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

IT-Sicherheit IN DER WIRTSCHAFT

Wen betrifft es und was bedeutet es für diese Unternehmen?

04.09.2026

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



Dr. Matthias Kampmann
ibi research an der Universität Regensburg GmbH

matthias.kampmann@ibi.de
Galgenbergstraße 25
93053 Regensburg

CRA kurz notiert

- Der CRA ist eine direkt und horizontal wirkende EU-Regulierung.
- Es gibt keine Pflicht zur Anpassung an deutsche Gesetze für die Bundesregierung.
- Am 11.09.2026 treten Meldepflichten in Kraft.
- Am 11.12.2027 wirkt das Gesetz vollständig.
- Ziel: Produktsicherheit.
- Betroffene Wirtschaftsakteure: Hersteller, Einführer, Händler
- **Ziel: Schutz von Anwendern und Nutzenden.**

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

Übersicht: Wovon wird die Rede sein?

1. Wen betrifft der CRA und warum?
2. Was sind die Ziele des CRA?
3. Welche Wirtschaftsakteure sind betroffen?
4. Welche Produkte sind betroffen?
5. Welche Pflichten haben Hersteller, Inverkehrbringer und Importeure?
    1. Welche Cybersicherheitsanforderungen gelten?
    2. Wie müssen Schwachstellen behandelt werden?
    3. Welche Hilfen müssen Nutzer bekommen?
    4. Wie funktioniert Konformität? Was ist das CE-Siegel und wie wird es vergeben?
6. Welche Produktkategorien gibt es? Was sind Kritikalitätsklassen?
7. Welche Rolle spielen Lieferketten, Haftungsfragen?
8. Ansätze zur Umsetzung sowie Zeitplanung.

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

Wen betrifft das Gesetz? Warum?

Der Cyber Resilience Act adressiert **alle Produkte mit digitalen Elementen** und ist Teil des *New Legislative Frameworks* der EU.

- Bedrohungen aus dem Cyberraum nehmen von Jahr zu Jahr zu. Produkte mit digitalen Elementen sind oft unsicher bzw. haben ein niedriges Cybersicherheitsniveau.
- Die Höhe der Schäden durch Cybercrime in weiterem Sinn (inkl. Sabotage, Spionage) lag 2025 laut BITKOM für die Wirtschaft der Bundesrepublik bei ca. 202 Milliarden Euro (ca. 4,5 Prozent des BIP).
- Zu viele schlechte Produkte überschwemmen den EU-Binnenmarkt.
- Mindeststandards werden nicht eingehalten.
- Sicherheitsmechanismen werden nicht von Beginn an implementiert.
- Kunden haben keine Kontrolle und sind schlecht informiert.

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

Vier Ziele des CRA

Produktsicherheit, Cybersicherheitsrahmen, Produkttransparenz, Nutzungssicherheit

- CRA fordert Produktsicherheit über den kompletten Lebenszyklus eines Produkts mit digitalen Elementen ein.
- CRA gewährleistet einen durchgängig stimmigen Rahmen für Cybersicherheit von Produkten mit digitalen Elementen als Orientierung für Hersteller.
- CRA fordert Transparenz der Sicherheitseigenschaften von Produkten, etwa mit Blick auf Schwachstellenmanagement.
- CRA befähigt Nutzende zur sicheren Nutzung der Produkte (IT-Sicherheitsgebrauchsanweisungen gefordert).

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

Welche Wirtschaftsakteure sind betroffen?

Hersteller, Einführer, Händler, Open-Source-Stewards

- Europäische oder außereuropäische **Hersteller** von Produkten mit digitalen Elementen (PdE), die für den Verkauf im europäischen Binnenmarkt vorgesehen sind; juristische Person, die entwickelt und herstellt oder unter dem Namen oder der Marke konzipieren, entwickeln und herstellen lässt.
- **Einführer**, niedergelassen in der EU, importiert PdE von außerhalb der EU, um sie in Verkehr zu bringen. Ist es der einzige Importeur, wird er der Bevollmächtigte und muss die Einhaltung der CRA-Pflichten Sorge tragen. Ist haftbar wie ein Hersteller.
- **Händler** (Teil der Lieferkette), die ein PdE auf den EU-Binnenmarkt in Verkehr bringen, ohne ihn zu verändern. Darunter wird weder der Einführer noch der Hersteller verstanden.
- Sonderfall **Open Source**: Stewards (etwa RedHat) übernehmen Verantwortung für Software. Sie sind weder Hersteller noch Importeure, übernehmen aber juristische „Patenschaft“ für Projekte, die keinen rein ökonomischen, privatwirtschaftlichen Charakter haben.

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

Worum geht‘s

Soft-/Hardware-Produkte oder Soft-Hardware-Produkte

- Art. 3 Abs. 1 weist auf „Datenfernverarbeitungslösungen“ hin. Aber:
- Wenn etwa ein Texteditor keine Online-Update-Funktion hat und nur lokal auf dem Desktop/Laptop laufen soll, ist er aufgrund der Einbindung in das System, das onlinefähig ist, betroffen.
- IoT, Smarthome: Alles, was vernetzte Sensoriken aufweist, fällt unter den CRA.
- Eine Netzwerkkarte kann zwar nicht allein sich selbst sinnbringend vernetzen, ist aber als „getrennt in den Verkehr gebracht[es]“ Produkt CRA-relevant.
- Damit ist so ziemlich jedes Produkt mit digitalen Elementen CRA-relevant. Ausgenommen sind Produkte, deren „bestimmungsgemäßer Zweck oder […] Verwendung“ gemäß Art. 2 Abs. 1 KEINE „direkte oder indirekte logische oder physische Datenverbindung mit einem Gerät oder Netz einschließt“.

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

Pflichten für Unternehmen

- *Konformitätspflicht*: Unternehmen, die Produkte mit digitalen Elementen herstellen und/oder auf den EU-Binnenmarkt bringen wollen, müssen konform sein mit den CRA-Regeln.
- *Konformitätserklärung (Conformité Européenne)*: Unternehmen erklären ihre Geräte konform mit den Regularien. Dies wird bei der ENISA hinterlegt. Ziel: CE-Kennzeichnungen auch für Software: Novum!
- *Kennzeichnungs-, Aufklärungspflichten*: Ist die Erklärung erteilt, muss das Produkt mit Kennzeichnungen ausgeliefert werden. Erstmalig erweitern Cybersicherheitshinweise die begleitenden Materialien.

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

Cybersicherheitsanforderungen

- *Schwachstellen*: Betroffene Produkte müssen ohne bekannte ausnutzbare Schwachstellen ausgeliefert werden.
- *Security by default*: Produkte müssen in der Standardkonfiguration bei Auslieferung und nach einem Reset sicher eingestellt sein.
- *Updatepflicht*: Schwachstellen müssen durch Sicherheitsaktualisierungen/Patches über den Lebenszyklus hinweg: sofort und unentgeltlich behoben werden (können). Benutzende werden informiert und bekommen eine Opt-out-Lösung.
- *Zugangskontrolle*: Unbefugter Zugriff muss durch Kontrollmechanismen verhindert werden.
- *Datenintegrität*: Daten, Befehle, Software, Konfigurationen sind vor einer nichtgenehmigten Manipulation zu schützen.
- *Minimierung der Angriffsfläche*: Was für den Betrieb nicht erforderlich ist, wird entfernt.

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

Cybersicherheitsanforderungen 2

- *Datensparsamkeit*: Verarbeitung personenbezogener und anderer Daten ist auf ein notwendiges Minimum zu beschränken.
- *Verfügbarkeit*: Funktionen und Daten müssen nach einem Notfall integer verfügbar sein. Das umfasst Maßnahmen gegen Denial-of-Service-Angriffe (DoS, DDoS).
- *Negative Auswirkungen*: dürfen nicht vom Produkt ausgehen. Ein Angriff soll möglichst auf das angegriffene Device beschränkt sein.
- *Security by Design*: Produkt muss so entwickelt sein, dass es möglichst geringe Angriffsflächen bietet. Das Ausnutzen muss so weit wie möglich erschwert werden.
- *Protokollfunktionen*: Logging muss möglich sein. Das Opt-out auch.
- *Information*: Sicherheitsanweisungen und klare Dokumentation sind verpflichtend.
- *Löschmöglichkeiten*: Nutzende müssen *dauerhaft und einfach* Einstellungen etc. löschen können.

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

Schwachstellenbehandlung

CRA, Anhang 1, Teil II, schreibt vor, wie mit Schwachstellen umzugehen ist.

- SBOM (maschinenlesbar) ist Pflicht.
- Sicherheitsaktualisierungen werden für die Lebenszeit verpflichtend (zu trennen von Funktionsupdates).
- Regelmäßiges, wirksames Testen wird Pflicht.
- Schwachstellen und Behebung werden veröffentlicht (CVE plus Scoring).
- Strategie zur Veröffentlichung aufstellen.
- Kontaktmöglichkeit für Meldung Dritter vorhalten.
- Auslieferung von Aktualisierungen muss sicher sein.
- Aktualisierungen müssen unverzüglich ausgeliefert und bekannt gemacht werden.

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

Hilfen für die Nutzenden

Schutz und Hilfen; Infos und Anleitungen, Anhang II

- Kontaktmöglichkeit (analog und digital), Name, Marke.
- Kontakt zur Meldung von und Information über Schwachstellen.
- Typenname, Spezifikationen zur eindeutigen Identifikation des Produkts.
- Zweckbestimmung, Sicherheitsumfeld, Funktionsbeschreibung.
- Liste und Beschreibung der Umstände für Fehlanwendung/Cyberrisiken.
- Internetquelle der CE-Erklärung.
- Support und EOL.
- Anleitungen (bzw. Adresse) zu: Inbetriebnahme, Änderungen und Datensicherheit, Aktualisierungshilfe, sichere Stilllegung, Entfernung Nutzerdaten […].
- SBOM kann/sollte beigelegt werden

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

Was ist Konformität? Was ist eine CE-Kennzeichnung?

Nachweise und Regeln des Nachweises der Compliance mit dem CRA

- CE ist eine Produktkennzeichnung.
- CE belegt, dass sie rechtlich bindenden Standards der EU für Produktsicherheit genügen.
- Es gibt eine interne und externe Konformitätsbewertung je nach Klasse (s. unten)
- Je nach Produktklasse (standard, wichtig, kritisch) müssen verschiedene „Bodies“ die Konformität kontrollieren oder am Produkt prüfen und nachweisen.
- Allgemeines Verfahren für Produkte.
- Kein stillstehendes Verfahren. Änderungen führen zu erneutem Check.

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

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:
    - 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?
    - 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.
    - Schlussbericht spätestens **14 Tage** nachdem ein Patch für die Schwachstelle veröffentlicht wurde. Root-Cause-Analyse und Beschreibung der Behebungsverfahren.
  - Nutzer sollten ebenfalls informiert werden.

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

Kritikalitätsklassen: Standard

Standard, wichtige Produkte (Klasse I und II), kritische Produkte. **Meldepflicht** vom **11.09.2026** an!

1. **Standard**: wird selbstbewertet, selbsterklärt bei ENISA, Schulung (etwa beim TÜV) ist hinreichend.
    1. Beispiele: Software, Geräte für den allgemeinen Gebrauch, Bildbearbeitung, Games, Videoschnitt.
    2. Pflichten:
        1. Security by Design/Default,
        2. Risikobewertung,
        3. technische Dokumentation und
        4. Schwachstellenmanagement, SBOM,
        5. Konformitätserklärung abgeben,
        6. CE-Kennzeichen anbringen.
2. **Erläuterung: Alle** Pflichten bleiben bestehen. Vereinfacht ist *nur das Prüfverfahren*. Die Pflicht zur Risikoanalyse, zur Erstellung der technischen Dokumentation und der **SBOM** gilt für Standardgeräte uneingeschränkt.

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

Kritikalitätsklassen: Wichtige Produkte

Wichtige Produkte (**Klasse I und II**)

1. Wichtige Produkte: Konformitätsbewertung und Zertifizierung durch Zertifizierungsstelle/benannte Stelle.
    1. Beispiele für **Klasse I**: Router, Betriebssysteme, Passwortmanager, VPN, physische, virtuelle Netzwerkschnittstellen, Smarthome-Sicherheitssysteme/-devices. (EU-Baumusterprüfung oder Konformität)
    2. Beispiele für **Klasse II**: Firewalls, Virtualisierungsumgebungen, Intrusion Detection Systeme (Art. 32, Abs. 2)
    3. Pflichten (s. vorherige Folie); **ACHTUNG**: für **Klasse II**: gilt Nachweis auf höchstem Niveau sowie lückenlose SBOM/Patchprozess. EU-Baumusterprüfung oder umfassende Qualitätssicherung durch Audit des gesamten Qualitäts- und Entwicklungssystems. Auditierung der kompletten technischen Dokumentation;
    4. **Klasse I**: Wenn nachweislich alle harmonisierten EU-Normen vollständig angewendet wurden, ist ein externer Prüfer nicht notwendig. Wer diese nicht nutzt (oder, wahrscheinlicher, es existieren noch keine), muss durch eine zugelassene externe Prüfstelle (*notified Body*: z. B. TÜV, secuvera, DEKRA) geprüft werden.
    5. **Klasse I**: Unterzeichnung der EU-Konformitätserklärung erst nach erfolgreicher Prüfung. Danach erst ist das Anbringen des CE-Siegels auf Verpackung etc. erlaubt. **Klasse II**: Erst wenn die benannte Stelle die Konformität offiziell *bestätigt und zertifiziert* hat, darf die EU-Konformitätserklärung unterzeichnet werden. Danach erst ist das Anbringen des CE-Siegels auf Verpackung etc. erlaubt.

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

Kritikalitätsklassen: Kritische Produkte

Meldepflicht vom **11.09.2026** an!

1. Kritische Produkte: Konformitätsbewertung und Zertifizierung erst nach Durchlauf eines europäischen Cybersicherheitszertifizierungsprogramms CSA*.
    1. Beispiele: Smartcards mit Biometrie, Smart-Meter-Gateways, „Geräte für fortgeschrittene Sicherheitszwecke, einschließlich sicherer Kryptoverarbeitung“ (Anhang IV).
    2. Pflichten: Einhalten maximaler Sicherheitsvorgaben (Anhang I; z. B. Hardware-Verschlüsselung, Isolierung kritischer Prozesse, physischer Manipulationsschutz). **Lückenloses** Schwachstellenmanagement/SBOM. **Alle** Komponenten sowie **alle** Komponenten von Drittanbietern müssen kontinuierlich, automatisiert überwacht werden; kryptografisch-signiertes und manipulationssicheres Einspielen von Updates.
    3. Zertifizierung zum Beispiel nach dem EU-Cybersecurity-Framework (EUCC) auf Basis der Comon Criteria; durch akkreditierte Prüfstelle; Laborprüfung, Quellcode-Audits.
    4. Audit der **gesamten** Lieferkette; Absicherung der Lieferkette.
    5. Erst wenn das Zertifikat erteilt worden ist, darf die EU-Konformitätserklärung unterzeichnet werden. Danach erst ist das Anbringen des CE-Siegels auf Verpackung etc. erlaubt.

* https://eur-lex.europa.eu/eli/reg/2019/881/oj

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

Lieferkette: Rollen und Verantwortlichkeiten

Abhängig von der Kritikalitätsklasse wird Kontrolle über Lieferkette notwendig

- In der Kette sind Hersteller, Händler, Importeure
  - Lieferkettenangriffe nehmen zu, daher SBOM, um sie transparent zu machen. In der Regel standardisiert, elektronisch gefordert. Es ist angeraten, offene Standards zu nutzen: SPDX, CycloneDX sowie die entsprechenden Tools aus dem Kosmos.
  - Alleinige Importeure übernehmen für EU-fremde Hersteller alle Pflichten gegenüber ENISA.
    - Müssen SBOMs ihrer Hersteller organisieren und alle Dokumente liefern, die auch europäische Hersteller liefern müssen.
  - Sonderregeln für Open Source: Stärkere Kontrolle nötig (s. Log4J).
    - Open-Source-Steward: juristische Person (z. B. Linux Foundation, Red Hat), die Software checkt und Entwicklung überwacht. Gelten aber nicht als Hersteller.
  - Probleme in der Lieferkette: Upgrades, Updates/Nachweis in Libraries oder Drittkomponenten.

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

Haftung

Auf dem Weg zur Optimierung der Organisation in drei Schritten

Bußgelder

- Schwerwiegende Verstöße (Nichteinhaltung zentraler Herstellerpflichten): bis 15 Millionen Euro oder 2,5 Prozent des Jahresumsatzes weltweit.
- Sonstige Verstöße bei Nichteinhaltung anderer Pflichten (Dokumentation/Kennzeichnung): bis zu 10 Millionen Euro oder 2 Prozent.
- Falschangaben (unvollständige oder irreführende Angaben):
  5 Millionen Euro oder 1 Prozent Jahresumsatz.

Haftungsrisiken

- Produkthaftung/Schadenersatzansprüche durch unsichere Produkte mit digitalen Elementen.
- Lifecycle-Haftung: Hersteller haften über den gesamten Lebenszyklus ihres Produkts hinweg etwa für unzureichenden Schwachstellenschutz, fehlenden Support, versäumte Sicherheitsupdates.
- Pflichtverletzungen: Kein Security by Default/Design, keine Risikobewertung, keine technische Security-Dokumentation usw. (s. Pflichten oben)

Marktverbote/Rückrufe

- Zusätzlich zu finanziellen Sanktionen können nationale Marktüberwachungsbehörden den Verkauf der betroffenen Produkte **verbieten**, den Rückruf anordnen oder sie ganz aus dem europäischen Markt nehmen. Bei der konkreten Festlegung der Bußgelder werden mildernde Umstände wie die Unternehmensgröße (insbesondere bei KMUs und Start-ups) berücksichtigt.

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

Umsetzung

Ein paar Schritte zur CRA-Compliance

1. Aufsetzen eines produktorientierten Risikomanagements,
2. Realisierung von Prozessen zur Dokumentation und zur Erstellung von cybersicherheitsrelevanten Produkthandbüchern und allen notwendigen Dokumenten sowohl zur EU-Konformitätserklärung als auch für die Kundeninformation,
3. Aufbau eines Prozesses zur Realisierung von sicheren Entwicklungslebenszyklen (Secure Development Livecycle, SDL),
4. engere Verzahnung zwischen Betrieb und Entwicklung (DevOps, DevSecOps),
5. Aufsetzen eines Schwachstellenmanagements,
6. Aufsetzen eines Lieferkettenmanagements und Implementierung automatisierter SBOM-Herstellung und anderer Tools, um die Wahrscheinlichkeit von Schwachstellen zu verringen,

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

Zeitplan

Meilensteine und Umsetzungszwänge*

- Am 11.09.2026 tritt die Meldepflicht für aktiv ausgenutzte Schwachstellen und schwerwiegende Sicherheitsvorfälle in Kraft.
  - ENISA, die EU-Cybersicherheitsbehörde, richtet bis zu diesem Zeitpunkt eine Plattform ein (SRP: Single Reporting Platform).
  - Weiterleitung ans CSIRT (verantwortlich ist CERT-Bund/BSI für Deutschland) erfolgt automatisch.
  - Beispiel: Ein Produkt mit digitalen Elementen wird als Teil eines Botnetzes detektiert und zweckentfremdet. Diese Schwachstelle ist CRA-relevant und muss gemeldet werden.
- Am 11.12.2027 ist der CRA voll anwendbar. Von diesem Zeitpunkt an müssen alle neu auf den Markt gebrachten Produkte mit digitalen Elementen sämtliche Anforderungen des CRA erfüllen und nachweisbar sein.

* https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber_Resilience_Act/cyber_resilience_act_node.html

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-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)
- ENISA-Playbook Securit by Design/Default: https://www.enisa.europa.eu/publications/enisa-secure-by-design-and-default-playbook
- ENISA-SBOM-Handreichung: https://www.enisa.europa.eu/publications/sbom-adoption-state-of-play-2026
- BSI-CRA-Infoseiten: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber_Resilience_Act/cyber_resilience_act_node.html

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

Europäische Gesetzgebung

„Es dürfte kaum noch eine Organisation in der EU (oder gar weltweit) geben, die nicht von irgendeinem EU-Cybersecurity-Regelwerk betroffen ist. Oft gelten sogar gleich mehrere.“

Dr. Sarah Fluchs, Cybersicherheitsexpertin, admeritia GmbH
https://fluchsfriction.medium.com/die-3-erfolgsfaktoren-um-alle-eu-cybersecurity-regularien-einzuhalten-15ea7c3ea0b8

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
Mittelstand-Digital
aufgrund eines Beschlusses des Deutschen Bundestages

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