EU Cyber Resilience Act

BEGRIFFE, DEFINITION, GRUNDLAGEN

Einheitlicher Rechtsrahmen für digitale Produkte

Was bedeutet Cyber Resilience? Ziele und Zweck?

Die Bedeutung von „Cyber Resilience“ ist nicht einheitlich festgelegt, kann jedoch mit „Widerstandsfähigkeit“ umschrieben werden.

Unter Cyber Resilience versteht man die Kapazität eines Systems oder einer Organisation, Cyberangriffe zu identifizieren, angemessen darauf zu reagieren und sich von deren Auswirkungen zu erholen.

Der EU Cyber Resilience Act (CRA) ist ein Gesetz, das im Zuge der Anstrengungen der EU entwickelt wurde, um die Abwehr gegen Cyberangriffe zu verstärken und die allgemeine Cybersicherheit zu verbessern.

Das Gesetz strebt danach, EU-weit einheitliche Cybersicherheitsstandards zu etablieren und zu gewährleisten.

Ziel des EU Cyber Resilience Act ist es, das Vertrauen in die digitale Infrastruktur der EU zu festigen und somit die internationale Wettbewerbsfähigkeit europäischer Unternehmen zu fördern.

CRA ist nicht gleich DORA (Digital Operational Resilience Act) oder NIS2

Die Regelwerke NIS2, DORA und CRA zielen alle darauf ab, die Sicherheit im Cyberraum und die Stabilität von Betriebssystemen zu verbessern. Dies stellt eine Art gemeinsame Basis dar. Bei genauerer Analyse treten allerdings signifikante Unterschiede zutage

DORA

DORA richtet sich an ein weites Feld von Finanzakteuren, nicht nur an Banken und Versicherungen, sondern auch an Börsen, Pensionsfonds, Krypto-Dienste und viele mehr.

Auch IT-Dienstleister wie Cloud-Anbieter, die für Finanzfirmen arbeiten, können nun reguliert werden, falls sie als essentiell angesehen werden.

Diese Einstufung hängt davon ab, wie wichtig ihre Dienste für den Finanzmarkt sind und wie abhängig die Finanzunternehmen von ihnen sind.

NIS2 will die EU-weite Cybersicherheit vereinheitlichen und verlangt eine Überprüfung der Sicherheit in der gesamten Lieferkette.

Der CRA setzt verpflichtende Sicherheitsstandards für digitale Produkte fest.

Die neuen Regeln bringen viel Arbeit für die betroffenen Firmen mit sich.

Im Finanzbereich könnte es einfacher sein, DORA umzusetzen, weil es schon ähnliche Vorschriften wie VAIT und BAIT gibt.

Für kleinere Unternehmen könnte NIS2 besonders aufwändig sein.

Der CRA gilt für Firmen, die digitale Produkte herstellen, und verlangt, dass diese von Anfang an sicher gestaltet werden **(„Security by Design“)**

CRA-Verordnung

Diese grundsätzlich für alle Sektoren. **Die Zeit der freiwilligen Selbstverpflichtungen ist vorbei.**

Während bisher vor allem Nutzer die Sicherheitslast zu tragen hatten, wird die Hauptlast nach Inkrafttreten des Cyber Resilience Act auf die Hersteller, Einführer und Händler von Hard- und Softwareprodukten verlagert.

Produzenten werden dazu aufgefordert, Risikobewertungen vorzunehmen, implementierte Sicherheitsvorkehrungen zu protokollieren und Systeme nach den Prinzipien der Sicherheit durch Gestaltung (Security-by-Design) einzurichten.

Darüber hinaus ist sicherzustellen, dass die Sicherheit während der gesamten Lebensdauer des Produkts, standardmäßig über einen Zeitraum von fünf Jahren, aufrechterhalten wird.

Zwei wichtige Gründe unterstützen diese Verschiebung: Zum einen ist es leichter, *Schwachstellen direkt an ihrem Ursprung zu korrigieren oder durch ein geeignetes Design von vornherein zu vermeiden*. Zum anderen haben die *Hersteller von Hardware- und Softwareprodukten das beste Wissen darüber, wie man Schwachstellen ausbessert und Updates verteilt*.

CRA: Inhaltsübersicht

Kapitel	Inhalt	Artikel
Cyber Resilience Act 2022/0272(COD)		
I	Allgemeine Bestimmungen	1-9
II	Pflichten der Wirtschaftsakteure	10-17
III	Konformität des Produkts mit digitalen Elementen	18-24
IV	Notifizierung von Konformitätsbewertungsstellen	25-40
V	Marktüberwachung und Durchsetzung	41-49
VI	Übertragene Befugnisse und Ausschussverfahren	0-51
VII	Vertraulichkeit und Sanktionen	52-53
VIII	Übergangs- und Schlussbestimmungen	54-57
Anhänge		
I	Grundlegende Cybersicherheitsanforderungen	
II	Informationen und Anleitungen für den Nutzer	
III	Kritische Produkte mit digitalen Elementen	
IV	EU-Konformitätserklärung	
V	Inhalt der technischen Dokumentation	
VI	Konformitätsbewertungsverfahren	

Die EU-Richtlinie NIS2 ordnet Unternehmen in **kritischen Sektoren** als **"wesentliche Einrichtungen"** ein. Der Cyber Resilience Act baut darauf auf, indem er vorschreibt, dass **IT-Produkte, die in diesen Einrichtungen genutzt werden, hohen Cybersicherheitsstandards entsprechen müssen.**

Produktklassen - Anwendungsbereich

Der CRA gilt für digitale Produkte, die in der EU verkauft werden. Dazu zählen alle Hardware- und Softwareprodukte und deren Online-Dienste. Ein Produkt muss für bestimmte Datenverarbeitungen konzipiert sein, ohne die es nicht funktionieren kann.

Im Wesentlichen betrifft dies Produkte, die mit dem Internet oder anderen Geräten verbunden sind. Cloud-Dienste sind auch betroffen, wenn sie für die Funktion eines Produkts notwendige Online-Dienste bieten.

Zudem definiert die Verordnung zwei Risikoklassen für kritische digitale Produkte. Es gibt auch eine dritte Klasse für besonders kritische Produkte, die wahrscheinlich unter die NIS-2-Richtlinie fallen.

Je nach Risikoklasse müssen die Produkte bestimmte Prüfverfahren durchlaufen und eine EU-Konformitätserklärung sowie eine CE-Kennzeichnung vorweisen.

Was fällt nicht unter CRA

Der Cyber Resilience Act gilt nicht für Hardware und Software, die bereits speziellen Regelungen unterliegen, wie Medizinprodukte, Kraftfahrzeugtypgenehmigungen sowie Produkte der Zivilluftfahrt und Flugsicherheit.

Reine Software-as-a-Service-Angebote ohne lokale Installationen sind ebenfalls ausgenommen.

Zudem betrifft die Verordnung keine Produkte, die nur für nationale Sicherheit, militärische Zwecke oder die Verarbeitung von geheimen Informationen entwickelt wurden.

Pflichten der Hersteller

Gemäß Artikel 10 (1) des Cyber Resilience Act müssen Hersteller sicherstellen, dass ihre Hard- und Softwareprodukte von Anfang an Mindestsicherheitsanforderungen erfüllen. Diese Anforderungen umfassen:

Schutzziele:

- **Schutz der Vertraulichkeit von Daten:** Einsatz modernster Verschlüsselungsmechanismen zur Wahrung der Datenvertraulichkeit.
- **Schutz der Integrität von Daten, Befehlen, Programmen und Konfigurationen:** Sicherstellung, dass diese Elemente nicht manipuliert werden können.
- **Schutz vor unbefugtem Zugriff:** Einsatz von Authentifizierungs-, Identitäts- oder Zugangsverwaltungssystemen.
- **Verfügbarkeit wesentlicher Funktionen:** Sicherstellung, dass wichtige Funktionen verfügbar sind, einschließlich Maßnahmen zur Abwehr und Eindämmung von Denial-of-Service-Angriffen.

Security by Default:

- **Sichere Standardkonfiguration:** Produkte werden mit einer sicheren Standardeinstellung ausgeliefert, mit der Möglichkeit, auf diese Konfiguration zurückzusetzen.
- **Datenverarbeitung:** Beschränkung der Datenverarbeitung auf das für den Zweck angemessene und relevante Maß.

Pflichten der Hersteller

Security by Design:

- **Minimierung negativer Auswirkungen:** Reduzierung der eigenen negativen Auswirkungen auf die Verfügbarkeit der Dienste anderer Geräte oder Netze.
- **Minimierung der Angriffsflächen:** Einschließlich der Begrenzung externer Schnittstellen.
- **Implementierung geeigneter Mechanismen:** Zur Minimierung der möglichen Auswirkungen eines Sicherheitsvorfalls.

Monitoring:

- **Loggen sicherheitsbezogener Informationen:** Erfassung einschlägiger interner Vorgänge, wie Zugang zu Daten, Diensten oder Funktionen sowie Änderungen daran.

Sicherheitsupdates:

- **Regelmäßige Sicherheitsupdates:** Bereitstellung von Sicherheitsupdates zur Behebung von Schwachstellen, gegebenenfalls auch durch automatische Aktualisierungen.

Diese Anforderungen zielen darauf ab, die Cybersicherheit von Hard- und Softwareprodukten von der Konzeption über die Entwicklung bis zur Herstellung zu stärken.

Anforderungen an die Behandlung von Schwachstellen

Der Cyber Resilience Act beschreibt **Schwachstellen als Mängel** in IKT-Produkten oder -Diensten, die eine Gefahr bei Cyberangriffen darstellen können.

Er fordert von Herstellern, Schwachstellen in ihren Produkten zu identifizieren und wichtige Abhängigkeiten in einer maschinenlesbaren Software Bill of Materials (SBOM) festzuhalten. Zudem müssen Hersteller eine Strategie für die offene Kommunikation über Schwachstellen entwickeln.

Schwachstellen müssen sofort angegangen und behoben werden, wobei Hersteller für die sichere Verteilung von Sicherheitsupdates sorgen müssen, die schnell und kostenlos zur Verfügung gestellt werden.

Hersteller müssen auch Informationen bereitstellen, aus denen hervorgeht, welches Produkt betroffen ist, wie schwerwiegend und welcher Art die Schwachstelle ist und wie sie behoben werden kann.

Zusätzlich sind Hersteller verpflichtet, die Sicherheit ihrer Produkte regelmäßig zu überprüfen und dies zu dokumentieren.

Anforderungen an Transparenz und Dokumentation

Anhang II des Cyber Resilience Act legt fest, welche Informationen Hersteller den Nutzern ihrer Produkte zur Verfügung stellen müssen. Dies ist ein wichtiger Schritt, um Transparenz und Sicherheit im Bereich der Cybersicherheit zu gewährleisten. Hier eine detaillierte Übersicht der erforderlichen Informationen:

- **Grundlegende Informationen zum Hersteller und zur Identifikation des Produktes:**
  *Name und Kontaktdaten des Herstellers.
  *Eindeutige Identifikationsmerkmale des Produkts

- **Kontaktstelle für Informationen zu Cybersicherheitslücken:**
  *Angabe einer Kontaktstelle (z.B. E-Mail-Adresse oder Telefonnummer), an die sich Nutzer bei Sicherheitsbedenken oder -vorfällen wenden können.

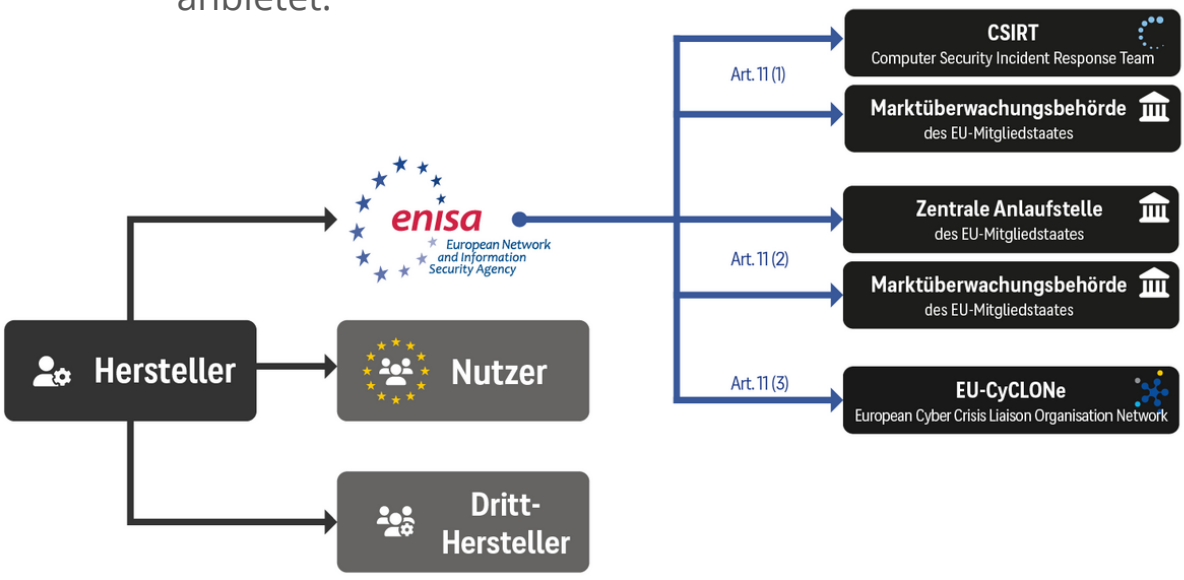
- **Informationen zu Haupteigenschaften und Sicherheitsfunktionen:**
  *Detaillierte Beschreibung der Haupteigenschaften des Produkts, einschließlich der implementierten Sicherheitsfunktionen.

Anforderungen an Transparenz und Dokumentation

- **Informationen zu Umständen, die zu erheblichen Cybersicherheitsrisiken führen können:**
  +Aufklärung über spezifische Situationen oder Konfigurationen, die das Produkt anfällig für Sicherheitsrisiken machen könnten.

- **Wo SBOMs (Software Bill of Materials) und CE-Kennzeichen abrufbar sind:**
  *Informationen darüber, wo Nutzer die SBOMs und das CE-Kennzeichen des Produkts einsehen können.

- **Informationen zu technischer Sicherheitsunterstützung durch den Hersteller:**
  *Details zur technischen Unterstützung, die der Hersteller in Bezug auf die Cybersicherheit des Produkts anbietet.



Pflichten der Einführer

In Zukunft dürfen Importeure Hard- und Softwareprodukte, die unter dem Namen oder der Marke eines Herstellers außerhalb der EU stehen, nur dann in der EU verkaufen, wenn diese die notwendigen Sicherheits- und Schwachstellenbehandlungsanforderungen erfüllen.

Bevor Importeure ein Produkt in der EU anbieten, müssen sie sicherstellen, dass es den EU-Richtlinien entspricht und alle erforderlichen Unterlagen wie die EU-Konformitätserklärung, CE-Kennzeichnung, Benutzerinformationen in angemessener Sprache und technische Dokumentation vorhanden sind.

Sollte ein Produkt nicht den Standards entsprechen, müssen Importeure sofort Maßnahmen ergreifen, um die Konformität zu gewährleisten oder das Produkt vom Markt zu nehmen.

Importeure sind zudem verpflichtet, bei Schwachstellen Meldungen zu machen und müssen daher ihre Kontaktdaten auf dem Produkt oder den Begleitpapieren vermerken.

Bei Entdeckung einer Schwachstelle müssen sie den Hersteller sofort informieren. Stellt das Produkt ein großes Cybersicherheitsrisiko dar, müssen auch die nationalen Marktüberwachungsbehörden informiert werden.

Falls ein Hersteller seine Geschäftstätigkeit einstellt, müssen Importeure dies den Marktüberwachungsbehörden melden.

Pflichten der Händler

Unter CRA dürfen Händler in der EU nur Hard- und Softwareprodukte verkaufen, die den grundlegenden Sicherheitsanforderungen und den Richtlinien zur Behandlung von Schwachstellen entsprechen.

Bevor Händler ein Produkt auf dem EU-Markt anbieten, müssen sie sicherstellen, dass:

- Das Produkt korrekt mit einer CE-Kennzeichnung versehen ist.
- Die EU-Konformitätserklärung vorhanden ist.
- Die Mindestinformationen des Herstellers oder Importeurs verfügbar sind.
- Ausführliche Nutzeranleitungen bereitgestellt werden.
- Sollte ein Produkt nicht den Konformitätsanforderungen entsprechen, sind Händler verpflichtet, umgehend Maßnahmen zu ergreifen, um die Konformität herzustellen oder das Produkt vom Markt zu nehmen.

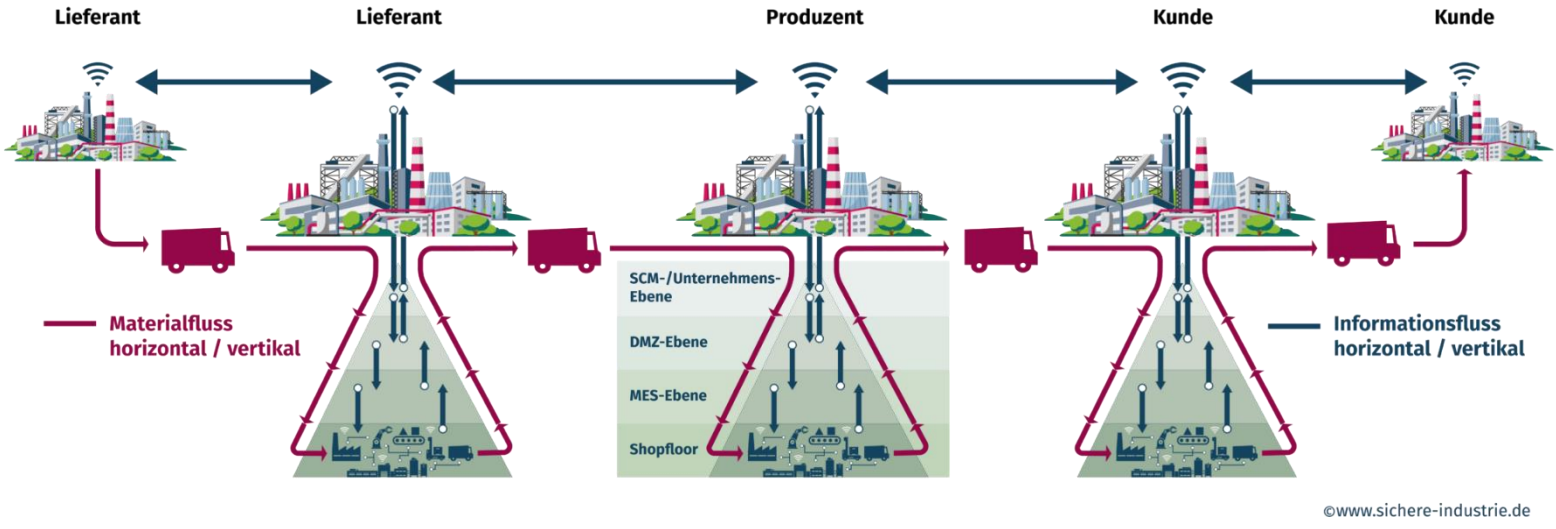
Entdecken Händler eine Schwachstelle in einem Produkt, müssen sie den Hersteller sofort darüber informieren. Falls das Produkt ein erhebliches Cybersicherheitsrisiko darstellt, ist es erforderlich, dass Händler die Marktüberwachungsbehörden der Mitgliedstaaten, in denen das Produkt verkauft wird, unverzüglich informieren.

Wenn bekannt wird, dass ein Hersteller seine Geschäftstätigkeit eingestellt hat, müssen Händler diese Information an die zuständigen Marktüberwachungsbehörden weiterleiten.

Warum ist der CRA so wichtig?

Sicherheitsanforderungen in vernetzten Lieferketten

Zwischenfälle in vernetzten Lieferketten können grenzüberschreitend die Wirtschaft beeinträchtigen oder teilweise zum Stillstand bringen. Mehr und mehr Sektoren werden als kritische Infrastrukturen identifiziert, die auf Lieferanten mit sicherheitsgeprüften Produkten angewiesen sind. Viele Hersteller haben der Sicherheit ihrer Produkte bisher nicht die nötige Bedeutung beigemessen, die angesichts der vorhandenen Cybergefahren geboten wäre. Neue regulatorische Maßnahmen setzen nun gezielt Druck auf, um die erforderlichen Sicherheitsstandards durchzusetzen.



Das ist der Plan!

Die Europäische Kommission reagiert auf die zunehmenden Cyberbedrohungen innerhalb der vernetzten Lieferketten, indem sie die Cybersicherheitsvorschriften mit dem Cyber Resilience Act aktualisiert. Dieses Gesetz legt fest, dass Hersteller nun klar verantwortlich sind, durchgängige Sicherheitsmaßnahmen für ihre digitalen Produkte zu ergreifen, die den gesamten Lebenszyklus dieser Produkte abdecken.

In der Zukunft ist es so, dass nur Produkte, die strenge Cybersicherheitskriterien erfüllen, in der EU verkauft werden dürfen. Dazu gehört auch, dass diese Produkte mit einem CE-Kennzeichen versehen sein müssen und ein effektives Management von Sicherheitslücken aufweisen müssen. Dies gibt den Betreibern kritischer Infrastrukturen einen besseren Überblick über die Cybersicherheit der IT-Produkte in ihren Systemen, wodurch sie schneller auf mögliche Schwachstellen reagieren und ihre Anlagen besser schützen können.

Wie gut dieser Plan in der Praxis funktionieren wird, steht allerdings noch aus. Für Betreiber wird sich ein wirklicher Mehrwert erst dann zeigen, wenn der Cyber Resilience Act über bloße Regelkonformität hinausgeht. Sollte dies der Fall sein, könnten die beträchtlichen Anstrengungen und Investitionen, die von den Herstellern erwartet werden, gerechtfertigt sein.

GET IN TOUCH

+43 512 272 271 0

office@automation.team

www.scada.online

Technikerstraße 1 - 3,
6020 Innsbruck

Bildquellen:

https://www.sichere-industrie.de/eu-cyber-resilience-act/

https://www.ecos.de/blog/cyber-resilience-act

März 2024