TRIOVEGA
SECURELY SHAPING YOUR FUTURE

CRA-BERATUNG

# CRA aus der Praxis, nicht aus dem Lehrbuch

**Wir gehen den Weg mit Ihnen, weil wir ihn selbst gegangen sind.**

# Wer den CRA zu spüren bekommt

Der EU Cyber Resilience Act (CRA) gilt ab dem **11. Dezember 2027** für alle Produkte mit digitalen Elementen, die Meldepflicht bereits seit dem **11. September 2026**. In Ihrem Unternehmen trifft er vor allem zwei Rollen, und jede spürt ihn anders.

## GESCHÄFTSFÜHRUNG

### Sie tragen das Risiko.

**Der Marktzugang steht auf dem Spiel**

Ohne CRA-Konformität keine CE-Kennzeichnung, ohne CE-Kennzeichnung keine Bereitstellung auf dem EU-Markt.

**Bußgelder bis 15 Mio. EUR**

Oder 2,5 % des weltweiten Jahresumsatzes, je nachdem, welcher Betrag höher ist.

**Die Meldepflicht läuft bereits**

Aktiv ausgenutzte Schwachstellen und schwerwiegende Vorfälle sind innerhalb von 24 Stunden an ENISA und das nationale CSIRT zu melden, lange bevor der Schwachstellenprozess Pflicht wird.

**Die Verantwortung ist nicht delegierbar**

Sie bleibt beim Hersteller, auch wenn Dienstleister unterstützen.

**Der Aufwand ist schwer planbar**

Budget und Kapazität werden über Jahre gebunden, ohne dass klar ist, wie groß der Aufwand tatsächlich wird.

**KERNFRAGE:**

Wie groß ist unser Risiko, und was brauchen wir, um es zu beherrschen?

## ENTWICKLUNGSLEITUNG

### Sie müssen es umsetzen.

**Keine genauen Vorgaben**

Der CRA verlangt ein angemessenes Cybersicherheitsniveau, sagt aber nicht, wie es zu erreichen ist. Die Begründung der getroffenen Maßnahmen liegt bei Ihnen.

**Sicherheit ist schwer zu greifen**

Wann ist ein Produkt sicher genug? Welche Anforderung gilt für welches Produkt, und wie weisen Sie sie nach?

**Pflichten über viele Jahre**

Der Support-Zeitraum beträgt in der Regel mindestens fünf Jahre. Langlebige Produkte wie Maschinen haben schnell 13 Jahre und mehr. So lange muss Software gepflegt und jede Schwachstelle behandelt werden.

**Parallel zum Tagesgeschäft**

Die Umsetzung konkurriert mit Roadmap und Kundenprojekten um dieselben Leute.

**KERNFRAGE:**

Was genau müssen wir bauen, und wie halten wir das über Jahre durch?

**Die Anforderungen zu kennen ist das eine. Sie auf Ihr Unternehmen zuzuschneiden das andere.**

Der CRA beschreibt, welches Ergebnis erreicht werden soll, nicht wie groß der Prozess dafür sein muss. Genau hier entscheidet sich, ob dieser im Alltag getragen wird, oder als Parallelstruktur nebenher läuft.

# Was unsere CRA-Beratung leistet

Ein modularer Beratungsbaukasten mit Schwerpunkt auf den drei Themenfeldern, die in der Umsetzung des CRA erfahrungsgemäß den größten Aufwand verursachen: **CRA-Grundlagen**, **Vulnerability Management** und **Secure Development**. Wir holen Sie dort ab, wo Sie stehen.

GESCHÄFTSFÜHRUNG

## Klarheit für Entscheidungen

**CRA Open Classroom**

Gemeinsames Verständnis von Pflichten, Rollen und Fristen, für Führungskreis und Team.

**CRA GAP-Analyse**

Ihr Umsetzungsstand gegen die Anforderungen, priorisiert nach dem, was zuerst zählt.

**ERGEBNIS**

Ein belastbares Lagebild, klare Prioritäten und eine Grundlage für Budget- und Kapazitätsentscheidungen.

ENTWICKLUNGSLEITUNG

## Umsetzbare Vorgaben

**Hands-on an Ihrem Produkt**

Vulnerability Handling, Authority Notification, Threat Modelling, Secure Design und Secure Coding an Ihrem eigenen Material.

**Accelerators**

Compliance Matrix, Templates und VuM-Tooling, vorinterpretiert und priorisiert nach MUST, SHOULD und COULD.

**ERGEBNIS**

Ein Prozess in der Größe, die Ihr Team über Jahre trägt, und Artefakte, die Sie selbst weiterpflegen.

**Gemeinsamer Startpunkt: Das Einstiegsgespräch**

30 Minuten, telefonisch oder remote. Wir klären, wo Ihr Unternehmen steht, was notwendig ist und wer beteiligt sein sollte: Geschäftsführung, Entwicklungsleitung oder beide. Danach wissen wir, wo der sinnvolle Einstieg liegt.

### 01

**Praxis statt Theorie**

TRIOVEGA entwickelt eigene Produkte, die unter den CRA fallen. Unser Entwicklungsprozess ist nach IEC 62443 zertifiziert und unsere Produktanforderungen orientieren sich daran.

### 02

**Einstieg auf Ihrem Stand**

Schulung für Orientierung, Hands-on für die Umsetzung an Ihren eigenen Beispielen, Accelerator für wiederverwendbare Artefakte. Einzelne Bausteine oder ein zusammenhängender Pfad.

### 03

**Ergebnisse, die bleiben**

Aus jedem Hands-on-Baustein geht ein Arbeitsergebnis hervor, das in Ihrer Organisation weiterlebt. Keine Foliensätze zum Ablegen.

# Unser Beratungsbaukasten

Der CRA-Beratungsbaukasten gliedert sich in drei Schwerpunktthemen mit jeweils drei Detailstufen:

| | CRA IN GENERAL | VULNERABILITY MANAGEMENT | SECURE DEVELOPMENT |
|---|---|---|---|
| **① TRAINING**<br>Überblick und Vorgehen. Gemeinsames Verständnis aufbauen, theoriebasiert, kein produktspezifisches Ergebnis. | CRA Open Classroom<br>MGMT | Vulnerability Process | Secure Development<br>Annex 1 - Full Overview<br>Annex 1 - Deep-Dive<br>Cybersecurity Risk Assessment |
| **② HANDS-ON**<br>Umsetzung an Ihrem Produkt und Ihren Prozessen. Gemeinsame Arbeit an Ihrem Material, erzeugt ein konkretes Arbeitsergebnis. | CRA Gap Analysis<br>MGMT | Vulnerability Handling<br>Authority Notification<br>VuM Tooling<br>Tool Integration | Secure Coding Workshop<br>Secure Design Workshop<br>Threat Modeling Workshop |
| **③ ACCELERATOR**<br>Wiederverwendbare Artefakte. Vorbereitete Templates, Matrizen und Werkzeuge, immer zusammen mit dem passenden Beratungsbaustein. | CRA-IEC Compliance Matrix<br>Template for Intended Purpose | VuM Tool<br>VuM Ticket Templates<br>VuM Process Templates<br>CVD Policy | Coding Guidelines<br>Threat Modeling Template<br>Risk Assessment Template<br>3rd-Party Assessment Tool |

MGMT Auch für die Geschäftsführung: CRA Open Classroom und CRA Gap-Analyse werden häufig von der Geschäftsführung beauftragt und schaffen die Entscheidungsgrundlage. Alle übrigen Bausteine richten sich an Entwicklungsleitungen und ihre Teams.

# Wo stehen Sie?

Der Baukasten hat drei Einstiegspunkte. Welcher passt, klären wir im Einstiegsgespräch.

### 01 NEULAND

Der CRA ist bekannt, aber niemand hat ihn auf Ihre Produkte übersetzt; es wurden keine Zuständigkeiten benannt.

**IHR EINSTIEG**

CRA Open Classroom, danach Portfolio-Einordnung.

### 02 GRUNDLAGEN

Task Force eingerichtet, erste Konzepte liegen vor, die Umsetzung stockt.

**IHR EINSTIEG**

CRA Gap-Analyse und Compliance Matrix, danach gezielt Hands-on-Bausteine.

### 03 UMSETZUNG

Prozesse laufen an, es fehlt die Absicherung an den kritischen Stellen.

**IHR EINSTIEG**

Hands-on-Bausteine und Accelerators, punktuell statt flächig.

# So läuft ein Baustein ab

**01 VORBEREITUNG**

Wir klären Ihren Ausgangspunkt, schneiden die Agenda zu und stimmen ab, welche Unterlagen wir brauchen.

**02 DURCHFÜHRUNG**

Schulung oder gemeinsame Arbeit an Ihrem Material. Vor Ort bewusst auf sieben Stunden begrenzt.

**03 ERGEBNIS**

Wir dokumentieren die Arbeitsergebnisse und übergeben sie in einem Format, das Sie selbst weiterpflegen.

**04 NACHBESPRECHUNG**

Remote-Termin für die Fragen, die erst auftauchen, wenn Ihr Team das Erarbeitete anwendet.

# So arbeiten wir mit Ihnen zusammen

Beratung wirkt nicht durch Wissen, sondern durch Übergabe. Fünf Prinzipien, nach denen wir arbeiten.

**Wir fangen beim Zweck an, nicht bei der Anforderungsliste**

Bevor es um einzelne Anforderungen geht, klären wir, was der CRA erreichen soll und welche Logik dahintersteht. Das ist die Basis dafür, dass Sie Ihre Umsetzung selbst gestalten und Ihre Entscheidungen begründen können, statt eine Liste abzuarbeiten, deren Zweck offen bleibt.

**Wir treffen Sie dort, wo Sie stehen**

Vor jedem Baustein klären wir in einem Vorbereitungstermin Ihren Ausgangspunkt: Was ist bereits vorhanden, wer ist verantwortlich, gibt es schon eine SBOM, wie sind Service und Bereitschaft organisiert. Danach schneiden wir die Agenda zu. Ein Team, das gerade eine Task Force gegründet hat, braucht etwas anderes als eines, das seit einem halben Jahr an einer Prozesslandschaft arbeitet.

**Sie gehen mit Artefakten heraus, nicht mit Hausaufgaben**

Compliance Matrix mit Ihrem Umsetzungsstand und passenden Handlungsempfehlungen. High-Level-Prozessbeschreibung inklusive der vom CRA geforderten Meldewege. Threat Model für die bearbeiteten Schnittstellen samt Template für die restlichen. Alles in einem Format, das Sie selbst weiterpflegen können.

**Wir arbeiten an Ihren Beispielen**

In den Hands-on-Bausteinen bringen Sie mit, was Sie tatsächlich beschäftigt: zwei real aufgetretene Schwachstellen, Ihre bestehenden Prozesse, Ihre Architektur. Wir analysieren gemeinsam, wo die Lücken sind. Das ist kein Audit von außen, sondern eine Bestandsaufnahme von innen.

**Wir sind nach dem Workshop noch da**

Vor-Ort-Workshops begrenzen wir bewusst auf sieben Stunden und planen einen Remote-Nachbesprechungstermin ein. Die entscheidenden Fragen kommen erfahrungsgemäß nicht im Workshop, sondern erst danach, wenn Ihr Team das Erarbeitete zum ersten Mal anwendet.

**Was Sie bei uns nicht bekommen**

Kein Audit von außen. Kein Zertifikat. Kein Standardprogramm, das für jedes Unternehmen gleich aussieht. Wir sind kein Prüfer, sondern der Partner, der neben Ihnen sitzt und mit Ihnen gemeinsam an Ihrem Material arbeitet.

# Wir wissen, wovon wir reden

Wir kennen den CRA aus der eigenen Umsetzung, mit allen Umwegen. Was wir dabei gelernt haben, geben wir direkt an Sie weiter.

### Unsere Ausgangslage

Ein Konzernprozess für unsere Größe: Wir bauten ein unternehmensweites Schwachstellen-management, anfangs ohne jeglichen Zuschnitt.

### Unsere Herausforderung

Ein Workflow, den niemand tragen konnte: Ein Extra-Ticketing neben dem Entwicklungsprozess; unsichtbar, nicht handhabbar, ohne definiertes Ende. Tickets blieben offen, niemand wusste, wann sie geschlossen werden konnten, und das Team war überfordert.

### Unser Lösungsweg

Ein Prozess in Teilen statt eines Monolithen: Incident im Service, Pre-Assessment im Tool, Vulnerability-Ticket in der Entwicklung, Nach-verfolgung über den Release.

# Handlungsfähigkeit schlägt Perfektion

| OHNE BEGLEITUNG | MIT TRIOVEGA |
|---|---|
| Ein Prozess nach Lehrbuch, den niemand versteht | Ein Prozess in der Größe, die Ihr Team trägt |
| Monate eigener Interpretationsarbeit am Verordnungstext | Vorinterpretierte Anforderungen, priorisiert nach MUST, SHOULD und COULD |
| Ein Foliensatz zum Ablegen | Ausgefüllte Artefakte, zum Weiterpflegen in Eigenregie |
| Anonyme Musterfälle als Anschauungsmaterial | Beispiele aus eigenen Produkten und aus dem eigenen Entwicklungsprozess |
| Dieselben Fehler, die wir schon gemacht haben | Unsere Learnings als Startpunkt anstatt als Ziel |

**Sie sind Maschinenhersteller? Dann nehmen Sie die Abkürzung mit edge.PSL.**

Die Sicherheitskomponente wird untrennbar mit Ihrer Maschine ausgeliefert und den Schwachstellen-Lebenszyklus übernimmt TRIOVEGA für Sie. Die CRA-Beratung zeigt Ihnen den Weg, edge.PSL nimmt Ihnen Arbeit ab.

TRIOVEGA
SECURELY SHAPING YOUR FUTURE

Wenn Sie wissen möchten, wie wir Sie beim Thema CRA bestmöglich unterstützen können, nehmen Sie Kontakt zu mir auf.

**René Janz**

Director Business Development

rja@triovega.com

**Securely shaping your future**

TRIOVEGA begleitet seit über 25 Jahren vom Standort Lübeck heraus Industrieunternehmen weltweit dabei, das Potenzial der Digitalisierung sicher und nachhaltig zu erschließen. Das Portfolio umfasst einsatzfertige Produkte und Dienstleistungen zur Steigerung von Produktionssicherheit und Effizienz sowie individuell entwickelte Softwarelösungen, die sich nahtlos in die Wertschöpfungsketten der Kunden integrieren lassen.

Mit mehrfach ausgezeichneter Innovationskraft und zertifizierter sowie patentierter Cybersicherheitsexpertise steht TRIOVEGA für partnerschaftliche Zusammenarbeit auf Augenhöhe – von der technischen Beratung über die Umsetzung bis zum After-Sales-Service.

MKT-SB-v001-20261005-öffentlich

**TRIOVEGA GmbH**
Kaninchenborn 31
23560 Lübeck, Deutschland
T: +49 451 39771 0
E: info@triovega.com

**www.triovega.de**