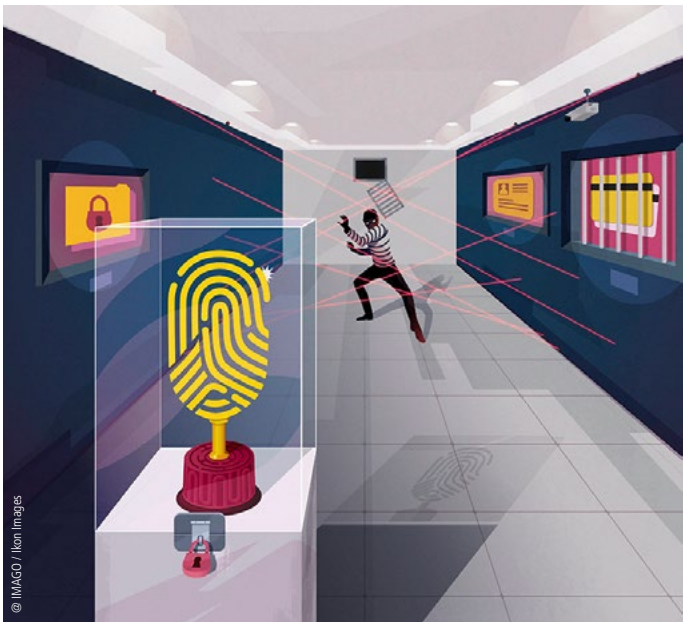
DORA – IT-Sicherheit im Finanzsektor

Am 27. Dezember 2022 wurde der „Digital Operations Resilience Act" („DORA") im Amtsblatt der Europäischen Union veröffentlicht. Regelungsgegenstand ist die Stärkung der digitalen operativen Resilienz von im Finanzsektor tätigen Unternehmen. Sie sollen Cyberbedrohungen bestmöglich vermeiden und mit ihnen angemessen umgehen können. Für diese Zwecke bringt DORA als erstes europäisches branchenspezifisches Gesetz zur IT-Sicherheit eine Fülle unterschiedlicher Pflichten für zahlreiche Marktteilnehmer mit sich. Deren Erfüllung wird mit hohen Aufwänden verbunden sein, aber zugleich das Potential mit sich bringen, einen neuen Marktstandard zu etablieren, wie Dr. Thorsten Ammann und Yannick Zirnstein erläutern.

„Ziel von DORA ist es, vor dem Hintergrund stetig steigender Cybersicherheitsrisiken im Finanzsektor europaweit einheitliche Regelungen zu etablieren", erklären Ammann und Zirnstein. So solle die IT-Sicherheit im europäischen Binnenmarkt auf ein einheitliches Niveau angehoben werden.

Derzeit hätten die vielen nationalen Regulierungsinitiativen und Aufsichtskonzepte auf Ebene der Mitgliedstaaten angesichts des grenzüberschreitenden Charakters von Informations- und Kommunikationstechnologie-Risiken nur eine begrenzte Wirkung zum Schutz gegen Cyberattacken. Außerdem seien unter den Mitgliedstaaten nur unzureichend abgestimmte nationale Alleingänge in der Vergangenheit Grund für Überschneidungen und erhebliche administrative Mehraufwände und Mehrkosten gewesen. Davon seien vor allem grenzüberschreitend tätige Finanzunternehmen betroffen gewesen.


© IMAGO / Ikon Images

Cyberbedrohung vermeiden: DORA soll als erstes europäisches branchenspezifisches Gesetz mehr IT-Sicherheit im Finanzsektor bringen.

Dem solle DORA nun mittels eines detaillierten, umfassenden, europaweit einheitlichen Regelungsrahmens zur Erreichung eines hohen Maßes an digitaler Betriebsstabilität für Finanzunternehmen entgegenwirken.


© Thorsten Ammann

Dr. Thorsten Ammann berät national und international operierende Unternehmen zu allen Belangen des Informationstechnologierechts mit besonderer Fokussierung auf Digitale Transformationsprojekte und Disruptive Technologien, insbesondere Blockchains, Künstlicher Intelligenz, IoT und Smart Factories.


© Yannick Zirnstein

Yannick Zirnstein berät nationale und internationale operierende Unternehmen zu allen Aspekten des deutschen und europäischen Rechts in den Bereichen Informationstechnologie, Cybersecurity und Datenschutz.

Hierzu führe die Verordnung detaillierte und umfassende Mindestanforderungen, insbesondere hinsichtlich des Risikomanagements im Bereich der Informations- und Kommunikationstechnologie (IKT) und des IKT-Drittparteienmanagements, ein, wie Ammann und Zirnstein erläutern. So sehe DORA verschiedene Standards sowie Regelungen für eine effizientere Koordinierung und Beaufsichtigung betroffener Unternehmen vor. Dazu gehöre u.a., dass IKT-Systeme regelmäßig geprüft und Sicherheitsvorfälle künftig gemeldet werden müssen. Außerdem sollen zuständige Aufsichtsbehörden von erweiterten Befugnissen profitieren. Dies insbesondere um auch solche Risiken verlässlich überwachen und steuern zu können, die sich aus oder im Zusammenhang mit der Abhängigkeit von Finanzunternehmen von eingeschalteten IKT-Drittdienstleistern, beispielsweise im Rahmen von Auslagerungen oder Ausgliederungen, ergeben. Insoweit treffe DORA zumindest mittelbar auch IT Services Provider.

Ammann und Zirnstein sehen in DORA einen elementaren Bestandteil der Cybersicherheitsstrategie der EU mit wesentlichen, sinnvollen Regelungen zur Schaffung eines einheitlich hohen Schutzniveaus für den Finanzsektor. Angesichts der Herausforderungen für Finanzunternehmen erscheint ihnen die Übergangsfrist von inzwischen weniger als 24 Monaten (DORA ist 20 Tage nach ihrer Veröffentlichung im Amtsblatt der Europäischen Union in Kraft getreten) als „durchaus sportlich". Betroffenen Unternehmen raten die beiden Autoren, bereits jetzt bestimmte Maßnahmen einzuleiten, um den knappen Zeitraum möglichst effizient zu nutzen:

„Im Bereich des Governance- und Kontrollrahmens, des IKT-Risikomanagementrahmens und der Prüfpflichten sollten Finanzunternehmen mittels einer Gap-Analyse die neuen Vorgaben mit sämtlichen bereits vorhandenen Prozessen abgleichen, um so festzustellen, für welche Prozesse welcher spezifische Handlungsbedarf besteht." Das Gleiche gelte für das IKT-Drittdienstleistermanagement. Neben einem Abgleich der bereits vorhandenen Prozesse zu Maßnahmen vor der Einbindung eines IKT-Drittdienstleisters mit den Vorgaben aus DORA sollten Finanzunternehmen sämtliche bestehenden IKT-Verträge im Hinblick auf Vertragsgegenstände, insbesondere deren kritische oder wichtige Funktionen prüfen. Sofern unter der Berücksichtigung der Vorgaben aus DORA Nachbesserungsbedarf bestehe, sollten Nachverhandlungen mit Dienstleistern frühzeitig initiiert werden. „Dies gilt insbesondere vor dem Hintergrund, dass sämtliche von DORA betroffenen Marktteilnehmer in den nächsten zwei Jahren mit einer überbordenden Anzahl an neuen Verhandlungen oder Nachverhandlungen mit sämtlichen ihrer Kunden, die als Finanzunternehmen gelten, verstärkt beschäftigt sein dürften", warnen Ammann und Zirnstein. *chk*

Einen ausführlichen Beitrag zum „Digital Operations Resilience Act" (DORA) von Dr. Thorsten Ammann und Yannick Zirnstein lesen Sie im Compliance-Berater (CB 2023, 21).