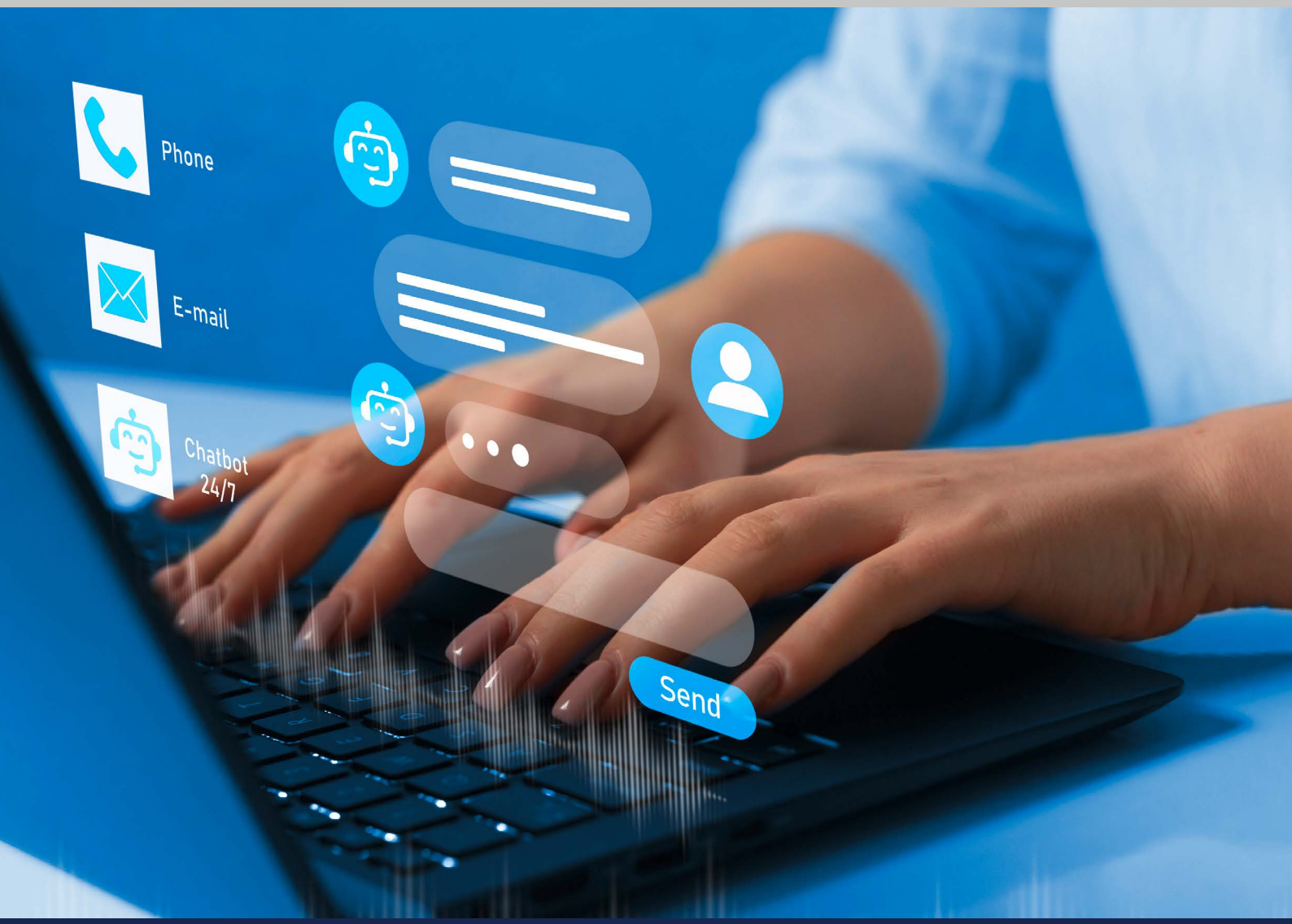
FORUM



Cyber Resilience Act: Das unterschätzte Puzzlestück für die Finanz-IT

Mehr Sicherheit, neue Regeln: Der CRA und seine Folgen für den Finanzsektor

Sehr geehrte Leser*innen,

mit dem Cyber Resilience Act (CRA) schafft die EU einen neuen, verbindlichen Rahmen für die Cybersicherheit von Produkten mit digitalen Komponenten. Die Anforderungen betreffen nicht nur Hersteller, sondern wirken sich entlang der gesamten Wertschöpfungskette aus – auch auf Finanzunternehmen.

Dieses Whitepaper gibt Ihnen einen kompakten Überblick über die zentralen Regelungen, Fristen und Pflichten sowie deren praktische Relevanz. Erfahren Sie, welche Maßnahmen jetzt erforderlich sind, um Risiken zu minimieren und regulatorische Vorgaben sicher zu erfüllen.

Über die Autorin:

Josefine Spengler ist Fachanwältin für IT-Recht und Expertin für Zahlungsdiensteaufsichtsrecht, IT- und Datenschutzrecht sowie Geldwäsche-Compliance. Sie berät insbesondere zu regulatorischen IT-Anforderungen im Finanzsektor und entwickelt praxisnahe Datenschutz- und Compliance-Konzepte. Als Spezialistin für das FinTech-Umfeld verbindet sie juristische Expertise mit technischem Verständnis und ist zudem Autorin des Blogs PAYMENT.TECHNOLOGY.LAW.

Cyber Resilience Act: Das unterschätzte Puzzlestück für die Finanz-IT

von **Josefine Spengler** 11. September 2025 4 Minuten

Von Babyphones bis Smartwatches – Produkte und Software mit digitalen Komponenten sind allgegenwärtig. Was vielen Anwendern weniger bewusst ist: Sie bergen erhebliche Sicherheitsrisiken, insbesondere wenn Hersteller Sicherheitsupdates verzögern oder gar nicht bereitstellen.

Um diese Lücke zu schließen, ist am 10. Dezember 2024 die EU-Verordnung (EU) 2024/2847 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen – der Cyber Resilience Act (CRA) – in Kraft getreten. Er ergänzt den europäischen Rechtsrahmen und verfolgt ein klares Ziel: Cybersicherheit von Anfang an in Produkte einzubauen.

Doch was bedeutet der CRA für die Finanzwelt?

Inhaltsverzeichnis

Worum geht es beim CRA?

Der CRA verpflichtet Hersteller, Importeure und Händler von Hard- und Software direkt, verbindliche Cybersicherheitsstandards einzuhalten. Betroffen sind praktisch alle „Produkte mit digitalen Elementen“ – von Routern über Betriebssysteme bis hin zu komplexen Unternehmensanwendungen.

Kernpunkte sind:

- Security-by-Design und Security-by-Default: Cybersicherheit muss von Anfang an in die Produkte eingebaut sein.
- Pflichten über den gesamten Produktlebenszyklus: Planung, Design, Entwicklung, Wartung.
- Pflicht zur Bereitstellung von Sicherheitsupdates.
- CE-Kennzeichnung für Produkte, die CRA-Anforderungen erfüllen.
- Drittprüfungen (Konformitätsbewertungen) für besonders sicherheitskritische Produkte

Damit wird die Verantwortung stärker in Richtung Hersteller verlagert. Käufer können künftig einfacher erkennen, ob Produkte den EU-Sicherheitsstandards entsprechen.

Die Anwendung des CRA erfolgt gestaffelt:

- **Ab Juni 2026:** Konformitätsbewertungsstellen (Conformity Assessment Bodies – CABs) werden ermächtigt, die Übereinstimmung von Produkten mit den Anforderungen des CRA zu bewerten.
- **Ab 11. September 2026** gelten die Meldepflichten für Sicherheitsvorfälle und Schwachstellen. Hersteller vernetzter Produkte unterliegen dann der verpflichtenden Meldung von Schwachstellen und Sicherheitsvorfällen.
- **Ab 11. Dezember 2027** sind sämtliche CRA Anforderungen an betroffene Produkte verbindlich, einschließlich der Einhaltung der wesentlichen Cybersicherheitsanforderungen vor dem Inverkehrbringen eines Produkts, der Behandlung von Schwachstellen während des gesamten Produktlebenszyklus sowie der Transparenz gegenüber den Nutzern.

Wer ist verpflichtet?

Der Cyber Resilience Act richtet sich an die Hersteller, Importeure und Händler von Produkten mit digitalen Elementen. Der Gesetzgeber geht hier bewusst in die Tiefe der Lieferkette, um Cybersicherheit „by design and by default“ in die Produkte selbst einzubauen.

Konkret verpflichtet sind:

- **Hersteller von Hard- und Software**: Sie müssen Cybersecurity-Anforderungen bereits in der Planung, Entwicklung und Wartung berücksichtigen und Sicherheitsupdates während des gesamten Lebenszyklus bereitstellen.
- **Importeure**: Sie dürfen nur Produkte auf den EU-Markt bringen, die den CRA-Anforderungen entsprechen.
- **Händler/Distributoren**: Sie müssen sicherstellen, dass die Produkte, die sie vertreiben, CRA-konform sind (u. a. durch CE-Kennzeichnung).

Nicht erfasst sind:

- bestimmte Open-Source-Software, sofern diese nicht im Rahmen einer kommerziellen Tätigkeit bereitgestellt wird,
- Produkte, die bereits spezialgesetzlich reguliert sind (z. B. medizinische Geräte, Luftfahrt, Automobile),
- reine Dienstleistungen, die keine Produkte mit digitalen Elementen darstellen.

Für kritische Produkte mit hoher Relevanz für die Cybersicherheit gelten verschärfte Anforderungen, u. a. verpflichtende Konformitätsbewertung durch Dritte (Notified Bodies), bevor sie auf den Markt gelangen. Dazu können z. B. Betriebssysteme, Firewalls, Passwort-Manager, Smart Cards oder weit verbreitete Netzwerkkomponenten gehören.

Zusammenspiel des Cyber Resilience Act mit DORA

Auch wenn Banken, Versicherungen, Zahlungsinstitute oder Wertpapierfirmen nicht unmittelbar unter den Cyber Resilience Act fallen, sind sie mittelbar betroffen – denn nahezu alle IT-Systeme und -Produkte, auf die sie angewiesen sind, stammen von Herstellern, die CRA-pflichtig sind. Das hat zwei Konsequenzen:

1. **Höhere Sicherheit in der Supply Chain**: Der CRA sorgt dafür, dass Standardsoftware, Sicherheitslösungen und Infrastrukturprodukte ein

durchgängig höheres Sicherheitsniveau aufweisen.
2. **Neue Prüfpflichten im Auslagerungsmanagement**: DORA verlangt von Finanzunternehmen, Risiken aus der Nutzung von Drittprodukten aktiv zu steuern. Künftig wird die Frage, ob ein Anbieter oder Produkt CRA-konform ist, ein zentraler Bestandteil von Due Diligence, Vertragsgestaltung und Monitoring sein.

Für Banken, Zahlungsinstitute, E-Geld-Institute, Versicherer, Wertpapierfirmen und alle anderen Verpflichteten nach DORA bedeutet der CRA also eine indirekte, aber wichtige Ergänzung:

- DORA verpflichtet Finanzunternehmen zu einem robusten IKT-Risikomanagement, zur kontinuierlichen Überwachung der IKT-Resilienz und zu einem strengen Auslagerungsmanagement.
- Der CRA erhöht parallel die Produktsicherheit der digitalen Elemente, auf die sich Finanzunternehmen verlassen – sei es Core-Banking-Software, Cloud-Services, Security-Tools oder Netzwerkinfrastruktur.

Das Ergebnis ist ein doppelter Schutzschirm. Während DORA (Digital Operational Resilience Act) unmittelbar für Banken und Finanzdienstleister gilt und deren IKT-Risiko- und Resilienzmanagement reguliert, stärkt der CRA die vorgelagerte Ebene: die Produktsicherheit. DORA-Verpflichtete müssen künftig bei der Auswahl und Überwachung von IKT-Drittanbietern darauf achten, dass diese ihre Produkte CRA-konform entwickeln und betreiben.

Praktische Auswirkungen für DORA-Verpflichtete:

Auch wenn der Cyber Resilience Act keine unmittelbaren Pflichten für Banken oder Finanzdienstleister begründet, ergeben sich spürbare Folgen:

- **Beschaffung & Vendor Management:** CRA-Pflichten sollten in Due-Diligence- und Vertragsprozesse einfließen.
- **Outsourcing & Drittanbietersteuerung:** Bei kritischen IKT-Dienstleistern (z. B. Cloud- oder Kernbanksystem-Anbieter) ist zu prüfen, ob deren Produkte CRA-konform sind.
- **IKT-Risikomanagement**: CRA-relevante Informationen, etwa zu Schwachstellenmeldungen, müssen in DORA-konforme Risikoprozesse integriert werden.

- **Compliance-Synergien:** Die Meldepflichten von Herstellern liefern zusätzliche Datenpunkte für das interne Incident-Reporting nach DORA.

Fazit

Der Cyber Resilience Act ist kein Finanzmarktgesetz – aber er verändert die Rahmenbedingungen, unter denen DORA-Verpflichtete ihre IT betreiben. Künftig werden digitale Produkte nur noch mit CE-Siegel für Cybersicherheit in den Markt gelangen. Für Banken, Zahlungsdienstleister, Wertpapierfirmen, Versicherer und andere DORA-Verpflichtete bedeutet das: höhere Produktsicherheit in der Lieferkette, neue Anforderungen an das Auslagerungsmanagement und zusätzliche Schnittstellen im IKT-Risikomanagement.

Wer DORA und Cyber Resilience Act zusammen denkt, schafft einen echten Wettbewerbsvorteil: mehr Resilienz, weniger Risiko – und Vertrauen in die eigene digitale Infrastruktur.

Praxiswissen für Ihren Erfolg im Job

Seminare zu Kredit und Finanzierung

Erfahren Sie in unseren Weiterbildungen praktisches und aktuelles Know-how zu unterschiedlichen Themen der Kredit- und Bonitätsanalyse sowie Kreditvergabe und Finanzierung. Jetzt informieren.

e-Learning – Klicken und Lernen

Das FORUM Institut bietet mit hochwertigen e-Learning-Programmen eine flexible Weiterbildungsform. Entscheiden Sie selbst, wann und wo Sie lernen.
Jetzt testen.

Inhouse-Seminare – Maßgeschneiderte Lösungen

Alle unsere Seminare eignen sich auch hervorragend als Inhouse-Training.
Jetzt individuelles Angebot anfordern.

FORUM · Institut für Management GmbH • Postfach 10 50 60 • 69040 Heidelberg • Germany
Telefon: +49 6221 500-500 • Fax: +49 6221 500-555 • www.forum-institut.de