Der Cyber Resilience Act (CRA): Anforderungen an die Sicherheit in Produkten

Vortrag von

Sabine Sobola
Geschäftsführerin der
LiiDU GmbH und Rechtsanwältin

Veranstalterin: IHK Regensburg für Oberpfalz/Kelheim

online
am 11.05.2026

Sabine Sobola

- Rechtsanwältin
- Geschäftsführerin

  der LiiDU GmbH
- IT- und Datenschutzrecht seit 1998

Der Cyber Resilience Act

- **Ziel** und **Anwendungsbereich** des **Cyber Resilience Acts der EU**
- Was genau sind „**Produkte mit digitalen Elementen**“?
- **Verpflichtung zu Cybersicherheit** in den verschiedenen Phasen der Herstellung von Hard- und Software
- **Dokumentations-, Melde-, Überwachungs- und Beseitigungspflichten**
- Stand des **Gesetzgebungsverfahrens** und Ausblick

Problemstellung und Intention

- **Cyberangriffe** und **Cyberkriminalität** ist in den letzten Jahren immer mehr **angestiegen**. Dies kostet Schätzungen zufolge weltweit viele Milliarden Euro. Ein großes Problem dabei ist, dass **Produkte mit digitalen Elementen mehr in den Fokus von Angriffen** rücken und durch ihre **europaweite Vernetzung** und branchenübergreifende Verwendung eine Ausbreitung deutlich erleichtern.
- Zwei Elemente wurden dabei als Hauptursache bezeichnet: ein **niedriges Cybersicherheitsniveau** bei den **Produkten** selbst (u.a. durch weitreichende Schwachstellen und unzureichende Sicherheitsupdates) und eine **unzureichende Informationslage beim Nutzer** (zum einen durch fehlendes Verständnis, aber auch durch fehlende Informationen und Transparenz).

Ziele

Im Entwurf zur Bekämpfung dieses Problems dem CRA (Cyber Resiliance Act) wurden daher vier Hauptziele formuliert:

1. Die Gewährleistung, dass die Sicherheit von Produkten mit digitalen Elementen von der Entwurfs- und Entwicklungsphase an, durch die ganze Lieferkette und während des gesamten Lebenszyklus verbessert wird ("cybersecurity by design").

2. Die Gewährleistung eines kohärenten Rahmens für die Cybersicherheit, der den Herstellern von Hardware und Software die Einhaltung der Compliance-Vorgaben erleichtert.

3. Die Verbesserung der Transparenz der Sicherheitseigenschaften von Produkten mit digitalen Elementen.
   Stichwort: Schwachstellenbehandlung

4. Die Befähigung von Unternehmen und Verbrauchern, Produkte mit digitalen Elementen sicher zu nutzen.

Für wen gilt der Cyber Resilience Act?

Der Cyber Resilience Act adressiert verschiedene Akteure in der Lieferkette von Produkten mit digitalen Elementen. Nach Artikel 3 Nr. 12 der Verordnung umfasst der Begriff „Wirtschaftsakteur“ folgende Personen:

1. Hersteller: Als „Hersteller“ gilt eine natürliche oder juristische Person, die Produkte mit digitalen Elementen entwickelt oder herstellt oder diese konzipieren, entwickeln oder herstellen lässt und sie unter ihrem Namen oder ihrer Marke vermarktet.
2. Einführer: „Einführer“ sind in der Union ansässige oder niedergelassene natürliche oder juristische Personen, die ein Produkt mit digitalen Elementen unter dem Namen oder der Marke einer außerhalb der Union ansässigen Person in der Union in den Verkehr bringen .
3. Händler: Als „Händler“ gelten natürliche oder juristische Personen in der Lieferkette, die ein Produkt mit digitalen Elementen ohne Änderung seiner Eigenschaften auf dem Unionsmarkt bereitstellen, mit Ausnahme des Herstellers oder des Einführers
4. Verwalter quelloffener Software: Eine besondere Rolle kommt „Verwaltern quelloffener Software“ zu. Das sind juristische Personen, die nicht als Hersteller gelten, aber systematisch und nachhaltig die Entwicklung spezifischer Produkte mit digitalen Elementen unterstützen, die als freie und quelloffene Software gelten und für kommerzielle Tätigkeiten bestimmt sind .
5. Bevollmächtigte Als „Bevollmächtigter“ wird eine in der Union ansässige oder niedergelassene natürliche oder juristische Person bezeichnet, die von einem Hersteller schriftlich beauftragt wurde, in seinem Namen bestimmte Aufgaben wahrzunehmen . Das ist insbesondere für Hersteller relevant, die ihren Sitz außerhalb der EU haben.

Anwendungsbereich: Produkte mit digitalen Elementen

- Das Herzstück des CRA ist das „Produkt mit digitalen Elementen“. Darunter ist gemäß Art. 3 Abs. 1 CRA „**ein Software- oder Hardwareprodukt** und **dessen Datenfernverarbeitungslösungen**, einschließlich Software- oder Hardwarekomponenten, die getrennt in Verkehr gebracht werden“ gemeint.

- Mit Produkten mit digitalen Elementen ist das „Internet of Things“ gemeint. Das **Internet of Things** (**IoT**) ist die Bezeichnung für das Netzwerk physischer Objekte („Things“), die mit Sensoren, Software und anderer Technologie ausgestattet sind, um diese mit anderen Geräten und Systemen über das Internet zu vernetzen, sodass zwischen den Objekten Daten ausgetauscht werden können. Die **Spannbreite** von betroffenen Artikeln ist **sehr weit** und umfasst quasi **alle smarten Produkte**.

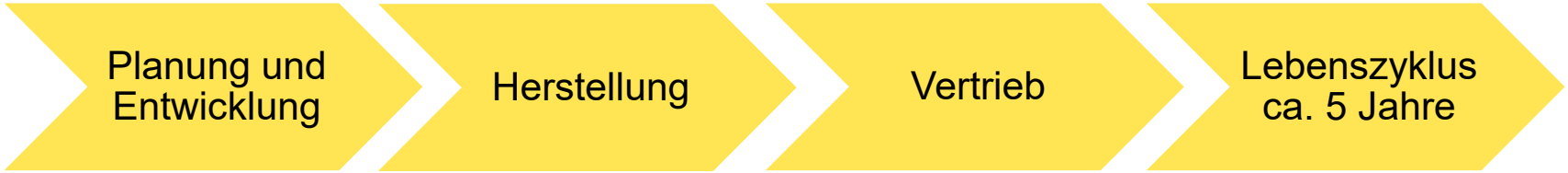
Was sind Produkte mit digitalen Elementen?

- **„normale“** Produkte mit digitalen Komponenten (ca. 90% aller Digitalprodukte)
  - Z.B. Software, Computer, Fotobearbeitungsprogramme, Grafikkarten, Smartwatches, Babyphone-Systeme.
- **„wichtige“** Produkte mit digitalen Elementen
  - Klasse I: z.B. eigenständige und eingebettete Browser, Passwortmanager, Anti-Viren-Software, Smart-Home-Geräte.
  - Klasse II: Firewalls und manipulationssichere Mikroprozessoren.
- **„kritische“** Produkte mit digitalen Elementen
  - Z.B. Hardware-Geräte mit Sicherheitsboxen, Smart-Meter-Gateways in intelligenten Messsystemen und Smartcards. Voraussetzungen: kritische Abhängigkeit von wesentlichen Einrichtungen i. S. d. Art. 3 der NIS-2-Richtlinie *oder* potenzielles Ausmaß schwerwiegender Unterbrechungen kritischer Lieferketten bei Vorfällen und ausgenutzten Schwachstellen

Die verschiedenen Phasen

- Bislang wurde auf EU-Ebene meist vertikal reguliert. Mit dem CRA soll eine **horizontale Regelung** zur Stärkung der Cybersecurity geschaffen werden. Um dies ganzheitlich einzuführen und entstandene Lücken zu schließen, wird auch der **komplette Prozess** eines Produkts mit digitalen Elementen vom Anwendungsbereich **erfasst**.

- So setzt der CRA bereits bei der **Entwicklung** und **Planung** des Produkts an, stellt Anforderungen an die **Herstellung** und den **Vertrieb** in Form verschiedener Bewertungs- und Transparenzpflichten und sorgt dafür, dass bis zu 5 Jahre (oder länger) des Lebenszyklusses eines Produkts Update- und andere Sicherheitspflichten erfüllt werden müssen.



Inhalte und Pflichten: Überwachungs- und Aufklärungspflichten

- Jedes digitale Produkt muss konzipiert, entwickelt und hergestellt werden **in** Übereinstimmung mit den **essentiellen Voraussetzungen des CRAs nach Art. 6 und 13**. Dabei muss bereits von Beginn an ein Risk Assessment durchgeführt und dokumentiert werden und auch in der Wartung und Weiterentwicklung Risiken der Cybersicherheit berücksichtigt werden. **Anhang I, Teil I und II muss eingehalten werden.**
- Die Produkte mit digitalen Elementen dürfen nur bereitgestellt werden, wenn sie **keine bekannten ausnutzbaren Schwachstellen** haben – und sie müssen eine **sichere Standardkonfiguration** haben. Zudem müssen Anforderungen an die **Behandlung von Schwachstellen** erfüllt werden.
- Dem **Nutzer** müssen **klar verständliche Informationen und Handlungsempfehlungen** bezüglich der **Aspekte der Cybersecurity** zu jedem Produkt bereit gestellt werden.

Inhalte und Pflichten: Überwachungs- und Aufklärungspflichten

Normale Produkte mit digitalen Elementen:

- Normale Produkte mit digitalen Elementen sind alle Produkte, die nicht in Anhang III (wichtige Produkte) oder Anhang IV (kritische Produkte) aufgeführt sind.
- Anforderungen: Diese Produkte müssen die grundlegenden Cybersicherheitsanforderungen gemäß Anhang I erfüllen. Die Hersteller müssen:
  - Eine Risikobewertung durchführen
  - Die Produkte ohne bekannte ausnutzbare Schwachstellen bereitstellen
  - Geeignete Sicherheitsmaßnahmen implementieren
- Konformitätsbewertungsverfahren: Für normale Produkte kann der Hersteller das interne Kontrollverfahren auf der Grundlage von Modul A anwenden. Der Hersteller stellt auf eigene Verantwortung sicher, dass das Produkt und die Prozesse die grundlegenden Cybersicherheitsanforderungen erfüllen. Der Hersteller kann freiwillig ein strengeres Verfahren unter Einbeziehung eines Dritten wählen .

Inhalte und Pflichten: Konformitätsbewertung

Was muss der Hersteller beim Modul A tun?

1. **Technische Dokumentation erstellen** Der Hersteller muss technische Unterlagen erstellen, die es ermöglichen, die Konformität des Produkts mit den grundlegenden Cybersicherheitsanforderungen zu bewerten. Diese müssen Folgendes enthalten :
   - Eine allgemeine Beschreibung des Produkts mit digitalen Elementen
   - Konstruktionsentwürfe, Fertigungszeichnungen und -pläne
   - Beschreibungen und Erläuterungen zur Funktionsweise
   - Bedingungen für die Integration in Systemumgebungen
   - Aufstellung der angewandten harmonisierten Normen oder technischen Spezifikationen
   - Ergebnisse der Konstruktionsberechnungen, Prüfungen und Prüfberichte

2. **Bewertung der Cybersicherheitsrisiken durchführen:** Der Hersteller muss eine systematische Bewertung der Cybersicherheitsrisiken durchführen und diese dokumentieren .

3. **Konformitätserklärung ausstellen:** Der Hersteller muss eine EU-Konformitätserklärung ausstellen, in der er erklärt, dass das Produkt der Verordnung (EU) 2024/2847 entspricht .

4. **CE-Kennzeichnung anbringen:** Nach erfolgreicher Konformitätsbewertung bringt der Hersteller die CE-Kennzeichnung an .

Inhalte und Pflichten: Konformitätsbewertung

Vorteile von Modul A:

- Es fallen keine Gebühren für notifizierte Stellen an
- Keine Wartezeiten auf externe Prüfungen
- Der Hersteller kann den Prozess eigenständig steuern
- Besonders geeignet für kleine und mittlere Unternehmen (KMU) und Start-ups

Inhalte und Pflichten: Überwachungs- und Beseitigungspflichten

Lebenszyklus:

- Die Pflichten hören aber nicht mit dem Vertrieb auf. Auch nach Bereitstellung des Produkts müssen **Schwachstellen überprüft und angemessen gehandhabt** werden inklusive der **Bereitstellung von Sicherheitsupdates**. Diese Pflicht gilt für **fünf Jahre** oder die Lebensdauer des Produkts, vgl. Art. 13 Abs. 8.
- Produkte müssen **zurückgerufen werden**, wenn Schwachstellen dies notwendig machen. Jedenfalls müssen diese ausgebessert werden.
- Wenn Produkte den Vorgaben des CRA nicht entsprechen, können sie auch von offizieller Seite vom Markt genommen werden.

Inhalte und Pflichten: Meldepflichten

Meldepflichten nach Art. 14

- Jeder Hersteller hat bei Vorliegen von **Sicherheitsvorfällen** und **ausgenutzten Schwachstellen innerhalb von 24 Stunden** das BSI informieren. https://digital-strategy.ec.europa.eu/de/policies/cra-reporting
- Darüber hinaus müssen bei **Sicherheitsvorfällen** auch unverzüglich, das heißt ohne schuldhaftes Zögern, die **Nutzer** durch den Hersteller **informiert werden** nach Art. 14 Abs. 8.
- Zudem gibt es die Möglichkeit der freiwilligen Meldung einer Schwachstelle oder einer Cyberbedrohung, die sich auf die Sicherheit eines Produkts mit digitalen Elementen auswirkt, nach Art. 15.

Inhalte und Pflichten: Überprüfungspflichten

- Importeure dürfen **nur Produkte** auf den Markt bringen, die **sämtliche Cybersecurity-Anforderungen** (näher definiert in der Anlag zum CRA) erfüllen, Art. 19.
- Es ist zudem Pflicht eines **jeden Händlers** sich zu **vergewissern**, ob sämtliche Anforderungen des CRA bei jedem Produkt **vollständig erfüllt** sind, Art. 20 Abs. 2. Vorher darf er das Produkt nicht „auf dem Markt bereitstellen“.

→ Dies überschreitet die Verpflichtungen aus dem bisherigen Produkthaftungsgesetz weit und macht neben den Herstellern auch die Importeure und Händler voll haftbar.

Inhalte und Pflichten: Dokumentationspflichten

- Der gesamte Prozess muss **dokumentiert** werden. Die technische Dokumentation muss alle relevanten Cybersecurity-Daten und Details enthalten. Die Parteien sind diesbezüglich zukünftig in der **Beweispflicht**.
- Dies gilt nicht nur für die selbst hergestellten Teile, sondern **auch für eingebaute Bestandteile** Dritter.

Überblick: Unterlagen des BSI

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

- https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CRA/CRA_Flyer-1_Produktanforderungen.pdf?__blob=publicationFile&v=5
- https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CRA/CRA_Flyer-2_Produktklassen_Konformitaet.pdf?__blob=publicationFile&v=2
- https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CRA/CRA_Flyer-3_Drittstellenbewertung.pdf?__blob=publicationFile&v=2

Überblick: Unterlagen des BSI

Wann ist was zu tun?

- **Risikobewertung eines Produkts**
  - **(1) Produktbezogene Anforderungen**
  - **(2) Anforderungen in Bezug auf den Umgang mit Schwachstellen**
  - **(3) Technische Dokumentation**
  - **Konformitätsbewertung**, CE-Kennzeichen, EU-Konformitätserklärung
- Kontinuierliche Einhaltung der Anforderungen während des gesamten Supportzeitraums

Design- und Entwicklungsphase | ***Wartungsphase*** (mindestens 5 Jahre ab Inverkehrbringen; ggf. kürzer oder länger, sofern zu erwarten ist, dass die Zeit, in der das Produkt verwendet wird, kürzer/länger ist) | ***Meldepflichten***

Sanktion und Reichweite

- Die Sanktionierung, wie auch schon die Implementierung, hat große Ähnlichkeiten mit der DSGVO. Ziel ist es, eine **wirksame, verhältnismäßige und abschreckende Wirkung** zu erzeugen.
- Die maximale Geldstrafe beträgt **15.000.000 €** oder bis zu **2,5 %** des weltweiten Jahresumsatzes im vorausgegangenen Geschäftsjahr, je nachdem welcher Betrag höher ist (Art. 64). Bereits bei **geringfügigen Verstößen** kann eine gemilderte Geldbuße von bis zu 5.000.000 € bzw. 1 % fällig werden. Eine **mehrfache Geldbuße** für dieselbe Zuwiderhandlung wird nicht ausgeschlossen.
- Durch die Sanktionshöhe, sollte der CRA, sofern er entsprechend umgesetzt wird, eine enorme Schlagkraft und Reichweite haben.

Historie zum Erlass des Cyber Resilience Acts

- Die Europäische Kommission hat am **15. September 2022** ihren **Entwurf** für eine Verordnung **veröffentlicht.**
- Im **Juni 2023** haben das Europäische Parlament und der Rat der Europäischen Union eine vorläufige Einigung über den Entwurf erzielt.
- Abschließend hat das Europäische Parlament am **12. März 2024** die endgültige und künftige „**Verordnung über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen“** angenommen. Der Rechtsakt wurde dann vom Rat im **Oktober 2024** offiziell angenommen.
- Der endgültige Text wurde am 20. November 2024 im Amtsblatt der EU veröffentlicht und trat 20 Tage später in Kraft.

Historie zum Erlass des Cyber Resilience Acts

- Als Verordnung ist der Cyber Resilience Act **direkt** in allen EU-Mitgliedstaaten **anwendbar.**
- Der CRA wird von Ende 2024 bis 2027 in **mehreren Stufen umgesetzt (siehe nächste Folie)**

Stufen der Umsetzung

11. Juni 2026: Die notifizierende Behörde hat die erforderlichen Verfahren für die Bewertung, Benennung und Notifizierung von Konformitätsbewertungsstellen festgelegt und veröffentlicht.

11. September 2026: Hersteller von vernetzten Produkten unterliegen der obligatorischen Meldung von Schwachstellen und Vorfällen über die einzige Berichtsplattform.

11. Dezember 2026: Die Mitgliedstaaten bemühen sich, bis zum 11. Dezember 2026 sicherzustellen, dass in der Union eine ausreichende Anzahl notifizierter Stellen für die Durchführung von Konformitätsbewertungen vorhanden sind, um Engpässe und Hindernisse für den Markteintritt zu vermeiden. (siehe Art. 35(2) CRA)

11. Dezember 2027: Alle CRACRA-Anforderungen gelten, einschließlich der Einhaltung der grundlegenden Cybersicherheitsanforderungen, bevor ein Produkt in Verkehr gebracht wird, wobei Schwachstellen während des gesamten Lebenszyklus des Produkts und Transparenz für die Benutzer behoben werden.

Blick in die Praxis und Kritik

- Eine weitere Herausforderung im Zeitalter globaler Krisen soll bekämpft werden, jedoch können durch die Verordnung **neue Krisen für die Unternehmer** entstehen.
- Hoher **Kosten- und Fachkräftefaktor.**
- **Zu viel Bürokratie** und daher nicht effizient.
- Sehr viel Verantwortung und **Selbstkontrolle** für die Parteien. Verstöße können wahrscheinlich schwer aufgedeckt werden.
- Wie immer gilt: 1. Anfangen, 2. Ein Schritt nach dem anderen. 3. Die Unterlagen des BSI nutzen, sowohl für den Überblick, als auch für die dataillierten Anleitungen.

Sicht des Europäischen Gesetzgebers

- Der CRA bezweckt einen großen Schritt in Richtung **besserer Cybersicherheit** und **schließt Lücken bzw. vereinheitlicht** die Gesetzesstruktur. Insbesondere die schwerwiegenden **Sanktionsmöglichkeiten** dürften Cybersecurity endgültig bei Vertreibern und Herstellern von Produkten mit digitalen Elementen in den Fokus rücken.
- Sofern der Entwurf so verabschiedet wird, ergänzt er eine **Reihe an geplanten und bereits erlassenen Maßnahmen**, so unter anderem auch die neuen Produkthaftungsregelungen, die Verordnung zur künstlichen Intelligenz (AI-Act bzw. KI-VO), die NIS-2 und die DSGVO. Dadurch entsteht ein gesamtheitliches Bild der digitalen Regelungszukunft Europas.

Fragen?

Sie brauchen Unterstützung? Wir sind für Sie da!

- Externer Datenschutzbeauftragter (Ext. DSB)
- Seminare und Fortbildungen im Bereich Recht und Datenschutz
- **Individuelle Beratung** im Bereich Datenschutz, IT und IT-Security
- Immer Up-to-date mit dem Datenschutz-Weekly

NIS-2 Beratung

Viele Unternehmen stehen derzeit vor diesen zentralen Fragen:

- **Ist NIS-2 für mein Unternehmen relevant?**
- **Welche Strafen drohen, wenn ich NIS-2 nicht umsetze?**
- **Was muss ich für die richtige Umsetzung der NIS-2-Richtlinie tun?**

Wir helfen Ihnen, diese Fragen zu klären und unterstützten Sie bei der **erfolgreichen Implementierung der erforderlichen Maßnahmen** in Ihrem Unternehmen.

Mehr Infos unter www.liidu.de/nis-2-beratung

Datenschutz-
Weekly

Jeden
Mittwoch von
12 -13 Uhr

ONLINE

- Immer mit einer **Datenschutzexpertin**
- Schnelle Beantwortung **Ihrer Fragen**
- **Austausch** mit anderen Datenschützern
- Immer **up-to-date bleiben**
- Wöchentlich alle **Infos per Mail**

Kostenlose Schnupperstunde

www.liidu.de/Datenschutz-Weekly

Zum kostenlosen Newsletter anmelden

www.liidu.de/newsletter

info@liidu.de

0941 46392460

www.liidu.de

Let`s connect - **LinkedIn**

Feedback

*** **LiiDU bewerten** ***

Wir freuen uns über jedes Feedback –
nur so können wir uns stetig verbessern
→ *Hier können Sie uns bewerten*