DORA: Neue EU-Vorgaben sollen digitale Systemstabilität verbessern

VON PEGGY STEFFEN | LEITERIN RISIKOMANAGEMENT

Finanzunternehmen nutzen immer mehr externe Anbieter für ihre IT und Software. Die Systeme in der Informations- und Kommunikationstechnik (IKT) werden so zunehmend komplexer und müssen besser gegen Ausfälle und Cyberangriffe geschützt werden. Die EU-Gesetzgeber haben Ende 2022 mit DORA (Digital Operational Resilience Act) neue Anforderungen verabschiedet, um die digitale Systemstabilität in der Finanzwirtschaft zu stärken. DORA ist die erste EU-Verordnung, die einheitliche Vorgaben unmittelbar für den gesamten europäischen Finanzmarkt aufstellt. Ab dem 17. Januar 2025 müssen alle beaufsichtigten Unternehmen wie Banken, Versicherer, Fondsgesellschaften und Wertpapierinstitute ihre internen Prozesse an DORA neu ausgerichtet haben.

Ergänzend zur DORA-Verordnung erarbeiten die EU-Behörden sektorübergreifend und in enger Abstimmung zahlreiche weitere Details über technische Umsetzungs- und Regulierungsstandards. Diese werden voraussichtlich erst Ende 2024 final vorliegen. Die nationale Umsetzung erfolgt über das Finanzmarktdigitalisierungsgesetz, für das die Bundesregierung Ende 2023 einen Gesetzentwurf verabschiedet hat. Da die EU-Gesetzgeber mit der DORA-Verordnung eine Regelungslücke schließen, müssen auch die nationalen und EU-Behörden ihre aktuellen Aufsichtspraktiken (z. B. ESMA-Leitlinien zu Cloud-Auslagerungen, EBA-Leitlinien zur Auslagerung, BaFin-Rundschreiben KAIT, BAIT, VAIT) überprüfen und anpassen.

Mit DORA kommt auf die betroffenen Unternehmen ein hoher operativer Aufwand zu. Dieser betrifft insbesondere die internen Governance- und Risikomanagementprozesse sowie den Umgang mit Störfällen. Dabei müssen sie für wesentliche Störfälle neue Meldewege sowie Testverfahren zur Prüfung der Widerstandsfähigkeit ihrer Systeme aufsetzen. Ein Schwerpunkt der DORA-Umsetzung liegt auf den Vertragsbeziehungen zwischen den Anbietern von IKT-Dienstleistungen wie Cloud-Computing, Software, Hardware oder Datenanalysen und den beaufsichtigten Finanzunternehmen. Letztere müssen künftig alle Verträge nebst Unterbeauftragungen überwachen und in einem Informationsregister dokumentieren. Daneben müssen sie die Konzentrationsrisiken und Abhängigkeiten bewerten und überwachen, die sich durch die Inanspruchnahme der IKT-Dienstleistungen für sie ergeben. Schließlich führt DORA erstmals Überwachungsbefugnisse der EU-Behörden für kritische IKT-Drittdienstleister ein, von denen voraussichtlich insbesondere große Cloudanbieter betroffen sein werden. Der Branche bleibt noch ein halbes Jahr Zeit, um sich abschließend vorzubereiten. ■

Informationen zur aktuellen Entwicklung erhalten Sie unter **www.bvi.de** oder im **BVI direkt** für unsere Mitglieder.