CYBERsicher | EASY.CRA Tool zur Umsetzung des Cyber Resilience Act

IT-Sicherheit IN DER WIRTSCHAFT

CRA: Welche Meldepflichten haben betroffene Unternehmen

16.09.2026

ibi research | OTH Regensburg

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

Mittelstand-Digital

aufgrund eines Beschlusses des Deutschen Bundestages

„Beim CRA geht es nicht um Audits, sondern darum, Verantwortung zu übernehmen.“

Sarah Fluchs, Selbstbewusste Entscheidungen statt CRA-Compliance-Panik, 02.06.2026, medium.com

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
Mittelstand-Digital
aufgrund eines Beschlusses des Deutschen Bundestages

CYBERsicher | EASY.CRA Tool zur Umsetzung des Cyber Resilience Act

Überblick

IT-Sicherheit IN DER WIRTSCHAFT



Dr. Matthias Kampmann
ibi research an der Universität Regensburg GmbH

matthias.kampmann@ibi.de
Galgenbergstraße 25
93053 Regensburg

- Einführung: Was ist der CRA?
- Geltungsbereich: Welche Produkte sind betroffen?
- EU-Konformitätserklärung – Gerät ist nicht im Markt.
- Meldepflichten bei Sicherheitsvorfällen – Software/ Gerät ist im Markt.
- Die Single Reporting Platform (SRP).
- Wesentliche Unterschiede: Konformität vs. Incident Reporting.
- Praktische Handlungsschritte für Unternehmen.
- Ansprechpartner und Ressourcen.
- Zusammenfassung & Fragen.

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
Mittelstand-Digital
aufgrund eines Beschlusses des Deutschen Bundestages

Was ist der Cyber Resilience Act?

- **Rechtsform:** Verordnung (EU) 2024/2847 (Regulation, direkt wirkend).
- **Veröffentlichung:** 10. Dezember 2024 (EU-Amtsblatt).
- **Vollständige Anwendbarkeit:** ab 11. Dezember 2027.
- **Ziel:** Verbesserung der Cybersicherheit von Hard- und Software im EU-Binnenmarkt.
- **Kernprinzip:** Kenntnis und Mitigierung von Cybersicherheitsrisiken im Produkt. Implementierung von Security by Default/Design und kontinuierliches Schwachstellenmanagement bei **jedem** Hersteller (bzw. kontrolliert durch Importeur, Händler), der Produkte im europäischen Binnenmarkt veräußern möchte.

Gefördert durch: Bundesministerium für Wirtschaft und Energie aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

Geltungsbereich – Welche Produkte sind betroffen?

Lösungen (Soft-/Hardware) mit Datenfernverarbeitungsmöglichkeit (vernetzt: aktiv/passiv)

- **„Produkte mit digitalen Elementen”:** Hard- und Software, die direkt oder indirekt ein Gerät vernetzen.
- **Ausnahmen:** Automotive, Medizinprodukte, Luftfahrt (bereits anderweitig reguliert)
- **Produktkategorien:**
  - Standardprodukte (Selbstbewertung),
  - Wichtige Produkte Klasse I (Einhaltung aller harmonisierter Standards oder zertifiziert) & II (zertifiziert),
  - Kritische Produkte (strengste Anforderungen).
- *Achtung:* Gilt unabhängig vom Firmensitz – nur Vertrieb in der EU zählt!

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
Mittelstand-Digital
aufgrund eines Beschlusses des Deutschen Bundestages

Teil 1: EU-Konformitätserklärung

Definition: Formaler Nachweis, dass das Produkt CRA-Anforderungen erfüllt

Aspekt	Detail
Wann?	Vor dem Inverkehrbringen
Wer?	Hersteller (oder bevollmächtigter Vertreter)
Inhalt:	(**Cyber-**)Technische Dokumentation, Konformitätsbewertung, CE-Kennzeichnung
Sprache:	Landessprache jedes Mitgliedstaats
Aufbewahrung:	**Zehn** Jahre nach Markteinführung

Gefördert durch: Bundesministerium für Wirtschaft und Energie aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

Konformitätsbewertung – Der Prozess

Für Hersteller: Schritt für Schritt

1. Produktklasse bestimmen,
2. Grundlegende Anforderungen (Anhang I) prüfen,
3. Risikobewertung durchführen,
4. Technische Dokumentation erstellen,
5. Konformitätsbewertung (Modul A: interne Kontrolle für meisten Fälle; Kategorie Standard),
6. EU-Konformitätserklärung unterzeichnen,
7. CE-Kennzeichnung anbringen,
8. Produkt auf den Markt bringen

- ***Hinweis:*** **Für wichtige/kritische Produkte sind notifizierte Stellen (TÜV oder ähnliche) erforderlich.**
  https://webgate.ec.europa.eu/single-market-compliance-space/notified-bodies

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
Mittelstand-Digital
aufgrund eines Beschlusses des Deutschen Bundestages

Die EU-Konformitätserklärung – Inhalt

Mindestinhalte laut Anhang VI (u. a.):

- Herstellername und Anschrift,
- Produktidentifikationsmittel (Typ, Seriennummer),
- Verwendete harmonisierte Standards (17 sind derzeit in Diskussion),
- Bestätigung der Konformität mit Anhang I (grundlegende Anforderungen),
- Ort und Datum der Unterzeichnung,
- Name/Funktion des Unterzeichners.

Praxis-Tipp: Musterdokumente finden sich auf der *EU-Digitalstrategy-Seite*

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
Mittelstand-Digital
aufgrund eines Beschlusses des Deutschen Bundestages

Teil 2: Meldepflichten

24/72/14 Tage

- Wie in jeder Regulierung der EU muss es auch ein Vorfallmanagement im CRA-Kontext geben. Fristen sind festgelegt. Fokus Schwachstellen:
  - Wird eine Schwachstelle **aktiv** ausgenutzt und festgestellt, gelten nachstehende Meldepflichten:
    - **Early Warning:** Nach Feststellung bleiben dem Herstellenden **24 Stunden**, um die Schwachstelle bei der ENISA zu melden. Kurze Erstmeldung. Ist böswillige Handlung Ursache? Hat es Auswirkungen auf EU-Mitgliedstaaten?
    - **Vulnarability Report:** Detaillierte Meldung nach **72 Stunden**. Umfassender Bericht, aktualisiert die Frühwarnung. Angaben zur Schwachstelle im Detail und erste Erkenntnisse über das Ausmaß, Risikobewertung, Überblick über die zu ergreifenden Maßnahmen.
    - **Final Report:** Schlussbericht spätestens **14 Tage** nachdem ein Patch für die Schwachstelle veröffentlicht wurde. Root-Cause-Analyse und Beschreibung der Behebungsverfahren.
  - *Nutzer* sollten ebenfalls informiert werden.
  - *Wichtig:* Fristbeginn = Zeitpunkt, zu dem der Hersteller Kenntnis erlangt!

Gefördert durch: Bundesministerium für Wirtschaft und Energie aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

Was genau wird gemeldet?

Auslösende Ereignisse (Art. 14 CRA)

Aktiv ausgenutzte Schwachstelle:	Eine bereits bekannte Sicherheitslücke, die derzeit **am Produkt** missbraucht wird. Wenn eine Lücke in einer Bibliothek ausgenutzt wird, aber nicht das Produkt betrifft, wird nicht gemeldet.
Schwerwiegender Sicherheitsvorfall:	Ein Sicherheitsvorfall mit erheblichen Auswirkungen auf Produktsicherheit des spezifischen Produkts.

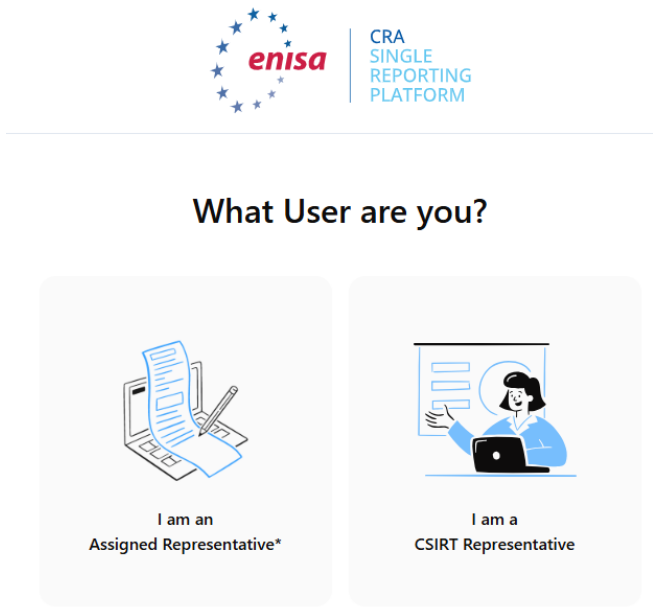
Startdatum der Meldepflicht war der 11. September 2026.

Gefördert durch: Bundesministerium für Wirtschaft und Energie aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

Die Single Reporting Platform (SRP) – Was ist das?

Definition: Online-Tool der ENISA für einmaliges Melden an alle zuständigen Behörden

- **Kernfunktionen:**
- Prinzip ***report once, reach all***.
- Meldung bei ENISA über die SRP reicht.
- Automatisierte Weiterleitung an das zuständige CSIRT (BSI).
- Verschlüsselte Übertragung.
- Verfügbarkeit: *portal.cra-srp.enisa.europa.eu*



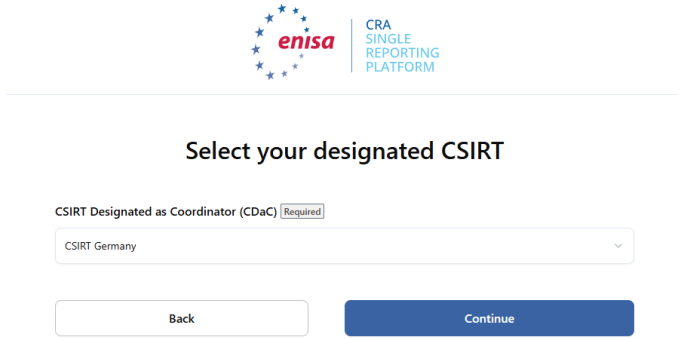
Startbildschirm der Meldeplattform

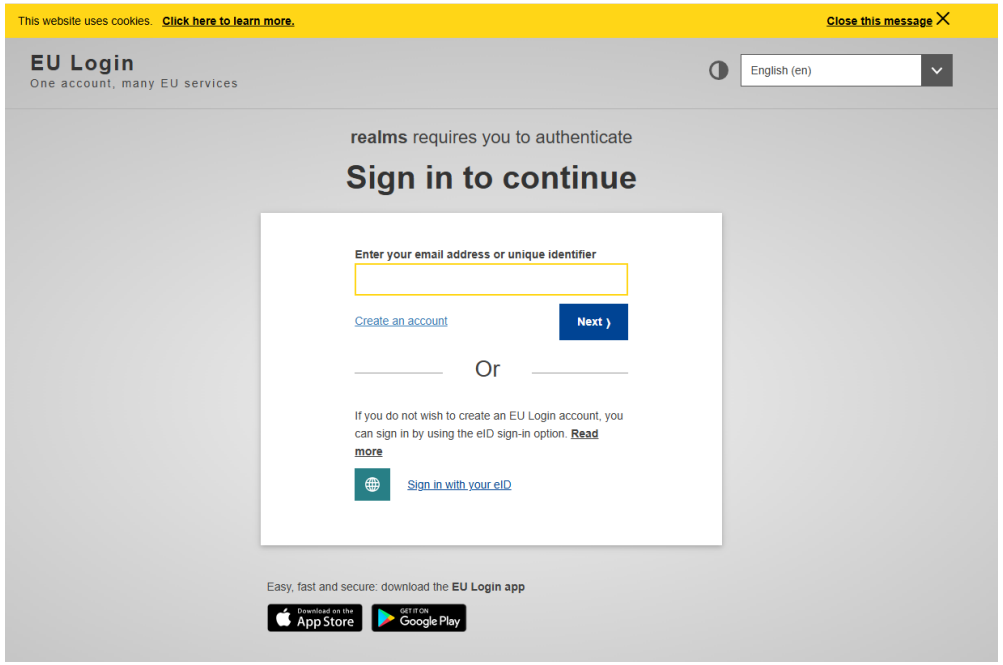
Gefördert durch:
Bundesministerium für Wirtschaft und Energie
Mittelstand-Digital
aufgrund eines Beschlusses des Deutschen Bundestages

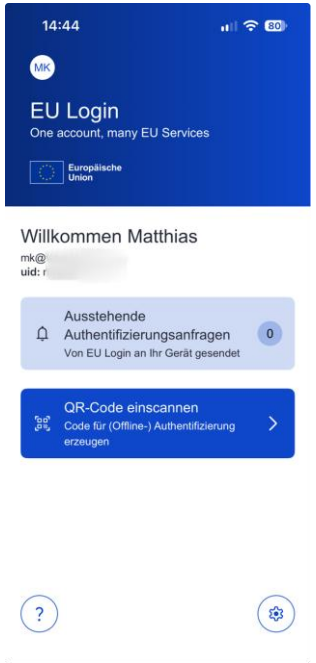
Vorgang (Anmeldung)

Von der EU-ID bis zur Vorfallsmeldung

1. Bestimmung des Nutzers: Hersteller oder BSI-Mitarbeiter,
2. CSIRT/Land wählen: Deutschland,
3. Teilnehmer braucht eine ID,
4. Login, Konto vorhanden?
5. Name, Firma, Übersicht.







Gefördert durch:
Bundesministerium für Wirtschaft und Energie
Mittelstand-Digital
aufgrund eines Beschlusses des Deutschen Bundestages

Assigned Representative Registration

1 Personal Details — 2 Manufacturer Details

Name Required

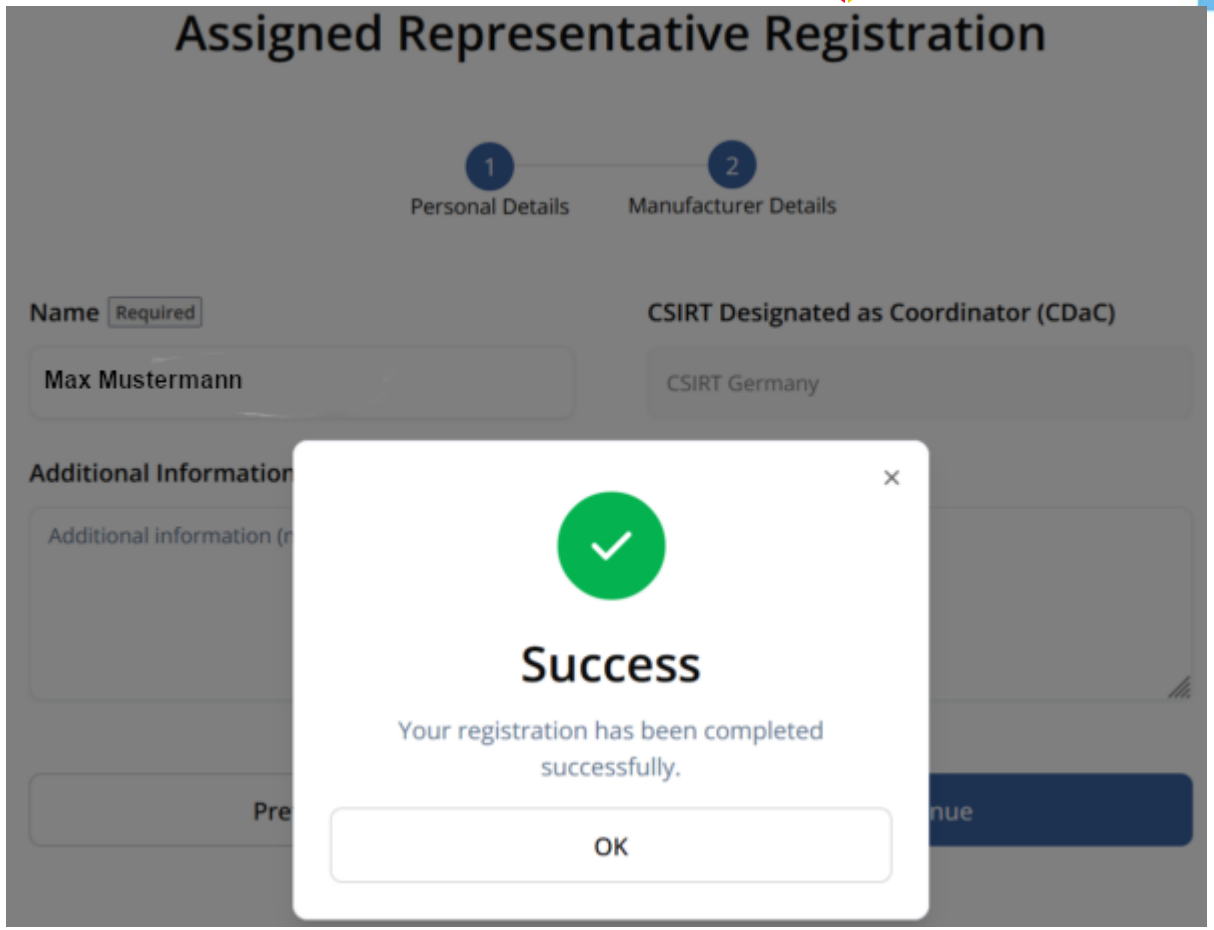
CSIRT Designated as Coordinator (CDaC)

CSIRT Germany

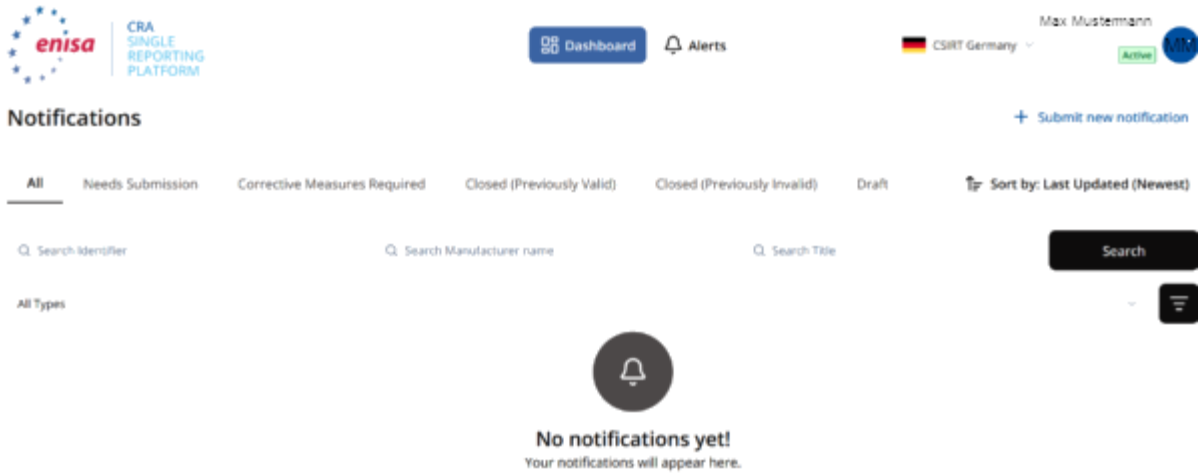
Additional Information

Additional information (max 255 characters)

Previous | Continue



Gefördert durch: Bundesministerium für Wirtschaft und Energie aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital



Links: Blick in den Account.

Wichtig: Bugs im herkömmlichen Sinn werden nicht gemeldet. Meldepflichtig sind nur Schwachstellen, **die nachweislich aktiv ausgenutzt werden**, und Vorfälle, **bei denen die Sicherheit des Produkts erheblich beeinträchtigt wurde**.

Das heißt: Ein leichter Zwang, zu dem, was man sowieso tun sollte: a. Risikoermittlung, b. Schwachstellenmanagement, c. Bugfix-Prozesse, d. Responsible-Desclosure-Verfahren implementieren!

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
Mittelstand-Digital
aufgrund eines Beschlusses des Deutschen Bundestages

Unterschiedliche Meldewege – Konformität vs. Incident

Unterschiede

Aspekt	EU-Konformitätserklärung	Schwachstellenmeldung
Zeitpunkt	Vor Markteintritt (einmalig)	Während Support-Zeit (kontinuierlich)
Ziel	Zulassung zum Markt	Reaktion auf laufende Bedrohungen
Empfänger	Marktüberwachungsbehörde (national)	CSIRT + ENISA (über SRP)
Form	Dokument + CE-Kennzeichnung	Elektronische Meldung über SRP
Häufigkeit	Einmal pro Produkt	Bei jedem relevanten Vorfall

Gefördert durch: Bundesministerium für Wirtschaft und Energie aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

Weitere Pflichten – Nutzerinformation

Neben Meldung bei der ENISA müssen Hersteller **Betroffene informieren** (Art. 14(8)):

- Bei aktiv ausgenutzten Schwachstellen,
- bei schweren Sicherheitsvorfällen.
- **Wo:** direkt an betroffene Endnutzer.
- **Wann:** ohne unverhältnismäßige Verzögerung.
- **Inhalt:** Beschreibung des Vorfalls, Risiken, empfohlene Maßnahmen.

Praxis-Tipp: Kommunikationsvorlagen vorbereiten (E-Mail, Push-Infos, Website-Banner, Social Media).
Realisieren Sie vorab schon eine Kommunikationsstrategie (z. B. Pro Modell je eine Webseite für ein Device liefern).

Gefördert durch: Bundesministerium für Wirtschaft und Energie aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

Produktklassen – Wer hat strengere Pflichten?

Klasse	Beispiele	Konformitätsbewertung	Besonderheiten
Standard	Router, Smart-Home-Geräte, Videoschnitt/Bild-bearbeitung etc.	Selbstbewertung (Modul A)	Basispflichten
Wichtig Klasse I	Firewalls, Authentifizierungsprodukte	Mit notifizierter Stelle oder Erfüllung harmonisierter Standards	Erhöhte Anforderungen
Wichtig Klasse II	Betriebssysteme, Datenbanken	Strenger Prüfprozess	Längere Dokumentation
Kritisch	Industriesteuerungen, Bank-Software, Biometrie	Vollständige Zertifizierung	Audits

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
Mittelstand-Digital
aufgrund eines Beschlusses des Deutschen Bundestages

Unternehmenshaushalt – Wer macht was intern?

Rollenverteilung im Unternehmen:

Rolle	Verantwortung
Legal/Compliance	Konformitätserstellung, Dokumentation, CE-Kennzeichnung
Produktsicherheit	Risikobewertung, Security-by-Design/Default, Vulnerability Management
Incident Response	24h-Meldung, SRP-Nutzung, Kommunikation mit CSIRT
Support/Service	Supportperiode determinieren, Updates bereitstellen
Management	Ressourcenzuteilung, Eskalationswege, Budget

Check: Sind alle Rollen klar benannt und geschult?

Gefördert durch: Bundesministerium für Wirtschaft und Energie aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

Ansprechpartner im Überblick

Primärkontakte

Institution	Aufgabe	Kontakt
ENISA	SRP-Betrieb, Guidance, Koordinierung	enisa.europa.eu/topics/product-security
Nationales CSIRT	Erstkontakt für Incident Reports	CSIRT-Liste EU (BRD: BSI)
Marktüberwachungsbehörde	Konformitätskontrolle, Sanktionen	Landesbehörden (Deutschland: Bundesamt für Sicherheit in der Informationstechnik - BSI)
Notifizierte Stelle	Konformitätsprüfung (für wichtige/kritische Produkte)	Notified Bodies Database

Gefördert durch: Bundesministerium für Wirtschaft und Energie aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

Checkliste – Vorbereitung für Hersteller

Wie bereite ich mein Unternehmen auf die CRA-Meldeanforderungen vor?

- **Vor Markteinführung (Konformität):**
- ☐ Produktklasse bestimmen
- ☐ Grundlegende Anforderungen prüfen (Anhang I)
- ☐ Technische Dokumentation erstellen
- ☐ Konformitätsbewertung durchführen
- ☐ EU-Konformitätserklärung unterzeichnen
- ☐ CE-Kennzeichnung anbringen
- ☐ Supportperiode festlegen und kommunizieren

- **Betrieb (Incident Reporting):**
- ☐ SRP-Zugang einrichten (EU Login + MFA, Passkey)
- ☐ Meldewege definieren (24h-Frist!)
- ☐ Vorfallskommunikation vorbereiten
- ☐ Schulung für Incident Response-Team

Gefördert durch: Bundesministerium für Wirtschaft und Energie aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

Zusammenfassung

Kernbotschaften

- **Konformität vor Markt** → CE-Kennzeichnung + Konformitätserklärung sind Ihre Eintrittskarte,
- **Meldepflicht während Betrieb** → Innerhalb 24h an CSIRT über SRP,
- **Zwei getrennte Prozesse** → Nicht verwechseln! Unterschiedliche Ansprechpartner, Fristen, Empfänger,

Next Steps:

- Produktbestand prüfen, Prozesse anpassen, SRP-Zugang einrichten, Teams schulen (regelmäßig!)

Gefördert durch: Bundesministerium für Wirtschaft und Energie aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

Wichtige Links

Offizielle Dokumente, die helfen, den CRA zu verstehen und zu realisieren.

- EU-Hersteller-Informationen: https://digital-strategy.ec.europa.eu/en/policies/cra-manufacturers
- EU-Infoseite: https://digital-strategy.ec.europa.eu/en/factpages/cyber-resilience-act-implementation
- EU-Seite FAQ: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-implementation-frequently-asked-questions
- EU-Seite f. Leitlinie: https://digital-strategy.ec.europa.eu/en/library/commission-publishes-new-guidance-support-timely-cyber-resilience-act-implementation (Übersetzung in Vorbereitung)
- ENISA-Reifegradmodell CRA: https://www.enisa.europa.eu/publications/sme-cyber-resilience-maturity-assessment-model (Übersetzung in Vorbereitung)
- BSI-CRA-Infoseiten: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber_Resilience_Act/cyber_resilience_act_node.html
- ENISA-SRP: https://www.enisa.europa.eu/topics/product-security/single-reporting-platform-srp

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
Mittelstand-Digital
aufgrund eines Beschlusses des Deutschen Bundestages

Was ist EASY.CRA?

Fokusprojekt, gefördert mit Mitteln des Bundesministeriums für Wirtschaft und Energie

- Konsortium aus ibi research an der Universität Regensburg GmbH und der Fakultät Informatik an der Ostbayerischen Technischen Hochschule, OTH, Regensburg.
- OTH erarbeitet ein **Tool** zum Selbstcheck. Ist mein Produkt betroffen? Was muss ich tun? Launch geplant Ende 09.2026 (Präsenz auf der it-sa Nürnberg, **27. bis 29. Oktober** am Stand der Transferstelle für Cybersicherheit. **Halle 9 (9-523)**).
- **Transfermaßnahmen** von ibi research: https://easycra.net, Webinare, Sprechstunden, Konvoiprojekte, Begleittagebücher, Workshops, CRA-“Selbsthilfegruppe“ (mit der Strategischen Partnerschaft Sensorik, Regensburg).

Gefördert durch: Bundesministerium für Wirtschaft und Energie aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

CYBERsicher

EASY.CRA
Tool zur Umsetzung
des Cyber Resilience Act

IT-Sicherheit
IN DER WIRTSCHAFT

VIELEN DANK

für Ihre Aufmerksamkeit!

Gefördert durch:

Bundesministerium
für Wirtschaft
und Energie

aufgrund eines Beschlusses
des Deutschen Bundestages

Mittelstand-
Digital