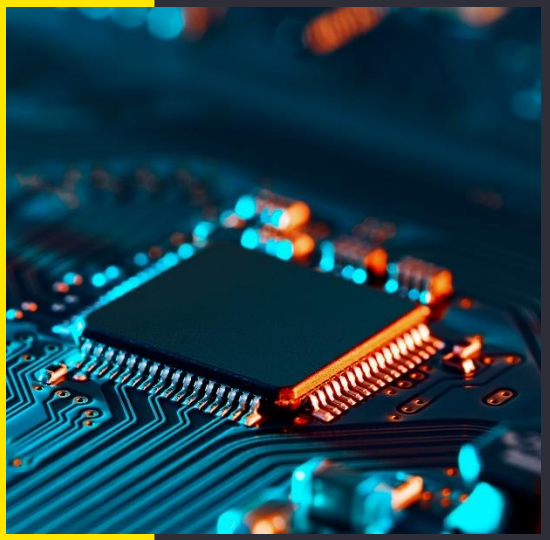
Cyber Resilience Act

Kritisch hinterfragt



Building a better working world

Pa

Agenda

1 Der CRA im Überblick

2 Was sagt die Industrie dazu?

3 7 Fokuspunkte in kritischer Betrachtung

4 Was macht der Rest der Welt?

5 Conclusio

Cyber Resilience Act (CRA)

Cybersicherheitsanforderungen für Produkte mit digitalen Elementen, um sicherere Hardware- und Softwareprodukte zu gewährleisten.

HERAUSFORDERUNGEN

Ausgangslage

- **Niedriges Sicherheitsniveau** bei Hard- und Softwareprodukten.
- Unzureichende und uneinheitliche **Sicherheitsaktualisierungen.**
- **Unzureichendes Verständnis** bei den Nutzern.
- **Unzureichender Zugang** zu Informationen für Nutzer.

HAUPTZIELE

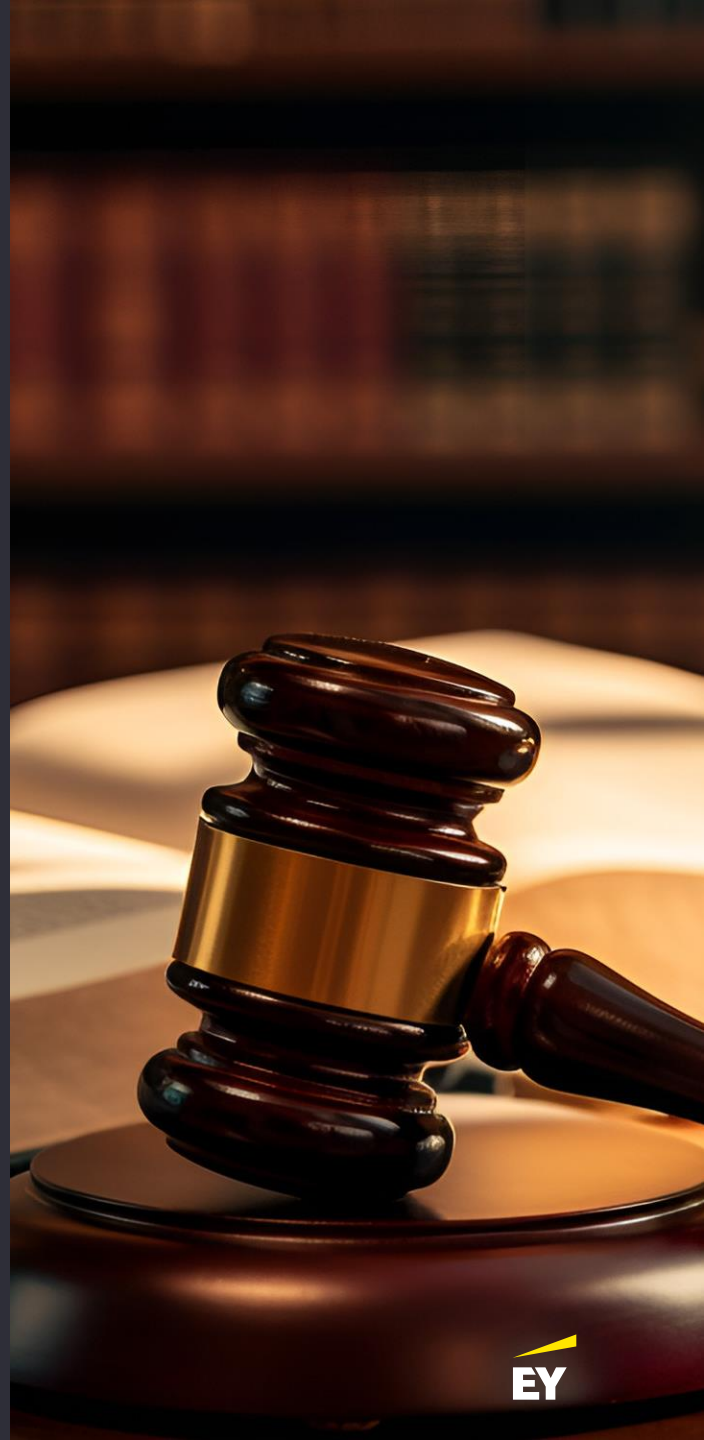
Strategie

- Voraussetzungen für die **Entwicklung sicherer Produkte** mit digitalen Elementen schaffen.
- Hersteller nehmen die **Sicherheit während des gesamten Lebenszyklus** eines Produkts ernst.
- Bedingungen, die es **Nutzern ermöglichen, die Cybersicherheit bei der Auswahl und Nutzung** von Produkten zu berücksichtigen.

SPEZIFISCHE ZIELE

Kokretisierung

- Hersteller beachten **Sicherheit ab der Konzeptions- und Entwicklungsphase** und verbessern diese während des **gesamten Lebenszyklus**.
- Gewährleistung eines **kohärenten Rahmens** für die Cybersicherheit.
- **Transparenz** der Sicherheitseigenschaften verbessern.
- Unternehmen und Verbraucher in die Lage versetzen, **Produkte mit digitalen Elementen sicher zu nutzen**.



Cyber Resilience Act (CRA)

Cybersicherheitsanforderungen für Produkte mit digitalen Elementen,
um sicherere Hardware- und Softwareprodukte zu gewährleisten.

KOM | Cyber Resilience Act

Cyber Resilience Act (CRA)

Ja, aber...

Marc Fliehe, TÜV-Verband

„Wir begrüßen das Vorhaben, erstmals grundlegende verpflichtende Cybersicherheitsanforderungen für vernetzte Produkte zu schaffen. Dieser Schritt ist längst überfällig, denn nur so können Unternehmen, Behörden und Bürger besser vor Cyberangriffen geschützt werden“ Marc Fliehe, TÜV-Verband

TÜV | 12.2022

Wolfgang Weber, ZVEI e.V.

„Diese Regulierung wird alle digitalen Produkte im europäischen Binnenmarkt betreffen. Auch wenn es unsere Unternehmen vor enorme Herausforderungen stellt, braucht der europäische Binnenmarkt ein solches harmonisiertes Level-Playing-Field in der Cybersicherheit“.

ZVEI | 17.09.2022

Siemens, Ericsson, SE, et al

„Die Unternehmen betonten, dass das Gesetz in seiner derzeitigen Form Engpässe schaffen könnte, die den Binnenmarkt stören würden. Sie wiesen darauf hin, dass Störungen Millionen von Produkten betreffen könnten, von Waschmaschinen bis hin zu Spielzeug, Cybersicherheitsprodukten sowie wesentlichen Komponenten für Wärmepumpen, Kühlanlagen und hochtechnologische Fertigung.

Reuters | 07.11.2023

Fokus

1 Produktions-Auswirkungen

2 Innovations-kraft

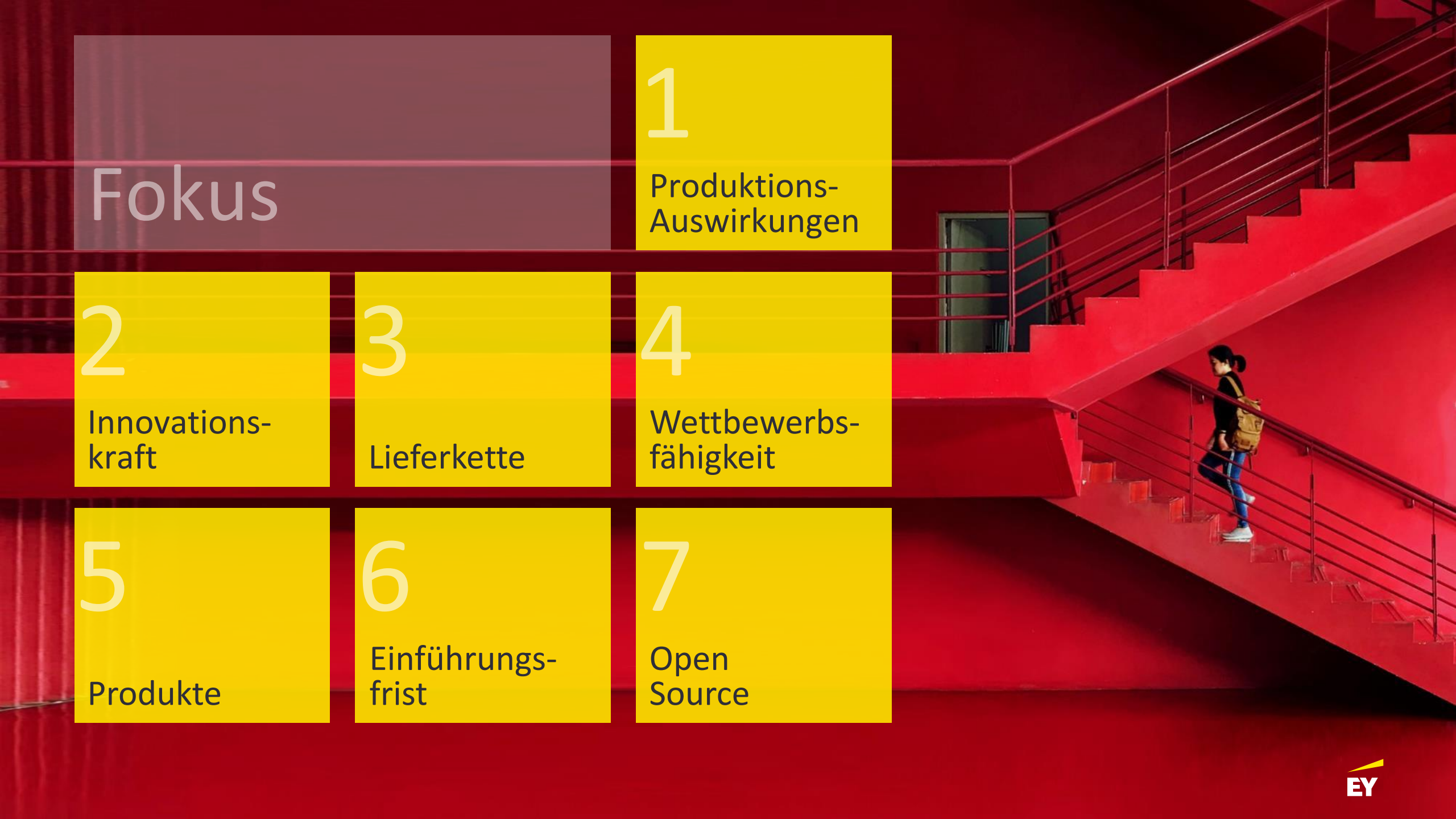
3 Lieferkette

4 Wettbewerbs-fähigkeit

5 Produkte

6 Einführungs-frist

7 Open Source

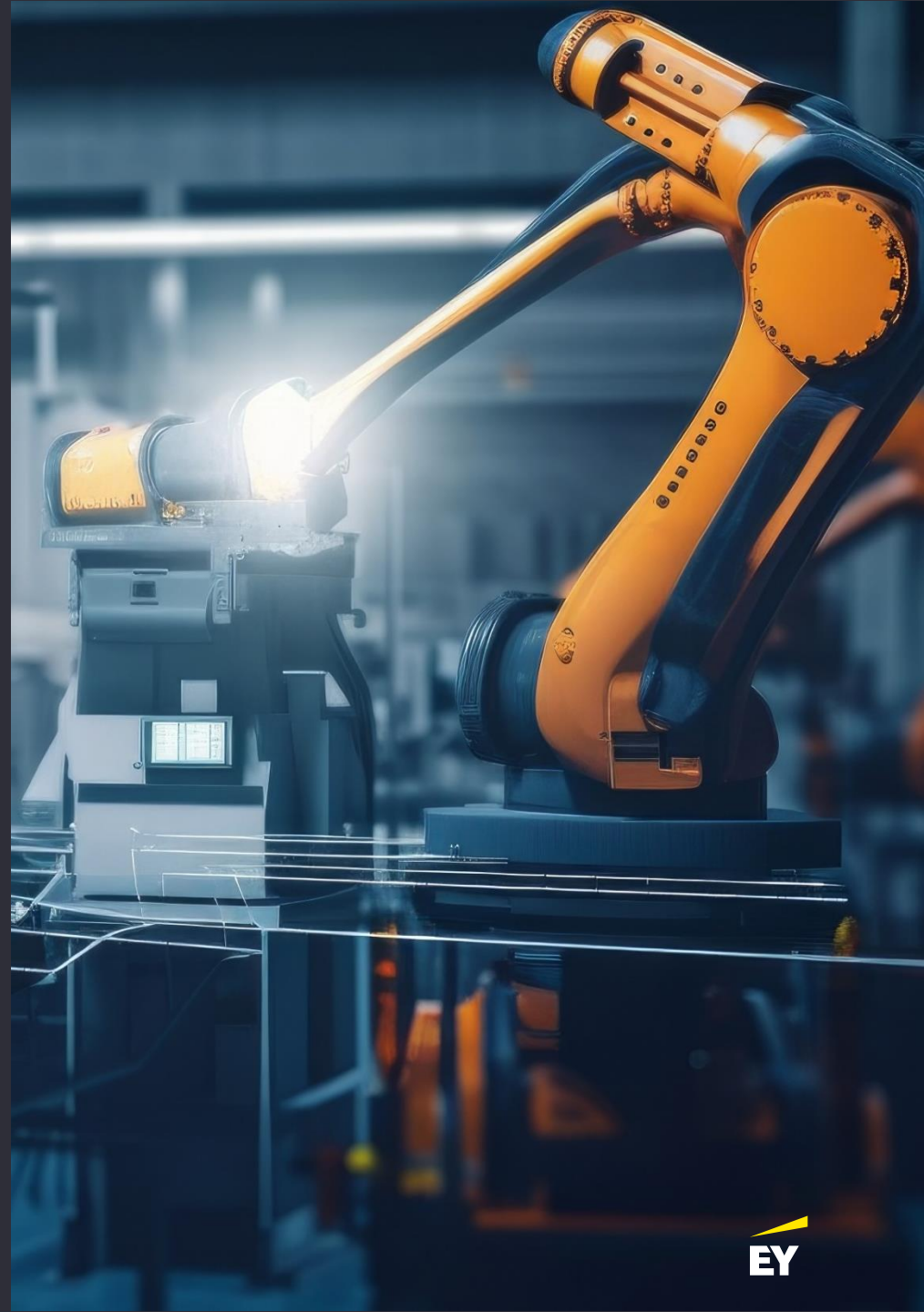


Cyber Resilience Act (CRA)

Was bedeutet der CRA für Entwicklung und Produktion?

Strenge Maßnahmen erfordert eine **Überarbeitung bestehender Prozesse**. Dazu zählen Risikobewertung vor Markteintritt, Anforderungen an die Produkt-entwicklung oder führen einer „Software Bill of Materials“ (SBOM), etc.

Problem langer Produktionszyklen!



Cyber Resilience Act (CRA)

Fördert oder zerstört der CRA die Innovationskraft?

Mindert der CRA die **Innovationskraft** von Unternehmen, oder macht er digitale Produkte aus der EU erst wettbewerbsfähig?

Grundsatz des „Security-by-Design forcieren. Jedoch kann der CRA ein Innovationshindernis für KMU darstellen.

Cyber Resilience Act (CRA)

Wirkt der CRA negativ auf Lieferketten?

Die Implementierung neuer Sicherheitsstandards und die Überprüfung der Compliance können zu Verzögerungen in der **Lieferkette** führen, insbesondere in den Anfangsphasen der Anpassung an die neuen Vorschriften.

Zu berücksichtigen ist insbesondere Lieferanten-management und –überprüfung, Risikomanagement und Haftung

Cyber Resilience Act (CRA)

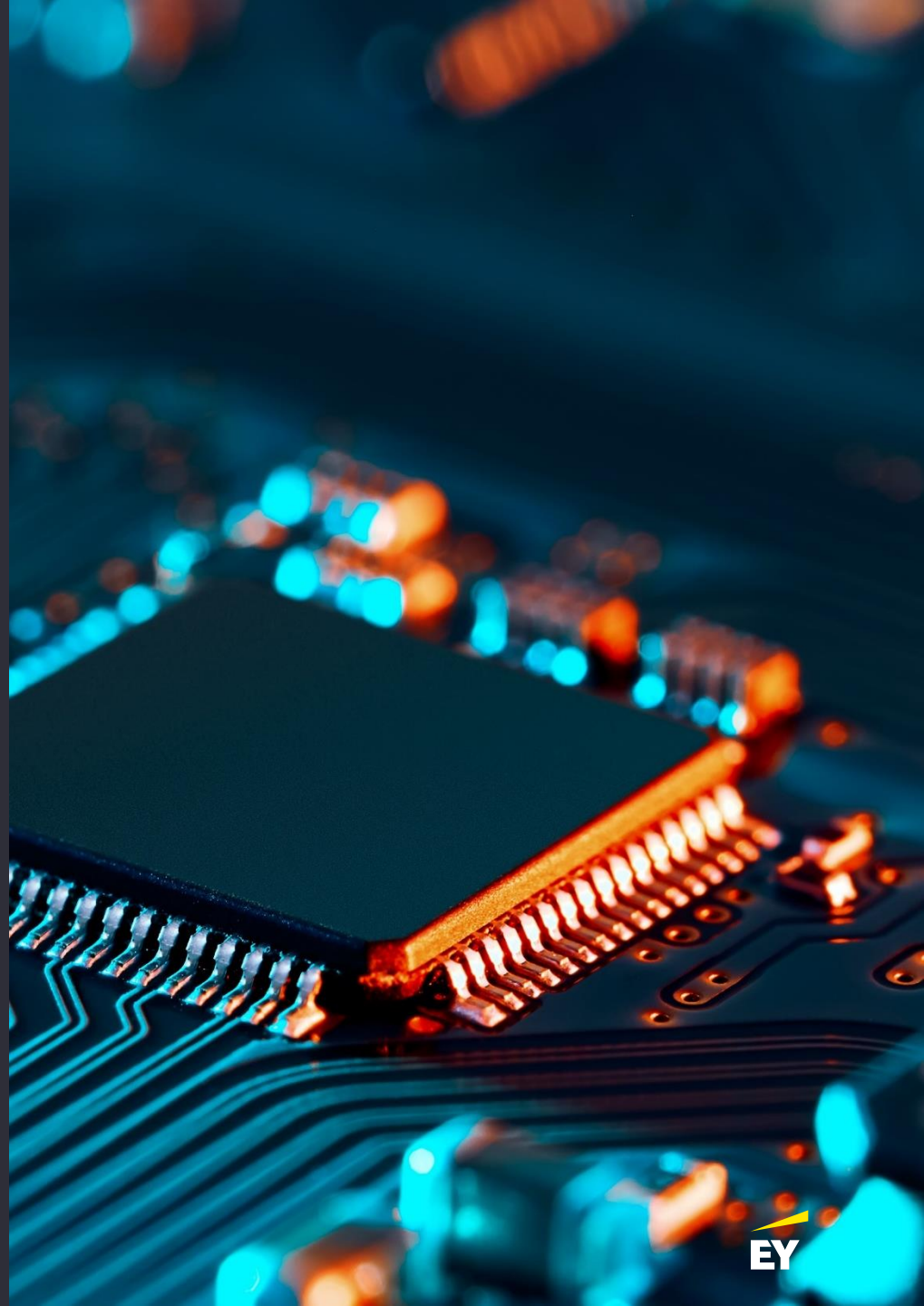
Mindert oder verstärkt der CRA die EU-Wettbewerbsfähigkeit?

Die Auswirkungen des CRA auf die **Wettbewerbsfähigkeit** von EU Produkten kann unterschiedlich bewertet werden. Von besserer Reputation der EU-Produkte durch mehr Sicherheit bis zu hohe Kosten für wenig regulierte Märkte.

Cyber Resilience Act (CRA)

Was bedeutet die Produkt-Klassifizierung?

Klassifizierung der Produkte rein nach Produktart ohne Berücksichtigung des Verwendungskontextes. Für viele Produkte mit erhöhtem Risiko (kritische Produkte nach Klasse I) nur Selbsterklärung.



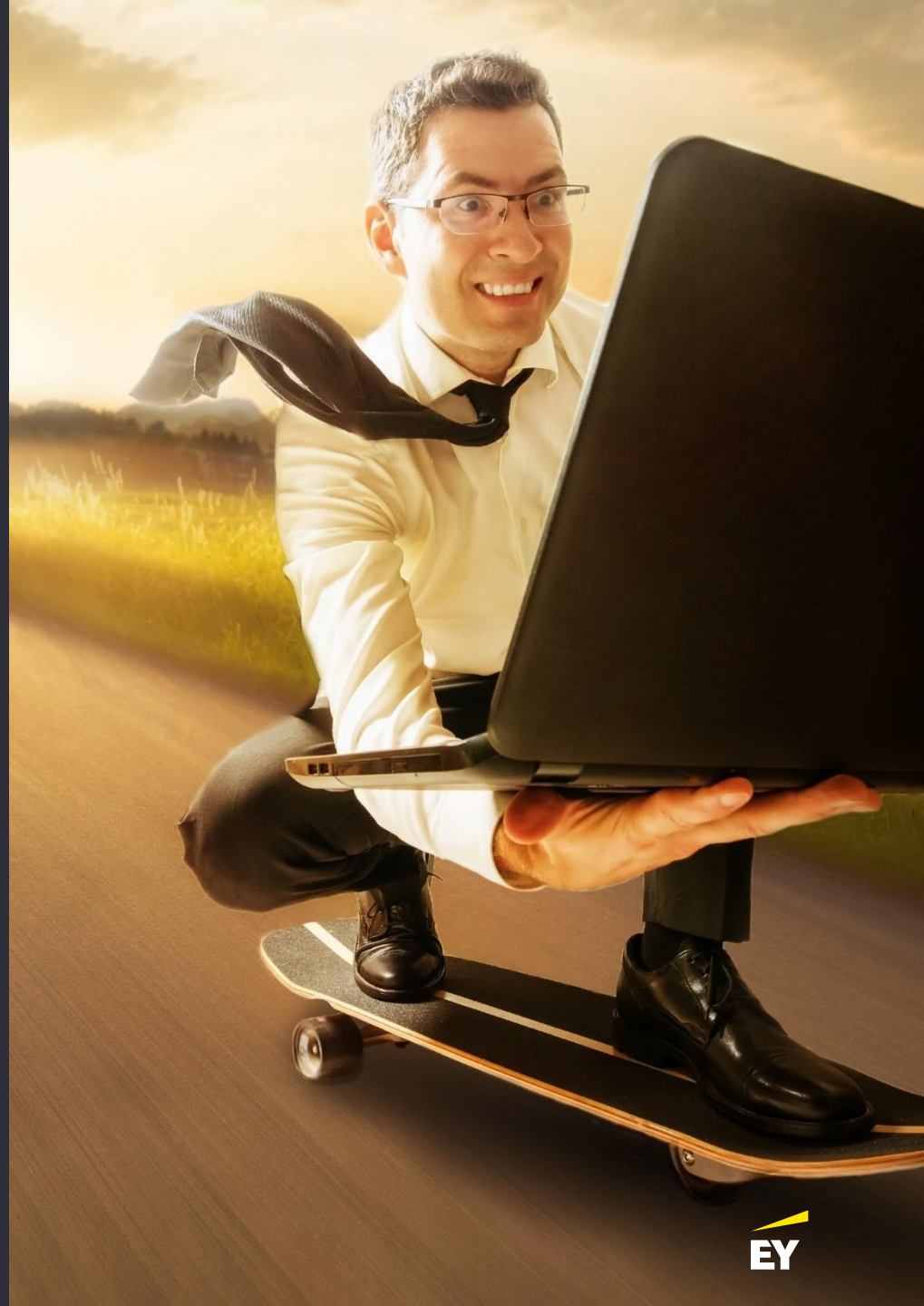
Cyber Resilience Act (CRA)

Wie schnell muss/kann es gehen?

Vorteilhaft ist, dass der CRA den Prinzipien des „New Legislation Frameworks (NLF) folgt, jedoch ist die **Übergangsfrist von 24 Monaten** zu kurz.

Aus den Erfahrungen der Medizinprodukte-VO (MDR) sollte gelernt werden, dass längere Übergangsfristen benötigt werden.

Wirksamkeit des CRA? (Wirksamkeitsprüfung)



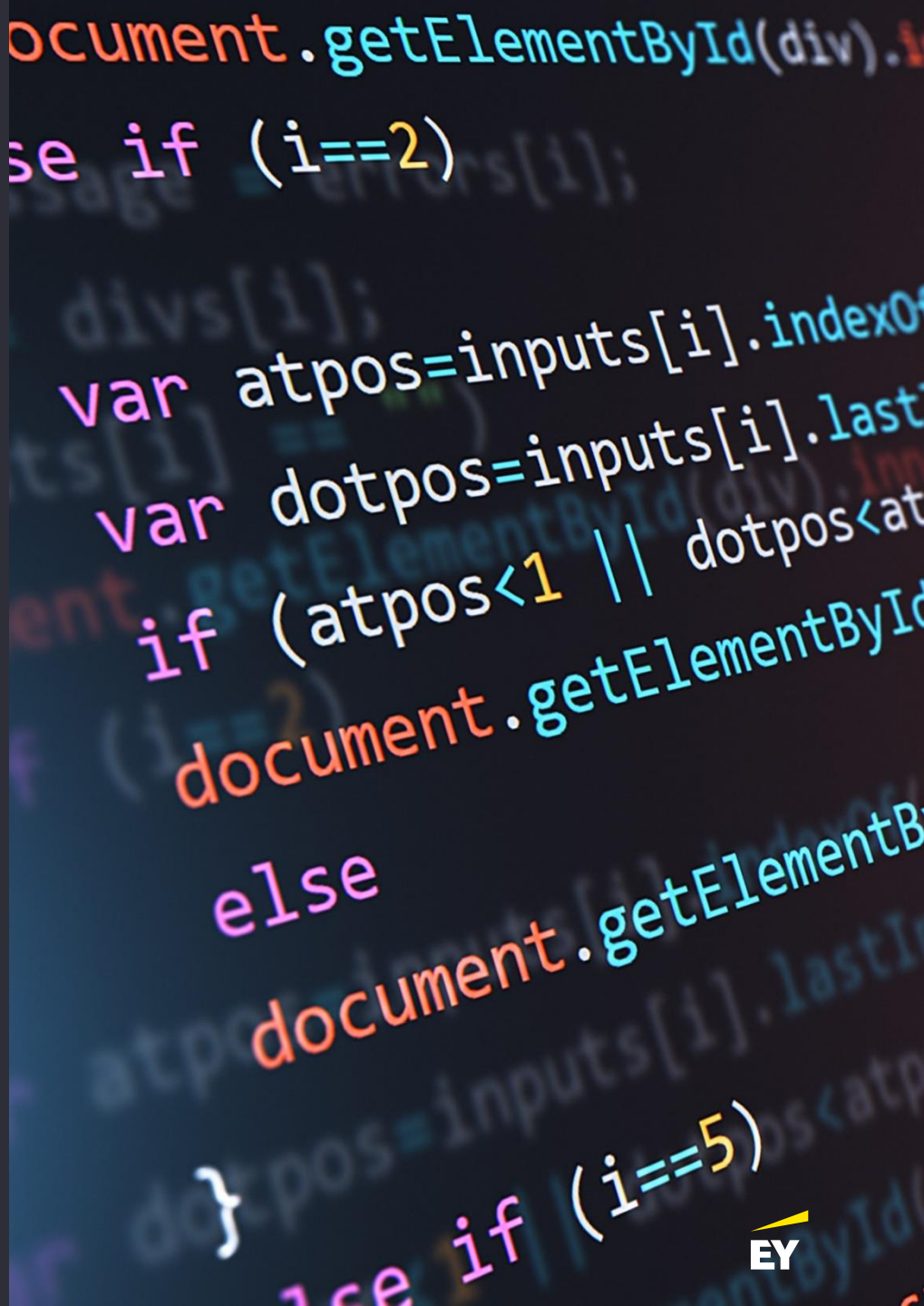
Cyber Resilience Act (CRA)

Open Source als Innovationskraft und Backbone der Industrie.

Open Source Software macht 70% der Software aus. Die Eigenschaften von Open Source Software soll anerkannt werden und das OSS-Ökosystem soll nicht zerstört werden.

Die OSS-Organisationen fordern von der EU Kommission einen ständigen Dialog mit den Europäischen Institutionen.

Offener Brief | Eclipse Foundation



Cyber Resilience Act (CRA)

Ist die EU mit der Regulation eine Vorreiterin?

USA - Internet of Things (IoT) Cybersecurity Improvement Act: Dieses Gesetz, das 2020 verabschiedet wurde, verpflichtet die US-Regierung, nur IoT-Geräte zu erwerben, die bestimmten Sicherheitsstandards entsprechen. Es legt Mindestanforderungen für die Cybersicherheit von IoT-Geräten fest, die von der Bundesregierung genutzt werden.

Kalifornien - SB-327 Information Privacy: Connected Devices: Kalifornien hat ein Gesetz verabschiedet, das Mindestsicherheitsanforderungen für IoT-Geräte vorschreibt. Ab 2020 müssen Hersteller von verbundenen Geräten angemessene Sicherheitsfunktionen einbauen, die dem Zweck und der Art des Geräts entsprechen.

Japan - IoT Security Guidelines: Japan hat Richtlinien für die Sicherheit von IoT-Geräten veröffentlicht, die Hersteller, Dienstanbieter und Benutzer von IoT-Geräten dazu anhalten, Maßnahmen zur Verbesserung der Sicherheit zu ergreifen. Diese Richtlinien sind zwar nicht gesetzlich bindend, haben aber einen starken Einfluss auf die Industrie.

Australien - Code of Practice for Securing the Internet of Things for Consumers: Australien hat einen Verhaltenskodex für die Sicherung des Internets der Dinge für Verbraucher herausgegeben. Dieser Kodex enthält eine Reihe von Prinzipien, die als beste Praktiken für die Sicherheit von IoT-Geräten gelten, und richtet sich an Hersteller, Dienstanbieter und Einzelhändler.

Singapur - Cybersecurity Labeling Scheme (CLS): Singapur hat ein Cybersecurity-Kennzeichnungsschema eingeführt, das ähnlich wie ein Energieeffizienzlabel funktioniert und Verbrauchern Informationen über das Sicherheitsniveau von IoT-Geräten bietet. Das CLS zielt darauf ab, das Bewusstsein für Cybersicherheit zu schärfen und Hersteller zur Verbesserung der Sicherheitsstandards ihrer Produkte anzuregen.

Cyber Resilience Act (CRA)

Conclusio

Die Richtung stimmt! – Mehr Cyber Security.

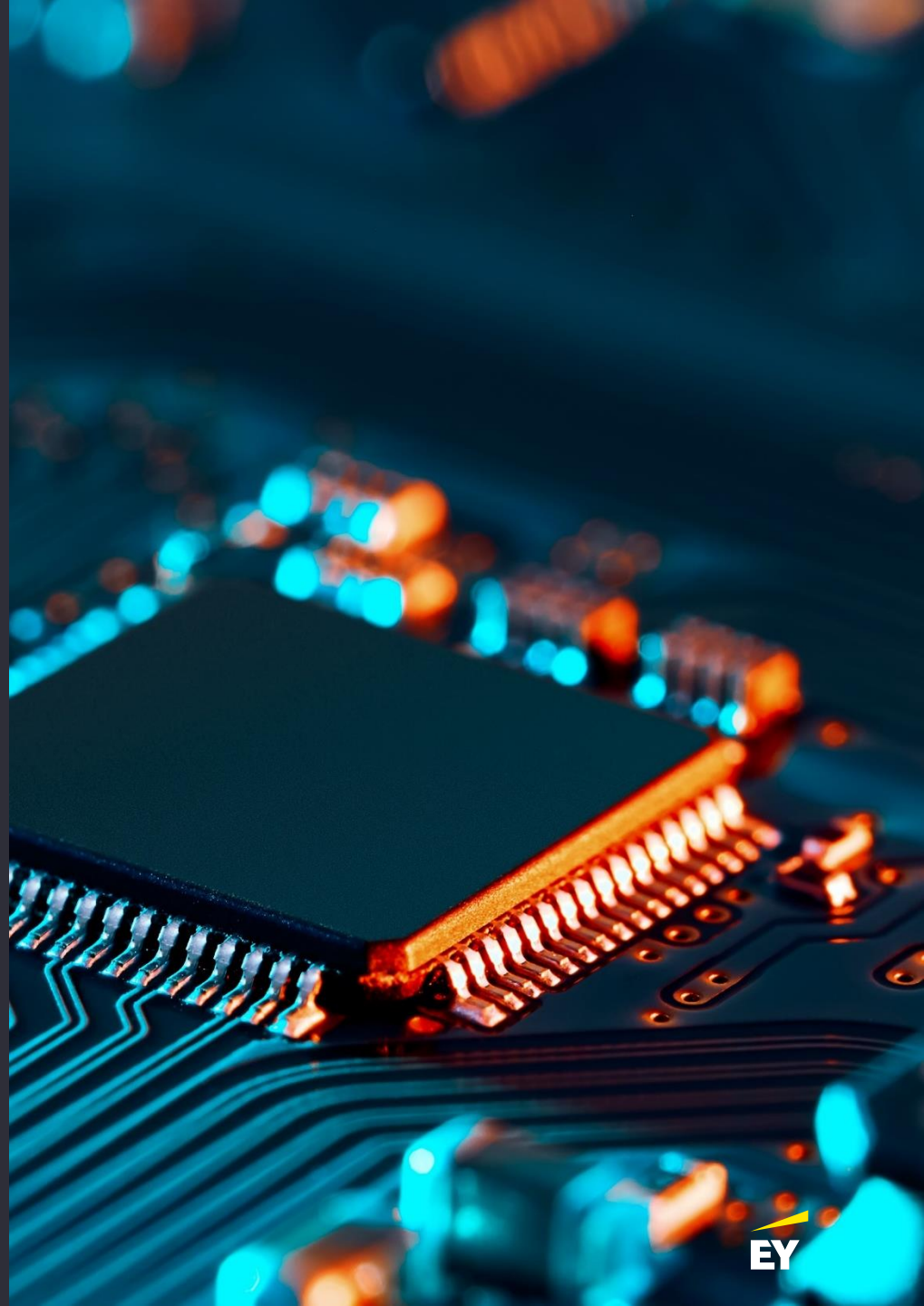
Wettbewerbsfähigkeit der EU-Unternehmen wird erhalten.

Standardisierung der Anforderungen – Chancengleichheit (?)

Knappe Umsetzungszeit – Jetzt beginnen!

Mögliche Innovationshemmung – „Security by Design“

Probleme in der Lieferkette – CRA das „digitale COVID“?



Unser Experte

Roman A. Tobler
Senior Manager Consulting
Roman.Tobler@at.ey.com
+43 664 60003 4392