dass sein Produktportfolio aus rund 80.000 Modellen besteht; eine vollumfängliche Neukonzeption ist nicht realistisch. Ausnahmen für „unkritische“ Produkte mit digitalen Elementen würden hier signifikant zur Entlastung beitragen: Schätzungen zufolge könnten etwa 60.000 Modelle dieses Portfolios – also 75 Prozent – darunterfallen.

Durch die Herausnahme dieser unkritischen Produkte aus dem Anwendungsbereich des CRA würde bei gleichbleibend hohem Sicherheitsniveau das Risiko von Engpässen bei wichtigen Komponenten wie Mikrochips demnach deutlich gesenkt, aber auch das Inverkehrbringen von Endprodukten, wie simplen DAB-Radios oder Funkuhren, signifikant erleichtert werden.

Eine Blaupause für einen solchen Ansatz findet sich in der Richtline zur Elektromagnetischen Verträglichkeit (Erwägungsgrund 12), der vorgibt, dass „Betriebsmittel, die aufgrund ihrer Beschaffenheit keine elektromagnetischen Störungen verursachen, […] durch diese Richtlinie nicht geregelt werden [sollten]“.

Eine ähnliche Bezugnahme auf Produkte mit digitalen Elementen, denen „aufgrund ihrer Beschaffenheit keine Cybersicherheitsrisiken innewohnen“, wäre im Zusammenhang mit dem CRA angemessen und sinnvoll.

Vereinfachte technische Dokumentation für Produkte der „Basiskategorie“ (ohne erhöhtes Cybersicherheitsrisiko)

Unter dem CRA müssen Hersteller, unabhängig von der Risikoklasse des Produkts, in ihrer technischen Dokumentation umfassend darstellen, welche Funktion das Produkt erfüllt, wie es technisch aufgebaut ist, welche Cybersicherheitsrisiken bestehen und mit welchen Maßnahmen und Prozessen sie diese Risiken beherrschen. Mit Art. 33 Abs. 5 erlaubt der CRA, dass Kleinst- und Kleinunternehmen diese Inhalte in einem vereinfachten Format vorlegen können. Diese Vereinfachung sollte für Produkte der Basiskategorie (nicht in Anhang III & IV aufgeführt) auf alle Hersteller ausgeweitet werden. Diese Kategorie umfasst den Großteil des CRA-Anwendungsbereichs. Insbesondere digitale Verbraucherprodukte (vernetzte Kaffeemaschinen, smarte Glühbirnen, etc.) würden davon profitieren. Laut einer aktuellen ZVEI-Umfrage würde dies die Inverkehrbringung von rund 65 % der vernetzten Produkte unserer Mitgliedsunternehmen maßgeblich erleichtern.

Klarstellung, dass CRA-Konformität für ausentwickelte Produktmodelle möglich ist

Der CRA verpflichtet Hersteller, Produkte mit digitalen Elementen so zu entwickeln und herzustellen, dass sie angesichts der Risiken ein angemessenes Cybersicherheitsniveau gewährleisten (Annex I Teil I Nummer 1). Diese Anforderung muss so ausgelegt werden, dass Nachqualifikation von zuvor entwickelten Produktmodellen möglich ist. Bereits auf dem Markt bereitgestellte Modelle von Produkten mit digitalen Elementen müssen weiterhin in Verkehr gebracht werden dürfen, wenn sie nachweislich die grundlegenden technischen Cybersicherheitsanforderungen erfüllen, auch wenn bei der ursprünglichen Entwicklung kein Prozess unter Berücksichtigung des CRA-Rechtstextes angewandt wurde. Auf dem Markt gibt es Produktmodelle, zum Beispiel im Kontext der Halbleiter-, aber auch der Bahnindustrie, die über Jahrzehnte hinweg entwickelt wurden. Sie werden von der Gesellschaft benötigt und können rein technisch nicht bis Dezember 2027 neu entwickelt werden. Daher muss klargestellt und festgehalten werden, dass CRA-Konformität für ausentwickelte Produktmodelle möglich ist, solange diese ein entsprechendes Cybersicherheitsniveau gewährleisten. Diese Klarstellung kann z.B. im Rahmen von Leitlinien erfolgen.

Realistische, technisch machbare Zeitpläne für die Erarbeitung der harmonisierten europäischen Normen

Hersteller müssen genügend Vorlauf haben, um die in den Normen konkretisierten rechtlichen Anforderungen in Entwicklung und Produktion zu verankern. Zwischen der Veröffentlichung der relevanten harmonisierten Normen im Amtsblatt der EU und dem Ende der CRA-Übergangsfrist sollten daher mindestens 36 Monate liegen – insbesondere bei vertikalen, produktspezifischen Normen, die eine Konformitätsvermutung auslösen. Liegen diese Normen nicht rechtzeitig vor, müssten sog. „wichtige“ Produkte der Klasse I – etwa Router, Betriebssysteme oder Mikroprozessoren mit sicherheitsrelevanten Funktionen – von einer externen Konformitätsbewertungsstelle zertifiziert werden. Dies betrifft rund 21 % der vernetzten Produkte der Elektro- und Digitalindustrie. Ist eine Verlängerung der Fristen nicht umsetzbar, sollten Herstellern dieser Produktkategorie übergangsweise eigenverantwortlich die Konformität ihrer Produkte mit dem CRA darlegen können (NLF-Modul A der internen Fertigungskontrolle), bis die vertikalen Normen verfügbar sind. Auch dann sollte, ab dem Zeitpunkt der Verfügbarkeit einer vertikalen Norm, eine adäquate Übergangszeit bis zu deren Anwendung vorgegeben werden. Ansonsten drohen massive Engpässe bei der Inverkehrbringung, wie es bei der Medizinprodukteverordnung schon einmal der Fall war.

Trennung bei der Festlegung des Support-Zeitraums im B2B-Bereich zwischen physischer und digitaler Lebensdauer

Während des Unterstützungszeitraums für ihre Produkte mit digitalen Elementen sind Hersteller durch den CRA verpflichtet, Sicherheitsupdates kostenlos bereitzustellen. Die Länge dieses Zeitraums wird grundsätzlich vom Hersteller selbst festgelegt, wobei er allerdings andere einschlägige Rechtsvorschriften berücksichtigen muss. Dies führt zu erheblichen Herausforderungen. Vorschriften wie die Ökodesign-Verordnung verpflichten Hersteller, die Lebensdauer von Produkten zu definieren. Viele Industrieprodukte haben eine physische Lebensdauer von mehr als zehn Jahren, während ihre digitalen Komponenten wesentlich kürzeren Innovations- und Supportzyklen unterliegen. Die Vorgabe des CRA könnte bedeuten, dass der Unterstützungszeitraum nicht signifikant von der unter anderen Vorschriften prognostizierten Lebensdauer abweichen darf und Hersteller bis zum Ende der physischen Nutzbarkeit eines Produktes kostenfreie Sicherheitsupdates bereitstellen müssen. Dies ist ein massiver Eingriff in die gängige Praxis im B2B-Bereich. Um risikobasierte und wirtschaftlich tragbare Supportverpflichtungen zu ermöglichen, schlagen wir daher eine klare regulatorische Unterscheidung zwischen der physischen und der digitalen Lebensdauer von Produkten mit digitalen Elementen im Rahmen des CRA vor.

Hintergrund

Scope des CRA

- Der CRA gilt für alle auf dem Markt bereitgestellte Produkte mit digitalen Elementen, deren bestimmungsgemäßer Zweck oder vernünftigerweise vorhersehbare Verwendung eine direkte oder indirekte logische oder physische Datenverbindung mit einem Gerät oder Netz einschließt. Jedes kommunizierende Produkt ist daher von den Anforderungen betroffen. Dabei macht es keinen Unterschied, ob das Produkt an „normale“ Verbraucher (B2C) oder an Unternehmenskunden (B2B) verkauft wird. Der CRA geht also von einem äußerst breiten, horizontalen Anwendungsbereich aus, mit diversen Produkten, von einfachen Haushaltsgeräten bis hin zu komplexen industriellen Systemkomponenten.
- Der CRA unterscheidet aktuell vier Kategorien von Produkten mit digitalen Elementen mit aufsteigendem Risiko und jeweils strengeren Konformitätsbewertungsverfahren (s. Abb. 1):
  1. Basiskategorie: Alle Produkte, die nicht ausdrücklich als „wichtig“ oder „kritisch“ gelistet sind;
  2. Wichtige Produkte (Annex III):
     a. Klasse I: Produkte mit erhöhtem Cybersicherheitsrisiko;
     b. Klasse II: Produkte mit höherem Cybersicherheitsrisiko;
  3. Kritische Produkte (Annex IV): Hochsicherheitsrelevante Produkte.

1) Produkt-Kategorien im CRA und ihr Anteil an dem aus Produkten mit digitalen Elementen bestehenden Produktportfolio der ZVEI-Mitgliedschaft

Herstellerpflichten

- Hersteller müssen für jedes Produkt eine Risikobewertung durchführen und die Cybersicherheitsanforderungen des CRA darauf basierend umsetzen. Dafür ist es irrelevant, in welche Kategorie das jeweilige Produkt fällt. Die vier Kategorien geben ausschließlich das für das Produkt einschlägige Konformitätsbewertungsverfahren vor. Hersteller müssen – abhängig vom jeweiligen Risiko – umfassende Design- und Schutzvorgaben erfüllen, aktives Schwachstellenmanagement über den gesamten Lebenszyklus gewährleisten, ausgenutzte Schwachstellen und Cybersicherheitsvorfälle melden, technische Dokumentationen anfertigen und Konformitätsbewertungsverfahren durchführen.
- Jedes einzelne ab Dezember 2027 in der EU in Verkehr gebrachte Produkt mit digitalen Elementen unterliegt den vollen CRA-Pflichten. Wird die Integration von zugekauften Komponenten außerhalb der EU durchgeführt, gelten diese Pflichten nur für den Hersteller des importierten Endprodukts.

- Das Konzept des Inverkehrbringens bezieht sich auf jede einzelne Produktinstanz (s. Blue Guide, Kap. 2.3). Hersteller haben ihre Produkte mit digitalen Elementen in der Vergangenheit ohne Berücksichtigung des CRA entwickelt und müssen nun ihr gesamtes einschlägiges Portfolio anpassen. Ein komplettes Re-Design bis 2027 ist für viele praktisch unmöglich. Produktabkündigungen wären die Folge, was, insbesondere im Kontext der Halbleiterindustrie, gravierende Folgen für die Lieferketten nach sich ziehen würde.
- Mit seinen umfangreichen Vorgaben für Hersteller, während des gesamten Lebenszyklus eines Produktes mit digitalen Elementen ein hohes Cybersicherheitsniveau zu gewährleisten, bindet die Umsetzung des CRA knappe Fachkräfte in den Unternehmen. Oft stehen diese vor der Wahl: Erfüllung der Anforderungen oder neue Investitionen in F&E. Eine Erleichterung der Dokumentationspflichten, sowie Ausnahmen für „unkritische“ Produkte mit digitalen Elementen würden hier Abhilfe schaffen.

Zahlen, Daten, Fakten

- Die Zahl vernetzter Geräte (Internet of Things, IoT) steigt laut Prognosen in Europa von rund 4,3 Mrd. (2025) auf etwa 6,7 Mrd. (2030) an. Darüber hinaus erfasst der CRA u.a. auch Standalone-Software und weitere Produkte mit digitalen Elementen, sodass die tatsächliche Zahl betroffener Produkte deutlich oberhalb Marke liegt.[1]
- Während auch die Elektro- und Digitalindustrie (EDI) von Angriffen nicht verschont bleibt, sind ihre Produkte sicher: Rund 60 % der Unternehmen der EDI wurden in den letzten 24 Monaten Ziel eines Cyberangriffs. Dennoch wurden nur rund 1,5 % der in Verkehr gebrachten Produkte der Unternehmen durch Cyberangriffe in den letzten 24 Monaten beeinträchtigt (z. B. in ihrer Funktion, Sicherheit oder Integrität).
- Die Unternehmen der Digital- und Elektroindustrie schätzen den finanziellen Aufwand für die Umsetzung der Cybersicherheitsregulierung insgesamt (hauptsächlich CRA und NIS-2-Richtlinie) bis 2030 auf etwa 1,4 % des geplanten Umsatzes.
- Rund 65 % der vernetzten Produkte des Produktportfolios unserer Mitgliedsunternehmen fallen in die sog. „Basiskategorie“ und würden somit maßgeblich von erleichterten Dokumentationspflichten profitieren.
- 67 % der ZVEI-Mitglieder bewerten den CRA, vor der NIS-2-Richtlinie, als die belastendste Cybersicherheitsregulierung.
- Über die Hälfte (61 %) der EU-Unternehmen hat große Schwierigkeiten, offene Stellen im Bereich Cybersicherheit qualifiziert zu besetzen. Als häufigste Herausforderungen bei der Rekrutierung werden „Schwierigkeiten, qualifizierte Kandidat:innen zu finden“ (45 %) und „Mangel an Bewerber:innen“ (44 %) genannt. [2]

Kontakt
Lennard Kreißl • Manager Digitalpolitik (Schwerpunkt Cybersicherheit) • Abteilung Digital- und Innovationspolitik • Bereich Digitalisierung & Recht
Tel.: +49 30 306960-582 • Mobil: +49 162 2664-941 • E-Mail: lennard.kreissl@zvei.org

Impressum
ZVEI e. V. • Verband der Elektro- und Digitalindustrie • Charlottenstr. 35/36 • 10117 Berlin
Lobbyregisternr.: R002101 • EU Transparenzregister ID: 94770746469-09 • www.zvei.org

Datum: 19.01.2026

[1] Statista (2024): Number of Internet of Things (IoT) connected devices from 2020 to 2033 (in millions), by region, https://www.statista.com/statistics/1194677/iot-connected-devices-regionally/.
[2] Europäische Kommission (2024): Flash Eurobarometer 547 – Cyberskills, https://europa.eu/eurobarometer/api/deliverable/download/file?deliverableId=93514.