bitkom

Positionspapier

August 2026

CRA: 15 Szenarien für Wirtschaft, Markt und Versorgungssicherheit

Der Cyber Resilience Act ist ein wichtiger Schritt für Europas Cybersicherheit. Er setzt EU-weit verbindliche Mindestanforderungen für Produkte mit digitalen Elementen und stärkt „Security by Design“. Die Digitalwirtschaft unterstützt dieses Ziel ausdrücklich: Höhere Cybersicherheitsstandards schützen Unternehmen, Bürgerinnen und Bürger, Lieferketten und kritische Infrastrukturen.

Zugleich ist der CRA eine industriepolitische Weichenstellung, dessen Wirkung von einer erfolgreichen Umsetzung abhängt. Dafür braucht es klare Standards, belastbare Leitfäden, ausreichende Prüf- und Zertifizierungskapazitäten sowie eine harmonisierte Marktaufsicht. Konformitätsbewertungsstellen müssen frühzeitig Prüfverfahren, Personal, Akkreditierungen und eine einheitliche Prüftiefe aufbauen, sonst droht ein struktureller Flaschenhals. Der administrative Mehraufwand sollte beherrschbar und damit verbundene Zusatzkosten müssen so gering wie möglich sein.

Derzeit bestehen erhebliche Umsetzungslücken. Unternehmen bereiten sich auf Dezember 2027 vor, obwohl harmonisierte Standards, delegierte Rechtsakte, Auslegungshilfen, Zertifizierungsverfahren und Vorgaben zur Marktaufsicht fehlen. Gleichzeitig können bei Nichtkonformität Sanktionen oder der Verlust des Marktzugangs drohen. Das betrifft Unternehmen jeder Größe.

Die Europäische Kommission, die Bundesregierung, das BSI und die zuständige Akkreditierungsstelle sollten die Umsetzung deutlich stärker priorisieren. Erforderlich sind frühzeitig verfügbare Standards, tragfähige Prüfkapazitäten, klare Ansprechpartner und eine einheitliche Aufsichtspraxis. Ist eine reguläre Listung der maßgeblichen harmonisierten Standards bis zum 11. Dezember 2026 nicht mehr möglich, sollte zwischen ihrer Veröffentlichung im EU-Amtsblatt und der erstmaligen Anwendung eine zweijährige Übergangsfrist gelten. Ziel muss sein, Cybersicherheit zu erhöhen, ohne Innovation, Produktverfügbarkeit und Wettbewerbsfähigkeit durch vermeidbare Unklarheiten zu beeinträchtigen.

Dieses Papier beschreibt konkrete Risikoszenarien aus Sicht der Wirtschaft und ergänzt damit die grundlegenden Bitkom-Forderungen zum CRA. Die Szenarien zeigen, welche praktischen Folgen entstehen können, wenn zentrale Umsetzungsfragen bis Dezember 2027 ungelöst bleiben.

1. Produktvarianten, Änderungen und Produktlebenszyklen

Szenario 1: Unverhältnismäßige Einzelbewertung kundenspezifischer UICC-/SIM-Varianten

Ausgangslage

SIM-Karten bestehen im Kern aus Hardware-Chip, Betriebssystem und Netzprofil. Mobilfunkanbieter definieren regelmäßig eigene Varianten, die vom Hersteller auf Basis eines allgemeinen Betriebssystems und identischer Hardware kundenspezifisch konfiguriert werden. Diese Varianten enthalten in der Regel keine zusätzlichen Funktionen, sondern sind eingeschränkte Ausprägungen des allgemeinen Betriebssystems. Ein bestimmtes SIM-Kartenprodukt kann daher nur an den Mobilfunkanbieter geliefert werden, der es spezifiziert hat.

CRA-Herausforderung

Nach dem CRA würden umfassende Konformitätsbewertungen für UICC-/SIM-Produkte erforderlich werden. Werden kundenspezifische Varianten jeweils separat zertifiziert, entstehen erhebliche zusätzliche Kosten für Hersteller und notifizierte Stellen. Diese Kosten wirken als struktureller Fixkostentreiber: Anbieter mit hohen Produktionsvolumina können sie auf größere Stückzahlen verteilen, kleinere Anbieter und neue Marktteilnehmer dagegen deutlich schwerer. Gerade bei geringen Anfangsvolumina können CRA-bedingte Zertifizierungskosten so zur erheblichen wirtschaftlichen Hürde werden.

Mögliche Konsequenz

Dies kann zu Marktverzerrungen und einer stärkeren Konzentration auf wenige große Anbieter führen. Mobilfunkanbieter könnten Beschaffungsvolumina aus Kostengründen weiter auf den günstigsten Anbieter konzentrieren. Kleinere Hersteller müssten prüfen, ob sich Zertifizierungen bei geringen Stückzahlen noch wirtschaftlich lohnen; neue Anbieter hätten deutlich höhere Markteintrittshürden. Eine reduzierte Anbieterlandschaft kann die Resilienz europäischer Lieferketten schwächen. Bei Produktionsausfällen, CRA-relevanten Schwachstellen, Rückrufen oder verpflichtenden Sicherheitsupdates eines großen Anbieters könnten mehrere Mobilfunkanbieter und nachgelagerte Bereiche gleichzeitig betroffen sein, etwa Mobilfunk, IoT-Anwendungen, vernetzte Fahrzeuge oder industrielle Anwendungen.

Verbesserungsvorschlag

Die CRA-Konformität sollte für ein allgemeines Betriebssystem, nachgewiesen werden können und auf daraus abgeleitete kundenspezifische Varianten leicht übertragbar sein, sofern diese keine über den geprüften Funktionsumfang hinausgehenden Funktionen enthalten. So ließe sich der Zertifizierungsaufwand deutlich reduzieren, ohne das Sicherheitsniveau des CRA abzusenken. Gleichzeitig würden notifizierte Stellen entlastet, Prüfkapazitäten effizienter genutzt, Markteintrittshürden begrenzt und die Vielfalt der Anbieter erhalten.

Szenario 2: Fehlende Zertifizierungsgrundlagen für Smartcards und Secure Elements

Ausgangslage

Smartcards und Secure Elements bilden die Sicherheitsbasis zahlreicher kritischer Anwendungen und globaler Infrastrukturen, etwa in den Bereichen Bezahlen, Mobilfunk, Gesundheitswesen, Pässen/Ausweisen, Identitätsmanagement sowie bei Authentisierungs- und Zugangskontrollsystemen. Sie tragen damit unmittelbar zu den Sicherheitszielen des CRA bei. Die Produkte werden häufig über lange Zeiträume eingesetzt und beruhen auf hochspezialisierten Hardware-, Betriebssystem- und Anwendungskomponenten.

CRA-Herausforderung

Für diese komplexen und sicherheitskritischen Komponenten fehlen bislang spezifische und anerkannte CRA-Standards. Entsprechende Standards befinden sich noch in der Entwicklung und werden voraussichtlich frühestens im Frühjahr 2027 verfügbar sein, vertikale spezifische Standards (z.B. Protection Profiles) erst in Jahren. Vorbereitung, Prüfung und Bewertung benötigen bei Smartcards mindestens einen vergleichbaren Vorlauf wie etablierte Common-Criteria-Verfahren. Zudem ist die nachträgliche Zertifizierung von (Bestands-) Produkten, die bisher nicht zertifiziert wurden, entweder unmöglich oder mit erheblichem Aufwand verbunden. Ohne frühzeitig verfügbare, verbindliche und produktspezifische Vorgaben fehlt Herstellern die notwendige Planungs- und Investitionssicherheit.

Mögliche Konsequenz

Hersteller könnten Smartcard-Lösungen abkündigen, wenn deren CRA-Konformität wirtschaftlich oder innerhalb des verbleibenden Zeitraums nicht nachweisbar ist. Für viele kundenspezifische Anwendungen steht kurzfristig kein gleichwertiger Ersatz bereit. Lösungsanbieter könnten deshalb auf leichter bewertbare, aber weniger sichere, reine Softwarelösungen ausweichen oder auf Hardware-Sicherheitselemente verzichten, was das Sicherheitsniveau entgegen der CRA-Ziele effektiv senken würde. Notwendige Re-Designs geraten zugleich unter erheblichen Zeitdruck und binden Ressourcen, die für die technische Weiterentwicklung benötigt werden.

Verbesserungsvorschlag

Etablierte Zertifizierungen wie EUCC, bestehende Common-Criteria-Prüfberichte und bestehende Qualitätsprozesse auf Basis von ISO 9001 sollten als Grundlage der CRA-Konformitätsbewertung anerkannt und wiederverwendet werden können. Ergänzend braucht es modulare Ansätze wie Produktfamilien- oder „Umbrella“-Bewertungen, damit nicht jede technische Variante vollständig neu geprüft werden muss. Europäische Kommission und zuständige Behörden sollten technikspezifische Anforderungen, Protection Profiles und belastbare Übergangsregeln frühzeitig veröffentlichen. Zertifizierungsschemata, die seit Langem in der Industrie angewendet werden und die nachweislich ein sehr hohes, gleichwertiges Sicherheitsniveau gewährleisten, müssen geeignet anerkannt werden, z.B. indem dafür spezielle CSA-Schemes und Anerkennungsverfahren ausgestaltet werden. Eine absehbare, nicht zu bewältigende Flut von Re-Zertifizierungen muss vermieden werden. Es sollten daher in jedem Fall ausreichende Übergangsfristen definiert werden.

Szenario 3: Neubewertungsrisiken bei konfigurierbarer Remote-Wartungssoftware

Ausgangslage

Sichere Remote-Zugriffs- und Wartungslösungen ermöglichen kontrollierte und protokollierte Zugänge zu Systemen in Industrie, Energieversorgung, Gesundheitswesen, öffentlicher Verwaltung und anderen sensiblen Umgebungen. Die Produkte bestehen häufig aus einem sicherheitsrelevanten Produktkern, der an die jeweilige Betriebsumgebung angepasst wird. Unterschiede betreffen etwa Deployment-Modelle, Authentifizierung, Rechteverwaltung, Protokollierung und Systemintegration. Diese Konfigurationen verändern den Produktkern nicht zwingend, sind für den sicheren Betrieb aber unverzichtbar.

CRA-Herausforderung

Für wichtige Produkte mit digitalen Elementen kann eine Drittbewertung durch eine notifizierte Stelle erforderlich sein. Unklar ist insbesondere, ob kundenspezifische Konfigurationen, Änderungen des Deployment-Modells oder sicherheitsrelevante Aktualisierungen eine neue oder ergänzende Konformitätsbewertung auslösen. Bei Remote-Wartungslösungen tritt diese Frage regelmäßig auf, obwohl Anpassungen häufig nur die Einbindung in die jeweilige Betriebsumgebung betreffen und den sicherheitsrelevanten Produktkern nicht verändern.

Mögliche Konsequenz

Hersteller könnten kundenspezifische Integrationen oder Härtungsmaßnahmen verzögern, um keine ungeklärten Neubewertungspflichten auszulösen. Anwender müssten dadurch länger mit weniger geeigneten oder weniger gehärteten Konfigurationen arbeiten. Besonders betroffen wären mittelständische und spezialisierte Anbieter mit variantenreichen Konfigurationsmodellen. Wenn jede Anpassung zum möglichen Bewertungsrisiko wird, begünstigt dies standardisierte Produkte großer Anbieter und kann Vielfalt und Resilienz in einer sicherheitskritischen Zugangsschicht schwächen.

Verbesserungsvorschlag

Die CRA-Konformität sollte auf Ebene eines klar definierten Produktkerns oder einer Produktfamilie nachgewiesen werden können. Kundenspezifische Konfigurationen und Deployment-Modelle sollten von dieser Bewertung erfasst sein, solange sie den geprüften Sicherheitsumfang nicht wesentlich verändern oder unterlaufen. Die Europäische Kommission sollte hierzu klare Kriterien und praxisnahe Beispiele für bewertungsauslösende Änderungen veröffentlichen.

Szenario 4: Neubewertungspflichten bei kontinuierlicher Softwareentwicklung

Ausgangslage

Moderne Software wird kontinuierlich weiterentwickelt. Sicherheitsupdates, Fehlerbehebungen und funktionale Erweiterungen erfolgen häufig in kurzen Entwicklungszyklen durch Continuous Integration, Continuous Deployment und agile Entwicklungsmethoden. Änderungen sind daher kein Ausnahmefall, sondern fester Bestandteil des regulären Entwicklungs- und Sicherheitsprozesses.

CRA-Herausforderung

Für reine Sicherheitsupdates besteht durch die CRA Guidance der Kommission inzwischen mehr Klarheit: Sie gelten grundsätzlich nicht als wesentliche Änderung, wenn sie das Cyberrisiko reduzieren und den bestimmungsgemäßen Zweck nicht verändern. In kontinuierlichen Entwicklungsprozessen bleibt jedoch die Abgrenzung bei funktionalen Änderungen und kombinierten Releases relevant. Hersteller müssen regelmäßig bewerten, ob neue oder veränderte Funktionen den bestimmungsgemäßen Zweck oder das Cybersicherheitsrisikoprofil so verändern, dass eine erneute oder ergänzende Konformitätsbewertung erforderlich wird. Bei kurzen Release-Zyklen kann diese Einzelfallprüfung zusätzlichen Dokumentations- und Bewertungsaufwand verursachen.

Mögliche Konsequenz

Hersteller könnten funktionale Änderungen stärker bündeln oder Release-Zyklen verlängern, um den Aufwand wiederholter Bewertungen zu begrenzen. Besonders kleine und mittlere Unternehmen könnten funktionale Weiterentwicklungen zurückstellen, um den Aufwand wiederholter Konformitätsbewertungen zu begrenzen. Dies bindet Entwicklungsressourcen, hemmt Innovationen und kann die kontinuierliche Weiterentwicklung von Produkten erschweren.

Verbesserungsvorschlag

Die bestehenden Kriterien für wesentliche Änderungen sollten für kontinuierliche Softwareentwicklung weiter operationalisiert werden. Änderungen, die den bestimmungsgemäßen Zweck und das Cybersicherheitsrisikoprofil nicht wesentlich verändern und das Sicherheitsniveau erhalten oder verbessern, sollten keine erneute vollständige Konformitätsbewertung auslösen. Ergänzend sind praxisnahe Leitlinien mit weiteren Beispielen insbesondere für funktionale Änderungen und kombinierte Releases in Continuous-Integration- und Continuous-Deployment-Prozessen erforderlich.

Szenario 5: Neubewertungspflichten gefährden die Ersatzteilversorgung

Ausgangslage

Produkte mit digitalen Elementen sind häufig über viele Jahre auf eine verlässliche Ersatzteilversorgung angewiesen. Die benötigten Komponenten werden vielfach speziell für ein bestimmtes Produkt entwickelt. Im Laufe des Produktlebenszyklus können Änderungen erforderlich werden, etwa weil ursprüngliche Komponenten nicht mehr verfügbar sind oder technische Verbesserungen umgesetzt werden müssen. Die Ursachen liegen nicht immer im Einflussbereich des Herstellers.

CRA-Herausforderung

Ersatzteile mit digitalen Elementen sind grundsätzlich von den Anforderungen des CRA ausgenommen. Nach der CRA-Auslegung der Europäischen Kommission kann diese Ausnahme jedoch entfallen, wenn ein Ersatzteil wesentlich geändert wird. Der Nachweis der vollständigen CRA-Konformität kann dann erhebliche Kosten verursachen. Bei spezialisierten Ersatzteilen mit geringen Stückzahlen stehen diese häufig in keinem wirtschaftlich vertretbaren Verhältnis zum tatsächlichen Sicherheitsrisiko der Änderung. Bereits die Prüfung, ob eine Änderung eine CRA-Pflicht auslöst, bindet Ressourcen und lässt ein Rechts- und Haftungsrisiko zurück.

Mögliche Konsequenz

Hersteller könnten notwendige Anpassungen unterlassen oder die Bereitstellung einzelner Ersatzteile vollständig einstellen. Dadurch würden bestehende Produkte möglicherweise vorzeitig unbrauchbar, obwohl sich ihre tatsächliche Cybersicherheit durch das geänderte Ersatzteil nicht verschlechtert. Wird eine Ersatzteilfertigung beendet, kann ihre spätere Wiederaufnahme mit erheblichen Kosten verbunden oder technisch nicht mehr möglich sein. Dies beeinträchtigt Reparaturfähigkeit, Produktlebensdauer und Versorgungssicherheit ohne entsprechenden Sicherheitsgewinn.

Verbesserungsvorschlag

Änderungen an Ersatzteilen sollten keine erneute CRA-Konformitätsbewertung auslösen, sofern sie der Aufrechterhaltung der Verfügbarkeit oder technischen Verbesserungen dienen, den bestimmungsgemäßen Zweck, die Kernfunktion und den geprüften Sicherheitsumfang nicht wesentlich verändern und das Sicherheitsniveau des Gesamtprodukts nicht verschlechtern.

Szenario 6: Kostenlose Sicherheitsupdates in individuell vereinbarten B2B-Supportmodellen

Ausgangslage

Hersteller komplexer Enterprise-Software unterstützen aus Stabilitäts- und Kompatibilitätsgründen meist nur wenige Produktversionen parallel. Unternehmenskunden betreiben diese Lösungen häufig on-premises oder hybrid und sind insbesondere in regulierten Branchen auf lange Validierungs- und Upgrade-Zyklen angewiesen. Grundlage sind individuell ausgehandelte Support- und Wartungsverträge. Diese umfassen neben Sicherheitspatches regelmäßig Kompatibilitätsprüfungen, Validierungen, Deployment-Planung, Service-Level-Agreements, Lifecycle-Management und Hotfix-Engineering.

CRA-Herausforderung

Der CRA verpflichtet Hersteller grundsätzlich, Sicherheitsupdates unverzüglich und kostenlos bereitzustellen. Unklar ist, ob individuell verhandelte Supportverträge für hochkonfigurierbare Enterprise-Software unter die Ausnahme für maßgeschneiderte Produkte mit digitalen Elementen fallen. Andernfalls müssten Hersteller entweder Altversionen gesondert pflegen oder einen Wechsel auf neuere Versionen kostenlos ermöglichen. Beides geht deutlich über die Bereitstellung eines reinen Sicherheitspatches hinaus. Unklar ist zudem, wie weit die Verantwortung des Herstellers reicht, wenn ein geeignetes Sicherheitsupdate bereitgestellt wurde, der Betreiber dieses aufgrund von Kompatibilitätsanforderungen, Freigabeprozessen oder seiner Legacy-Umgebung aber nicht einsetzen kann.

Mögliche Konsequenz

Ressourcen würden von aktuellen Produktlinien in die Pflege historischer Versionen verlagert. Hersteller könnten Supportzeiträume verkürzen und die Zahl unterstützter Versionen reduzieren. Gerade in regulierten Branchen können Kunden auf älteren Versionen verbleiben, obwohl ein Sicherheitsupdate verfügbar ist. Ohne klare Verantwortungsabgrenzung entstehen zusätzliche Haftungs- und Compliance-Unsicherheiten. Zugleich entstehen Fehlanreize für proaktive Schwachstellenforschung, wenn Erkenntnisse zu Altversionen zusätzliche Backport-Pflichten auslösen. Cloud- und Abonnementmodelle wären strukturell weniger betroffen als on-premises und hybrid bereitgestellte Lösungen.

Verbesserungsvorschlag

Der Begriff des maßgeschneiderten Produkts mit digitalen Elementen sollte auch hochkonfigurierbare Enterprise-Software erfassen, die kundenspezifisch integriert und on-premises oder hybrid betrieben wird. Falls diese Klarstellung nicht ausreicht, sollte in Anhang I im Rahmen eines Digitalen Omnibus das Wort “maßgeschneidert” gestrichen werden, um so zu verdeutlichen, dass die Cybersicherheitsziele des CRA uneingeschränkt erreicht werden können, ohne vertragliche Abreden, Wahlfreiheit und technologieoffene Geschäftsmodelle zu begrenzen. Zudem sollte klar abgegrenzt werden, welche Pflichten beim Hersteller verbleiben und welche Verantwortung beim Betreiber liegt, wenn ein geeignetes Sicherheitsupdate bereitgestellt wurde, aufgrund der konkreten Betriebsumgebung aber nicht installiert werden kann.

Szenario 7: Unverhältnismäßige CRA-Pflichten für risikoarme Massenprodukte

Ausgangslage

Der CRA erfasst auch einfache Peripheriegeräte der Kommunikationstechnik, etwa Computermäuse, Tastaturen oder Webcams. Diese verfügen über eine physische oder logische Datenverbindung und nutzen damit ein digitales Element. Der erforderliche Treiber ist jedoch häufig weder produktspezifisch noch Bestandteil des Geräts, sondern ein geräteunabhängiger, bereits auf dem Computer installierter HID-Treiber. Das produktspezifische Sicherheitsrisiko ist bei solchen Geräten daher regelmäßig begrenzt.

CRA-Herausforderung

IT-Peripheriegeräte werden häufig von Handelsunternehmen vertrieben, die Entwicklung und Produktion an externe Anbieter ausgelagert haben. Diese Unternehmen verfügen vielfach nicht über die technischen Kompetenzen und internen Strukturen, um die Cybersicherheitsrisiken einfacher Massenprodukte eigenständig und rechtssicher zu bewerten. Zwar erlaubt der CRA bei Produkten mit geringem Sicherheitsrisiko eine interne Konformitätsbewertung. Ohne klare Kriterien und praxisnahe Vorgaben bleibt jedoch unsicher, welche Prüfungen und Nachweise erforderlich sind.

Mögliche Konsequenz

Um Haftungs- und Sanktionsrisiken zu vermeiden, dürften viele Unternehmen trotz des geringen Produktrisikos externe Prüfstellen beauftragen. Dies würde vorhandene Prüfungskapazitäten mit Produkten geringer Kritikalität binden und könnte zu Engpässen bei tatsächlich sicherheitsrelevanten Produkten führen. Die dadurch entstehenden Fixkosten treffen insbesondere KMU und spezialisierte Anbieter, die zusätzliche Compliance-Kosten nur begrenzt auf hohe Stückzahlen oder große Kundenbasen verteilen können. Einzelne Produkte könnten unwirtschaftlich werden und vom europäischen Markt verschwinden, ohne dass damit ein entsprechender Gewinn für die Cybersicherheit verbunden wäre.

Verbesserungsvorschlag

Die Europäische Kommission sollte klar definierte, inhärent sichere Produktgruppen von den CRA-Anforderungen ausnehmen und für Produkte mit begrenztem Risiko vereinfachte Nachweisverfahren vorsehen. Dazu sollten standardisierte Selbsterklärungen und möglichst automatisierte Prüfverfahren gehören; bestehende Zertifizierungen und Prüfberichte sollten soweit möglich wiederverwendbar sein. Praxisnahe Leitlinien zur internen Konformitätsbewertung nach Artikel 32 CRA sollten hierfür klare Prüfkriterien festlegen.

2. Lieferketten, Komponenten und Schwachstellenmanagement

Szenario 8: Schwachstellenmeldung und -behebung in mehrstufigen Lieferketten

Ausgangslage

Die Lieferketten der Consumer-Electronics-Branche sind häufig mehrstufig aufgebaut. Produktionspartner entwickeln entweder eigene Software oder beziehen Komponenten von weiteren Zulieferern. Dadurch können etwa Smart-Home-Produkte Softwarebestandteile enthalten, die ursprünglich von mehreren unterschiedlichen Unternehmen entwickelt wurden. Mit jeder zusätzlichen Lieferkettenstufe sinken Verfügbarkeit und Transparenz der Informationen, die europäische Hersteller für das Schwachstellenmanagement benötigen.

CRA-Herausforderung

Zwischen dem europäischen Hersteller und dem ursprünglichen Softwareentwickler liegen häufig mehrere Lieferantenebenen, ohne dass eine direkte wirtschaftliche oder vertragliche Beziehung besteht. Wird eine Schwachstelle entdeckt, müssen Informationen dennoch innerhalb kurzer Fristen über die gesamte Lieferkette ausgetauscht werden. Der europäische Hersteller ist dabei auf die Mitwirkung sämtlicher Vorlieferanten angewiesen, kann diese aber nur eingeschränkt steuern.

Mögliche Konsequenz

Die Beschaffung vollständiger Software Bills of Materials verursacht für viele Produktgruppen erheblichen Aufwand. Einzelne Vorlieferanten können möglicherweise keine vollständige SBOM bereitstellen, Schwachstellenanalysen nicht rechtzeitig durchführen oder notwendige Sicherheitsupdates nicht verfügbar machen. In der Folge können Melde- und Reaktionsfristen faktisch unerfüllbar werden. Für europäische Inverkehrbringer entstehen erhebliche Haftungs- und Rückrufrisiken, obwohl die betroffene Software außerhalb ihres Unternehmens entwickelt wurde. Im äußersten Fall kann nur ein Produktrückruf als risikomindernde Maßnahme verbleiben.

Verbesserungsvorschlag

Bei der Anwendung der Melde- und Reaktionsfristen muss berücksichtigt werden, ob Hersteller die erforderlichen Informationen von Vorlieferanten trotz angemessener und dokumentierter Bemühungen rechtzeitig erhalten können. Leitlinien sollten festlegen, welche risikomindernden Zwischenmaßnahmen anerkannt werden, wenn Schwachstelleninformationen oder Sicherheitsupdates aus vorgelagerten Lieferstufen noch nicht verfügbar sind. Für klar definierte Produkte mit begrenztem Cyberrisiko sollten zudem vereinfachte SBOM-Nachweise gelten.

Szenario 9: Unklare CE-Kennzeichnung bei Software und eingebetteten Komponenten

Ausgangslage

Für Software ist die CE-Kennzeichnung neu, während sie bei Hardwareprodukten bereits etabliert ist. Halbleiter und andere eingebettete Komponenten werden in großer Zahl in komplexe Endprodukte integriert. Nach dem Einbau sind sie für Verbraucherinnen und Verbraucher regelmäßig nicht mehr zugänglich oder sichtbar. Die Konformität der einzelnen Komponente wird gegenüber Kunden und Marktteilnehmern über die EU-Konformitätserklärung dokumentiert, während das fertige Endprodukt eine eigene CE-Kennzeichnung trägt. Halbleiterhersteller verfügen zudem häufig über umfangreiche Produktportfolios mit zahlreichen Varianten und Konfigurationen. Für Software stellt die CE-Kennzeichnung hingegen eine neue Anforderung dar, bei der insbesondere Form und Ort der Kennzeichnung weiterer Klarstellung bedürfen.

CRA-Herausforderung

Artikel 30 CRA regelt die Anbringung der CE-Kennzeichnung auf Produkten mit digitalen Elementen. Für Software und kleine oder komplex geformte Hardwareprodukte bleibt jedoch unklar, wie die Vorgaben in einzelnen Konstellationen anzuwenden sind. Bei Halbleitern verursacht eine physische Kennzeichnung zudem erheblichen administrativen Aufwand und ist aufgrund der geringen Produktgröße teilweise kaum lesbar. Nach der Integration in ein Endprodukt bietet sie für Verbraucherinnen und Verbraucher regelmäßig keinen zusätzlichen Informationswert.

Mögliche Konsequenz

Unklare Vorgaben können zu unterschiedlichen Auslegungen und damit zu formaler Nichtkonformität führen. Gleichzeitig müssten Hersteller umfangreiche Kennzeichnungs- und Produktänderungsprozesse durchführen, obwohl eine physische Kennzeichnung eingebetteter Komponenten nach dem Einbau nicht mehr zugänglich ist. Die zusätzlichen Belastungen binden insbesondere während der Umstellung erhebliche Ressourcen, ohne die Marktüberwachung oder den Verbraucherschutz entsprechend zu verbessern.

Verbesserungsvorschlag

Die Europäische Kommission sollte in ihren FAQ oder CRA-Leitlinien klarstellen, wie die CE-Kennzeichnung bei Software sowie bei kleinen oder komplex geformten Hardwareprodukten praktisch anzubringen ist. Hersteller von Halbleitern und anderen eingebetteten Komponenten sollten die CE-Kennzeichnung wahlweise in der EU-Konformitätserklärung statt auf der einzelnen Komponente anbringen können, wenn eine Kennzeichnung auf dem Produkt aufgrund seiner Größe, Lesbarkeit oder Integration in ein Endprodukt nicht praktikabel ist. In Verbindung mit der CE-Kennzeichnung des Endprodukts bliebe die Konformität nachvollziehbar dokumentiert.

Szenario 10: Doppelte Meldepflicht bei aktiv ausgenutzten Schwachstellen und schwerwiegenden Sicherheitsvorfällen

Ausgangslage

Artikel 14 CRA sieht Meldepflichten sowohl für aktiv ausgenutzte Schwachstellen als auch für schwerwiegende Sicherheitsvorfälle vor. In der Praxis können beide Kategorien miteinander verbunden sein: Die aktive Ausnutzung einer Schwachstelle in einem Produkt kann zugleich einen schwerwiegenden Sicherheitsvorfall verursachen.

CRA-Herausforderung

Unklar ist, wie Hersteller mit einem Ereignis umgehen müssen, das gleichzeitig beide Tatbestände erfüllt. Insbesondere ist nicht eindeutig, ob die Meldung der aktiv ausgenutzten Schwachstelle ausreicht, wenn diese die unmittelbare Ursache des Sicherheitsvorfalls ist, oder ob zusätzlich eine separate Meldung des schwerwiegenden Sicherheitsvorfalls erforderlich ist. Da für beide Meldewege unterschiedliche Informationen erforderlich sein können, besteht für Hersteller keine ausreichende Rechtssicherheit über Umfang und Form der Meldung.

Mögliche Konsequenz

Hersteller könnten dasselbe Ereignis vorsorglich mehrfach melden, um das Risiko einer formalen Nichtkonformität zu vermeiden. Dadurch entstehen zusätzliche administrative Aufwände und möglicherweise doppelte oder voneinander abweichende Informationen bei den zuständigen Stellen. Umgekehrt besteht bei einer einzigen Meldung das Risiko, dass diese nachträglich als unvollständig bewertet wird.

Verbesserungsvorschlag

Die Europäische Kommission sollte in ihren FAQ oder CRA-Leitlinien eindeutig regeln, wie Fälle zu behandeln sind, in denen eine aktiv ausgenutzte Schwachstelle zugleich einen schwerwiegenden Sicherheitsvorfall verursacht. Bei identischer Ursache sollte ein gemeinsamer oder eindeutig verknüpfter Meldeprozess ermöglicht werden. Dabei sollte klar festgelegt werden, welche Fristen und Informationsanforderungen gelten, damit Doppelmeldungen und formale Compliance-Risiken vermieden werden.

Szenario 11: Fehlende Zuliefernachweise für die CRA-Konformität

Ausgangslage

Produkte mit digitalen Elementen entstehen häufig in arbeitsteiligen und mehrstufigen Lieferketten. Hersteller beziehen spezialisierte Hardware- und Softwarekomponenten von unmittelbaren Zulieferern, die ihrerseits auf weitere Vorlieferanten zurückgreifen. Die für das Endprodukt relevanten technischen Informationen liegen daher bei unterschiedlichen Akteuren entlang der Lieferkette.

CRA-Herausforderung

Für den Nachweis der eigenen CRA-Konformität benötigen Hersteller belastbare Informationen und Nachweise zu den eingesetzten Zulieferprodukten. Sie können komplexe Komponenten jedoch nicht in jedem Fall eigenständig überprüfen. Insbesondere bei spezialisierten Zulieferungen fehlen ihnen häufig die technischen Fähigkeiten oder notwendigen Informationen für eigene Prüfungen. Selbst wenn Zulieferer die CRA-Anforderungen umsetzen, können entsprechende Nachweise erst kurz vor dem Geltungsbeginn verfügbar werden. Bei mehrstufigen Lieferketten verschärft sich der Zeitdruck. Einzelne Zulieferer, insbesondere außerhalb der EU, stellen möglicherweise keine ausreichenden Nachweise bereit oder orientieren sich nicht an europäischen Anforderungen.

Mögliche Konsequenz

Unvollständige oder verspätete Zulieferinformationen können den Nachweis der CRA-Konformität erheblich erschweren oder praktisch unmöglich machen. Hersteller könnten gezwungen sein, Produkte trotz eigener Vorbereitungen nicht weiter bereitzustellen oder kurzfristig alternative Zulieferer zu suchen. Das Risiko regulatorischer Versäumnisse läge damit bei Unternehmen, die die fehlende Mitwirkung innerhalb ihrer Lieferkette nur begrenzt beeinflussen können.

Verbesserungsvorschlag

Hersteller sollten ausreichend Zeit erhalten, um Zulieferinformationen zu prüfen und in ihre Konformitätsbewertung einzubeziehen. Leitlinien müssen festlegen, wie mit verspäteten, unvollständigen oder trotz angemessener Bemühungen nicht verfügbaren Nachweisen umzugehen ist. Für besonders komplexe und mehrstufige Lieferketten sollten zusätzliche Übergangsfristen vorgesehen werden, sofern der Hersteller seine Beschaffungs- und Prüfmaßnahmen nachvollziehbar dokumentiert.

Szenario 12: Fehlende Nachweis- und Verantwortungsstrukturen für Open-Source-Komponenten

Ausgangslage

Moderne Softwareprodukte setzen sich regelmäßig aus zahlreichen eigenen und extern entwickelten Komponenten zusammen. Dazu gehören häufig Hunderte oder Tausende Abhängigkeiten von Open-Source-Software. Die einzelnen Komponenten werden unter unterschiedlichen organisatorischen Strukturen und Wartungsmodellen entwickelt und anschließend in zahlreiche kommerzielle Produkte integriert.

CRA-Herausforderung

Hersteller müssen die Verantwortung für Open-Source-Komponenten übernehmen, die sie in ihre Produkte integrieren. Im Unterschied zu klassischen Zulieferbeziehungen gibt es bei vielen dieser Komponenten jedoch keinen vertraglich verpflichteten Akteur, von dem Hersteller Sicherheitsnachweise, Schwachstelleninformationen oder langfristige Updates einfordern können. Ein Austausch sämtlicher Bibliotheken oder eine umfassende individuelle Sicherheitsprüfung ist angesichts der Zahl und Komplexität der Abhängigkeiten praktisch kaum umsetzbar. Hinzu kommt, dass Hersteller nicht für jede Komponente über das erforderliche Fachwissen verfügen, insbesondere in sicherheitskritischen Bereichen wie Kryptografie. Open-Source-Software-Stewards können diese Lücke nur teilweise schließen.

Mögliche Konsequenz

Ohne verlässliche Nachweiswege müssen Hersteller zahlreiche Open-Source-Komponenten selbst bewerten, obwohl ihnen dafür teilweise Ressourcen, Informationen oder Fachkenntnisse fehlen. Eine vollständige Prüfung jeder einzelnen Bibliothek ist für komplexe Softwareprodukte kaum realistisch. Hersteller könnten deshalb auf bewährte Open-Source-Komponenten verzichten oder Produkte nicht mehr wirtschaftlich bereitstellen. Zugleich können zusätzliche regulatorische Verpflichtungen potenzielle Stewards abschrecken und bestehende Verantwortungsstrukturen schwächen.

Verbesserungsvorschlag

Für verbreitete Standardbibliotheken sollten risikobasierte, standardisierte und möglichst automatisierte Testverfahren entwickelt werden. Das Bestehen solcher Verfahren sollte eine Konformitätsvermutung begründen oder bei der Konformitätsbewertung angemessen berücksichtigt werden. Für Komponenten mit erhöhtem Sicherheitsrisiko sollten praktikable Supply-Chain-Risk-Management-Modelle und klar zugeordnete Verantwortlichkeiten vorgesehen werden. Zusätzliche Prüfpflichten sollten sich auf besonders kritische Bibliotheken und Komponenten konzentrieren.

3. Fehlende Voraussetzungen für die CRA-Anwendung

Szenario 13: Zu spät verfügbare harmonisierte Standards

Ausgangslage

Technische Standards schaffen gemeinsame Kriterien für Produktgestaltung, Prüfverfahren und Konformitätsnachweise und dienen Herstellern, Prüfstellen, Marktüberwachungsbehörden und Kunden als zentrale Referenz. Harmonisierte Standards können zudem eine Konformitätsvermutung begründen.

CRA-Herausforderung

Für zahlreiche CRA-Anforderungen befinden sich die maßgeblichen Standards noch in der Entwicklung, darunter die ETSI-EN-Reihe und die 40000-Normenreihe. Nach dem aktuellen Entwurf des Standardisierungsauftrags in der Fassung vom 7. Juli 2026 sollen wesentliche Standards voraussichtlich zwischen Oktober 2026 und Oktober 2027 veröffentlicht werden. Weitere Terminverschiebungen sind nicht ausgeschlossen. Obwohl harmonisierte Standards rechtlich freiwillig sind, werden sie in der Praxis von Marktüberwachungsbehörden, Prüfstellen und Kunden als maßgebliche Referenz herangezogen. Unternehmen müssen daher entweder auf die finalen Standards warten oder vorläufige Entwürfe umsetzen, die sich bis zur Veröffentlichung noch ändern können.

Mögliche Konsequenz

Die späte Verfügbarkeit der Standards verkürzt den Zeitraum für ihre praktische Umsetzung erheblich. Insbesondere bei komplexen Produkten, langen Entwicklungszyklen und umfangreichen Produktportfolios kann eine vollständige Anpassung bis zum Geltungsbeginn kaum oder nicht mehr realisierbar sein. Unternehmen drohen Verzögerungen bei Konformitätsbewertungen, zusätzliche Entwicklungskosten und Rechtsunsicherheit, obwohl die notwendigen Referenzanforderungen nicht rechtzeitig feststanden. Bei zu später Veröffentlichung der Standards und zugleich begrenzten Zertifizierungskapazitäten kann dies zudem die Versorgung mit z.B. sicherheitsrelevanten digitalen Basiskomponenten unterbrechen und damit kritische Infrastrukturen beeinträchtigen.

Verbesserungsvorschlag

Der Zeitraum zwischen der Veröffentlichung der wesentlichen harmonisierten Standards und der erstmaligen Verpflichtung zur Einhaltung der entsprechenden Anforderungen muss ausreichend bemessen sein. Ist am 11. Dezember 2026 eine rechtzeitige Listung der maßgeblichen harmonisierten Standards im regulären Verfahren nicht mehr möglich, sollte ab ihrer Veröffentlichung im Amtsblatt der Europäischen Union eine zweijährige Übergangsfrist gelten. Währenddessen sollten Produkte der Standardkategorie sowie Produkte der Klassen I und II weiterhin im Wege der Hersteller-Selbsterklärung nach Modul A bewertet werden können.

Szenario 14: Fehlende Kapazitäten notifizierter Stellen

Ausgangslage

Der CRA sieht abhängig von der Produktkategorie unterschiedliche Wege der Konformitätsbewertung vor. Für wichtige und kritische Produkte mit digitalen Elementen kann eine Bewertung durch eine unabhängige notifizierte Stelle erforderlich sein. Diese Stellen müssen vor Aufnahme ihrer Tätigkeit benannt und akkreditiert werden sowie die notwendigen fachlichen und organisatorischen Prüfungskapazitäten aufbauen.

CRA-Herausforderung

Der Aufbau dieser Strukturen ist bislang nicht ausreichend fortgeschritten. Derzeit stehen nur wenige für den CRA benannte Stellen zur Verfügung, während Benennung, Akkreditierung und Kapazitätsaufbau erheblichen Vorlauf benötigen. Mit dem näher rückenden Geltungsbeginn im Dezember 2027 ist zugleich mit einer starken Nachfragespitze zu rechnen. Es besteht daher das Risiko, dass die Nachfrage nach Konformitätsbewertungen deutlich schneller steigt als das verfügbare Angebot. Selbst frühzeitig eingereichte Anträge bieten keine Gewähr, dass eine Bewertung rechtzeitig abgeschlossen wird.

Hinzu kommt, dass der CRA produktbezogen ansetzt. Bei Produktserien und fortentwickelten Produktgenerationen kann dies bedeuten, dass auch neue Serien bereits etablierter Legacy-Produkte erneut CRA-konformitätsbewertet werden müssen. Dadurch entsteht fortlaufend ein erheblicher zusätzlicher Bewertungsbedarf. Die Nachfrage nach notifizierten Stellen könnte dadurch deutlich über die ohnehin erwartete Umstellungsspitze hinausgehen.

Mögliche Konsequenz

Lange Wartezeiten könnten insbesondere kleine und mittlere Unternehmen sowie Hersteller mit geringen Stückzahlen treffen. Sie laufen Gefahr, bei der Auftragsannahme und Terminvergabe gegenüber großen, umsatzstarken Kunden nachrangig behandelt zu werden. Im ungünstigsten Fall stehen für einzelne Produktkategorien zum Stichtag nicht genügend Bewertungskapazitäten zur Verfügung. Technisch konforme Produkte könnten dann allein wegen fehlender Prüfkapazitäten nicht rechtzeitig in Verkehr gebracht werden. Dies würde Marktzugänge verzögern, Wettbewerb verzerren und die Produktverfügbarkeit einschränken.

Verbesserungsvorschlag

Die Europäische Kommission und die nationalen Akkreditierungsstellen sollten die Benennung notifizierter Stellen priorisieren und transparent über verfügbare und geplante Kapazitäten berichten. Zeichnen sich Engpässe ab, müssen frühzeitig befristete und rechtssichere Übergangslösungen greifen. Dazu sollten – soweit gleichwertig – bestehende produktbezogene Zertifizierungen und Nachweise sowie geeignete Konformitätsbewertungsstellen aus ausgewählten Drittstaaten anerkannt werden. Ergänzend sollte während der in Szenario 12 beschriebenen Übergangsfrist die Hersteller-Selbsterklärung nach Modul A möglich bleiben.

Szenario 15: Fehlende risikoorientierte Durchsetzung in der CRA-Einführungsphase

Ausgangslage

Die Herstellung vollständiger CRA-Konformität erfordert in vielen Unternehmen nicht nur technische Anpassungen. Dokumentierte, nachvollziehbare und auditierbare Entwicklungs-, Schwachstellenmanagement- und Compliance-Prozesse müssen aufgebaut und in bestehende Abläufe integriert werden. Ausgangsniveau, Reifegrad und Produktportfolio unterscheiden sich erheblich, insbesondere bei kleinen und mittleren Unternehmen.

CRA-Herausforderung

Abhängig von Unternehmensgröße und Produktportfolio kann diese Transformation mehrere Jahre dauern. Unternehmen müssen technische und organisatorische Defizite parallel beheben, obwohl zentrale Auslegungshilfen und Nachweisgrundlagen teilweise noch nicht vorliegen. Zum Geltungsbeginn können deshalb auch bei Produkten ohne konkretes Sicherheitsproblem formale oder prozessuale Lücken verbleiben. Eine unterschiedslose Durchsetzung sämtlicher Anforderungen ab dem ersten Tag würde tatsächliche Produktrisiken und bloße Nachweisdefizite gleichbehandeln.

Mögliche Konsequenz

Kleine und mittlere Hersteller könnten gezwungen sein, Produkte vorübergehend vom Markt zu nehmen oder deren Weiterentwicklung einzustellen, obwohl von ihnen kein konkretes zusätzliches Cybersicherheitsrisiko ausgeht. Hersteller, Händler und Anwender wären mit erheblicher Rechtsunsicherheit konfrontiert, während notwendige Prozess- und Produktanpassungen nicht kurzfristig nachgeholt werden können. Dies könnte Marktaustritte, Versorgungsengpässe und Belastungen bestehender digitaler Wertschöpfungsketten auslösen.

Verbesserungsvorschlag

Für die Anfangsphase der CRA-Anwendung sollte die Marktüberwachung risikoorientiert und verhältnismäßig vorgehen. Bei formalen oder prozessualen Defiziten ohne konkretes Sicherheitsrisiko sollten Unternehmen zunächst eine angemessene Frist zur Abstellung erhalten. Unmittelbare Vertriebsbeschränkungen und andere einschneidende Maßnahmen sollten vorrangig auf Fälle konzentriert werden, in denen von einem Produkt ein tatsächliches Cybersicherheitsrisiko ausgeht.

Querschnittsbedarf: Risikobasierte Auslegung von Anhang I

Produkte mit digitalen Elementen unterscheiden sich erheblich hinsichtlich Architektur, Einsatzumgebung, Bedrohungsmodell und Aktualisierungsmöglichkeiten. Einzelne Anforderungen des Anhangs I können deshalb je nach Kontext unterschiedliche Auswirkungen auf das tatsächliche Sicherheitsniveau haben. Dies betrifft etwa die Bewertung der Ausnutzbarkeit von Schwachstellen sowie Updatekanäle, die in besonders abgeschotteten Systemen selbst zusätzliche Angriffsflächen schaffen können. Fehlen klare Bewertungsmaßstäbe, können Hersteller, Konformitätsbewertungsstellen und Marktüberwachungsbehörden zu unterschiedlichen Ergebnissen gelangen. Eine rein formale Anwendung kann im Einzelfall technisch ungeeignete Maßnahmen begünstigen oder bewährte Sicherheitsarchitekturen beeinträchtigen.

Die Anforderungen des Anhangs I sollten daher konsequent risikobasiert und unter Berücksichtigung des konkreten Einsatzkontexts ausgelegt werden. Europäische Kommission und ENISA sollten hierzu praxisnahe Leitlinien mit Kriterien, Bedrohungsmodellen und relevanten Grenzfällen entwickeln. Alternative technische Maßnahmen sollten möglich sein, wenn nachvollziehbar ein mindestens gleichwertiges Sicherheitsniveau erreicht wird.

Fazit

Die mit dem CRA verfolgten Ziele werden von der Wirtschaft ausdrücklich unterstützt. Die dargestellten Szenarien zeigen jedoch wiederkehrende strukturelle Herausforderungen. Sie beruhen weniger auf mangelnder Umsetzungsbereitschaft als auf regulatorischen Vorgaben, die technische Abhängigkeiten, komplexe Lieferketten, unterschiedliche Produktlebenszyklen, begrenzte Bewertungskapazitäten und die Vielfalt der erfassten Produkte nicht ausreichend berücksichtigen.

Dadurch entstehen Rechtsunsicherheit, unverhältnismäßiger Nachweisaufwand und praktische Umsetzungsprobleme. Auch Hersteller mit hohem Sicherheitsniveau können Schwierigkeiten haben, die Anforderungen fristgerecht nachzuweisen, wenn maßgebliche Standards, Leitlinien, Zulieferinformationen oder Bewertungskapazitäten nicht rechtzeitig verfügbar sind. Zugleich besteht das Risiko, dass sichere Produkte vom Markt genommen, notwendige Updates oder Anpassungen verzögert und spezialisierte Anbieter strukturell benachteiligt werden. Dies kann Wettbewerb, Produktverfügbarkeit und die Resilienz europäischer Lieferketten schwächen.

Der CRA sollte daher stärker risikobasiert, verhältnismäßig und entlang des Produktlebenszyklus umgesetzt werden. Erforderlich sind klare Auslegungshilfen, praktikable Nachweisverfahren, die Anerkennung bestehender Zertifizierungen und Prüfberichte sowie angemessene Übergangsregelungen, wenn Voraussetzungen für die Konformitätsbewertung fehlen. Entscheidend ist, dass die regulatorische Umsetzung tatsächliche Sicherheitsrisiken adressiert und Unternehmen Handlungsspielraum für geeignete technische und organisatorische Maßnahmen in unterschiedlichen Produkten und Einsatzumgebungen lässt.