Bundesverband
Gesundheits-IT – bvitg e. V.

bvitg-Positionspapier

zum Cyber Resilience Act

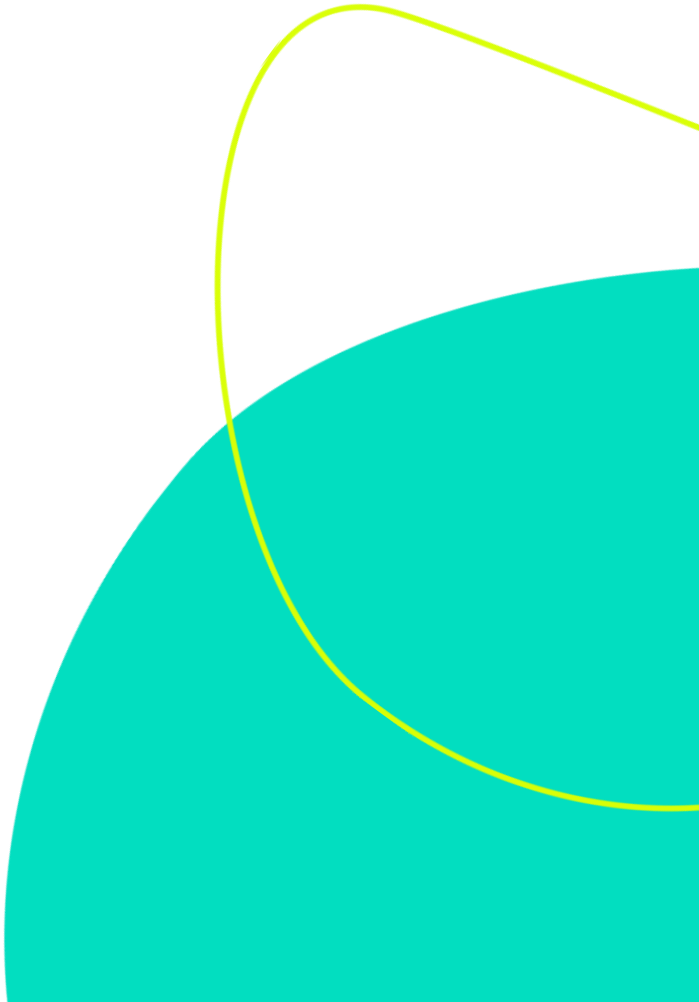
Kontakt:

Elias Kaiser

Referent eHealth

elias.kaiser@bvitg.de

bvitg.de



Gemeinsam mit seinen Mitgliedsunternehmen arbeitet der Bundesverband Gesundheits-IT – bvitg e. V. intensiv daran, die Gesundheits-IT für alle Versorgungsbereiche zu etablieren, um so die Gesundheitsversorgung der Menschen in Deutschland nachhaltig zu verbessern.

Der bvitg nimmt zu den Vorgaben der Europäischen Union zum Cyber Resilience Act aus 2026 und deren Umsetzung Bezug. Die folgende Ausarbeitung hat zum Ziel, betroffenen Organisationen und Einrichtungen eine Orientierung zur Umsetzung der Anforderungen des Cyber Resilience Act an die Hand zu geben.

1. Einleitung/ Herleitung des Themas

Der von der Europäischen Union 2024 verabschiedete Cyber Resilience Act (CRA) stellt einen wichtigen Schritt zur Stärkung der Cybersicherheit von Produkten am europäischen Markt dar. Bis zu seinem vollständigen Wirksamwerden am 11. Dezember 2027 bestehen jedoch weiterhin zahlreiche Fragen hinsichtlich der konkreten Ausgestaltung und Umsetzung, die für die betroffenen Industriezweige von zentraler Bedeutung sind.

Diese Ausarbeitung hat das Ziel, unseren Mitgliedsunternehmen sowie weiteren interessierten Akteuren aus angrenzenden Sektoren eine Handreichung zur Orientierung zu bieten. Dabei werden sowohl grundlegende Anforderungen des CRA als auch spezifische Fragestellungen aus der praktischen Umsetzungsperspektive beleuchtet:

- Pflichten für die Industrie & Geltungsbereich des CRA
- Umfang der Cybersicherheitsanforderungen & Umgang mit identifizierten Schwachstellen
- TR03183 – Betrachtung der Anforderungen des BSI
- Hinweise zur Marktüberwachung durch das BSI

1.1. Geltungsbereich & Anwendungsbereich des CRA

Der Cyber Resilience Act (Verordnung (EU) 2024/2847) schafft erstmals einen einheitlichen europäischen Rechtsrahmen für die Cybersicherheit vernetzter Hard- und Software-produkte. Er gilt branchenübergreifend sowohl für den B2B-, als auch den

B2C-Bereich und richtet sich an Hersteller, Importeure und Händler von Produkten mit digitalen Elementen.

Der CRA gilt für alle Produkte mit digitalen Elementen, die auf dem EU-Markt breitgestellt werden, also Hard- und Software sowie dazugehörige Datenfernverarbeitungslösungen, die eine direkte oder indirekte Netzwerkverbindung mit einem Gerät oder Netz auf-bauen können.

In der nachfolgenden Übersicht (kein Anspruch auf Vollständigkeit) werden erfasste und nicht erfasste Produkttypen dargestellt:

Geltungsbereich des CRA:

- Software mit Netzverbindung (lokal installiert oder als herstellerseitige Datenfernverarbeitungslösung)
- Vernetzte Hardware sowie Komponenten, die separat in den Verkehr gebracht werden.

Kein Geltungsbereich des CRA:

- Medizinprodukte (MDR, Verordnung (EU) 2017/745) und In-vitro-Diagnostika (IVDR, Verordnung (EU) 2017/746)
- Produkte der Kfz-, Luftfahrt- und Schifffahrtsbranche
- SaaS, wenn es sich um eine reine Dienstleistung handelt und die Cloud-Komponente nicht funktionsnotwendiger Bestandteil des Produkts ist
- Produkte für nationale Sicherheit und Verteidigung
- Nicht-kommerzielle Open-Source-Software
- Weitere Ausnahmen können per delegiertem Rechtsakt auf Basis von Artikel 61 CRA festgelegt werden, wenn sektorspezifische Regelungen ein gleichwertiges Schutzniveau gewährleisten.

1.2. Produktkategorien mit gestuften Anforderungen

Alle erfassten Produkte unterliegen Basisanforderungen. Darüber hinaus unterscheidet der CRA zwei erhöhte Sicherheitsstufen mit strengeren Konformitätsbewertungsverfahren:

- Wichtige Produkte (Anhang III, Klasse I) umfassen u. a. am Körper tragbare Produkte zur Gesundheitsüberwachung (z. B. Tracking-Funktionen), die nicht unter MDR oder IVDR fallen, sowie tragbare Produkte für Kinder.
- Wichtige Produkte der Klasse II erfordern grundsätzlich die Prüfung durch eine notifizierte Stelle.
- Kritische Produkte (Anhang IV), wie Smartcards oder Sicherheitsboxen, benötigen zwingend eine Zertifizierung nach einem europäischen Cybersicherheitsschema.

1.3. Grundlegende Cybersicherheitsanforderungen an Produkte mit digitalen Elementen sowie Pflichten der Wirtschaftsakteure

Die in Verkehr zu bringenden Produkte müssen so konzipiert, entwickelt und produziert werden, dass sie ein angemessenes Cybersicherheitsniveau aufweisen –auch als "Security by Design" bekannt. Dies bedeutet konkret, dass der Schutz vor unbefugten Zugriffen und Maßnahmen zur Sicherstellung von Vertraulichkeit und Integrität im Zuge der Entwicklung des Produktes mitgedacht werden.

Neben Herstellern trifft der CRA auch Importeure und Händler. Sie müssen sicherstellen, dass die von ihnen vertriebenen Produkte die Anforderungen erfüllen. Wer ein Produkt wesentlich verändert, gilt dabei als neuer Hersteller und übernimmt sämtliche Herstellerpflichten. So gilt der CRA für den gesamten Lebenszyklus eines Produkts, sprich die Cybersicherheitsanforderungen müssen ab der Konzeptionsphase und über einen Unterstützungszeitraum von in der Regel mindestens fünf Jahren erfüllt werden.

1.4. Grundlegende Cybersicherheitsanforderungen an die von den Herstellern festgelegten Verfahren zur Behandlung von Schwachstellen

Die Hersteller von Softwareprodukten sind verpflichtet, Schwachstellen aktiv zu identifizieren, zu dokumentieren und zu beheben und dafür strukturierte interne Prozesse vorzuhalten. Dazu gehört eine öffentlich zugängliche Kontaktmöglichkeit für Schwachstellenmeldungen (Coordinated Vulnerability Disclosure).

Im Falle von aktiv ausgenutzten Schwachstellen und schweren Sicherheitsvorfällen sind innerhalb enger Fristen Meldungen an die zuständigen Behörden durchzuführen. Eine Erstmeldung ist innerhalb von 24 Stunden nach Kenntnisnahme vorgesehen.

Es ist wichtig hervorzuheben, dass die Meldepflicht für Schwachstellen und Vorfälle bereits **ab dem 11. September 2026** gilt (vgl. Anhang 7.1).

1.5. Vorschriften für die Marktüberwachung

Der CRA etabliert ein europaweit koordiniertes System zur Marktüberwachung. Für den deutschen Raum wird das BSI als Aufsichtsbehörde gesehen. Zu den Pflichten gehören die Prüfungen von Produkten, die Anforderung von Konformitätsnachweisen sowie bei Verstößen entsprechende Sanktionen zu erlassen.

So sind Softwarehersteller aufgefordert, eine EU-Konformitätserklärung abzugeben und technische Unterlagen über die getroffenen Maßnahmen vorzuhalten. Je nach Risikoeinstufung (siehe 1.2) ist eine Selbstbewertung oder die Prüfung durch eine notifizierte Stelle erforderlich.

Relevanter Hinweis zur Abgrenzung: Medizinprodukte (MDR), In-vitro-Diagnostika (IVDR), Produkte der nationalen Sicherheit sowie nicht-kommerzielle Open-Source-Software fallen nicht in den Anwendungsbereich des CRA. Diese Abgrenzung ist für Hersteller aus der Gesundheits-IT von zentraler Bedeutung und wird in den folgenden Abschnitten vertieft.

2. Relevanz für die Industrie

Der CRA betrifft einen erheblichen Teil der digitalen Wertschöpfungskette im Bereich der Gesundheits-IT. Neben klassischen Softwareherstellern können auch Anbieter von Plattformen, Schnittstellen und Add-ons in den Anwendungsbereich fallen.

Wie aus der Entwicklung von Medizinprodukten bekannt, setzt der CRA voraus, dass die Hersteller früh im Produktdesign die Zweckbestimmung und eine „vernünftigerweise vorhersehbare Verwendung" festlegen. Da viele Gesundheits-IT-Lösungen als komplexe Gesamtsysteme mit zahlreichen Abhängigkeiten betrieben werden (z. B.

Betriebssysteme, Datenbanken, Middleware, Drittsoftware) berücksichtigt der Hersteller idealerweise die sicherheitsrelevanten Abhängigkeiten und Schnittstellen bereits beim Produktdesign.

Eine nachträgliche Implementierung des notwendigen Sicherheitsniveaus bei der Weiterentwicklung bestehender Lösungen kann zu einem hohen Aufwand führen. Das ist vor allem bei den zahlreich vorhandenen Legacy-Systemen eine Herausforderung, weil zu erwarten ist, dass diese über teilweise gesetzlich vorgegebene funktionale Weiterentwicklungen (z. B. ePA-Anbindung, E-Rezept-Integration) wesentliche Änderungen erfahren und damit in den Geltungsbereich des CRA fallen. In diesem Fall wird der Hersteller zum „neuen Hersteller" im Sinne des CRA und muss sämtliche Anforderungen erfüllen.

Zudem entfalten die Strafvorschriften nach Artikel 64 der Verordnung (EU) 2024/2847 eine erhebliche Wirkung: Bei Verstößen können gemäß Absatz 2 bis 4 Geldbußen von bis zu 2,5 % des jährlichen weltweiten Umsatzes oder bis zu 15 Mio. Euro verhängt werden. Dies unterstreicht die Bedeutung einer frühzeitigen und sorgfältigen Auseinandersetzung mit den regulatorischen Anforderungen.

3. Umgang mit den Anforderungen aus dem CRA

3.1. Bewertung der Cyberrisiken

Der Artikel 13 Absatz 2 verpflichtet die Hersteller, eine Bewertung der Cybersicherheitsrisiken vorzunehmen, die mit einem Produkt mit digitalen Elementen verbunden sind, und das Ergebnis dieser Bewertung bei der Planung, Gestaltung, Entwicklung zu berücksichtigen; Produktions-, Liefer- und Wartungsphasen des Produkts mit digitalen Elementen, um Cybersicherheitsrisiken zu minimieren, Vorfälle zu verhindern und ihre Auswirkungen zu minimieren, auch im Hinblick auf die Gesundheit und Sicherheit der Benutzer.

Gibt es essenzielle Anforderungen, die für das Produkt nicht relevant sind, kann dies mit einer Begründung in der Bewertung der Sicherheitsrisiken dokumentiert werden.

Gibt es technische Gründe, warum eine bestimmte Anforderung nicht umgesetzt, aber die Cybersicherheit mit anderen Maßnahmen erreicht werden kann, kann dies in der Bewertung dokumentiert werden.

Die Hersteller sollten das Produkt mit einer secure-by-default-Einstellung ausliefern, auch wenn diese unter bestimmten Bedingungen beim praktischen Einsatz auf eine weniger sichere Einstellung geändert werden.

3.2. Berücksichtigung der Lieferketten

Der Hersteller bestätigt mit dem CE-Kennzeichen, dass das Produkt die Anforderungen nach Anhang I einhält und stellt dem Anwender die Informationen nach Anhang II bereit.

Dabei muss er auch Komponenten, Drittprodukte, Bibliotheken oder Open-Source-Software berücksichtigen, die das Produkt enthält. Als Lieferant von Komponenten kann es wichtig werden, ein entsprechendes Design zu wählen und entsprechende Informationen für den Hersteller bereit zu halten. Der Lieferant der Komponenten braucht für diese nur ein CE-Kennzeichen, wenn er sie auch unabhängig von der Produktintegration auf den Markt bringt.

3.3. Stand der Technik – BSI TR 03183

Der CRA verweist auf den Stand der Technik. Dieser wird konkretisiert durch harmonisierte Normen oder „essential Requirements" der EU.

Da beide Rechtsnormen noch nicht vorliegen, kann man sich an der technischen Richtlinie BSI TR-03183 orientieren, die die Cyber-Resilienz-Anforderungen an Hersteller und Produkte aus Sicht des BSI beschreibt. Dieses Dokument stellt eine Hilfestellung ohne verpflichtenden oder verbindlichen Charakter dar und kann nicht für eine Konformitätsvermutung genutzt werden. Die BSI TR-03183 wird sukzessive weiterentwickelt und durch die korrespondierenden harmonisierten europäischen Standards ersetzt, sobald diese bereitstehen.

3.4. Zertifizierung - Konformitätsbestätigungen

Die FAQs der EU weisen bezüglich verschiedener parallel geltender Gesetze darauf hin, dass der CRA die Konformität zu den in Anhang I genannten Sicherheitsanforderungen fordert. Fordern andere Regelungen, wie die Maschinenrichtlinie, primär

wichtige Gesundheits- und Sicherheitsanforderungen sind diese ebenfalls zu erfüllen.

Die derzeit am Markt befindlichen TI-Produkte durchlaufen bereits heute umfangreiche Prüf- und Zulassungsverfahren durch die gematik.

Im Sinne einer pragmatischen Umsetzung sollte davon auszugehen sein, dass die gematik die Anforderungen des CRA in die KOB aufnimmt. Dies ist allerdings so ist derzeit noch nicht gegeben und nicht in Aussicht gestellt.

Nach aktueller Auslegung des CRA durch das BSI sind die Prüf- und Zulassungsverfahren der gematik für TI-Produkte nicht ausreichend und decken die Anforderungen des CRA nicht ab. Für Inverkehrbringer (Hersteller & Anbieter) kommt deshalb eine weitere regulatorische Ebene hinzu.

3.5. Definition von wesentlichen Änderungen

Eine wesentliche Änderung liegt vor, wenn eine Softwareaktualisierung die Zweckbestimmung des Produkts ändert, die Art der Gefahr verändert oder das Cybersicherheitsrisiko erhöht – und die aktualisierte Version auf dem Markt bereitgestellt wird. Reine Sicherheitsupdates zur Risikominderung sowie geringfügige Funktionsanpassungen (z. B. visuelle Verbesserungen oder neue Sprachen) gelten hingegen nicht als wesentliche Änderung.

Nach Erwägungsgrund 39 gibt es bereits eine Empfehlung, dass die Europäische Kommission Leitlinien für eine wesentliche Änderung bereitstellen soll. Es wird die Definition von konkreten und keinen abstrakten Beispielen als zielführend gesehen.

3.6. Fernwartung

Die Verwendung von Fernwartungslösungen für Zugriffe auf Kundensysteme ist im Gesundheitswesen alltäglich und nicht mehr wegzudenken. Die Hersteller haben eine Risikobewertung für die eingesetzten Werkzeuge durchzuführen. Es ist jedoch hervorzuheben, dass der Hersteller nicht für Fehlkonfigurationen oder Sicherheitsmängel bei externen IT-Dienstleistern haften darf. Vor diesem Hintergrund spricht sich

der bvitg für eine eindeutige vertragliche und regulatorische Trennung der Verantwortlichkeiten aus.

Fallbeschreibung: Fernwartung in einer Arztpraxis

1. Ausgangslage und Zweck der Fernwartung

In Arztpraxen und Krankenhäusern werden in Praxisverwaltungssystemen (PVS) und Krankenhausinformationssystemen (KIS) angebundene IT-Komponenten eingesetzt, die für den laufenden Betrieb, die Abrechnung sowie die Behandlung von Patientinnen und Patienten erforderlich sind. Zur Fehleranalyse, Störungsbeseitigung, Wartung und Unterstützung kann es erforderlich sein, dass der IT-Dienstleister im Einzelfall Fernzugriff auf die Systeme erhält.

Ziel der Fernwartung ist ausschließlich die technische Unterstützung (z. B. Fehlerbehebung, Konfigurationsprüfung), nicht jedoch eine inhaltliche Verarbeitung von Patientendaten.

2. Beteiligte Rollen

- Arztpraxis / Auftraggeber (AG)
  Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO und Geheimnisherr nach § 203 StGB.
- Softwarehersteller
  IT-Dienstleister und an der beruflichen Tätigkeit des Arztes mitwirkende Person (§ 203 Abs. 3 StGB), tätig als Auftragsverarbeiter i. S. d. Art. 28 DSGVO.
- Fernwartungslösung
  Einsatz der betriebenen Fernwartungslösung auf Basis und aktuellem Stand der Technik nach Artikel 32 DSGVO

3. Ablauf der Fernwartung

1. Die Fernwartung (FW) wird ausschließlich durch die Arztpraxis initiiert.
2. Der Auftraggeber ruft FW-Adresse auf.
3. 2FA Authentifizierung der Arztpraxis, Klinik
4. Der Auftraggeber erhält einen **einmalig gültigen Sitzungsschlüssel** vom Support.

5. Ein **temporärer Session-Client** wird heruntergeladen und gestartet.
6. Vor Beginn der Sitzung:
    a. Anzeige von Datenschutzhinweisen
    b. **Aktive Zustimmung** des Auftraggebers erforderlich
7. Erst nach Zustimmung kommt die Fernwartungssitzung zustande.
8. Nach Beendigung der Sitzung wird die ausführbare Datei **automatisch vom System des Auftraggebers gelöscht**.

Eine dauerhafte Installation oder ein permanenter Fernzugang bestehen nicht.

4. Zugriffsumfang und technische Einschränkungen

- Fernwartungssitzungen:
    - sind zeitlich begrenzt
    - werden **automatisch beendet**, sofern die maximale Sitzungsdauer erreicht ist
    - können nach Beendigung **nicht wiederhergestellt** werden
- Standardmäßig erfolgt der Zugriff **ohne administrative Rechte**
    - Administrative Rechte müssen gesondert angefordert und explizit freigegeben werden
- Mehrere Support-Mitarbeiter können bei Bedarf im Rahmen einer Teamsitzung teilnehmen
- Dateiübertragungen und Zwischenablage sind technisch möglich, erfolgen jedoch nur, **soweit für die Störungsbehebung erforderlich**

5. Sitzungsaufzeichnung

- Eine Aufzeichnung der Fernwartung ist **optional**
- Die Aufzeichnung erfolgt nur nach ausdrücklicher Zustimmung des Auftraggebers je Sitzung
- Aufzeichnungen werden maximal 30 Tage gespeichert und anschließend automatisch gelöscht

6. Umgang mit Patientendaten und Geheimhaltung (§ 203 StGB)

Im Rahmen der Fernwartung kann es nicht ausgeschlossen werden, dass Support-Mitarbeitende technisch Zugriff auf Bildschirminhalte erhalten, auf denen Patientendaten sichtbar sind.

Die Offenbarung erfolgt dabei:

- ausschließlich auf Veranlassung des Arztes
- nur soweit für die Durchführung der Fernwartung erforderlich
- im Rahmen des zulässigen „Mitwirkens an der beruflichen Tätigkeit“ gemäß § 203 Abs. 3 StGB

Organisatorisch ist vorgesehen, dass:

- Fernwartungen möglichst außerhalb laufender Patientenbehandlungen erfolgen
- Mitarbeiter sind angehalten, keine patientenbezogenen Inhalte aktiv zu verarbeiten
- sämtliche Support-Kontakte dokumentiert werden

7. Technische und organisatorische Schutzmaßnahmen (Auszug)

- Betrieb der Fernwartungslösung **in einer sicheren Umgebung**
- Vollständige **Verschlüsselung** der Daten auf der Fernwartungs-Appliance
- Keine Zugriffsmöglichkeit des Herstellers der Fernwartung auf Kundendaten
- Kein permanenter Fernzugang
- Einmalige Sitzungstokens
- Protokollierung und Dokumentation der Supportfälle

8. Bewertung

Die Fernwartung stellt ein erforderliches und angemessenes Mittel zur Sicherstellung des IT-Betriebs der Arztpraxis dar. Durch die Kombination aus:

- Initiierung durch den Verantwortlichen
- expliziter Zustimmung je Sitzung
- technischen Zugriffsbeschränkungen
- kurzer Speicherfristen
- vertraglicher Einbindung als Auftragsverarbeiter

wird das Risiko für Patientendaten auf ein vertretbares Mindestmaß reduziert.

3.7. SaaS mit funktionsnotwendiger Cloud

Wie in Kapitel 1.1 beschrieben, erfasst der CRA als Produktregulierung grundsätzlich keine reinen SaaS-Dienstleistungen, sobald jedoch eine Cloud-Komponente funktionsnotwendiger Bestandteil eines ausgelieferten Produkts mit digitalen Elementen ist, wird sie als Datenfernverarbeitungslösung Teil des regulierten Produkts und muss sämtliche CRA-Anforderungen erfüllen.

Für Gesundheits-IT-Hersteller, die bereits über ein C5-Testat des BSI verfügen, stellt sich daher die Frage, ob dieses als Konformitätsnachweis für den Cloud-Anteil herangezogen werden kann, dies ist jedoch nicht der Fall, da C5 die Betriebssicherheit des Cloud-Anbieters adressiert, während der CRA produktbezogene Anforderungen wie SBOM-Erstellung, Schwachstellenmeldepflichten an ENISA, Secure-by-Design-Nachweise und die CE-Konformitätsbewertung verlangt.

Dennoch ist ein bestehendes C5-Testat ein wertvoller Baustein, da viele seiner Kontrollen – etwa in den Bereichen Verschlüsselung, Zugriffsmanagement und Incident Response, als Nachweismittel in die CRA-Risikobewertung und technische Dokumentation einfließen können. Herstellern wird empfohlen, ein systematisches Mapping zwischen C5-Kontrollen und CRA-Anforderungen durchzuführen, um Synergien zu nutzen und gezielt die verbleibenden Lücken zu schließen. Perspektivisch könnte das in Entwicklung befindliche EU Cloud Security Scheme (EUCS) eine Brücke zwischen nationalen Cloud-Zertifizierungen wie C5 und der CRA-Konformitätsvermutung schaffen, was die regulatorische Anerkennung bestehender Testate erheblich vereinfachen würde.

3.8. Vorgaben für die Inbetriebnahme

Der Anhang II des CRA gibt vor, dass dem Produkt Konfigurationsanleitungen beigefügt sein müssen, die erklären, welche Maßnahmen bei der ersten Inbetriebnahme und während der gesamten Lebensdauer zu treffen sind, um die sichere Verwendung sicherzustellen. Ferner besteht die Anforderung, dass aus diesen Konfigurationsanleitungen hervorgeht, wie das Produkt in dritte Systeme sicher integriert werden kann. Das bedeutet konkret, der Hersteller muss im Handbuch bzw. in der technischen Dokumentation darlegen, wie sein Produkt sicher eingerichtet, konfiguriert und in Betrieb genommen werden kann.

Während bei Softwareprodukten für unternehmenskritische Funktionen ein CE-Kennzeichen und ein entsprechender Härtungsleitfaden in Zukunft selbstverständlich sein sollte, muss der Betreiber auch bei vermeintlich unkritischer Software prüfen, wie sich seine Angriffsfläche vergrößert und passende technisch-organisatorische Maßnahmen treffen. Produkte, die hier ausreichende Informationen bieten, werden einen Vorteil haben.

3.9. Meldepflichten

„Ein Hersteller meldet jede aktiv ausgenutzte Schwachstelle ... von der er Kenntnis erlangt ... über ... eingerichtete einheitliche Meldeplattform."

Dabei sieht der CRA eine Frist von 24 Stunden für die Erstmeldung vor und danach regelmäßige Updates.

Oft erfährt der Hersteller von einer aktiv ausgenutzten Schwachstelle nach einem Sicherheitsvorfall bei einem Betreiber, der diesen bereits im Kontext des BSI-Gesetzes gemeldet hat, oder im Kontext eines Datenschutzvorfalls, den der Verantwortliche (Leistungserbringer) bereits der Datenschutzaufsicht gemeldet hat.

So kann ein Sachverhalt in drei verschiedenen Meldeketten behandelt werden. Auf jeden Fall ergibt sich bei der Meldung von Schwachstellen nach CRA und Sicherheitsvorfällen nach NIS2/BSIG eine parallele Bearbeitung, die in der Abstimmung, was wann öffentlich gemacht wird, Herausforderungen enthält.

Vor diesem Hintergrund ist eine kritische Überprüfung etwaiger paralleler Meldewege durch den Gesetzgeber erforderlich, gleichermaßen wie das sinnvolle Zusammenführen von Meldepflichten aus diversen Verfahren.

Aus den kurzen Fristen bei der Meldung ergibt sich, dass der Hersteller ein internes Meldewesen mit klaren Regeln und Prozessen etablieren muss.

3.10. Coordinated Vulnerability Disclosure (CVD) Prozess

Der Coordinated Vulnerability Disclosure (CVD) Prozess ist eine (Praxis-)Richtlinie des BSI entsprechend internationaler Normen. Da das BSI-CERT als Meldestelle bzw.

Computer Security Incident Response Team (CSIRT) für Deutschland benannt wurde, ist der CVD als Vorgehen verpflichtend (vgl. TR 03183-3).

Über den CVD wird einerseits die Meldung von Schwachstellen geregelt, andererseits enthält er Vorschläge zur Schwachstellenbewertung und zur koordinierten Offenlegung. Über den CVD können auch Sicherheitsforschende erkannte oder vermutete Schwachstellen in den Prozess einbringen. Die Hersteller müssen in diesem Prozess die Meldung analysieren, ggf. die Schwachstellen beheben und als Security Advisory ihren Kunden kommunizieren.

Typischerweise wird eine Wartungsverpflichtung von mindestens 5 Jahren erwartet, in der auch der CVD-Prozess unterstützt wird. Wird diese Zeit deutlich unterschritten, muss das aus der erwarteten Nutzung begründet werden (z.B., wenn das Produkt von zeitlich begrenzten Ressourcen abhängig ist).

3.11. Abgrenzung von betroffenen Produkten und zentrale Unterstützung für Hersteller

Die im Referentenentwurf zum Gesetz zur Durchführung der Verordnung (EU) 2024/2847 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen (Cyberresilienz-Verordnung) angekündigten Unterstützungsleistungen, vor allem auch für KMU, in Form von spezifischer Sensibilisierungs- und Schulungsmaßnahmen und die Einrichtung eines Reallabors für Cyberresilienz begrüßen wir als Verband außerordentlich. In Verbindung mit der zugehörigen Gesetzesbegründung wird auf den Umstand hingewiesen, dass eine Individualberatung nicht möglich ist. Vor diesem Hintergrund sehen wir die Notwendigkeit, die Anforderungen so transparent darzustellen, dass Unternehmen die Betroffenheitsprüfung ohne juristischen Beistand durchführen können.

Ferner greift eine pauschale Einordnung sämtlicher Software als CRA-relevant aus Sicht der Industrie zu kurz. Vielmehr bedarf es klarer Kriterien, wann eine Software als eigenständiges Produkt mit digitalen Elementen anzusehen ist.

Die Bewertung soll sich in diesem Kontext an folgenden Kriterien orientieren:

- Kritikalität für die Patientenversorgung
- Exponiertheit gegenüber externen Netzen

- Grad der Systemintegration

Ein weiteres im Gesundheitswesen relevantes aber bisher nicht betrachtetes Szenario ist der Umgang mit Medizinprodukten. So werden in der Praxis häufig lokal betriebene Medizinprodukte über definierte Schnittstellen an ein Produkt angebunden. Die Verantwortung für die Sicherheit dieser Schnittstellen ist dabei klar aufzuteilen.

Der Hersteller des Produktes kann ausschließlich für die bereitgestellte und ordnungsgemäß dokumentierte (transparente Datenflüsse) Schnittstellen Verantwortung übernehmen, nicht jedoch für die Sicherheit des angebundenen Drittprodukts. Eine gesamtheitliche Haftung entlang der gesamten Kette ist für die Hersteller faktisch nicht umsetzbar und würde zu einer wirtschaftlichen nicht vertretbaren Mehrbelastung der Industrie führen.

4. Zu klärende Punkte:

4.1. ZETA – Umgang mit hard- und softwarebasierter Verifikation

Aus den aktuellen gematik Vorhaben zu ZETA geht hervor, dass eine hard- und softwarebasierte Verifikation erforderlich ist. Durch den technologischen Fortschritt bedingt, setzen immer mehr Architekturen auf einen virtualisierten Ansatz der Verifikation und Cloud-Technologien. Die enthaltenen Vorgaben zur physischen Hardwaremerkmalen spiegeln nicht den aktuellen Stand der Technik wider und führen zu einer vermeidbaren Einschränkung in den verfügbaren Technologien. So ist die zentrale Fragestellung zu klären, ob die erforderlichen ZETA-Komponenten verpflichtend einzubauen sind und in welcher Form die Lieferkette (Versionen, Meldepflicht, CVSS) unterstützt werden kann.

5. Fazit/Zusammenfassung

Mit dem vollständigen Wirksamwerden des CRA am 11. Dezember 2027 werden erstmals horizontale Cybersicherheitsanforderungen für sämtliche Produkte mit digitalen Elementen verbindlich. Für Hersteller von PVS, KIS, TI-Produkten oder auch Gesundheitsplattformen ergibt sich hieraus unmittelbarer Handlungsbedarf.

Besondere Dringlichkeit entfaltet die bereits ab dem 11. September 2026 geltende Meldepflicht für aktiv ausgenutzte Schwachstellen und schwerwiegende Sicherheitsvorfälle. Die Einrichtung entsprechender Melde- und Reaktionsprozesse ist daher kurzfristig zu priorisieren.

Die vorliegende Ausarbeitung hat folgende zentrale Erkenntnisse herausgearbeitet:

- Die Betroffenheit der Gesundheits-IT ist erheblich. Insbesondere Legacy-Systeme, die durch gesetzlich vorgegebene funktionale Erweiterungen, wie etwa die ePA-Anbindung oder die E-Rezept-Integration, wesentlich verändert werden, fallen in den Geltungsbereich des CRA. Der jeweilige Hersteller übernimmt in diesem Fall sämtliche Herstellerpflichten im Sinne der Verordnung.
- Bestehende Prüf- und Zulassungsverfahren werden als nicht ausreichenden eingestuft. Nach aktueller Auslegung des BSI decken die Konformitätsbewertungen der gematik die Anforderungen des CRA nicht ab. Für Hersteller und Anbieter entsteht somit eine zusätzliche regulatorische Ebene, deren Verhältnis zu bestehenden Verfahren dringend der Klärung bedarf.
- Harmonisierte europäische Normen liegen noch nicht vor. Bis zu deren Veröffentlichung bietet die Technische Richtlinie BSI TR-03183 eine fachliche Orientierung, begründet jedoch keine Konformitätsvermutung. Hersteller sind angehalten, diese Richtlinie als Ausgangspunkt für die Umsetzung heranzuziehen und die Entwicklung der harmonisierten Standards aufmerksam zu verfolgen.
- Bestehende Zertifizierungen können Synergien entfalten. Insbesondere C5-Testate, ISO-27001-Zertifizierungen sowie gematik-Nachweise lassen sich als Bausteine in die CRA-Risikobewertung und technische Dokumentation einbringen. Ein systematisches Mapping auf die CRA-Anforderungen ist gleichwohl erforderlich, um verbleibende Lücken gezielt zu schließen.
- Die Abgrenzung und Harmonisierung paralleler Meldepflichten sind ungelöst. Die Überschneidungen zwischen CRA, DSGVO und weiteren IT-Sicherheitsvorgaben bergen das Risiko redundanter Meldungen zum selben Sachverhalt. Der bvitg spricht sich für eine kritische Überprüfung und sinnvolle Zusammenführung der bestehenden Meldewege durch den Gesetzgeber aus.

- Die Verantwortungsabgrenzung in der Lieferkette bedarf klarer Regelungen. Hersteller können ausschließlich für die von ihnen bereitgestellten und dokumentierten Schnittstellen Verantwortung übernehmen. Eine gesamtheitliche Haftung entlang der gesamten Integrationskette ist weder fachlich noch wirtschaftlich vertretbar.
- Der bvitg empfiehlt seinen Mitgliedsunternehmen, unverzüglich mit der systematischen Umsetzung der CRA-Anforderungen zu beginnen. Dies umfasst insbesondere die Durchführung einer produktbezogenen Betroffenheitsanalyse, die Integration von SBOM-Prozessen in die Entwicklungspipelines, die Einrichtung von CVD-Kontaktstellen sowie die vertragliche Klärung von Verantwortlichkeiten in der Lieferkette. Die im Referentenentwurf des BMI angekündigten Unterstützungsleistungen, insbesondere das Reallabor für Cyberresilienz, werden ausdrücklich begrüßt.

Angesichts des Sanktionsrahmens von bis zu 15 Millionen Euro oder 2,5 Prozent des weltweiten Jahresumsatzes ist eine frühzeitige und strukturierte Auseinandersetzung mit den regulatorischen Anforderungen geboten.

6. Danksagung

Besonderen Dank ist an dieser Stelle den beteiligten Autor:innen auszusprechen, ohne deren Engagement die Ausarbeitung nicht möglich gewesen wäre.

- Christoph Isele (Oracle Health)
- Christof Schelian (RpDoc Solutions GmbH)
- Jens Schreiber (medatixx GmbH & Co. KG)
- Susann Schnabel (KoSyMa GmbH)

7. Anhang

7.1. Übersicht zum Zeitplan und Meilensteinen der CRA-Umsetzung (Stand Mai 2026)

Datum	Meilenstein	Status
28. Nov. 2025	Durchführungsverordnung (EU) 2025/2392 zu technischen Beschreibungen der Kategorien wichtiger und kritischer Produkte (Anhang III/IV). Veröffentlicht am 1.12.2025, in Kraft seit 21.12.2025.	Umgesetzt
11. Dez. 2025	Delegierte Verordnung (EU) 2026/881 zu den Bedingungen, unter denen CSIRTs die Weiterleitung von Schwachstellenmeldungen über die Single Reporting Platform verzögern dürfen. Am 11.12.2025 angenommen, veröffentlicht.	Umgesetzt
3. März 2026	EU-Kommission veröffentlicht **Entwurf** der Guidance zur CRA-Umsetzung (Art. 26 CRA). Öffentliche Konsultation bis 31. März 2026.	Teilweise umgesetzt – Entwurf veröffentlicht, finale Fassung steht aus
Vor 11. Sept. 2026	ENISA entwickelt die Single Reporting Platform (SRP), die bis zum 11. September 2026 betriebsbereit sein muss. Dafür wurde ein externer Dienstleister über eine öffentliche Ausschreibung beauftragt (Volumen ca. 11 Mio. €). Eine Testphase unter Einbindung des CSIRTs Network ist vor dem Go-Live vorgesehen.	In Umsetzung
11. Juni 2026	Vorschriften zur Notifizierung von Konformitätsbewertungsstellen treten in Kraft. Mitgliedstaaten müssen notifizierende Behörden benennen.	Steht unmittelbar bevor

Q3 2026	Erste Standardisierungslieferungen der europäischen Normungsorganisationen (CEN/CENELEC/ETSI) – horizontale und produktspezifische Normen.	Geplant
11. Sept. 2026	**Meldepflichten treten in Kraft.** Aktiv ausgenutzte Schwachstellen und schwere Sicherheitsvorfälle müssen über die Single Reporting Platform (ENISA) gemeldet werden. Erstmeldung innerhalb von 24 Stunden.	In 4 Monaten
Q4 2026	Delegierter Rechtsakt zur Konformitätsvermutung zwischen dem europäischen Cybersicherheitszertifizierungsschema EUCC (Common Criteria) und dem CRA.	Geplant
11. Dez. 2026	Zielvorgabe: Ausreichende Anzahl notifizierter Konformitätsbewertungsstellen in den Mitgliedstaaten.	Zielvorgabe – Erreichung unsicher
30. Okt. 2027	Weitere Standardisierungslieferungen der Normungsorganisationen.	Geplant
11. Dez. 2027	**Vollständige Anwendung des CRA.** Alle neu in Verkehr gebrachten Produkte mit digitalen Elementen müssen sämtliche Anforderungen erfüllen. CE-Kennzeichen inkl. Cybersicherheit erforderlich.	Harte Deadline