VÖB DIGITAL

EU-Regulierungen zur Cybersicherheit im Finanzsektor: Abgrenzung und Bedeutung für Banken

Die digitale Transformation und die zunehmende Zahl an Cyberbedrohungen stellen für Banken und Finanzinstitute enorme Herausforderungen dar. Die Europäische Union reagiert mit mehreren regulatorischen Maßnahmen, die darauf abzielen, die Cybersicherheit und digitale Resilienz zu stärken. Drei zentrale Rahmenwerke sind der Cyber Resilience Act (CRA), der Digital Operational Resilience Act (DORA) und die Network and Information Systems Directive (NIS 2). Diese Vorschriften haben unterschiedliche Schwerpunkte und Anforderungen, betreffen jedoch alle auch den Bankensektor. Im Folgenden werden Regelwerke abgegrenzt und ihre jeweilige Bedeutung für Banken erläutert.

Cyber Resilience Act (CRA): Fokus auf IT-Produkte und -Dienste

Der Cyber Resilience Act (CRA), der Ende 2024 veröffentlicht wurde, verfolgt das Ziel, die Cybersicherheit von Produkten und Dienstleistungen auf dem EU-Markt zu erhöhen. Im Mittelpunkt steht die Verpflichtung, dass alle Produkte, die in die EU eingeführt oder innerhalb der Union verkauft werden, eine ausreichende Sicherheitsresilienz gegenüber Cyberbedrohungen aufweisen. Auch wenn die Vorgaben aus der Verordnung erst ab dem 11. Dezember 2027 anzuwenden sind, gelten die Artikel 14 (Meldewesen bei Schwachstellen) jedoch bereits ab dem 11. September 2026, und Kapitel IV (Artikel 35 bis 51, Notifizierung bei Konformitätsbewertung) ab dem 11. Juni 2026.

Bedeutung für Banken: Banken sind vor allem dann betroffen, wenn sie IT-Produkte oder -Dienste erwerben oder selbst entwickeln, wie beispielsweise Softwarelösungen, Netzwerkausrüstung oder Cloud-Dienste. Der CRA verlangt, dass alle von Banken eingesetzten IT-Produkte bestimmte Sicherheitsstandards erfüllen, um potenzielle Schwachstellen in der Cybersicherheit zu minimieren. Der Fokus liegt hier nicht auf der Bankinfrastruktur selbst, sondern auf den Produkten, die für den Betrieb der Bank von entscheidender Bedeutung sind.

DORA (Digital Operational Resilience Act): Stärkung der Resilienz im Finanzsektor

Der Digital Operational Resilience Act (DORA) wurde speziell für den Finanzsektor entwickelt, um sicherzustellen, dass Banken und andere Finanzinstitute gegen IKT-bezogene Risiken (Information and Communication Technology) gewappnet sind. Ziel ist es, die digitale Resilienz zu erhöhen und den Schutz vor Ausfällen und Störungen zu gewährleisten, die die Geschäftskontinuität gefährden könnten. DORA legt besonderen Wert darauf, dass Finanzinstitute auf ICT-Ausfälle vorbereitet sind und nach einem Vorfall schnell wieder arbeitsfähig sind.

Bedeutung für Banken: Für Banken bedeutet DORA, dass sie robuste Maßnahmen zur Risikominderung implementieren müssen, um IKT-Ausfälle zu vermeiden und sich von ihnen schnell zu erholen. Zu den Anforderungen gehören unter anderem die Entwicklung von Notfallplänen, regelmäßige Tests der Resilienz gegenüber IKT-Störungen und die Absicherung gegen digitale Bedrohungen. Es geht hierbei vor allem um die Sicherstellung der operationellen Resilienz, die den stabilen Betrieb der Bank auch bei IT-Ausfällen oder Cyberangriffen garantiert.

NIS 2 (Network and Information Systems Directive): Cybersicherheit von Netzwerken und Informationssystemen

Die Network and Information Systems Directive (NIS 2) verfolgt das Ziel, die Cybersicherheit für alle EU-Mitgliedstaaten zu verbessern und sicherzustellen, dass kritische Infrastrukturen, darunter auch Banken, bestmöglich geschützt sind. NIS 2 richtet sich an Unternehmen und Organisationen, die wesentliche Dienste bereitstellen, und verpflichtet diese zur Umsetzung strengerer Sicherheitsvorkehrungen, um Cybervorfälle zu vermeiden und angemessen darauf zu reagieren.

Bedeutung für Banken: Als Betreiber wesentlicher Dienste fallen Banken unter die NIS 2. Diese Verpflichtung umfasst unter anderem die Einführung robuster Sicherheitsmaßnahmen zur Abwehr von Cyberangriffen, regelmäßige Risikobewertungen und die Meldung von Cybervorfällen an die zuständigen Behörden. Banken müssen ihre Netzwerke und Informationssysteme dauerhaft sichern und gewährleisten, dass diese auch im Falle eines Cyberangriffs oder einer Störung weiterhin betriebsfähig bleiben. Die NIS 2 stellt sicher, dass Finanzinstitute bei einem Vorfall schnell reagieren und die Auswirkungen auf die Nutzer und Kunden minimieren.

Abgrenzung der drei Regelwerke

Obwohl alle drei Regulierungen dem Ziel dienen, die Cybersicherheit und Resilienz zu verbessern, haben sie unterschiedliche Schwerpunkte:

- Der CRA konzentriert sich auf die Sicherheit von IT-Produkten und -Diensten und fordert von Banken, dass die von ihnen eingesetzten Technologien den erforderlichen Sicherheitsstandards entsprechen. Dabei geht es primär um die Produkte, die Banken kaufen oder entwickeln, um ihre Dienstleistungen zu erbringen.
- DORA zielt auf die operationelle Resilienz von Finanzinstituten ab. Banken müssen sicherstellen, dass sie im Falle eines IKT-Versagens handlungsfähig bleiben, indem sie entsprechende Notfallpläne entwickeln, Resilienztests durchführen und ihre Reaktionsfähigkeit auf IKT-bezogene Vorfälle optimieren.
- Die NIS 2 legt den Fokus auf die Cybersicherheit von Netzwerken und Informationssystemen und verlangt von Banken, dass sie ihre IT-Infrastruktur gegen Bedrohungen absichern und gegebenenfalls Cybervorfälle melden.

Zusammenfassung: Die Relevanz der Regulierungen für Banken

Für Banken bedeutet dies, dass sie alle drei regulatorischen Rahmenwerke berücksichtigen müssen, um ihre Cybersicherheit und Resilienz auf einem hohen Niveau zu halten:

- Der **CRA** verpflichtet Banken sicherzustellen, dass alle von ihnen eingesetzten IT-Produkte und -Dienste den Sicherheitsanforderungen entsprechen, um mögliche Schwachstellen zu vermeiden.
- Mit **DORA** müssen Banken ihre operationelle Resilienz stärken und sicherstellen, dass sie auch bei einem IKT-Ausfall handlungsfähig bleiben und ihre Dienstleistungen fortführen können.
- **NIS 2** erfordert, dass Banken ihre Netzwerke und Informationssysteme gegen Cyberbedrohungen schützen und Cybervorfälle schnell und effektiv melden.

Der VÖB wird sich weiter für rechtlichen Klarheit und die Vermeidung von Doppelregulierung einsetzen – insbesondere bei überlappenden und verwandten Fragestellungen, die über mehrere Regelwerke verteilt sind. Dazu gehört auch eine Einschränkung oder einen Ausschluss der CRA-Anwendung auf bestimmte Produkte, wenn sektorspezifische Vorschriften wie DORA ein gleichwertiges oder höheres Schutzniveau gewährleisten.

VÖB DIGITAL

Über VÖB Digital

Die Digitalisierung verändert das Bankgeschäft tiefgreifend und stellt Banken vor enorme Herausforderungen, denen es aktiv zu begegnen gilt. Diesen Transformationsprozess wollen wir mit unserem Newsletter VÖB Digital beleuchten – aber auch aktiv mitgestalten. Mit VÖB Digital zeigen wir nicht nur Herausforderungen, sondern auch Chancen auf, suchen nach Lösungen und stellen Entwicklungsperspektiven dar.

Sie wollen VÖB Digital abonnieren?

*Dann schreiben Sie bitte eine E-Mail an **presse@voeb.de**.*
Geben Sie einfach den Betreff „Anmeldung VÖB Digital“ an.

*Alle VÖB-Newsletter können Sie zudem unter **www.voeb.de/publikationen/newsletter** bestellen und abbestellen.*

IMPRESSUM
Bundesverband Öffentlicher Banken Deutschlands, VÖB
Lennéstraße 11, 10785 Berlin | Telefon: 030 8192-0
E-Mail: presse@voeb.de | Internet: www.voeb.de
Redaktion: Team Presse und Kommunikation,
Bereich Zahlungsverkehr und Digitalisierung
Redaktionsschluss: 14. Januar 2025
Foto: shutterstock, whiteMocca
Registernummer im Transparenz-Register der EU: 0767788931-41