Der EU Cyber Resilience Act

Orientierung, Herausforderungen

und

praktische Tipps zur Umsetzung

THOMAS KRENZKE

SEKAS GmbH | Baierbrunner Str. 23, 81379 München

SEKAS
SOFTWARE ENGINEERING

Executive Summary

Cybersecurity wird Pflicht – und strategischer Vorteil.

Mit dem **EU Cyber Resilience Act (CRA)** bringt die Europäische Union erstmals verbindliche Cybersicherheitsanforderungen für vernetzte Produkte auf den Weg. Ab 2027 dürfen nur noch digitale Systeme in der EU verkauft werden, die konkrete Vorgaben zu Risikoanalyse, Sicherheitsupdates, Dokumentation und Schwachstellenmanagement erfüllen – über den gesamten Lebenszyklus hinweg.

Der CRA ist weit mehr als ein juristisches Regelwerk. Er beeinflusst Architekturentscheidungen, Produktdesign, Entwicklungsprozesse und Updatefähigkeit. Wer künftig digitale Produkte entwickelt, vertreibt oder importiert, trägt neue **regulatorische Verantwortung** – mit direkter Auswirkung auf Marktzugang, Time-to-Market und technische Wartbarkeit.

Dieses Whitepaper bietet eine kompakte Orientierung:

- Was ist der EU Cyber Resilience Act – und welche Produkte sind betroffen?
- Wie werden digitale Produkte in Risikoklassen eingestuft – und was bedeutet das?
- Welche Anforderungen gelten für Entwicklung, Updatefähigkeit und Schwachstellenmanagement?
- Was sind typische Umsetzungsfehler – und wie lassen sie sich vermeiden?
- Welche rechtlichen Vorgaben gelten – und wie unterscheiden sie sich von NIS2 & Co?
- Warum Technik und Recht zusammen gedacht werden müssen – und wie externe Partner helfen können

Ob mittelständischer Hersteller oder OEM-Zulieferer: CRA-Compliance ist kein Selbstzweck – sondern ein notwendiger Baustein für **mehr Security, Vertrauen und Zukunftsfähigkeit**.

Wer jetzt handelt, gewinnt Sicherheit und Gestaltungsspielraum.

Inhalt

1 Orientierung: Was ist der CRA – und wen betrifft er?

1.1 Überblick über den EU Cyber Resilience Act

Der **Cyber Resilience Act (CRA)** ist eine neue EU-Verordnung. Sie legt zum ersten Mal einheitliche **Cybersicherheitsanforderungen für Produkte mit digitalen Elementen** fest. Ziel ist es, das wachsende Risiko durch Schwachstellen in vernetzter Hard- und Software systematisch zu reduzieren - über den gesamten Lebenszyklus eines Produkts hinweg.

Mit dem CRA führt die EU zum ersten Mal verbindliche Cybersicherheitsstandards ein, die als rechtliche Voraussetzung für den Verkauf in Europa gelten. Das ist vergleichbar mit CE- oder RoHS-Vorgaben, allerdings liegt beim CRA der Schwerpunkt auf digitaler Sicherheit.

1.2 Sind Sie betroffen?

Entwickeln, vertreiben oder importieren Sie technische Systeme oder Softwarelösungen mit digitalen Funktionen, die **in der EU genutzt** werden?

Dann kann der CRA auch für Sie relevant sein.

Der CRA gilt für alle Produkte mit digitalen Elementen, die sich **direkt oder indirekt** mit anderen **Geräten, Systemen oder Netzwerken verbinden** können. Es ist dabei egal, ob dies über das Internet, ein lokales Netzwerk oder interne Schnittstellen geschieht. Eine weitere Bedingung ist, dass sie **in der EU verkauft** werden. Dabei spielt es keine Rolle, ob sie für industrielle oder private Anwendungen bestimmt sind.

Sie sind betroffen, wenn Sie beispielsweise:

- vernetzte Geräte oder Komponenten für technische Anlagen entwickeln
- Applikationen bereitstellen, die in verteilten oder eingebetteten Systemen eingesetzt werden
- Plattformen oder Tools zur Steuerung, Überwachung oder Optimierung technischer Prozesse anbieten
- Systeme liefern, die hohe Anforderungen an Verfügbarkeit, Sicherheit oder Wartbarkeit erfüllen müssen – über viele Jahre hinweg
- digitale Produkte mit Netzwerkanbindung auf dem europäischen Markt vertreiben oder importieren

Nicht betroffen sind z. B.

- nicht-kommerzielle Open-Source-Software
- Produkte, die technisch nicht vernetzbar sind (also keine Möglichkeit zur Netzwerkverbindung besitzen – weder direkt noch über andere Komponenten)

1.3 Was fordert der CRA konkret?

Die Vorgaben des Cyber Resilience Act gelten nicht nur für **neue Entwicklungen**. Auch **bereits am Markt befindliche Produkte** können betroffen sein. Wenn Sie digitale Produkte entwickeln oder vertreiben, müssen Sie künftig die Anforderungen des CRA erfüllen.

Der CRA verpflichtet Hersteller, Importeure und Händler zu verschiedenen Maßnahmen:

- **Risikobewertung & Risikoklassifizierung**
  → Bevor etwas entwickelt oder geändert wird, muss geklärt werden:
  Welches Risiko hat das Produkt?
  Welcher Risikoklasse gehört es an?
- **Security by Design & by Default**
  → Basierend auf der Risikobewertung muss das Produkt von Anfang an sicher gestaltet und vorkonfiguriert sein. Sicherheit ist nicht optional, sondern integraler Bestandteil der Produktentwicklung.
- **SBOM (Software Bill of Materials)**
  → Schon im Designprozess müssen sämtliche Software-Komponenten erfasst und dokumentiert werden – **auch bei bestehender Software**. So wird Transparenz geschaffen und die Nachverfolgbarkeit für spätere Updates sichergestellt.
- **Sicherheitsarchitektur & Schwachstellenmanagement**
  → Sicherheitsmaßnahmen müssen von Anfang an eingeplant und im Betrieb durch laufendes Monitoring, Schwachstellenscans und Updates abgesichert werden.
- **Updatefähigkeit & Supportpflichten**
  → Bereits vor Markteinführung muss geklärt sein, wie Sicherheitsupdates im Einsatz erfolgen – auch bei älteren oder bereits ausgelieferten Produkten.
- **Lebenszyklus-Dokumentation & Nachweispflicht**
  → Alle Sicherheitsmaßnahmen, Prüfungen und Änderungen müssen vollständig dokumentiert werden, um bei Audits oder Behördenanfragen transparent Rechenschaft ablegen zu können.
- **Konformitätsbewertung & CE-Kennzeichnung**
  → Je nach Risikoklasse erfolgt die Konformitätsprüfung entweder intern (Selbsterklärung) oder extern (benannte Stelle). Das CE-Kennzeichen dient als sichtbarer Nachweis der Einhaltung.
- **Meldepflichten**
  → Sobald ein Produkt im Feld ist, gelten strikte Meldepflichten: Bei einem Sicherheitsvorfall muss dieser innerhalb von **24 Stunden** gemeldet werden.

Dabei betrifft der CRA nicht nur klassische IT-Produkte, sondern auch **industrielle**

Systeme, technische Anwendungen und Embedded Software, wenn diese mit Netzwerken oder anderen Geräten verbunden sind.

1.4 Warum CRA-Compliance mehr ist als NIS2 & Co

Der Cyber Resilience Act (CRA) ergänzt bestehende EU-Regelwerke wie **NIS2**, die **RED-Richtlinie** oder die **Medizinprodukteverordnung (MDR)**, richtet sich jedoch mit eigenständigen Anforderungen gezielt an **Hersteller, Händler und Importeure von Produkten mit digitalen Elementen**. Während NIS2 vorrangig organisatorische Anforderungen an kritische Infrastrukturen stellt, legt der CRA produktbezogene Pflichten fest.

Auch wenn es inhaltliche Überschneidungen gibt – etwa bei Sicherheitsanforderungen, Meldepflichten oder Software-Integrität –, **führt die Erfüllung dieser Regelwerke nicht automatisch zur CRA-Konformität**. Der CRA bringt eigene, produktbezogene Pflichten mit sich, insbesondere im Hinblick auf sichere Entwicklung, Schwachstellenmanagement, CE-Kennzeichnung und Support über den gesamten Produktlebenszyklus hinweg.

Für viele Unternehmen bedeutet das: eine neue, eigenständige regulatorische Verantwortung – mit entsprechendem organisatorischem und technischem Umsetzungsaufwand.

1.5 Diese CRA-Termine sollten Sie kennen

11. Juni 2026: Benannte Konformitätsbewertungsstellen dürfen die CRA-Konformität von Produkten prüfen

11. September 2026: Die Meldepflicht für Sicherheitsvorfälle und Schwachstellen tritt in Kraft

11. Dezember 2027: Alle betroffenen Produkte müssen die vollständigen Anforderungen erfüllen

1.6 Wie der CRA Risiken klassifiziert – und warum das wichtig ist

Der CRA ordnet Produkte mit digitalen Elementen einer von vier Risikoklassen zu. Diese Klassifizierung bestimmt, wie streng die regulatorischen Anforderungen sind – von einfachen Selbsterklärungen bis hin zu unabhängigen Prüfverfahren.

Risikoklasse	Beschreibung
Standardklasse	In diese Klasse fallen die meisten Produkte. Eine Selbsterklärung des Herstellers genügt. Das sind z.B. Smartphones, Laptops, Smarthome-Geräte (z. B. smarte Leuchten oder Staubsauger-Roboter), Smartwatches, vernetztes Spielzeug,

	allgemeine PC- oder Konsolen-Software
Wichtige Klasse I	Produkte mit erhöhtem Risiko, z. B. sicherheitsrelevante Software, für die zusätzliche Anforderungen gelten. Das sind z.B. Passwort-Manager, Identity- & Access-Management-Systeme, Betriebssysteme (Desktop/Server), Netzwerk-Management-Software, Router / Switches
Wichtige Klasse II	Produkte mit stark erhöhtem Zugriffspotenzial oder kritischem Netzwerkzugang. Das sind z.B. Firewalls, Intrusion-Detection/Prevention-Systeme
Kritische Klasse	Nur wenige Produkte, aber mit besonders hohen Sicherheitsanforderungen. Externe Prüfstellen sind hier verpflichtend. Das sind z.B. Hardware-Security-Module (HSM), Smartcards / Secure-Elements, intelligente Strom-/Gas-Zähler (Smart-Meter-Gateways)

Je höher die Risikoklasse, desto strenger die Regeln: **Prüfpflichten steigen, Dokumentationsaufwand wächst**. Die zentrale Herausforderung für Unternehmen ist es daher, die richtige Einstufung frühzeitig vorzunehmen – und das passende Verfahren zu wählen.

Warum das wichtig ist:
Eine falsche Klassifizierung kann teure Verzögerungen nach sich ziehen. Wer von Anfang an klar plant, reduziert Aufwand, spart Ressourcen und bleibt regulatorisch auf Kurs.

Eine **kompetente Beratung** unterstützt dabei, **Risiken realistisch einzuschätzen** – und den **Aufwand auf das nötige Maß zu begrenzen**.

1.7 Was passiert, wenn der EU CRA nicht beachtet wird?

Wer die Vorgaben des CRA ignoriert, riskiert empfindliche Konsequenzen:

- Bußgelder durch Aufsichtsbehörden
- Produktrückrufe oder Verkaufsverbote
- erheblicher Reputationsverlust gegenüber Kunden und Partnern
- erhöhtes Haftungsrisiko bei Sicherheitsvorfällen

In einem Umfeld wachsender Sicherheitsanforderungen ist es deshalb ratsam, die **CRA-Vorgaben frühzeitig umzusetzen** – nicht nur aus rechtlicher Sicht, sondern auch als Zeichen für verantwortungsbewusste Produktentwicklung.

2 Fachbeiträge: Herausforderungen in der Praxis

2.1 Warum viele Hersteller vor einer Make-or-Buy Entscheidung stehen – und was dabei zu bedenken ist

2.1.1 Vom Hardwareanbieter zum Softwareverantwortlichen

In den letzten Jahren hat sich die Rolle vieler Gerätehersteller grundlegend verändert. Früher war es eine klassische Hardware-Disziplin. Heute ist diese ohne Software kaum noch denkbar. Maschinen, Steuerungen und Sensoren sind zunehmend vernetzt, smart und digital gesteuert. Damit rückt ein Thema in den Fokus, das lange nur eine untergeordnete Rolle spielte: **IT-Sicherheit**.

2.1.2 Der Cyber Resilience Act verändert die Spielregeln

Der EU Cyber Resilience Act (CRA) führt eine **neue gesetzliche Verpflichtung** ein. Er bringt Anforderungen mit sich, die weit über technische Schutzmaßnahmen hinausgehen.

Der CRA verlangt ein **strukturiertes, ganzheitliches Vorgehen**:

- Risiken analysieren und Bedrohungsszenarien ableiten
- ein Sicherheitskonzept erstellen
- technische Schutzmaßnahmen planen und umsetzen
- laufendes Schwachstellenmonitoring und geregeltes Patchmanagement einführen
- Nachweisdokumentation während der gesamten Nutzungsdauer führen

Für viele kleine und mittlere Hersteller stellt dies eine **echte Herausforderung** dar. Zwar liefern sie schon lange Software mit aus, doch **Security und Compliance sind selten Teil ihrer DNA**. Es fehlen Prozesse zur sicheren Entwicklung, ebenso Kapazität oder Know-how. Oftmals sollen sich die eigenen Experten aber auch schlicht auf ihr **Kerngeschäft konzentrieren** können.

Der Geschäftsführer eines mittelständischen Herstellers bringt es auf den Punkt:

> *„CRA – damit muss ich mich beschäftigen. Aber habe ich einen Vorteil, wenn ich das alles selbst mache? Eher nicht. Für mich ist das eine einfache Make-or-Buy-Entscheidung.“*

2.1.3 Make-or-Buy: Eine Frage der Effizienz und Sicherheit

Genau diese Frage stellt sich derzeit vielen Unternehmen: **Bauen wir die nötigen Kompetenzen und Strukturen intern auf? Oder holen wir uns gezielt externe Unterstützung ins Haus?**

Wer sich für den zweiten Weg entscheidet, erhöht die Sicherheit für eine angemessene und lückenlose Umsetzung. Zudem bindet er keine Entwicklungsressourcen und muss keine neuen internen Rollen schaffen.

Der **Aufwand** ist tatsächlich **nicht zu unterschätzen**, wenn man das Thema eigenständig und ohne externe Unterstützung angehen möchte. Wer CRA-konform entwickeln will, muss sich nicht nur technisch absichern. Eine **umfassende Einarbeitung in ein neues regulatorisches Umfeld** ist ebenfalls notwendig. Das

bedeutet, **rechtliche Anforderungen** zu verstehen und Prozesse neu zu denken. Gleichzeitig muss man bewerten können, was sicherheitstechnisch überhaupt als „***Stand der Technik***" gilt.

Diese Vielschichtigkeit ist **anspruchsvoll**. Sie erfordert **juristische Expertise**, ein gutes **Gespür für Prozessgestaltung** und **tiefes technisches Verständnis**, besonders im Bereich Software-Security.

2.1.4 Die Risiken der Eigenverantwortung

Die **Einarbeitung ist aufwendig und fehleranfällig**. Sie birgt ein doppeltes Risiko:

- wichtige Aspekte werden **übersehen oder falsch interpretiert** – das führt zu **fehlender Compliance**
- es entstehen **unnötig hohe Kosten** durch überdimensionierte oder zu komplexe Lösungen

Der CRA ist **dynamisch**. Viele Vorgaben sind bewusst vage formuliert, beispielsweise die Anforderung, ein „***angemessenes Sicherheitsniveau nach dem Stand der Technik***" zu erreichen. Was heute als ausreichend gilt, ist womöglich morgen schon veraltet.

Wer allein die Verantwortung übernimmt, muss diese Entwicklungen kontinuierlich verfolgen, bewerten und in bestehende Prozesse überführen. Auch dies bindet dauerhaft Ressourcen und erhöht das Risiko, durch kleine Versäumnisse später Probleme zu bekommen.

2.1.5 Ein starker Partner bringt Sicherheit und Vertrauen

Oft ist es **sinnvoller, sich Unterstützung zu holen**. So wird sichergestellt, dass die Anforderungen des CRA vollständig berücksichtigt werden, **ohne unnötig Entwicklungsressourcen zu binden** oder neue interne Rollen zu schaffen. Dies gilt besonders, wenn die technische und rechtliche Begleitung **aus einer Hand** kommt.

Security ist beim CRA nicht nur Technik, sondern auch Dokumentation, Verantwortung und Nachweisführung. Ein erfahrener Partner, der individuell unterstützt, ist daher oft der Schlüssel zu einer **pragmatischen und wirtschaftlich tragfähigen Lösung**.

Dabei bedeutet **externe Unterstützung keineswegs, die Kontrolle aus der Hand zu geben**: Ein guter Partner arbeitet transparent. Statt auf Alleingänge setzt er auf Zusammenarbeit – damit **Ihre Experten Knowhow aufbauen** und Sie langfristig **selbstständig agieren** können. Der Partner versteht sich im Idealfall als Unterstützer und Begleiter, der sich aber selbst prinzipiell ersetzbar macht.

Ein zusätzlicher Vorteil: Der CRA erlaubt zwar grundsätzlich die Selbsterklärung der Konformität für viele betroffene Produkte. Allerdings wirkt eine **externe Einschätzung durch einen spezialisierten Partner gegenüber Kunden und Geschäftspartnern deutlich glaubwürdiger**.

Wer ein fundiertes, von außen begleitetes Vorgehen nachweisen kann, signalisiert Professionalität und Verantwortung. Dies kann gerade in komplexen Lieferketten ein echter **Vertrauensvorsprung** sein.

2.2 Der CRA aus juristischer Sicht – Beitrag von SFRP

2.2.1 Rechtliche Anforderungen

Nach der Verabschiedung von **DORA** für den Finanzsektor und der **NIS-2-Richtlinie** für kritische Infrastrukturen wird mit dem **CRA** nun erstmals eine **horizontal anwendbare Verordnung** eingeführt, die **auf alle Wirtschaftsbereiche** abzielt.

Typische Beispiele sind vernetzte Haushaltsgeräte, IoT-Komponenten oder industrielle Steuerungseinheiten. Ausgenommen sind hingegen digitale Dienstleistungen, insbesondere SaaS-Angebote, sowie quelloffene Software, die ohne kommerziellen Hintergrund entwickelt wird. Diese Abgrenzung trägt der fortschreitenden Dienstleistungsorientierung digitaler Inhalte Rechnung.

Besonders hervorzuheben ist die Einbeziehung sogenannter **Datenfernverarbeitungslösungen**, die Bestandteil eines Produkts sind und für dessen Funktionalität erforderlich bleiben. Hierdurch wird sichergestellt, dass **cloudbasierte Backend-Dienste**, die zur Aufrechterhaltung der Produktsicherheit beitragen, den gleichen Sicherheitsanforderungen unterliegen wie das physische Produkt selbst.

2.2.2 Was ist neu?

Der CRA differenziert zwischen verschiedenen Risikoklassen: Neben Standardprodukten gibt es **kritische** sowie **hochkritische Produkte mit digitalen Elementen**. Die Einstufung erfolgt anhand festgelegter Kriterien, wie der Nutzung in sensiblen Umgebungen oder dem potenziellen Ausmaß der Auswirkungen eines Vorfalls. **Hochkritische Produkte** müssen zusätzlich ein **europäisches Cybersicherheitszertifikat** nach der Verordnung (EU) 2019/881 vorweisen. Die Europäische Kommission ist befugt, per **delegierter Rechtsakte** weitere Produktkategorien zu definieren und diesen Risikoklassen zuzuordnen.

Die Klassifizierung hat unmittelbare Auswirkungen auf die **Konformitätsbewertungsverfahren, Dokumentationspflichten und technische Anforderungen**. Für Hersteller bedeutet dies eine Pflicht zur **proaktiven Risikoanalyse bereits in der Designphase**, da spätere Umklassifizierungen erhebliche Auswirkungen auf die Produktstrategie und Marktzulassung haben können.

2.2.3 Typische juristische Fallstricke - und wie man sie vermeidet

Hersteller sind verpflichtet, von der Konzeption bis zum Inverkehrbringen und darüber hinaus umfassende Sicherheitsmaßnahmen zu gewährleisten.

Kernpflichten sind die **Gewährleistung eines angemessenen Schutzniveaus** gegen bekannte Schwachstellen, die Durchführung von **Risikobewertungen**, ein stringentes **Lieferkettenmanagement** und die Implementierung eines **effektiven Schwachstellenmanagements** über die gesamte Produktlebensdauer. **Sicherheitsupdates** müssen für mindestens fünf Jahre oder die zu erwartende Lebensdauer bereitgestellt werden.

Die Pflicht zur kontinuierlichen Überwachung umfasst auch die Einrichtung von **Prozessen zur Annahme und Verarbeitung von Schwachstellenmeldungen** aus externen Quellen.

Hersteller werden damit verpflichtet, sog. „**Coordinated Vulnerability Disclosure-Verfahren**" vorzuhalten, um mit ethischen Hackern, Sicherheitsforschern und

anderen Hinweisgebern effizient kommunizieren zu können. Die Etablierung eines **Bug-Bounty-Programms** wird dabei als **Best Practice** angesehen.

2.2.4 Warum technische und rechtliche Perspektiven zusammen gedacht werden müssen

Der CRA verpflichtet Hersteller, **aktiv ausgenutzte Schwachstellen und sicherheitsrelevante Vorfälle innerhalb von 24 Stunden** nach Bekanntwerden an die **ENISA** zu melden. Auch Nutzer der betroffenen Produkte sind unverzüglich zu informieren. Die Meldung muss neben Details zur Schwachstelle auch Angaben zu eingeleiteten Korrektur- und Minderungsmaßnahmen enthalten. Ergänzend bestehen Informationspflichten gegenüber den zuständigen Marktüberwachungsbehörden.

Diese Meldepflicht erfordert die Einrichtung **permanenter interner Überwachungs- und Incident-Response-Strukturen**, die im Idealfall rund um die Uhr verfügbar sind. Für kleinere Unternehmen stellt dies eine erhebliche Herausforderung dar. Die Meldepflicht kollidiert außerdem potenziell mit anderen gesetzlichen Vorgaben, etwa jenen der Datenschutz-Grundverordnung (DSGVO), was ein sorgfältiges Koordinationsmanagement mit rechtlicher Expertise erforderlich macht.

Verstöße gegen die Pflichten des CRA können mit **erheblichen Bußgeldern** geahndet werden. Abhängig von der Schwere des Verstoßes drohen Geldbußen von bis zu 15 Millionen Euro oder 2,5 % des weltweiten Jahresumsatzes. Auch die parallele Anwendbarkeit weiterer Regelwerke wie der DSGVO erhöht das Haftungsrisiko. Für Unternehmen ist daher eine **frühzeitige Anpassung der internen Prozesse und vertragsrechtlichen Dokumente** unerlässlich.

Zusätzlich zu den finanziellen Sanktionen besteht die Gefahr erheblicher **Imageschäden, Marktverbote und zivilrechtlicher Inanspruchnahme** durch betroffene Kunden.

Der CRA verlangt daher eine **strategische Verankerung von Cybersicherheits-Compliance auf Vorstandsebene** und die Einführung **robuster Governance-Strukturen.**

3 Praxisorientierte Umsetzung: Was jetzt zu tun ist

3.1 Schritte zur Herangehensweise

3.1.1 Übersicht: Von der ersten Einordnung bis zur Umsetzung

Der EU Cyber Resilience Act betrifft eine Vielzahl technischer Produkte – doch der **Weg zur Umsetzung** ist für viele Unternehmen noch unklar. Wichtig ist zunächst eine fundierte Einordnung: Welche Produkte oder Komponenten sind betroffen? Welche Rolle spielt das eigene Unternehmen – Hersteller, Importeur oder Vertreiber? Und welche Risikoklasse trifft auf die Produkte zu?

Auf dieser Grundlage lassen sich erste Maßnahmen strukturieren. Der Prozess beginnt mit einer technischen und organisatorischen **Bestandsaufnahme**, gefolgt von einer **Risikobewertung** und einer strategischen Maßnahmenplanung.

Die technische Umsetzung umfasst z. B. Schwachstellenmanagement, sichere Softwarearchitektur, Updatefähigkeit, Dokumentation und SBOMs. Parallel dazu müssen auch rechtliche Anforderungen berücksichtigt werden – etwa Nachweisfähigkeit, Konformitätsbewertung oder Meldepflichten.

Wichtig dabei: **CRA endet nicht mit der Produktfreigabe**. Sicherheitsmaßnahmen müssen über den **gesamten Lebenszyklus des Produkts** dauerhaft sichergestellt werden. Das umfasst **Monitoring, Patchmanagement, Meldeprozesse und kontinuierliche Dokumentation**. Konformität ist keine Momentaufnahme – sondern ein kontinuierlicher Zustand.

3.1.2 Was man selbst leisten kann und wo externe Unterstützung sinnvoll ist

Nicht jedes Unternehmen muss alle Anforderungen des CRA allein stemmen. Aber jedes Unternehmen sollte wissen, was intern leistbar ist – und wo externe Expertise hilft, effizient und rechtssicher zu handeln.

Viele **technische Grundlagen** wie Architekturentscheidungen, Build-Prozesse oder Testverfahren sind oft im Unternehmen vorhanden. Dagegen fehlen häufig **Strukturen für rechtliche Dokumentation**, SBOM-Management oder Schwachstellenmonitoring – also genau dort, wo CRA-Anforderungen besonders hoch sind.

Externe Unterstützung kann hier gezielt entlasten: Sie bringt Struktur, Erfahrung und fachübergreifende Perspektive – ohne die Verantwortung abzugeben. Ein erfahrener Partner arbeitet nicht hinter verschlossenen Türen, sondern **begleitet transparent, integriert und auf Augenhöhe**. Das interne Know-how bleibt erhalten – und kann sogar gestärkt werden.

3.1.3 CRA: Pflicht ja – aber zielgerichtet und angemessen

Der CRA ist verbindlich – aber **kein starrer Katalog**. Er lässt bewusst Raum für Abwägung:

- Was gilt als angemessen?
- Welche Maßnahmen sind verhältnismäßig?
- Wie lässt sich Sicherheit nachweisen, ohne Prozesse zu überfrachten?

Es braucht keine Übererfüllung – sondern ein **praxisnahes Sicherheitskonzept, das zum Produkt und zur Organisation passt**. Wer frühzeitig und mit Augenmaß

handelt, kann Aufwand und Wirkung sinnvoll austarieren. Das schützt vor regulatorischen Risiken und schafft langfristige Vorteile in Wartbarkeit, Weiterentwicklung und Qualitätssicherung.

3.2 Worauf es bei der Partnerwahl ankommt

3.2.1 Technik trifft Recht

Der CRA ist **kein rein technisches Thema**. Regulatorische Vorgaben, die Einhaltung formaler Pflichten, Nachweisdokumente, Verantwortlichkeiten und Prozesse spielen eine Rolle. Die **Schnittstelle zwischen Technik und Recht** ist daher ein wichtiger **Erfolgsfaktor**.

Wer hier nicht von Anfang an interdisziplinär denkt, riskiert, viel Aufwand in technische Maßnahmen zu stecken – ohne am Ende die regulatorischen Anforderungen wirklich zu erfüllen.

3.2.2 Kein Schema F – sondern individuell und praxisnah

Ein **erfahrener und umsichtiger Partner** hilft, übertriebene Maßnahmen zu vermeiden – und trotzdem ein tragfähiges Sicherheitsniveau zu erreichen. Entscheidend ist dabei die Herangehensweise.

Standardisierte „Schema-F"-Lösungen greifen entweder zu kurz oder sind überdimensioniert. Gefragt ist ein **individueller, zielorientierter Ansat**z, der sowohl die technischen Möglichkeiten als auch die betrieblichen Gegebenheiten berücksichtigt.

Doch das allein genügt nicht: Der CRA ist nicht nur ein technisches, sondern ebenso ein rechtliches Projekt. Wer Sicherheit „angemessen" umsetzen will, muss **Technik und Recht zusammenbringen**. In der Praxis ist das anspruchsvoll – denn beide Seiten denken und sprechen unterschiedlich. Was fehlt, ist ein abgestimmter Dialog, ein gemeinsames Verständnis von **Anforderungen, Machbarkeit und sinnvoller Priorisierung**.

3.2.3 Erfahrungsbasierte Umsetzung vs. theoretische Konzepte

Ein Partner, der diese Perspektiven integriert, ist Gold wert.

Auf juristischer Seite kommt es nicht nur auf Formalitäten an, sondern auf ein praxisnahes, umsetzungsorientiertes Verständnis.

Und auf technischer Seite zählt neben dem Fachwissen vor allem die Fähigkeit, Lösungen wirtschaftlich und strukturiert umzusetzen.

Beide Disziplinen sollten mit **Hands-on-Mentalität** agieren – damit ein **Sicherheitskonzept entsteht, das nicht nur auf dem Papier überzeugt**, sondern auch im Alltag funktioniert: dauerhaft, verlässlich und mit Augenmaß.

3.3 Unser Angebot: Begleitung durch SEKAS und SFRP

3.3.1 Ihre Partner: SEKAS und SFRP

Kurzprofil SEKAS GmbH aus München:

Spezialisiert auf: Entwicklung anspruchsvoller Softwarelösungen im technisch- / wissenschaftlichen Umfeld.

SEKAS ist ein Experte für Software- und Systemengineering mit Sitz in München. Seit über 35 Jahren bringen wir Kundenprojekte ans Ziel. Wir entwickeln im Kundenauftrag innovative und anspruchsvolle IT-Systeme im technisch-wissenschaftlichen Umfeld. Dies reicht von der Einbindung von Geräten und Sensoren, über die Applikations- bis zur modernen Webentwicklung. Typische Anwendungsgebiete liegen im Bereich Messtechnik, Kommunikation, Funküberwachung und in der Energietechnik.
Weitere Informationen unter: www.sekas.de

Kurzprofil SFRP - Kanzlei Schmid Frank Rechtsanwälte aus Augsburg:

Spezialisiert auf: IT-Recht, Datenschutz, Compliance, IT-Sicherheit

Rechtsanwalt Wolfgang Schmid und die Kanzlei Schmid Frank Rechtsanwälte sind seit über 20 Jahren auf die Bereiche IT-Recht, IT-Sicherheits-Recht, Datenschutz und IT-Compliance spezialisiert. Die derzeit 9 Rechtsanwälte und IT-Fachanwälte arbeiten als Anwaltsboutique ausschließlich in den genannten Bereichen und begleiten Unternehmen bei der rechtlichen Absicherung und Compliancevorgaben ihrer digitalen Infrastruktur und Projekte.
Weitere Informationen unter: www.schmid-frank.de

3.3.2 Unser Versprechen an Sie

Technik & Recht – abgestimmt aus einer Hand

Mit SEKAS und Schmid Frank Rechtsanwälte PartG mbB (SFRP) bündeln wir über 35 Jahre technologische und juristische Erfahrung. Unser gemeinsames Ziel:
Cybersecurity, die nicht nur regulatorisch erfüllt wird – sondern im Alltag handhabbar bleibt.

SEKAS begleitet Sie bei der technischen Umsetzung – von der Risikoanalyse über sichere Softwarearchitektur bis zum Schwachstellen- und Patch-Management.

SFRP sorgt für die rechtliche Absicherung – mit fundierter Beratung, konkreten Handlungsempfehlungen und einem klaren Fokus auf die Anforderungen des EU CRA.

Was diese Partnerschaft besonders macht: Sie ist über Jahre gewachsen, fachlich wie persönlich abgestimmt. Recht und Technik greifen nahtlos ineinander – **für Lösungen, die in der Praxis funktionieren, nicht nur auf dem Papier.**

Ihre Vorteile auf einen Blick

- **Recht und Technik nahtlos verzahnt:**
  Technische Maßnahmen werden von Anfang an juristisch mitgedacht – keine doppelten Abstimmungsschleifen, keine widersprüchlichen Empfehlungen.
- **Klares Vorgehen statt lose Einzelbausteine:**
  Wir liefern ein abgestimmtes Gesamtpaket – von der Risikoanalyse bis zur rechtssicheren Dokumentation. Keine offenen Flanken, keine Insellösungen.
- **Langfristig wartbare Sicherheitsarchitektur:**
  Maßnahmen, die in Ihren Entwicklungsprozess passen – und nicht bei jedem Audit oder Update zum Problem werden.
- **Praxis statt Theorie:**
  Unsere Lösungen entstehen aus konkreter Projekterfahrung – kein akademisches Whiteboard, sondern erprobte Umsetzung.

4 Starten Sie jetzt

Jetzt ins Handeln kommen

Der EU Cyber Resilience Act stellt viele Hersteller vor neue Anforderungen – technisch, rechtlich und organisatorisch. Wer frühzeitig handelt, gewinnt nicht nur Zeit und Sicherheit, sondern auch einen klaren Wettbewerbsvorteil.

Ob erste Einschätzung, konkrete Umsetzungsfragen oder der Wunsch nach einer abgestimmten Begleitung:

Wir sind für Sie da – als Partner auf Augenhöhe, mit technischer Tiefe und rechtlicher Klarheit.

Sprechen Sie uns an. Gemeinsam finden wir einen pragmatischen Weg durch den CRA – strukturiert, effizient und individuell auf Ihr Unternehmen abgestimmt.

CRA-Ready werden – schnell, sicher, effizient

Starten Sie mit unserem CRA Ready-Check und gewinnen Sie Klarheit über Ihren aktuellen Status und Ihre nächsten Schritte.

Kontaktieren Sie mich jetzt für ein unverbindliches Erstgespräch – gemeinsam machen wir Ihre Produkte fit für die Zukunft.

Dipl.-Inf. MBA Thomas Krenzke

Telefon: +49 (89) 74 81 34 – 0

E-Mail: thomas.krenzke@sekas.de

Weitere Informationen: www.sekas.de

SEKAS
SOFTWARE ENGINEERING