TEIL II

DORA 2022: Die To-do-Liste für Banken

Ein Artikel von **Dunja Koelwel** | 01.03.2022 - 08:39

Der vorgeschlagene Rechtsakt zur digitalen Betriebsstabilität (Digital Operational Resilience Act, DORA) ist Teil eines Maßnahmenpakets zur Digitalisierung des Finanzsektors, das die Europäische Kommission Ende September 2020 vorgelegt hat. Mit dem Paket will die Kommission Europas Wettbewerbsfähigkeit und Innovation im Finanzsektor fördern. Andreas Bruckner, Manager, PPI, gibt eine Einschätzung, was 2022 zu erwarten ist.

Welche praktischen Auswirkungen hat DORA?

Andreas Bruckner : Die neue EU-Regelung zur digitalen Resilienz wird naturgemäß einiges an Arbeit mit sich bringen. So schreibt DORA vor, dass IT-Systeme robust und stabil auszulegen sind. Banken haben umfangreiche Notfallpläne und Maßnahmen zur Sicherstellung einer Business Continuity zu implementieren. Dies gilt insbesondere für Ausfälle kritischer Systeme, beispielsweise infolge von Cyberattacken. Diese Pläne sind regelmäßig auf ihre Durchführbarkeit zu testen. Dazu zählen auch – und das ist neu – periodische End-to-End- sowie Penetration-Tests zur Sicherung der digitalen Betriebsstabilität, und zwar unter Berücksichtigung sich verändernder IKT-Risikoszenarien. Die praktische Umsetzung der Pen-Tests wird eine Herausforderung, denn die externen Tester müssen sehr hohen Anforderungen genügen. Aktuell können dies nur wenige Firmen leisten.

Weitere Veränderungen gibt es bei den Berichtspflichten, die sich durch DORA nochmals erweitern. Sollte ein Risiko eintreten, ist die Aufsicht unmittelbar zu informieren. Dies gilt zukünftig auch für Ausfälle bei Drittanbietern. Banken tun gut daran, ihre Meldeverfahren entsprechend anzupassen, oder – soweit notwendig – neue zu entwickeln. Dabei ist es sinnvoll. Outsourcing-Partner in diese Reportings einzubeziehen. Im Sinne möglichst ressourcenschonender Prozesse ist es sinnvoll, interne Meldewege an den DORA-Erfordernissen auszurichten und so Doppelarbeiten zu vermeiden.

Gleichzeitig fordert die Richtlinie explizit, dass sich Europas Finanzinstitute untereinander über mögliche Cyberbedrohungen austauschen und so ihre Abwehrfähigkeiten verbessern. Soweit noch nicht geschehen, müssen Kreditinstitute also entsprechende Infrastrukturen und Abläufe schaffen sowie sich darüber klar zu werden, welche Informationen überhaupt geteilt werden sollen.

> *Veränderungen gibt es bei den Berichtspflichten, die sich durch DORA nochmals erweitern. Sollte ein Risiko eintreten, ist die Aufsicht unmittelbar zu informieren. Dies gilt zukünftig auch für Ausfälle bei Drittanbietern.*

Andreas Bruckner, Manager, PPI

Aspekte der Business Continuity und Meldepflicht

Was müssen Finanzunternehmen künftig bei der Wahl eines IKT-Drittanbieters beachten?

Andreas Bruckner: Die Aufsicht wird bei Auslagerungen von Geschäftsprozessen künftig noch genauer hinschauen, als sie es bislang schon tut. Die Anforderungen an die Auswahl des Drittanbieters steigen deutlich. Banken müssen sehr genau prüfen, ob dieser dauerhaft zur Erfüllung sämtlicher Pflichten für den zuverlässigen und sicheren IT-Betrieb in der Lage ist. Das hat naturgemäß Auswirkungen auf die künftige Vertragsgestaltung, die deutlich komplexer werden dürfte. Gleiches gilt für die Definition der Key Performance Indicators (KPIs) in den zugehörigen Service-Level-Agreements (SLA). Hier ist eine sehr engmaschige Kontrolle der Vertragspartner durch die Institute gefordert.

Auf der strategischen Seite sollten Kreditinstitute ihre Auslagerungsstrategie auf Kohärenz überprüfen. Außerdem müssen dort künftig Aspekte zur Bewertung der Drittanbieter, Business Continuity und Meldepflichten enthalten sein. Sofern ein Dienstleister mehrere Outsourcing-Verträge hält, ist eine Prüfung im Hinblick auf Konzentrationsrisiken angezeigt. Hier ist nicht völlig auszuschließen, dass Banken Vorgänge von einem Servicepartner zu einem alternativen Anbieter transferieren, um ihr Risikoprofil insgesamt zu verbessern. Neu ist zudem die Pflicht, die Aufsichtsbehörden bereits bei der Planung einer Auslagerung in Kenntnis zu setzen und nicht erst, wenn die Verträge unterschrieben sind.

An dieser Stelle noch die Anmerkung, dass zukünftig auch Outsourcing-Anbieter der Finanzaufsicht unterliegen können. Ob dies tatsächlich der Fall ist, hängt von den jeweiligen Gegebenheiten ab. Maßgeblich ist der Grundsatz: „Gleiche Tätigkeit, gleiches Risiko, gleiche Regeln“. Dieser gilt sowohl für Institute im Finanzsektor als auch für Drittanbieter.

DORA wird teuer

Die drei Kernziele von DORA sind: Vereinheitlichung bestehender europäischer und nationaler Standards und Vorgaben; Sicherstellung, dass Finanzunternehmen alle notwendigen Maßnahmen zur Absicherung gegen Cyberrisiken und -angriffe treffen; Etablierung eines Rechtsrahmens für die

direkte Überwachung von IT-Drittanbietern durch die Aufsichtsbehörden, wenn diese für Finanzunternehmen tätig sind. Was ist Ihrer Meinung nach der kniffeligste Part für Banken und Versicherungen?

Andreas Bruckner: Das Kniffelige ist die Kombination aus neuen Vorschriften zu Outsourcing, Business Continuity und Meldevorschriften. Hier kommt eine Menge Arbeit auf die Banken zu. So ist davon auszugehen, dass nahezu alle Outsourcing-Verträge Überarbeitungsbedarf aufweisen. Möglicherweise stehen sogar erzwungene Anbieterwechsel ins Haus, sollten die Konzentrationsrisiken zu groß werden oder falls – und auch das ist denkbar – der Vertragspartner als kritisch eingestuft wird.

Die Gültigkeit der Vorschriften zu Maßnahmen bei Notfallplänen und zur Sicherstellung der Business Continuity auch für Drittanbieter verursachen darüber hinaus Arbeit bei den Instituten. Denn die Finanzdienstleister werden gezwungen sein zu prüfen ob die Vorgaben eingehalten werden. Die Unternehmen müssen sich dafür weitreichende Prüfungsrechte einräumen lassen. Anders wird der Nachweis kaum möglich sein, es sei denn, der Vertragspartner stellt die Ergebnisse durchgeführter Tests zur Verfügung.

Andreas Bruckner ist Manager im Bereich Gesamtbanksteuerung und Regulatorik bei PPI. Er berät seit zehn Jahren Banken und Finanzdienstleister rund um regulatorische Fragestellung und deren Umsetzung in klassischen und agilen Projekten. In seinen aktuellen Projekten erarbeitet er mit und für seine Kunden Lösungen zum Management von IKT-Risiken.

Das alles wird teuer, denn die Dienstleister werden die ins Haus stehenden Kosten zur Anpassung ihrer Infrastrukturen und Prozesse sicherlich weiterreichen. Hinzu kommt, dass sich eventuell einige Finanzinstitute neue Outsourcing-Partner suchen müssen. Denn es ist keinesfalls klar, dass alle Anbieter die künftigen Anforderungen auch tatsächlich erfüllen können.