CRAwerk

HANDBUCH · VERSION 2.0

PRAXISLEITFADEN FÜR CRAWERK

Schritt für Schritt durch den Cyber Resilience Act.

Ein verständliches Handbuch für kleine und mittlere Maschinen- und Anlagenbauer - von der ersten Einrichtung bis zur vollständigen CRA-Akte.

CRA verstehen

Wichtige Begriffe, Termine und Anforderungen in klarer Sprache.

CRAwerk bedienen

Unternehmen, Team, Produkte, Support, Abrechnung und Exporte.

Akte abschließen

Offene Punkte erkennen und strukturiert bis zur Vollständigkeit bearbeiten.

Stand: September 2026

CRAwerk · info@crawerk.de

HANDBUCH

So benutzen Sie dieses Handbuch

Dieses Handbuch erklärt zuerst, wie CRAwerk benutzt wird, und danach die CRA-Themen, die hinter den Eingaben stehen. Sie müssen den Cyber Resilience Act nicht auswendig kennen. Wichtig ist, dass Ihre Angaben technisch belastbar und nachvollziehbar sind.

Empfohlener Start

Vervollständigen Sie zuerst die Unternehmensdaten. Danach legen Sie ein Produkt an und arbeiten die offenen Bereiche nacheinander ab. CRAwerk zeigt Ihnen, was fehlt und führt Sie direkt zur passenden Eingabe.

CRAwerk organisiert

Produkte, Software, Bauteile, Risiken, Nachweise, Supportzeitraum, CRA-Abschluss und Exporte bleiben an einem Ort zusammen.

Sie entscheiden fachlich

Technische Bewertungen, Risikoeinschätzungen, Konformitätsentscheidungen und Freigaben müssen von den zuständigen Personen im Unternehmen getroffen werden.

Wichtig

CRAwerk ist eine Organisations- und Dokumentationshilfe. Es ersetzt keine Rechtsberatung, keine technische Sicherheitsprüfung und keine Konformitätsbewertungsstelle.

NAVIGATION

Inhalt

Die Kapitel sind so sortiert, wie ein neuer CRAwerk-Kunde normalerweise arbeitet.

1. Der Cyber Resilience Act in kurzer Form

Der Cyber Resilience Act (CRA), Verordnung (EU) 2024/2847, legt Cybersicherheitsanforderungen für Produkte mit digitalen Elementen fest, die auf dem EU-Markt bereitgestellt werden.

Für Hersteller bedeutet das unter anderem: Cybersicherheitsrisiken müssen berücksichtigt, relevante Produktinformationen dokumentiert, Schwachstellen während des Unterstützungszeitraums behandelt und bestimmte Vorfälle bzw. aktiv ausgenutzte Schwachstellen gemeldet werden.

Vor dem Inverkehrbringen

- Produkt einordnen
- Cybersicherheitsrisiken bewerten
- grundlegende Anforderungen berücksichtigen
- technische Dokumentation aufbauen
- Konformitätsverfahren festlegen

Während des Unterstützungszeitraums

- Schwachstellen beobachten
- Sicherheitsupdates bereitstellen
- Informationen und Nachweise pflegen
- Meldepflichten beachten
- Änderungen nachvollziehbar dokumentieren

CRAwerk-Prinzip

CRAwerk übersetzt diese Themen in konkrete Datensätze und offene Aufgaben. Die Software zeigt nicht nur, was vorhanden ist, sondern auch, welche Angaben noch fehlen.

2. Fällt unser Produkt unter den CRA?

Nicht jede Maschine fällt automatisch unter den CRA. Entscheidend ist, ob es sich um ein Produkt mit digitalen Elementen handelt, das in den Anwendungsbereich der Verordnung fällt.

Typische Hinweise auf CRA-Relevanz

- ✓ Das Produkt enthält Software oder Firmware.
- ✓ Es kann direkt oder indirekt Daten verarbeiten oder austauschen.
- ✓ Es besitzt Netzwerk-, Fernwartungs- oder andere digitale Schnittstellen.
- ✓ Es wird unter dem eigenen Namen oder der eigenen Marke auf dem EU-Markt bereitgestellt.

Zugekaufte Komponenten ändern die Verantwortung nicht automatisch

Hersteller können Unterlagen ihrer Zulieferer nutzen. Für das eigene Endprodukt muss aber weiterhin bewertet werden, wie Komponenten, eigene Software, Schnittstellen und Einsatzumgebung zusammenspielen.

> **Der kostenlose CRA-Kurzcheck**
>
> Auf der CRAwerk-Startseite führen sieben einfache Fragen zu einer ersten Orientierung. Die Auswertung ist keine rechtliche Einstufung, sondern ein Einstiegspunkt.

3. Wichtige Termine

Der CRA gilt gestaffelt. Für die Planung sind insbesondere diese Daten wichtig.

Datum	Bedeutung
11. Juni 2026	Bestimmungen zur Notifizierung von Konformitätsbewertungsstellen gelten.
11. September 2026	Die Berichtspflichten aus Artikel 14 gelten, insbesondere für aktiv ausgenutzte Schwachstellen und schwere Sicherheitsvorfälle.
11. Dezember 2027	Die übrigen Hauptpflichten des CRA gelten vollständig.

Stand dieses Handbuchs: September 2026

Leitlinien, harmonisierte Normen und technische Umsetzungsdetails entwickeln sich weiter. Prüfen Sie bei relevanten Entscheidungen den aktuellen Rechts- und Normenstand.

4. Begriffe, die in CRAwerk vorkommen

Begriff	Einfach erklärt
Produkt mit digitalen Elementen	Hardware- oder Softwareprodukt mit digitalen Funktionen, das in den CRA-Anwendungsbereich fallen kann.
Firmware	Gerätenahe Software, z. B. in Steuerungen, Gateways oder Embedded-Komponenten.
Schwachstelle	Eine technische Schwäche, die ausgenutzt werden kann.
SBOM	Strukturierte Liste von Softwarekomponenten und Abhängigkeiten.
CVD	Coordinated Vulnerability Disclosure: geregelter Umgang mit gemeldeten Schwachstellen.
Unterstützungszeitraum	Zeitraum, in dem der Hersteller sicherheitsrelevante Pflege und Schwachstellenbehandlung vorsieht.
Konformitätsbewertung	Verfahren, mit dem der Hersteller nachweist, dass die einschlägigen Anforderungen erfüllt sind.

5. So ist CRAwerk aufgebaut

CRAwerk trennt Stammdaten, Produktarbeit und CRA-Abschluss bewusst. So bleibt die tägliche Arbeit übersichtlich.

1. **Unternehmen**
   Stammdaten, Firmenlogo, Benutzer & Team sowie Tarif & Abrechnung.

2. **Produkte / Maschinen**
   Grunddaten, Software, Bauteile, Risiken, Sicherheitsprobleme, Dokumente und Unterstützungszeitraum.

3. **Geführter CRA-Abschluss**
   Produkt einordnen, Schutz prüfen, Dokumentation, Sicherheitsprozess, Konformität und abschließende Aktenprüfung.

4. **Dokumente & Exporte**
   Produktakte, Kurzakte, Nutzerinformationen und EU-Konformitätserklärung aus den gepflegten Angaben erzeugen.

5. **Support**
   Fragen direkt aus CRAwerk stellen, Verlauf sehen und auf Antworten reagieren.

6. Unternehmensdaten zuerst

Bevor Sie das erste Produkt anlegen, sollten die Unternehmensdaten vollständig sein. CRAwerk verwendet diese Angaben später in Dokumenten und beim CRA-Abschluss.

Wo finden Sie den Bereich?

Öffnen Sie in der Kopfzeile **Unternehmen**. Solange wichtige Angaben fehlen, zeigt das Dashboard einen Hinweis mit dem direkten Link dorthin.

Diese Angaben sollten gepflegt sein

- ✓ Firmenname
- ✓ Straße und Hausnummer
- ✓ PLZ und Ort
- ✓ Land
- ✓ E-Mail-Adresse
- ✓ Ansprechpartner und weitere Kontaktdaten, soweit vorhanden

> **Warum das wichtig ist**
>
> Firmenname, vollständige Anschrift und E-Mail sind Teil der Vollständigkeitsprüfung der Akte. Fehlen sie, zeigt CRAwerk die Akte nicht als vollständig an.

7. Firmenlogo hinterlegen

Im Unternehmensbereich kann optional ein Firmenlogo hinterlegt werden. Das Logo wird privat im CRAwerk-Speicher abgelegt und Ihrem Unternehmen zugeordnet.

Funktion	Verhalten
Hochladen	PNG, JPG, WEBP oder SVG, maximal 2 MB.
Ersetzen	Ein neues Logo ersetzt die bisherige Datei.
Löschen	Das Logo kann jederzeit entfernt werden.
Verwendung	Unter anderem in Produktakte, Kurzakte, Nutzerinformationen und EU-Konformitätserklärung.

Tipp: Verwenden Sie ein Logo mit transparentem oder hellem Hintergrund und ausreichend Rand. Sehr breite Logos sollten nicht unnötig kleine Schrift enthalten.

8. Benutzer & Team

Mehrere Mitarbeiter können im selben CRAwerk-Unternehmen arbeiten. Jede Person verwendet einen eigenen Login. Gemeinsame Passwörter sind nicht erforderlich.

Mitarbeiter einladen

1. **Unternehmen öffnen**
   Wählen Sie „Benutzer & Team“.

2. **E-Mail und Rolle wählen**
   Der Inhaber oder ein Admin lädt die Person ein.

3. **Einladung annehmen**
   Die Person legt über den Einladungslink ein eigenes Passwort fest.

4. **Gemeinsam arbeiten**
   Nach dem Login sieht das Team dieselben Unternehmens- und Produktdaten entsprechend der Rolle.

Inhaber

Voller Zugriff einschließlich Teamverwaltung, Unternehmensdaten sowie Tarif und Abrechnung.

Admin

Kann Produkte, Unternehmensdaten, Team und Abrechnung verwalten.

Mitarbeiter

Arbeitet an Produkten, hat aber keine Team- oder Tarifverwaltung und kann Unternehmensdaten nicht ändern.

Offene Einladungen

Noch nicht angenommene Einladungen können erneut gesendet oder zurückgezogen werden. Entfernte Benutzer verlieren die Zuordnung zum Unternehmen.

9. Produkt oder Maschine anlegen

CRAwerk beginnt bewusst nur mit wenigen Grunddaten. Weitere Informationen werden anschließend im Produktdatensatz ergänzt.

Feld	Beispiel
Name	Fräsanlage MX200
Baureihe / Modell	MX200
Interne Produktnummer	MX200-2026-014
Verantwortlich	Produktmanagement / Max Mustermann
Software oder Firmware?	Ja / Nein / Unklar
Netzwerk oder andere Verbindung?	Ja / Nein / Unklar

Tarifgrenzen

Die Zahl der Produkte richtet sich nach dem gewählten CRAwerk-Tarif. Ist das Limit erreicht, erscheint die Meldung direkt im Anlagefenster und führt zu „Tarif & Abrechnung“.

10. Software, Firmware und Versionen

Erfassen Sie die Software- und Firmwarestände, die im Produkt eingesetzt werden. Für die spätere Schwachstellenbehandlung ist die konkrete Version entscheidend.

Typische Einträge

- SPS-Programm und Runtime
- HMI-Projekt und HMI-Runtime
- Firmware von Steuerungen, Gateways und Antrieben
- Embedded Linux oder andere Betriebssysteme
- eigene Service- oder Kommunikationssoftware

> **Keine Versionsstände erfinden**
>
> Wenn eine Version nicht bekannt ist, bleibt sie offen. Holen Sie die Information bei Entwicklung, Einkauf oder Zulieferer nach und dokumentieren Sie die belastbare Antwort.

SBOM

Die Softwareliste in CRAwerk ist die Grundlage für die SBOM-Dokumentation. Je vollständiger Versionen und Komponenten gepflegt sind, desto schneller lässt sich später prüfen, ob eine veröffentlichte Schwachstelle ein Produkt betrifft.

11. Digitale Bauteile und Zulieferer

Digitale Komponenten und ihre Zulieferer sollten direkt dem Produkt zugeordnet werden. Dadurch bleiben technische Abhängigkeiten nachvollziehbar.

Bauteil	Was erfassen?
SPS / Controller	Hersteller, Typ, ggf. Firmware und relevante Unterlagen
HMI	Hersteller, Modell, Runtime/Firmware
Remote Gateway	Hersteller, Typ, Fernwartungsfunktion, Firmware
Vernetzter Antrieb	Hersteller, Typ, Kommunikationsschnittstelle

Nach dem Speichern eines Bauteils bleibt der Detailbereich geöffnet, damit Sie weitere Komponenten direkt weiter erfassen können.

12. Risiken und Schutzmaßnahmen

Die Risikobewertung verbindet technische Beobachtungen mit konkreten Maßnahmen, Verantwortlichen und Status.

Gute Risikoeinträge sind konkret

Zu allgemein

„Fernwartung unsicher“

Besser

„Gemeinsamer Service-Account für Fernwartung; Risiko unklarer Benutzerzuordnung. Maßnahme: personenbezogene Konten und MFA einführen.“

Abschluss der Risikoprüfung

Erst wenn die relevanten Risiken bewertet und offene Maßnahmen bearbeitet sind, sollte die Risikoprüfung als abgeschlossen markiert werden. CRAwerk verwendet diesen Status später für die Vollständigkeitsprüfung.

13. Sicherheitsprobleme und Updates

Bekannte Schwachstellen und andere Sicherheitsprobleme werden als konkrete Vorgänge geführt. Dadurch ist später nachvollziehbar, wann ein Problem bekannt wurde, welche Produkte betroffen waren und wie es behandelt wurde.

Zu einem Vorgang gehören typischerweise

- ✓ Bezeichnung des Problems
- ✓ Bekannt seit
- ✓ betroffene Komponente oder Version
- ✓ Bewertung / Schweregrad
- ✓ Maßnahme
- ✓ bereitgestellte Patch- oder Firmware-Version
- ✓ Datum der Behebung
- ✓ Advisory- oder Nachweisreferenz

Interner Ablauf

Zusätzlich wird festgelegt, wer Sicherheitsprobleme verantwortet und wie sie intern bearbeitet, bewertet, eskaliert und abgeschlossen werden.

14. Unterlagen und Nachweise

Dokumente können einem Produkt zugeordnet werden. So liegen technische Unterlagen, Lieferantennachweise, Prüfberichte oder andere relevante Dateien direkt dort, wo sie gebraucht werden.

Beispiele

- Security Advisories von Zulieferern
- Prüf- und Testberichte
- Architektur- oder Netzwerkunterlagen
- Freigaben und interne Nachweise
- Produkt- und Komponenteninformationen

Dateien liegen in einem privaten Speicherbereich. Zugriffsregeln trennen die Daten der Unternehmen voneinander.

15. Unterstützungszeitraum

Der Unterstützungszeitraum beschreibt, wie lange der Hersteller die sicherheitsbezogene Pflege eines Produkts vorsieht.

Angabe	Warum sie gebraucht wird
Beginn und Ende	Definiert den vorgesehenen Zeitraum.
Verantwortliche Stelle	Zeigt, wer den Zeitraum und seine Einhaltung betreut.
Begründung	Dokumentiert, warum die Dauer für das Produkt angemessen ist.
Kommunikation beim Kauf	Hält fest, wo der Zeitraum gegenüber Kunden sichtbar gemacht wird.
Information zum Supportende	Dokumentiert, ob und wie Nutzer über das Ende informiert werden können.

Die Dauer ist keine pauschale Zahl

Der CRA und die Leitlinien verlangen eine produktbezogene Betrachtung. Lebensdauer, Nutzererwartung, Komponentenverfügbarkeit und weitere Faktoren können relevant sein.

16. Geführter CRA-Abschluss

Der CRA-Abschluss führt die zuvor gepflegten Informationen in sechs Schritten zusammen. Die Prozentanzeige wurde bewusst durch eine klare Schrittanzeige ersetzt: zum Beispiel „5 / 6“.

1. **Produkt einordnen**
   Produktklasse, Kategorie und Begründung festhalten.

2. **Schutz prüfen**
   Die grundlegenden Cybersicherheitsanforderungen aus Anhang I bewerten.

3. **Maschine beschreiben**
   Technische Beschreibung, Einsatzumgebung, Architektur und Nutzerinformationen vervollständigen.

4. **Sicherheitsprozess**
   CVD, Schwachstellenkontakt, Updateverteilung und Drittkomponentenprozess dokumentieren.

5. **Konformität**
   Konformitätsweg, EU-Erklärung, CE und ggf. benannte Stelle vervollständigen.

6. **Akte prüfen**
   Fehlende Bereiche werden aufgelistet und können direkt geöffnet werden.

Unternehmensdaten gehören zur Vollständigkeit

Auch wenn alle sechs CRA-Schritte fachlich ausgefüllt sind, gilt die Akte erst als vollständig, wenn Firmenname, vollständige Anschrift und E-Mail vorhanden sind.

17. Die 22 Schutzanforderungen verständlich

CRAwerk zerlegt die Anforderungen aus Anhang I in einzelne prüfbare Punkte. Jeder Punkt erhält einen Status und - je nach Status - eine Begründung oder einen Nachweis.

So arbeiten Sie damit

1. Lesen Sie die Frage im Kontext des konkreten Produkts.
2. Bewerten Sie, ob sie erfüllt, offen oder nicht anwendbar ist.
3. Begründen Sie „nicht anwendbar“ nachvollziehbar.
4. Hinterlegen Sie bei erfüllten Punkten eine technische Begründung oder einen Nachweis.

Typische Themen der Schutzanforderungen

- Secure by default
- Authentifizierung und Zugriff
- Vertraulichkeit und Integrität
- Angriffsfläche minimieren
- Protokollierung und Erkennung

- sichere Updates
- Schwachstellenbehandlung
- Schutz vor Manipulation
- Wiederherstellung
- Minimierung unnötiger Daten

18. Technische Dokumentation und Nutzerinformationen

Die technische Dokumentation muss nachvollziehbar zeigen, was das Produkt ist, in welcher Umgebung es eingesetzt wird, welche Sicherheitsannahmen gelten und wie die Anforderungen bewertet wurden.

CRAwerk fragt unter anderem ab

- ✓ bestimmungsgemäße Verwendung
- ✓ Sicherheitsumgebung
- ✓ Sicherheitseigenschaften
- ✓ vorhersehbarer Fehlgebrauch
- ✓ Architektur und technische Beschreibung
- ✓ Produktions- und Monitoringprozess
- ✓ angewendete Normen und technische Lösungen
- ✓ Zusammenfassung von Sicherheitsprüfungen und Testberichten

Nutzerinformationen

Zusätzlich werden Hinweise für sichere Inbetriebnahme, Änderungen, Updates, Außerbetriebnahme, Integratoren sowie der Unterstützungszeitraum erfasst. Daraus kann CRAwerk die Nutzerinformationen erzeugen.

19. Sicherheitsprozess, CVD und Meldungen

Der Sicherheitsprozess beschreibt, wie Hinweise auf Schwachstellen entgegengenommen, bewertet, behoben und gegenüber Nutzern bzw. Behörden behandelt werden.

Wichtige Bausteine

- ✓ Kontakt für Schwachstellenmeldungen
- ✓ CVD-Richtlinie und Veröffentlichungsort
- ✓ sichere Verteilung von Updates
- ✓ Prozess für Drittanbieter-Komponenten
- ✓ Aufbewahrung und Nachvollziehbarkeit

Berichtspflichten seit 11. September 2026

Artikel 14 ist seit 11. September 2026 anwendbar. Bei aktiv ausgenutzten Schwachstellen und schweren Sicherheitsvorfällen gelten gestufte Meldepflichten. CRAwerk kann die Vorgänge und Fristen dokumentieren, sendet die Meldung aber nicht selbst an ENISA oder Behörden.

Fristen sind ernst zu nehmen

Bei einem realen meldepflichtigen Vorgang sollte unverzüglich geprüft werden, welche Meldung wann und über welchen offiziellen Meldeweg erforderlich ist.

20. Konformität, EU-Erklärung und CE

Am Ende muss der passende Konformitätsweg dokumentiert und die EU-Konformitätserklärung auf die tatsächliche Produktsituation abgestimmt werden.

CRAwerk hält fest

- Produktklasse und ggf. Kategorie
- gewählten Konformitätsweg
- Normenabdeckung
- ggf. benannte Stelle, Kennnummer und Zertifikatsreferenz
- Status und Ort der CE-Kennzeichnung
- Ort, Datum, Unterzeichner und Funktion der EU-Konformitätserklärung
- Referenz auf die unterzeichnete Fassung

Kein automatisches „Freigeben“

CRAwerk erzeugt Dokumente aus Ihren Daten. Die fachliche Prüfung und Unterzeichnung bleibt bei den verantwortlichen Personen im Unternehmen.

21. Sonderfälle und Behördenanfragen

Bestimmte Bereiche werden erst wichtig, wenn ein konkretes Ereignis eintritt. CRAwerk hält sie deshalb außerhalb des normalen täglichen Ablaufs.

Aktiv ausgenutzte Schwachstelle oder schwerer Sicherheitsvorfall

Dokumentieren Sie Kenntniszeitpunkt, betroffene Produkte, Bewertungen, Meldeschritte, Maßnahmen und Abschlussnachweise.

Nichtkonformität

Wird festgestellt, dass ein Produkt oder ein Prozess nicht mehr konform ist, sollte dokumentiert werden, welche Korrekturmaßnahme durchgeführt wurde und ob weitere Marktmaßnahmen notwendig waren.

Anfrage einer Marktüberwachungsbehörde

Behörde, Aktenzeichen, angeforderte Unterlagen, übermittelte Informationen und Übermittlungsnachweis sollten nachvollziehbar zusammengeführt werden.

22. Supportbereich in CRAwerk

Fragen können direkt aus CRAwerk gestellt werden. Sie müssen keine separate E-Mail suchen und der gesamte Verlauf bleibt dem Unternehmen zugeordnet.

Neue Anfrage

Öffnen Sie **Support**, wählen Sie einen Bereich, tragen Sie Betreff und Frage ein und senden Sie die Anfrage.

Status

Status	Bedeutung
Offen	Die Anfrage wartet auf Bearbeitung.
In Bearbeitung	CRAwerk Support arbeitet an der Frage.
Beantwortet	Eine Antwort wurde hinterlegt.
Erledigt	Der Vorgang ist abgeschlossen.

Sie können auf eine Antwort wieder reagieren. Eine neue Nachricht zu einem erledigten Vorgang öffnet ihn wieder. Support bleibt auch erreichbar, wenn eine Testphase abgelaufen oder der reguläre Produktzugang pausiert ist.

23. Tarif, Abrechnung und Rechnungen

Tarif und Abrechnung werden über den Bereich „Tarif & Abrechnung“ verwaltet. Die Zahlungsabwicklung erfolgt über Stripe.

Testphase

Neue Kunden können CRAwerk zunächst für 14 Tage testen. Für die Testphase werden bei der Registrierung keine Zahlungsdaten benötigt. Nach Ablauf bleibt der reguläre Produktzugang gesperrt, bis ein Tarif gewählt wurde.

Tarif wählen

Im Abrechnungsbereich sehen Inhaber und Admins die verfügbaren Tarife. Mitarbeiter können an Produkten arbeiten, aber keine Abrechnung verwalten.

Rechnungen

Nach der Abrechnung stellt Stripe die Rechnung für den CRAwerk-Tarif bereit. Firmenanschrift und steuerrelevante Angaben werden im Checkout bzw. Kundenportal gepflegt. Rechnungen können über **Abo verwalten** im Stripe-Kundenportal heruntergeladen werden.

Preise

Die aktuellen Tarifpreise und Produktgrenzen stehen immer direkt in CRAwerk. Das Handbuch nennt bewusst keine dauerhaften Preisbeträge, damit es bei Tarifänderungen nicht veraltet.

24. Beispiel: Verpackungsanlage VP-240

Das folgende Beispiel ist frei erfunden und zeigt, wie ein gut gepflegter Datensatz aussehen könnte.

Bereich	Beispiel
Grunddaten	VP-240, Produktnummer VP240-2026-017, verantwortlich: Produktmanagement
Software	Steuerungsprogramm 2.7.4, SPS-Firmware 3.2.1, HMI-Runtime 5.4.2, Remote-Gateway 4.8.1
Bauteile	PLC-500, Panel-12, RG-100 Remote Gateway, Drive-X
Risiko	Gemeinsamer Fernwartungsaccount; Maßnahme: personenbezogene Konten, MFA und Rollen
Sicherheitsproblem	Schwachstelle im Remote Gateway; Update auf Firmware 4.8.1; Advisory SA-2026-88
Support	01.01.2027 bis 31.12.2034, begründet über Nutzungsdauer und Komponentenverfügbarkeit
CRA-Abschluss	Produktklasse begründet, 22 Schutzfragen bewertet, Dokumentation und Sicherheitsprozess vollständig, CE/EU-Erklärung geprüft

25. Checkliste für den ersten Durchlauf

Wenn Sie CRAwerk zum ersten Mal einrichten, ist diese Reihenfolge am einfachsten.

1. **Unternehmensdaten vervollständigen**
   Firmenname, Anschrift, Land, E-Mail und Ansprechpartner prüfen.
2. **Optional Firmenlogo hochladen**
   Damit Exporte direkt dem Unternehmen zugeordnet werden können.
3. **Team einrichten**
   Weitere Mitarbeiter nur dann einladen, wenn sie mitarbeiten sollen.
4. **Erstes Produkt anlegen**
   Name, Modell/Produktnummer, Verantwortlichen und digitale Grundmerkmale erfassen.
5. **Software und Bauteile pflegen**
   Reale Versionen und Komponenten erfassen; Unbekanntes nicht erfinden.
6. **Risiken und Sicherheitsprobleme bearbeiten**
   Maßnahmen, Verantwortliche und Status nachvollziehbar dokumentieren.
7. **Unterlagen und Supportzeitraum ergänzen**
   Nachweise zuordnen und geplante Sicherheitsunterstützung dokumentieren.
8. **CRA-Abschluss öffnen**
   Die sechs Schritte in Reihenfolge durcharbeiten.
9. **Akte prüfen**
   Offene Punkte direkt aus der Abschlussliste öffnen und ergänzen.
10. **Exporte fachlich prüfen**
    Produktakte, Kurzakte, Nutzerinformationen und EU-Erklärung vor Verwendung prüfen.

26. Glossar

Begriff	Bedeutung
Angriffsfläche	Alle erreichbaren Funktionen, Schnittstellen und Wege, über die auf das Produkt eingewirkt werden kann.
Authentifizierung	Prüfung, wer ein Nutzer oder System ist.
Autorisierung	Festlegung, was ein angemeldeter Nutzer oder Dienst tun darf.
CVE	Öffentliche Kennung einer bekannten Schwachstelle.
CVD	Geregelter Prozess für koordinierte Offenlegung von Schwachstellen.
Firmware	Gerätenahe Software in Controllern oder Embedded-Geräten.
HMI	Human Machine Interface, also Bedienoberfläche einer Maschine.
MFA	Multi-Faktor-Authentifizierung, z. B. Passwort plus zweiter Faktor.
Patch	Änderung, die einen Fehler oder eine Schwachstelle behebt.
SBOM	Maschinenlesbare Liste von Softwarekomponenten und Abhängigkeiten.
Supportzeitraum	Zeitraum, in dem der Hersteller Schwachstellen behandelt und Sicherheitsupdates bereitstellt.

27. Offizielle Quellen und Rechtsstand

Bei rechtlichen Zweifelsfragen gilt der veröffentlichte Verordnungstext. Leitlinien der Kommission sind wichtige Auslegungshilfen, ersetzen aber nicht den Rechtstext.

Quelle	Adresse
Verordnung (EU) 2024/2847 - Cyber Resilience Act	https://eur-lex.europa.eu/eli/reg/2024/2847/oj/deu
EU-Kommission - CRA Umsetzung und Zeitplan	https://digital-strategy.ec.europa.eu/de/factpages/cyber-resilience-act-implementation
EU-Kommission - FAQ zur CRA-Umsetzung, zuletzt aktualisiert 04.09.2026	https://digital-strategy.ec.europa.eu/de/library/cyber-resilience-act-implementation-frequently-asked-questions
EU-Kommission - Leitlinien zur Anwendung des CRA, veröffentlicht 27.07.2026	https://digital-strategy.ec.europa.eu/en/library/commission-publishes-new-guidance-support-timely-cyber-resilience-act-implementation

Rechtsstand

Stand dieses Handbuchs ist September 2026. Artikel 14 gilt seit 11. September 2026; die übrigen Hauptpflichten gelten ab 11. Dezember 2027.