Der EU Cyber Resilience Act – neue Markteintrittshürden für Schweizer IoT-Produkte

Die EU hat in den letzten Jahren eine Vielzahl von Regulierungen erlassen, die sich mit datengetriebenen Märkten und digitalen Sachverhalten befassen (z.B. AI Act, DSGVO, NIS-2-Richtlinie, Data Act, Digital Markets Act, Digital Services Act, RED Delegated Act (Radio Equipment Direktive) und sektorspezifische Vorschriften wie DORA oder die EU Maschinenverordnung). Wie können Schweizer Unternehmen, die in die EU exportieren, den Überblick behalten?

Dr. Martin Eckert
Legal Partner

Fachleute sprechen von einem Regulierungstsunami. Es ist auch für Spezialist:innen schwer, am Ball zu bleiben. Und es zeigt sich zudem, dass diese Regeln nicht widerspruchsfrei sind. Die EU selbst hat dieses Manko erkannt. Mit einem sog. Omnibus-Verfahren will die Kommission einen Marschhalt einlegen und den Regulierungsdschungel lichten.

Heisst das für die Schweizer Hersteller: «wait and see»?
Leider nein. Erlasse, die in Kraft sind, bleiben in Kraft, bis die neuen Regeln stehen. Mein Rat ist vielmehr in erster Priorität abzuklären, ob es Erlasse gibt, die bei Nichtbeachtung dazu führen, dass für das Unternehmen der Zugang zum europäischen Markt blockiert oder erschwert wird. Diese Vorschriften sind nicht nur ein Governance-Thema, sondern können direkten negativen Business Impact haben.

Können Sie uns ein Beispiel für eine Regulierung geben, die bei Nichteinhaltung dazu führt, dass schweizerische Produkte nicht in die EU eingeführt werden können?
Viele Schweizer Unternehmen haben den Cyber Resilience Act (CRA) – zu Deutsch: Cyberresilienzgesetz – nicht auf dem Radar, obwohl er im Dezember 2024 in Kraft getreten ist. Der CRA legt flächendeckend und technologieneutral Cybersicherheitsanforderungen für Produkte mit digitalen Elementen fest. Auf die Hersteller kommen weitreichende neue Pflichten zu mit Auswirkungen auf die Produktentwicklung, die Produktion und das Lifecycle Management. Businesskritisch ist vor allem, dass nur Produkte mit digitalen Elementen in der EU in den Verkehr gebracht werden dürfen, für die eine technische Dokumentation erstellt wurde und die ein Konformitätsbewertungsverfahren durchlaufen haben. Diese Schritte sind Voraussetzung für die Konformitätserklärung und das CE-Kenneichen. Die EU-Importeure und Händler fungieren dabei als «Kontrollinstanzen». Vereinfacht gesagt: ohne CE-Kennzeichen und die neuen erforderlichen Unterlagen zur Cyber Sicherheit (technische Dokumentation und Software Bill of Materials) dürfen Produkte mit digitalen Elementen nicht mehr in die EU eingeführt werden.

Welche Produkte sind vom Cyber Resilience Act betroffen?
Der CRA erfasst sämtliche «Produkte mit digitalen Elementen», die «… eine direkte oder indirekte logische oder physische Datenverbindung mit einem Gerät oder Netz einschliesst». Es geht mithin um vernetzte Produkte – Hardware und Software (embedded oder stand alone). Erfasst sind sog. IoT-Produkte, die in ein grösseres elektronisches Informationssystem integriert oder mit ihm – zum Beispiel über eine Software-Schnittstelle - verbunden sind und daher böswilligen Akteuren als Angriffsvektor dienen können. Beispiele sind Endgeräte (Smartphones, Laptops, Smartwatches, Smarthome Geräte, Maschinen und Industrieanlagen mit Fernsteuerungssysteme), Netzwerkkomponenten (Router, Modems und Switches etc.) oder Software (mobile Apps, Betriebssysteme, industrielle Steuerungssysteme). Es gibt eine Liste von Ausnahmen, weil für diese Produktkategorien spezifische EU-Vorschriften bestehen (zum Beispiel. Medizinprodukte, Zivilluftfahrt, Kraftfahrzeuge, Schiffsausrüstungen, Produkte für die nationale Sicherheit oder Verteidigungszwecke). Spezialregeln gibt es für Open source Software und Datenfernverarbeitungslösungen (Cloud-Lösungen).

Sind auch Unternehmen in der Schweiz betroffen?
Ja. Der CRA hat exterritoriale Wirkung. Unternehmen mit Sitz in der Schweiz, die auf dem Unionsmarkt Produkte mit digitalen Elementen im Rahmen einer Geschäftstätigkeit bereitstellen, müssen die Vorgaben des CRA einhalten. Sie müssen als Hersteller ihre Produktdesign und Produktionsprozesse entsprechend anpassen, wenn sie ihre Produkte in der EU verkaufen wollen. Neben den Herstellern sind die EU-Importeure und Händler in der Pflicht. Importeure müssen sicherstellen, dass die vernetzten Produkte den Anforderungen des CRA entsprechen, bevor diese in die EU eingeführt werden. Händler haben Prüfpflichten und dürfen nur konforme Produkte mit CE-Kennzeichnung in der EU vertreiben. Ebenfalls Pflichten haben die Verwalter quelloffener Software. Diese Open-Source-Software Stewards sind juristische Personen, die die Entwicklung von kommerzieller Open source Software systematisch und nachhaltig unterstützen und die Brauchbarkeit dieser Produkte sicherstellen.

> **Es braucht eine straffe Roadmap, um rechtzeitig für den CRA bereit zu sein. Erster Schritt als Hersteller ist eine rechtliche Analyse, welche eigenen und allenfalls integrierten Produkte mit digitalen Elementen vom CRA betroffen sind.**
>
> – Dr. Martin Eckert, Legal Partner

Welche allgemeinen Pflichten treffen die Hersteller?
Auf die Hersteller kommt ein ganzes Paket von Pflichten zu, deren Einhaltung sorgfältig zu dokumentieren ist:

- (regelmässig nachgeführte) **Risikobewertungen** und die **Einhaltung grundlegender Cybersicherheitsanforderungen** («Security by Design» und «Security by Default»)
- **Sorgfaltspflichten in der Lieferkette** (Risikobewertung der Komponenten; Verifizierung der Herkunft von Produkten und der Vertrauenswürdigkeit der Zulieferer; Dokumentation der Sicherheitsmerkmale der Drittkomponenten; vertragliche Vereinbarungen inkl. Schwachstellenmanagement); zentral ist eine transparente Auflistung aller verwendeten Softwarekomponenten (Software Bill of Materials)
- **Schwachstellenmanagement** (Bereitstellung von kostenlosen und zeitnahen Sicherheitsupdates über den gesamten Supportzeitraum) und **Meldepflichten** (Meldung an die Agentur der EU für Cybersicherheit (ENISA) und die nationalen CSIRT Organisationen; unverzügliche Information der Nutzer)
- **Konformitätsbewertung** und **CE-Kennzeichnung** (Erstellung einer technischen Dokumentation und Durchführung eines Konformitätsbewertungsverfahrens; je nach Produktkategorie kann der Hersteller die Konformitätsbewertung selbstdurchführen oder die Bewertung muss durch eine externe benannte Stelle erfolgen oder eine Zertifizierung nach einem europäischen Cybersicherheitsschema vorliegen)
- **Transparenz und Informationspflichten zur sicheren Nutzung des Produkts** (Sicherheitsfunktionen und Verwendungszweck; Support-Zeitraum und Update-Verfahren; Informationen über bekannte Cyberrisiken)

Welche Cybersicherheitsanforderungen gibt die EU konkret vor?
Der CRA regelt im Anhang I «Grundlegende Cybersecurity Anforderungen». Produkte mit digitalen Elementen müssen so konzipiert, entwickelt und hergestellt werden, dass sie angesichts der Risiken ein angemessenes Cybersicherheitsniveau gewährleisten (Risikobasierter Ansatz). Es folgt eine Liste von Anforderungen, die je nach Risikobewertung umgesetzt sein müssen. Wichtigste Anforderung: Produkte mit digitalen Elementen müssen ohne bekannte ausnutzbare Schwachstellen auf dem Markt bereitgestellt werden. Bis heute gibt es noch wenig konkrete, produktspezifische Vorgaben der EU. Der Hersteller selbst ist für die Sicherheit verantwortlich («Security by Design») und wird sich an den anerkannten Industriestandards (Frameworks) und Best Practice Grundsätzen orientieren.

Welche Risiken entstehen bei der Nichteinhaltung der CRA-Vorschriften für schweizerische Hersteller?
Das kommerziell grösste Risiko ist, dass EU-Importeure und Händler die schweizerischen Produkte nicht in die EU einführen können, wenn Voraussetzungen gemäss CRA fehlen. Produkte, die in der EU eingeführt worden sind, werden zudem von nationalen Behörden überwacht. Diese Marktüberwachungsbehörden in der EU haben weitgehende Kompetenzen (Verbote, Einschränkungen, Anordnung von Produktrückrufen, Anforderung von technischen Dokumentationen, unangekündigte Kontrollen). Der CRA sieht scharfe, abgestufte verwaltungsrechtliche Sanktionen vor (Bussen bis zu 2,5% des weltweiten Jahresumsatzes). Dazu kommen zivilrechtliche Risiken (Vertragsverletzung; Produkthaftung). Ein Produkt ist fehlerhaft, wenn es nicht die Sicherheit bietet, die berechtigterweise erwartet werden darf. Ich gehe daher davon aus, dass ein vernetztes Produkt, das nicht die wesentlichen Cybersicherheitsanforderung gemäss Anhang I Teil 1 CRA erfüllt, auch als fehlerhaft im Sinne der EU-Produkthaftungsrichtlinie gelten dürfte. Der Hersteller haftet in diesem Fall – auch ohne Verschulden – für den daraus resultierenden Schaden. Der CRA ist daher sehr ernst zu nehmen.

Wie sieht der Fahrplan der EU aus? Was bedeutet das für die Hersteller auf der Zeitachse?
Die Zeit drängt. Die Regeln für die Notifizierung von Konformitätsbewertungsstellen gelten ab 11. Juni 2026. Das Schwachstellenmanagement mit Meldepflichten für Hersteller muss ab 11. September 2026 funktionieren. Die Allgemeinen Pflichten gelten ab 11. Dezember 2027 (vollständige Anwendbarkeit des CRA für den Grossteil der betroffenen Produkte).

Das bedeutet für schweizerische Hersteller, dass sie bis Juni 2026 einen rechtsgenügenden Prozess für das Schwachstellenmanagement und die Meldepflichten aufsetzen müssen. Vernetzte Produkte – auch langjährige Produkte – dürfen am 11. Dezember 2027 nur noch in der EU verkauft werden, wenn diese dem CRA entsprechen. Bereits in Verkehr gebrachte Produkte werden vom CRA nur erfasst, wenn diese Produkte nach dem 11. Dezember 2027 einer wesentlichen Änderung unterliegen.

Ist das Thema Cyber Resilience auch im schweizerischen Recht ein Thema?
Cyber Attacken machen nicht vor den Landesgrenzen halt. In der Schweiz gibt es heute kaum produktspezifische Cybersicherheitsvorgaben. Der Bundesrat will die Cyberresilienz von digitalen Produkten steigern und hat das VBS (BACS) am 20. August 2025 beauftragt, in Zusammenarbeit mit dem UVEK (BAKOM) und dem WBF (SECO) bis Herbst 2026 eine Vernehmlassungsvorlage für eine schweizerische Gesetzgebung zu erarbeiten.

Herr Eckert, was raten Sie schweizerischen Unternehmen, die Produkte mit digitalen Elementen herstellen, ganz konkret?
Es braucht eine straffe Roadmap, um rechtzeitig für den CRA bereit zu sein. Erster Schritt als Hersteller ist eine rechtliche Analyse, welche eigenen und allenfalls integrierten Produkte als Hersteller von CRA betroffen sind. Der zweite Schritt ist eine Risikobewertung. Gestützt darauf kann eine Gap-Analyse erfolgen und ein Actionplan zur Füllung der Lücken erstellt werden. Im Vordergrund steht ein CRA-konformes Schwachstellenmanagement, die Implementierung von Sicherheitsfunktionen und für jedes Produkt eine rechtskonforme technische Dokumentation mit einer vollständigen SBOM (Software Bill of Materials).

Neben den regulatorischen Anforderungen sind auch die Vorgaben von Kunden im Auge zu behalten. Es zeichnet sich ab, dass in der Praxis die Produktzertifizierung nach Normenreihe IEC 62443 (Industrielle Kommunikationsnetze – IT Sicherheit für Netze und Systeme) an Bedeutung gewinnt.

Das Thema Cybersicherheit von vernetzten Produkten gehört auf den Radar des Verwaltungsrates. Die Umsetzung des CRA sollte von der obersten Führungsstufe (Geschäftsleitung) konsequent adressiert, delegiert und kontrolliert werden. Es zeichnet sich ab, dass zahlreiche Prozesse in den betroffenen Unternehmen angepasst und besser dokumentiert werden müssen (allgemeines Risikomanagement; IKS; Verträge mit Lieferanten; Versicherungsschutz; QES und technische Dokumentation; Verträge mit Kunden; Verkaufsdokumentation; Support-Prozesse mit Sicherheitsupdates; Marktüberwachung; etc.). Die Sicherstellung der Cybersicherheit von Produkten ist keine einmalige «Übung», sondern der CRA verlangt eine systematische, kontinuierliche und regelmässig aktualisierte Bearbeitung und Dokumentation. Eine interdisziplinäre Herausforderung (Produktentwicklung; Qualitätssicherung; Rechts- und Complianceabteilung; Vertrieb) für jedes betroffene Unternehmen.

Weitere Informationen unter:
mme.ch

MME
Legal | Tax | Compliance