ÜBERBLICK ÜBER DIE WESENTLICHEN REGELUNGEN DES CYBER RESILIENCE ACT

Stephan Schmidt | TCI Rechtsanwälte Mainz

IT Security Update - Special Edition "IT-Sicherheitsrecht kompakt"

16.05.2024

TCILAW.DE

Grundlagen

Cyberangriffe sind ein Thema von öffentlichem Interesse, da sie sich nicht nur auf die Wirtschaft der Union, sondern auch auf die Demokratie und die Sicherheit und Gesundheit der Verbraucher kritisch auswirken.

Es ist deshalb nötig, das **Cybersicherheitskonzept der Union** zu stärken, sich mit **Cyberresilienz auf Unionsebene** zu befassen und das Funktionieren des Binnenmarkts zu verbessern und dazu einen **einheitlichen Rechtsrahmen für grundlegende Cybersicherheitsanforderungen für das Inverkehrbringen von Produkten mit digitalen Elementen** auf dem Unionsmarkt festzulegen.

(Erwgr. 1 CRA)

Aktueller Stand

- Noch nicht final beschlossen
- Entwurf vom 12.03.2024 (abrufbar unter https://www.europarl.europa.eu/doceo/document/TA-9-2024-0130_DE.pdf) vom Europäischen Parlament verabschiedet
- Verabschiedung und Inkrafttreten voraussichtlich noch 2024
- Vorschriften über Meldepflichten der Hersteller gem. Art. 14 CRA finden 21 Monate nach Inkrafttreten Anwendung
- die restlichen Vorgaben des CRA finden 36 Monate nach Inkrafttreten Anwendung
- Produkte, die vor Ablauf der Umsetzungsfrist in den Verkehr gebracht werden, unterfallen nur dann den Anforderungen des CRA, wenn nach Ablauf der Umsetzungsfrist wesentliche Änderungen am Produkt durchgeführt werden (Art. 69 Abs. 2 CRA)

Für wen, was und wo gilt der CRA?

- branchenübergreifende einheitliche, horizontale Regelung
- Gilt für Produkte mit digitalen Elementen (B2B- und B2C-Bereich)
- Software, Hardware und vernetzte, physische Produkte, die Datenverbindungen mit einem Gerät oder Netz aufbauen können, sowie Komponenten hiervon, die getrennt in den Verkehr gebracht werden
- Produkte die innerhalb der EU bereitgestellt werden
- verpflichtet Hersteller sowie weitere Akteure entlang der Lieferkette (sog. Einführer und Händler)

Produkte mit digitalen Elementen

- materielle und immaterielle Produkte mit digitalen Elementen, deren bestimmungsgemäße oder vorhersehbare Verwendung eine **direkte oder indirekte logische oder physische Datenverbindung** mit einem Gerät oder Netz einschließt (Art. 2 Abs. 1 CRA)

  (und die in keine der Ausnahmen z.B. für Medizinprodukte, In-vitro-Diagnostika, KFZ, Luftfahrt, Schiffsausrüstung und Verteidigung fallen

- Produkte mit digitalen Elementen sind **sowohl Software als Hardware** und die dazugehörigen „**Datenfernverarbeitungslösungen**, einschließlich Soft- oder Hardwarekomponenten, die getrennt in den Verkehr gebracht werden“ (Art. 3 Nr. 1 CRA)
- die Art von Netz bzw. System mit dem ein Produkt gemeinhin verbunden wird, wird im CRA nicht weiter spezifiziert

- **Kurz gesagt: alles, was Daten austauscht**
- Mögliche Produkte: mobile Geräte, IoT-Geräte, Netzwerkinfrastrukturgeräte, Vernetzte industrielle Steueranlagen (Industrie 4.0), Software, die lokal auf elektronischen Geräten installiert wird, z.B. Treiber, Apps, Office-Programme

Produkte mit digitalen Elementen

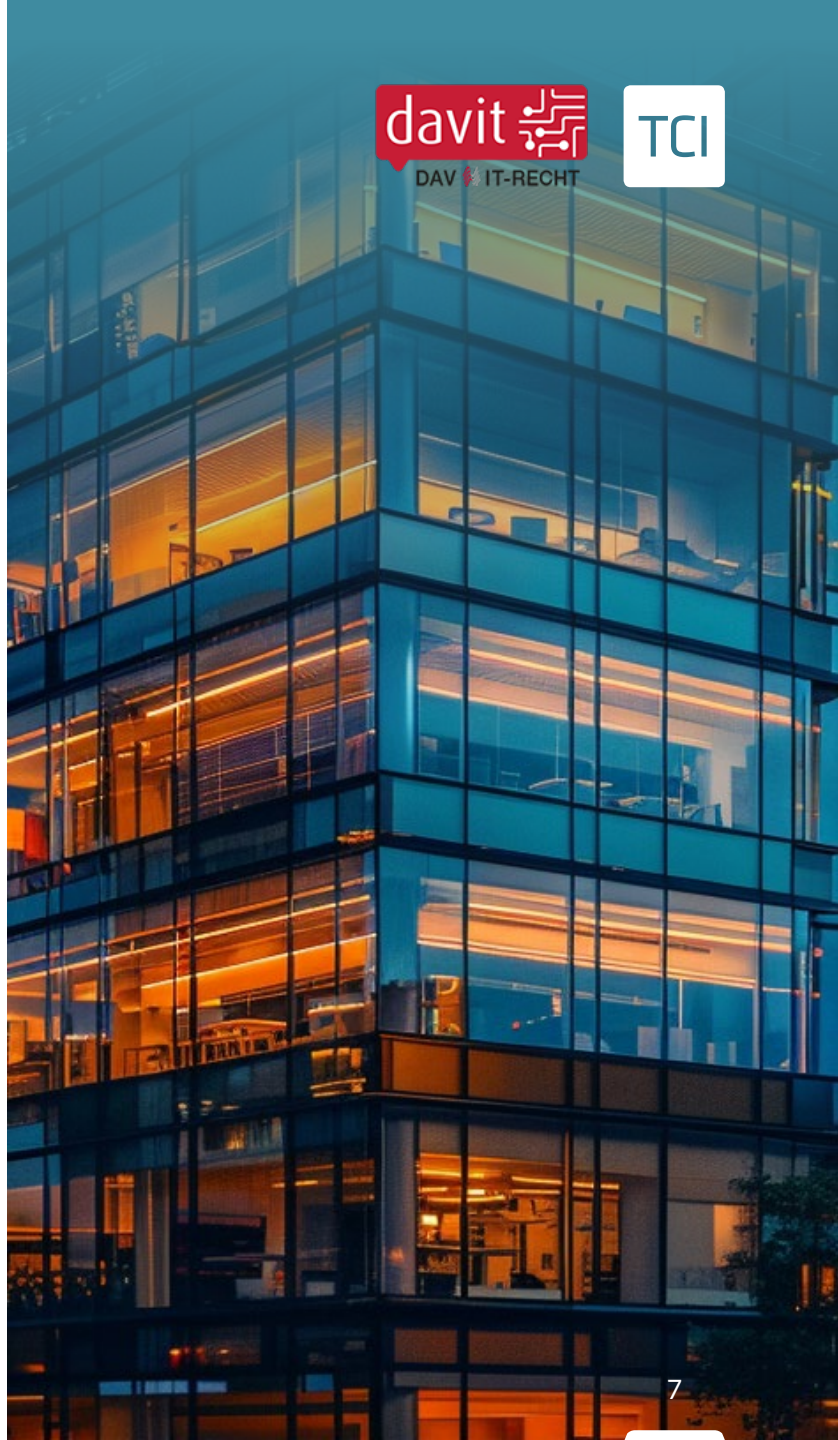
- CRA bezieht nicht auf Dienstleistungen
- zur Unterscheidung z.B. bei SaaS-Anwendungen muss man die CRA-Definitionen der Datenfernverarbeitungslösung beachten
- Datenfernverarbeitungslösung = „jede entfernt stattfindende Datenverarbeitung, für die eine Software vom Hersteller selbst oder unter dessen Verantwortung konzipiert und entwickelt wurde und ohne die das Produkt eine seiner Funktionen nicht erfüllen könnte“ (Art. 3 Nr. 2 CRA)
- hierfür ist es unerheblich, ob eine Software lokal auf dem Gerät des Nutzers oder aus der Ferne durch den Hersteller ausgeführt wird (Erwgr. 11 CRA).
- Cloud-Lösungen fallen also nur dann in den Anwendungsbereich des CRA, wenn sie diese Definition von Datenfernverarbeitungslösungen erfüllen (Erwgr. 12 CRA)
- im Einzelfall kann die Abgrenzung zwischen Dienstleistung und Produkt mit digitalen Elementen bei Clouddiensten und SaaS-Lösungen komplex sein und eine individuelle Bewertung erfordern

Wer ist betroffen?

- Betroffen sind gemäß Art. 3 Nr. 12 CRA **Wirtschaftsakteure**, insbesondere **Hersteller, Bevollmächtigte, Einführer, Händler, Verwalter quelloffener Software** sowie jede andere natürliche oder juristische Person, die im Rahmen des CRA verpflichtet wird

- Aufgaben und Pflichten des CRA hängen davon ab, welche der Rollen eine Organisation in Bezug auf ein Produkt einnimmt

- in Bezug auf ein Produkt mit digitalen Elementen hat eine Organisation regelmäßig nur jeweils eine der drei Rollen (Hersteller, Einführer oder Händler)



Wer ist betroffen?

- **Hersteller** ist eine „natürliche oder juristische Person, die Produkte mit digitalen Elementen **entwickelt oder herstellt** [bzw.] konzipieren, entwickeln oder herstellen lässt und dieses Produkt unter dem eigenen Namen oder eigener Marke vermarktet, sei es entgeltlich oder unentgeltlich“. (Art. 3 Nr. 13 CRA)

- **Einführer** ist eine in der EU ansässige oder niedergelassene natürliche oder juristische Person, die ein Produkt mit digitalen Elementen **auf dem Unionsmarkt in Verkehr** bringt, welches den Namen oder die Marke einer natürlichen oder juristischen Person mit Sitz außerhalb der EU trägt (Art. 3 Nr. 16 CRA)

- **Händler** ist jede natürliche oder juristische Person in der Lieferkette, die ein Produkt mit digitalen Elementen **auf dem Unionsmarkt bereitstellt**, dabei nicht Hersteller oder Einführer ist – und die Eigenschaften des Produkts nicht ändert. (gemäß Art. 3 Nr. 17 CRA)

Wo gilt der CRA

- **Bereitstellen** des Produktes mit digitalen Elementen **auf dem Unionsmarkt**
  - „jede entgeltliche oder unentgeltliche Abgabe eines Produktes mit digitalen Elementen zum Vertrieb oder zur Verwendung auf dem Unionsmarkt im Rahmen einer Geschäftstätigkeit“
- Bereitstellung ist gegeben, wenn ein Angebot zum Vertrieb, wie es bereits bei einer Aufforderung zum Kauf oder bei einer Werbekampagne vorliegt, besteht und welches zu einer tatsächlichen Bereitstellung des Produktes führt
- bei Software knüpft die Bereitstellung an die Einräumung der Nutzungsmöglichkeit an (z.B. durch Downloadmöglichkeit oder die Übermittlung von Zugangsdaten)

Aufgaben und Pflichten für betroffene Unternehmen

1. verschiedene Produktanforderungen zur Cybersicherheit
2. Anforderungen an Umgang mit Schwachstellen
3. verschiedene Dokumentations- und Aufbewahrungspflichten
4. Verpflichtung zur Durchführung eines geeigneten Konformitätsbewertungsverfahrens
5. EU-Konformitätserklärung und CE-Kennzeichnung
6. Informations- und Meldepflichten
7. Verpflichtung (für die Dauer von 5 Jahren) die Cybersicherheit eines Produkts aufrecht zu erhalten

Produktanforderungen

- inhaltlichen Anforderungen während des Produktdesigns und während des Betriebs sind in Annex I aufgeführt
- Annex I ist sehr kurz und die Anforderungen sind sehr generisch
- konkrete Ausgestaltung der Anforderungen soll in sogenannten “harmonisierten Standards” auf Basis bestehender Standards erfolgen

- Erfüllung der “essential requirements” muss dokumentiert werden
  - CE-Kennzeichen (Art. 28,32; Annex V / VI / VIII)
  - Technische Dokumentation (Art. 31; Annex VII)
  - Nutzeranleitungen (Art. 13; Annex II)

Sicherheitsstufen für Konformitätsbewertung

Kritische Produkte	Wichtige Produkte Klasse II	Wichtige Produkte Klasse I	Produkte mit digitalen Elementen (Basiskategorie)
Art. 8, Anhang IV CRA	Art. 7, Anhang III CRA	Art. 7, Anhang III CRA	Art. 3 Nr. 1 CRA
Produkte wie Sicherheitsboxen oder Smartcards (Sicherheit ist der Kernaspekt des ganzen Produkts	Sicherheitskomponenten (z.B. Firewalls) und Hypervisoren	Produkte mit Sicherheitsbezug (z.B. Betriebssysteme, Passwortmanager)	alle Produkte mit digitalen Elementen

Liste wurde deutlich gekürzt und die meisten Betroffenen werden wohl nur eine Selbsterklärung abgeben müssen

Verwalter quelloffener Software (Open-Source-Stewards)

- Einrichtungen die keine kommerziellen Produkte anbieten, aber dennoch durch die Verbreitung der dort betreuten Open-Source-Komponenten erheblichen indirekten Einfluss auf die Sicherheit kommerzieller Produkte ausüben, definiert der CRA als „**Verwalter quelloffener Software**" (Open-Source-Stewards)
- wiederkehrende Sicherheitsanalyse derselben Komponente im Rahmen jedes einzelnen Produkts mit digitalen Elementen würde den Nutzen von Open-Source-Komponenten unterminieren
- Verwalter quelloffener Software haben **Sonderstellung für Open-Source-Projekte**, die zwar nicht im Rahmen einer Geschäftstätigkeit bereitgestellt werden, aber nachhaltig von juristischen Personen in einem geschäftlichen Umfeld getragen werden, und die für eine Verwendung in einem kommerziellen Kontext gedacht sind (Art. 3 Nr. 14 CRA)
- gilt z.B. dann, wenn Entwickler kommerzieller Produkte regelmäßig und substanziell zum Open-Source-Projekt beitragen – ein solcher Beitrag muss nicht aus Entwicklungsarbeit (Code) bestehen, sondern kann z.B. auch durch finanzielle Zuwendungen (Spenden), die Bereitstellung von Software oder Hardware oder die Übernahme von Dienstleistungen (Projektmanagement, Hosting der Entwicklungsplattform, usw.) geschehen (Erwgr. 19 CRA)

Besonderheiten für Verwalter quelloffener Software

- bringen kein CE-Zeichen an den Open-Source-Produkten an
- Europäische Kommission wird dazu ermächtigt, in Form von delegierten Rechtsakten freiwillig „Sicherheitsbescheinigungen“ (security attestation) für Open-Source-Software zu schaffen (Art. 25 CRA) („Sponsorings“ von Sicherheitsbescheinigungen ist möglich)
- Verstöße sind nicht bußgeldbewährt

Sanktionen

- Mitgliedstaaten sind gemäß Art. 64 Abs. 1 CRA verpflichtet, Regelungen über wirksame, verhältnismäßige und abschreckende Sanktionen zu treffen
- Entzug der CE-Kennzeichnung
- Übermittlung unrichtiger, unvollständiger oder irreführender Informationen an notifizierte Stellen oder Marktüberwachungsbehörden → Bußgeld von bis zu 5 Mio. Euro oder bis zu 1 % des Vorjahresumsatzes
- Verletzung anderer in Art. 64 Abs. 3 CRA genannter Pflichten → Bußgeld von bis zu 10 Mio. Euro oder bis zu 2 % des Vorjahresumsatzes
- Verstoß gegen die grundlegenden Anforderungen an die Cybersicherheit (Anhang I) oder gegen die Herstellerpflichten (Art. 13 und 14 CRA) → Bußgeld von bis zu 15 Mio. Euro oder bis zu 2,5 % des Vorjahresumsatzes

- Bei Festlegung der Sanktion ist neben der Schwere und der Dauer des Verstoßes auch die Größe des Unternehmens zu berücksichtigen (Art. 64 Abs. 5 CRA).
- Kleinstunternehmen oder kleine Unternehmen sind von Bußgeldern ausgenommen, wenn sie die in Art. 14 Abs. 2 lit. a oder Abs. 4 lit. b CRA genannten Fristen der Meldepflichten nicht einhalten

Vielen Dank.

STEPHAN SCHMIDT

Rechtsanwalt

Fachanwalt für IT-Recht, CIPP/E

TCI Rechtsanwälte Mainz

+49 6131 30290460

sschmidt@tcilaw.de

davit DAV IT-MITGLIED

Alle Illustrationen KI generiert