Der Cyber Resilience Act: Ein Überblick über Hintergründe und Ziele

The Cyber Resilience Act: overview of its background and goals

Die zunehmende Digitalisierung und Vernetzung unserer Gesellschaft bringt nicht nur immense Vorteile, sondern auch erhebliche Herausforderungen mit sich. Hierzu gehören vor allem Cyberangriffe, die stetig zunehmen und immense wirtschaftliche Schäden verursachen. Vor diesem Hintergrund hat die Europäische Kommission den Cyber Resilience Act (CRA) verabschiedet.

VON MANUEL PONCZA UND MICHAEL KUSKA, LL.M., LL.M.

Hintergründe und Ziele des CRA: Der Cyber Resilience Act ist Teil der EU-Cybersicherheitsstrategie. Sie zielt darauf ab, die digitale Souveränität Europas zu sichern und die Cyberresilienz europäischer Unternehmen zu erhöhen. Der CRA verfolgt dabei mehrere zentrale Ziele. Diese umfassen insbesondere:

- **Die Erhöhung der Cybersicherheit von Produkten mit digitalen Elementen:** Der CRA soll sicherstellen, dass alle in der EU verkauften „Produkte mit digitalen Elementen" grundlegende Sicherheitsanforderungen einhalten. Dies umfasst sowohl Hard- als auch Software, solange diese über sogenannte „Datenfernverarbeitungslösungen" verfügen, also etwa internetfähig sind.
- **Die Förderung der Verantwortlichkeit und Transparenz:** Hersteller von Produkten mit digitalen Elementen sollen

The increasing digitalisation and networking of our society has not only produced immense advantages but also considerable challenges. These above all include cyber-attacks, which are continuously increasing and causing immense economic damage. Against this background, the European Commission passed the Cyber Resilience Act (CRA).

BY MANUEL PONCZA AND MICHAEL KUSKA, LL.M., LL.M.

Background and goals of the CRA: *The Cyber Resilience Act is part of the EU's cybersecurity strategy. Its aim is to secure the digital sovereignty of Europe and enhance the cyber-resilience of European companies. In*

> **„Hersteller von Produkten mit digitalen Elementen sollen Sicherheitsrisiken identifizieren und beheben."**
>
> MICHAEL KUSKA

> **"Manufacturers of products with digital elements are to identify and correct security risks."**
>
> MICHAEL KUSKA

Sicherheitsrisiken identifizieren und beheben. Zudem sollen sie transparent über die Sicherheitsmerkmale und -lücken ihrer Produkte informieren. Dies soll das Vertrauen der Verbraucher stärken und die Marktanreize für sichere Produkte erhöhen.

CYBERSICHERHEIT ALS PRODUKTSICHERHEITSANFORDERUNG

Systematisch erreicht der CRA diese Ziele, indem er Herstellern, Einführern und Händlern von Produkten mit digitalen Elementen im Produktsicherheitsrecht weitreichende Pflichten auferlegt. Dazu zählt etwa die Pflicht zur fortwährenden Gewährleistung der grundlegenden Cybersicherheitsanforderungen während der Produktentwicklung. Diese grundlegenden Cybersicherheitsanforderungen sind in einem umfangreichen Katalog im CRA festgelegt.

Zu den weiteren Pflichten gehören:

- die Durchführung einer Konformitätsbewertung,
- die Anfertigung und Bereitstellung einer technischen Dokumentation,
- die CE-Kennzeichnung sowie
- die Pflicht zum Beheben und Melden von bekannt werdenden Sicherheitsschwachstellen.

Einführer und Händler müssen vor dem Inverkehrbringen von Produkten mit digitalen Elementen prüfen, ob die Hersteller diese und andere Verpflichtungen einhalten.

Die regulatorische Vorgabe von Cybersicherheitsanforderungen in der Aufzugs- und Fahrtreppenbranche ist dabei grundsätzlich nichts Neues. So folgen bereits aus der von der Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (BAuA) im März 2023 veröffentlichten „TRBS 1115 Teil 1: Cybersicherheit für sicherheitsrelevante Mess-, Steuer- und Regeleinrichtungen" zahlreiche Anforderungen an das Cybersicherheits-Risikomanagement.

Der zentrale Unterschied zwischen der TRBS 1115-1 und dem CRA ist jedoch, dass die TRBS 1115-1 ein Rahmenwerk für das Cybersicherheits-Risikomanagement darstellt. Der CRA reguliert

this regard, the CRA pursues several goals. These cover in particular:

- ***Enhancing the cybersecurity of products with digital elements:*** *The CRA is intended to ensure that all "products with digital elements" sold in Europe observe basic security requirements. This covers both hard – as well as software as long as these have so-called "remote data processing solutions", i.e. can be linked to the Internet.*
- ***The promotion of responsibility and transparency:*** *Manufacturers of products with digital elements are to identify and correct security risks. Moreover, they are to provide transparent information about the security features and gaps of their products. This is intended to reinforce the trust of consumers and increase market incentives for secure products.*

CYBERSECURITY AS PRODUCT SECURITY REQUIREMENT

The CRA achieves these goals systematically by imposing far-reaching obligations in product safety law on manufacturers, importers and traders of products with digital elements. This for example includes the obligation to provide an ongoing guarantee of basic cybersecurity requirements during product development. These basic cybersecurity requirements are specified in a comprehensive catalogue in the CRA.

The other obligations include

- *conducting a conformity evaluation,*
- *preparing and providing technical documentation,*
- *CE labelling and*

Der CRA führt ein neues Sanktionsregime ein. Hiernach erhalten die zuständigen Aufsichtsbehörden die Befugnis, direkt gegen relevante Wirtschaftsakteure vorzugehen. Dies kann auch Bußgelder und Zwangsrückrufe umfassen.
The CRA introduces a new sanctions regime. According to it, the responsible supervisory authorities are given the power to take action directly against relevant economic players. These can also include fines and mandatory recalls.

dagegen die Sicherheit der gegenständlichen Produkte mit digitalen Elementen selbst und richtet sich damit nicht an die Betreiber, sondern an Hersteller, Einführer und Händler solcher Produkte. Der CRA enthält zudem zahlreiche Vorgaben für die Produktentwicklung und -überwachung, etwa zum Schwachstellenmanagement, die die TRBS 1115-1 in dieser Form nicht kennt. Damit besteht ein signifikanter Unterschied hinsichtlich des Adressatenkreises und des Pflichtenkreises.

Daneben führt der CRA ein neues Sanktionsregime ein. Hiernach erhalten die zuständigen Aufsichtsbehörden die Befugnis, direkt gegen relevante Wirtschaftsakteure vorzugehen. Dabei

- *the obligation to correct and report security weaknesses as they become known.*

Before distributing products with digital elements, importers and traders must check whether the manufacturer observed these and other obligations.

EFFECTS ON THE MANUFACTURE AND DISTRIBUTION OF LIFTS

Today, many modern lift systems have networked hardware and software components. Consequently, these will in future be covered by the CRA. However, it must be borne in mind that the CRA makes provision for particular transition periods with exceptions and reverse exceptions. In view of this, close examination is needed in each case to determine whether the CRA affects lifts already distributed or planned for the future.

The regulatory prescription of cybersecurity requirements in the lift and escalator sector is not fundamentally new. For example, numerous cybersecurity risk management requirements already arise from "TRBS 1115 Part 1: cybersecurity for safety-relevant instrumentation and control systems", published in March 2023 by the Federal Institute for Occupational Safety and Health (BAuA).

„Zum Zeitpunkt des Erstkontaktes mit Herrn Dr. Watermann war die Veräußerung unseres Familienunternehmens lediglich eine Option für uns. Die unaufdringliche, ergebnisoffene und kompetente Beratung von Dr. Watermann hat uns im Entscheidungsprozess enorm geholfen. In der folgenden Verkaufsphase zeigte sich besonders die Branchenerfahrung vom WATERMANN AGENS-Team, so dass die Abarbeitung der nicht wenigen Detailaufgaben zu einem schnellen und erfreulichen Ergebnis geführt hat."

Gesellschafterkreis der Joh. Holtz GmbH & Co. KG, Bremen

WATERMANN AGENS

Persönlicher Kontakt: Dr. Lars Watermann
+49 178 808 7777 · lars.watermann@watermann.ag
WATERMANN AGENS GmbH · Jungfernstieg 7 · 20354 Hamburg · www.watermann.ag

„Der CRA gilt erst ab September 2026 bzw. Dezember 2027, es sollte jedoch bereits jetzt geprüft werden inwiefern bestehende Prozesse angepasst werden müssen."

MICHAEL KUSKA

"The CRA will only apply from September 2026 or December 2027 but a review should already be conducted regarding the extent to which existing processes are in need of adaptation."

MICHAEL KUSKA

können sie – bei Vorliegen der entsprechenden Voraussetzungen – Aufsichts- und Durchsetzungsmaßnahmen unmittelbar gegen diese ergreifen. Dies kann auch Bußgelder und Zwangsrückrufe umfassen.

FAZIT

Der CRA ist ein wichtiger Schritt zur Stärkung der Cybersicherheit in der Europäischen Union und findet zusätzlich zu der TRBS 1115-1 Anwendung. Dies führt zu einer deutlichen Erhöhung der Cybersicherheit von Aufzugsanlagen und ihren technischen Systemen. Zwar gilt der CRA erst ab September 2026 bzw. Dezember 2027, es sollte jedoch bereits jetzt geprüft werden, inwiefern bestehende Entwicklungs-, Prüf- und Beschaffungsprozesse angepasst werden müssen, um die Vorgaben des CRA angemessen zu berücksichtigen. I←

heuking.de

Die Autoren sind auf IT-Sicherheitsrecht spezialisierte Rechtsanwälte und Salaried Partner der Kanzlei Heuking. Beide wurden mehrfach im Bereich des IT-Sicherheitsrechts zertifiziert und ausgezeichnet.

But the central difference between TRBS 1115-1 and the CRA is that TRBS 1115-1 constitutes a framework for cybersecurity risk management. By contrast, the CRA regulates the safety of the products involved with digital elements themselves and as a result is directed not at the operators but rather the manufacturers, importers and traders of such products. Moreover, the CRA includes numerous requirements for product development and monitoring, for example, weakness management, which TRBS 1115-1 does not do in this form. This means there is a significant difference in the groups addressed and subject to obligations.

In addition, the CRA introduces a new sanctions regime. According to it, the responsible supervisory authorities are given the power to take action directly against relevant economic players. If the necessary preconditions exist, they can institute regulatory and enforcement measures directly against the latter. These can also include fines and mandatory recalls.

CONCLUSION

The CRA is an important step towards reinforcing cybersecurity in the European Union and applies in addition to TRBS 1115-1. This will lead to a clear enhancement in cybersecurity for lifts and their technical systems. Admittedly, the CRA will only apply from September 2026 or December 2027 but a review should already be conducted regarding the extent to which existing development, testing and procurement processes are in need of adaptation to make appropriate allowance for the CRA's requirements. I←

heuking.de

The authors are lawyers specialised in IT security law and salaried partners at the law firm Heuking. Both hold multiple IT security law certifications and awards.

TRBS 1115-1

Die TRBS 1115-1 ist ein Rahmenwerk für das Cybersicherheits-Risikomanagement. Diese Regelung findet neben dem CRA weiterhin Anwendung.

TRBS 1115-1

TRBS 1115-1 is a framework for cybersecurity risk management. This regulation continues to apply in addition to the CRA.