DORA

Dora ist das neue Schreckgespenst der Finanzbranche. Hinter dem Namen verbirgt sich eine EU-Verordnung über die digitale Resilienz im Finanzsektor. Sie wurde Ende 2022 beschlossen und soll dazu beitragen, die IT von Finanzunternehmen gegen Angriffe von außen zu härten und intern stabil und zuverlässig aufzustellen.

Die Verordnung betrifft die gesamte Informations- und Kommunikationstechnologie (IKT) von Finanzunternehmen. Die Verordnung verpflichtet Finanzunternehmen zu einer digitalen operationellen Resilienz, d.h. Fähigkeiten zu entwickeln, die Integrität und Zuverlässigkeit der IKT aufzubauen, um die Sicherheit der Netzwerk- und Informationssysteme zu gewährleisten, und die kontinuierliche Erbringung von Finanzdienstleistungen und deren Qualität, auch bei Störungen, zu unterstützen.

DORA verpflichtet die Unternehmen zu einem IKT-Risikomanagementrahmen, d.h. zu Strategien, Richtlinien und Verfahren, um die Computer-Software, Hardware und Server angemessen zu schützen, einschließlich der Räumlichkeiten von Rechenzentren und sensiblen Bereichen, damit diese vor Beschädigung und unbefugtem Zugriff gefeit sind. Durch IKT-Risikomanagementverfahren sollen die Risiken für die IKT ermittelt und reduziert werden.

Dazu ist erforderlich, den IKT-Risikomanagementrahmen zu ermitteln und zu klassifizieren, d.h. alle IKT-gestützten Unternehmensfunktionen, einschließlich Verantwortlichkeiten, zu ermitteln und zu klassifizieren. Durch IKT-Sicherheitsrichtlinien und Verfahren sollen Resilienz, Kontinuität und Verfügbarkeit der IKT-Systeme sichergestellt werden.

Finanzunternehmen sollen unnormale Aktivitäten umgehen erkennen, um Schwachstellen zu ermitteln. Dazu sind Erkennungsmechanismen und Kontrollebenen vorzusehen, z.B. automatische Warnmechanismen für Mitarbeiter. Zum Beispiel sollen Systeme erkennen, ob sie verzögert arbeiten oder einen höheren Energieverbrach aufweisen, was auf Schadsoftware oder andere Manipulationen hindeuten kann.

Für den Fall von Störungen und Manipulationen sollen IKT-Geschäftsfortführungsleitlinien dafür sorgen, dass sich Störungen im Geschäftsablauf bei IKT-Störungen in Grenzen halten. Dazu sollen Eindämmungsmaßnahmen und Technologien vorgehalten werden, einschließlich Krisenkommunikationspläne. Durch Datensicherungen und Wiedergewinnungs- und Wiederherstellungsverfahren an einem sekundären Verarbeitungsort soll die Kontinuität der Geschäftsdurchführung gewährleistet sein. Das erfordert Sicherungssysteme, zweite Rechenzentren und ein stabiles Back-up für die gesamte IKT.

Mitarbeiter sollen Informationen über Schwachstellen und Cyberbedrohungen, IKT-bezogene Vorfälle, insbesondere Cyberangriffe, sammeln und schnell auf Sicherheitswarnungen reagieren können. Dazu sollen Qualität und Schnelligkeit bei der Durchführung forensischer Analysen gesteigert werden und wirksame Eskalationsverfahren bei Vorfällen innerhalb des Unternehmens vorliegen, einschließlich einer entsprechenden internen und externen Kommunikation.

All diese Maßnahmen sind nicht ganz neu. Bereits durch die bankaufsichtsrechtlichen Anforderungen an die IT (BAIT) hat die BaFin in einer Ergänzung zu den MaRisk entsprechende Maßnahmen angefordert. Da das aber nur ein Merkblatt der BaFin war und die Umsetzung der Branche leider nicht zur Zufriedenheit der Aufsichtsbehörden gereift war, wird das ganze nun europaweit in der EU-Verordnung DORA geregelt. Sie alle kennen wahrscheinlich die Rundmails der BaFin, in der diese immer wieder die Mangelhaftigkeit von Geschäftsorganisationen anprangert. Durch die Bank wurden bei Sonderprüfungen der Bundesbank in den einzelnen Kreditinstituten Missstände in der Geschäftsorganisation festgestellt. Diese beziehen sich zumeist auf die IT und die Nichteinhaltung der Anforderungen der BAIT. Diese Sonderprüfungen der Bundesbank im Auftrag der BaFin waren sehr intensiv und vor allen die größeren Institute können ein leidvolles Lied davon singen.

Durch DORA werden aber nicht alle Unternehmen über einen Kamm geschoren. An sich gilt DORA für Wertpapierfirmen und Versicherungsvermittler. Es gibt aber Ausnahmen für die von der MiFID II ausgenommenen 34 f Vermittler und für Versicherungsvermittler, bei denen es sich um Kleinstunternehmen oder kleine oder mittlere Unternehmen handelt. Das sind Unternehmen mit weniger als 50 Beschäftigten und einem Jahresumsatz bzw.einer Bilanzsumme von weniger als 2 Millionen Euro. Auch für „kleine und nicht verflochtene“ Wertpapierfirmen gibt es Erleichterungen. Nach Art. 16 DORA gelten für sie die detaillierten Vorgaben aus Art. 5-15 DORA nicht. Sie müssen aber immer noch

- über einen soliden und dokumentierten IKT-Risikomanagementrahmen verfügen,
- die Sicherheit und das Funktionieren aller IKT-Systeme fortlaufen überwachen,
- die Auswirkungen von IKT-Risiken minimieren,
- die rasche Ermittlung und Aufdeckung von IKT-Risiken und -Anomalien ermöglichen,
- die wesentliche Abhängigkeit von IKT-Drittdienstleistern ermitteln,
- die Kontinuität kritischer oder wichtiger Funktionen durch Geschäftsfortführungspläne und Wiederherstellungsmaßnahmen gewährleisten,
- die Wirksamkeit ihrer Schutzmaßnahmen regelmäßig testen.

Damit bleibt einer gewisser Grundaufwand aus DORA auch für kleine Wertpapierfirmen.

Alle Institute müssen IKT-bezogene Vorfälle erkennen und melden und hinsichtlich ihrer Schwere klassifizieren. Ein besonderer Augenmerk der DORA gilt dem Drittparteienrisiko, d.h. den Fällen der Auslagerung von IKT-Funktionen auf Dritte. Verträge mit IKT-Dienstleistern müssen bestimmte Rechte für die Finanzunternehmen gewährleisten. Die Qualität der Dienstleister muss überwacht, kontrolliert und gemonitort werden. Das Finanzunternehmen muss sich Inspektions-, Zugangs- und Auditrechte einräumen lassen. Vereinbarungen mit Dienstleistern müssen bei mangelhafter Qualität beendet werden können. Vor allem müssen dazu in den Verträgen alle Funktionen des Dienstleisters klar und vollständig beschrieben werden, notwendig sind Regeln zu den Standorten der Dienstleistungserbringung, zum Schutz von Daten, zur Sicherstellung des Zugangs, zur Beschreibung der Dienstleistungsgüte und zur vollständigen Berichterstattung des Dienstleisters.

DORA gilt ab dem 17. Januar 2025. Je früher Sie mit der Umsetzung beginnen, je besser.

Gerne halte ich Sie auf dem Laufenden
Ihr

Dr. Christian Waigel
Rechtsanwalt