"Dora" beschert Finanzunternehmen neue Cyberabwehr-Pflichten

EU-Regelung muss spätestens 2025 in nationales Recht überführt sein

Vor allem der Finanzsektor sollte "Dora" im Auge behalten, denn es stehen komplexe Verpflichtungen bevor

Mit dem Digital Operational Resilience Act, kurz Dora, schafft die EU neue Verpflichtungen für das Management von Risiken bei Cybersicherheit sowie Informations- und Kommunikationstechnologien (ITK) im Finanzsektor. Betroffen sind nicht nur nahezu alle Finanzunternehmen, sondern auch ITK-Dienstleister.

In Kraft getreten ist Dora (nachzulesen unter **eur-lex.europa.eu**) bereits im Januar 2023 ; nun läuft die zweijährige Umsetzungsfrist. Das Bundesfinanzministerium verfolgt das Ziel, die EU-Verordnung noch 2023 in nationales Recht zu überführen und einen Entwurf für das Umsetzungsgesetz vorzulegen.

Zwar ist mit dem Wirksamwerden der Verordnung auf nationaler Ebene erst zum Jahreswechsel 2024/25 zu rechnen, aufgrund der Komplexität der neuen Anforderungen sollten sich Finanzinstitute und Aufsichtsbehörden aber schon jetzt mit den Inhalten vertraut machen. Im Fokus stehen dabei der Aufbau von IKT-Risikomanagementsystemen, Kontroll- und Überwachungsmaßnahmen sowie neben den bestehenden Meldepflichten nach der Datenschutz-Grundverordnung auch neue an die jeweils zuständigen Aufsichtsbehörden.

Regelmäßige Risikokontrollen

Zentrales Element von Dora ist die regelmäßige Evaluierung der Abwehrbereitschaft gegen Cyberrisiken. Mithilfe von Schwachstellenbewertungen und -scans, Penetrationstests, Netzsicherheitsbewertungen, Open-Source-Analysen, Überprüfungen der physischen Sicherheit, Scans von Softwareprodukten, wenn möglich Quellcodeüberprüfungen, Kompatibilitäts- und Leistungstests sowie End-to-End-Tests müssen kritische ITK-Systeme künftig mindestens einmal jährlich auf Einfallstore für Cyberangriffe überprüft werden.

Vornehmen sollen die Prüfungen externe Dienstleister, die im Bereich Penetrationstests besonders akkreditiert und zertifiziert werden, über technische und organisatorische Fähigkeiten verfügen und spezifische Fachkenntnisse in den Bereichen Bedrohungsanalyse, Penetrationstests und Red-Team-Tests nachweisen können. Lediglich im Ausnahmefall und nur wenn spezifische Bedingungen eingehalten werden, können interne Tester zum Einsatz kommen. Diese müssen aber durch die Aufsichtsbehörden zugelassen werden. Es gilt dabei auch Interessenkonflikte durch Design und Ausführung der Tests auszuschließen. Die für den Test erforderlichen Bedrohungsinformationen müssen darüber hinaus von einem unabhängigen dritten Unternehmen stammen.

Umfangreiche Meldepflichten

Zudem vereinheitlicht Dora die Meldepflichten bei schwerwiegenden ITK-Vorfällen und weitet diese auf den gesamten Finanzsektor aus. So werden Finanzunternehmen verpflichtet, einen Managementprozess zur Überwachung und Protokollierung ITK-bezogener Sicherheitsvorfälle einzurichten. Schwerwiegende Vorfälle müssen den Finanzaufsichtsbehörden gemeldet werden. Zusätzlich können Finanzinstitute sich bei erkannten Cyberbedrohungen freiwillig an die Aufsicht wenden.

Auch externe Dienstleister betroffen

Grundsätzlich gilt Dora für alle Banken und Kreditinstitute, Versicherungs- und Rückversicherungsunternehmen, Investmentfirmen, Zentralverwahrer, Dienstleister für Krypto-

Assets, Zahlungsdienstleister und elektronische Zahlungsanbieter, Kreditratingunternehmen, Kapitalverwaltungsunternehmen, Dienstleister im Bereich des Crowdfunding, Entwickler von Banking-Apps, Hersteller von Geldautomaten sowie für weitere Unternehmen wie Transaktions- und Verbriefungsregister, Handelsplätze und Datenbereitstellungsdienste – in der Summe als "Finanzunternehmen" definiert.

Ausgenommen sind einzelne Unternehmensgruppen wie Verwalter alternativer Investmentfonds und Einrichtungen der betrieblichen Altersversorgung, Versicherungsvermittler in Nebentätigkeit sowie kleine Versicherungsvermittler und Rückversicherungsvermittler und kleine Unternehmen mit kumulativ weniger als zehn Mitarbeitern beziehungsweise unter zehn Millionen Euro Bilanzsumme.

Des Weiteren gilt Dora nicht für Hardwarehersteller, allgemeine oder elektronische Kommunikationsdienste, wohl aber für externe ITK-Anbieter, die digitale Dienste und Datendienste erbringen, einschließlich Anbietern von Cloud-Computing-Diensten, Software, Datenanalysediensten und Rechenzentren. Finanzinstitute sind mit der neuen Verordnung verpflichtet, ein Verzeichnis ihrer ITK-Verträge mit Dritten zu führen und den Aufsichtsbehörden auf Verlangen vorzulegen. Außerdem müssen sie die ITK-Dienstleister vor Vertragsabschluss sorgfältig prüfen.

Gemäß Dora müssen die Drittanbieter zudem bestimmte IT-Sicherheitsstandards einhalten – und die Verträge haben Kündigungsmöglichkeiten für bestimmte Szenarien zu enthalten. Werden kritische oder wichtige Funktionen von den Finanzinstituten outgesourct, kommen zusätzliche Pflichten hinzu. Die Aufsichtsbehörden werden ermächtigt, weitere Vorgaben einschließlich technischer Standards für solche Verträge zu definieren.

Quelle: DIHK, Katharina Lehmann, Artikel vom 18.07.2023
URL: https://www.dihk.de/de/themen-und-positionen/wirtschaft-digital/daten-und-informationssicherheit/-dora-beschert-finanzunternehmen-neue-cyberabwehr-pflichten--99348