expertenReport

Quelle: Experten/KI

DORA nach dem ersten Stresstest: Warum Drittanbieter zum Aufsichtsrisiko werden

Ute Pappelbaum

Nicht Hacker sind derzeit das größte operative Risiko für Europas Finanzbranche. Sondern Dienstleister.

Damit verschiebt sich der Fokus der Aufsicht. Die entscheidende Frage lautet nicht mehr, wie gut einzelne Unternehmen gegen Angriffe geschützt sind. Sondern wie stabil die Infrastruktur ist, auf der ganze Marktsegmente gleichzeitig aufbauen.

Die eigentliche Botschaft von DORA hat mit Cybersecurity nur teilweise zu tun

Viele Banken, Versicherer und Finanzvertriebe haben DORA zunächst als weiteres IT-Sicherheitsregime verstanden. Diese Lesart greift zu kurz.

Die Verordnung verfolgt ein anderes Ziel. Sie soll sicherstellen, dass Finanzunternehmen auch dann funktionsfähig bleiben, wenn kritische digitale Systeme ausfallen. Dabei spielt es keine Rolle, ob die Ursache im eigenen Haus liegt oder bei einem externen Anbieter entsteht.

Für die Aufsicht wird damit die gesamte digitale Wertschöpfungskette relevant.

Cloud-Anbieter, Rechenzentren, Softwarehäuser, Maklerverwaltungsprogramme, Vergleichsplattformen und Outsourcing-Dienstleister werden zu Bestandteilen des operationellen Risikoprofils eines Unternehmens.

Der Blick verschiebt sich vom einzelnen Institut auf die Infrastruktur, von der zahlreiche Institute gleichzeitig abhängen.

Die neue Verwundbarkeit heißt Konzentration

Die Digitalisierung der vergangenen Jahre folgte einer einfachen ökonomischen Logik.

Standardisierung senkt Kosten. Auslagerung erhöht Effizienz. Gemeinsame Plattformen beschleunigen Prozesse.

Genau deshalb konzentrieren sich heute zentrale Funktionen der Finanzwirtschaft auf wenige Anbieter. Viele Versicherer arbeiten mit identischen Kernsystemen. Vermittler nutzen dieselben Vergleichsplattformen und Maklerverwaltungsprogramme. Große Teile der europäischen Finanzbranche laufen auf denselben Cloud-Infrastrukturen.

Was betriebswirtschaftlich sinnvoll erscheint, erzeugt jedoch eine neue Form von Verwundbarkeit.

Der DORA-Bericht zeigt, dass inzwischen rund ein Drittel aller schweren Vorfälle auf Ausfälle bei Drittanbietern zurückzuführen ist. Gleichzeitig hatten etwa ein Drittel aller gemeldeten Ereignisse grenzüberschreitende Auswirkungen. Die Risiken verlaufen damit längst nicht mehr entlang von Unternehmensgrenzen, sondern entlang gemeinsamer technischer Infrastrukturen.

Aus Sicht der Aufsicht entsteht daraus ein klassisches Konzentrationsproblem.

Je mehr Marktteilnehmer dieselben Systeme nutzen, desto größer wird die Wahrscheinlichkeit, dass ein einzelner Ausfall zahlreiche Unternehmen gleichzeitig trifft.

Das digitale Pendant zu „Too big to fail“

Die Finanzkrise hat die Aufsicht gelehrt, dass bestimmte Banken systemrelevant werden können.

DORA erweitert dieses Denken auf die digitale Welt.

Nicht mehr nur Institute können systemkritisch sein. Auch technische Infrastrukturen können eine Größe erreichen, bei der ihr Ausfall erhebliche Teile des Finanzsystems beeinträchtigt.

Der Bericht verweist ausdrücklich auf die Bedeutung kritischer ICT-Drittdienstleister und auf das DORA-Register of Information, mit dem die Aufsicht erstmals die vertraglichen Abhängigkeiten der Branche systematisch erfasst. Ziel ist es, Konzentrationen sichtbar zu machen, bevor sie zum Stabilitätsproblem werden.

Damit entsteht schrittweise eine neue Form der Finanzaufsicht: die Aufsicht über digitale Infrastruktur.

Warum Vermittler das Thema unterschätzen

Auf den ersten Blick scheint die Debatte vor allem große Banken und Versicherungskonzerne zu betreffen.

Tatsächlich sind Vermittler oft noch stärker von externen Systemen abhängig.

Maklerverwaltungsprogramme, Kundenportale, Vergleichsrechner, Dokumentenmanagement, digitale Signaturen oder KI-gestützte Anwendungen bilden heute den operativen Kern vieler Vermittlungsbetriebe.

Fällt eines dieser Systeme aus, steht nicht selten der gesamte Geschäftsbetrieb still.

Die relevante Frage lautet deshalb nicht, ob ein Vermittler unmittelbar unter DORA fällt.

Entscheidend ist, wie handlungsfähig das Unternehmen bleibt, wenn der wichtigste Dienstleister plötzlich nicht mehr erreichbar ist.

Die Aufsicht interessiert sich zunehmend für den Plan B

Die praktische Konsequenz aus DORA ist weitreichend.

Die Aufsicht prüft nicht mehr allein, ob Dienstleister vertraglich eingebunden sind. Sie interessiert sich zunehmend dafür, was im Störungsfall tatsächlich geschieht.

Gefragt wird nach Wiederanlaufzeiten, Exit-Strategien, Notfallkonzepten, Ersatzprozessen und Testnachweisen.

Ein Vertrag dokumentiert eine Beziehung.

Resilienz zeigt sich erst im Ausfall.

Genau deshalb gewinnen Notfallübungen und Wiederanlauftests an Bedeutung. DORA verschiebt den Schwerpunkt von Dokumentation auf Nachweisfähigkeit.

Digitalisierung wird zur Lieferkettenfrage

Der erste DORA-Bericht offenbart einen grundlegenden Zielkonflikt der digitalen Transformation.

Die Finanzbranche hat über Jahre Effizienzgewinne durch Standardisierung und Outsourcing realisiert. Diese Entwicklung hat Kosten gesenkt, Skaleneffekte geschaffen und Innovation beschleunigt.

Gleichzeitig entstanden neue Abhängigkeiten, die lange kaum sichtbar waren.

Je digitaler ein Unternehmen wird, desto stärker hängt seine Stabilität von der Stabilität externer Infrastrukturen ab.

Die digitale Lieferkette wird damit zu einem Risikofaktor, der strategisch gesteuert werden muss.

Erkenntnis für die Zukunft

Der erste DORA-Bericht verändert den Blick auf operative Risiken in der Finanzbranche.

Die zentrale Erkenntnis lautet nicht, dass Cyberangriffe gefährlich sind. Das war bereits bekannt. Neu ist die Einsicht, dass die größte Verwundbarkeit zunehmend dort entsteht, wo viele Unternehmen dieselben technischen Infrastrukturen nutzen.

Damit rückt eine Frage in den Mittelpunkt, die weit über IT-Sicherheit hinausgeht: Wie viel Konzentration verträgt die digitale Finanzwirtschaft?

DORA macht aus dieser Frage keine technische Detaildiskussion mehr. Die Verordnung behandelt sie als Stabilitätsfrage des gesamten Finanzsystems.

Was ist DORA eigentlich?

DORA (Digital Operational Resilience Act) ist die europäische Verordnung zur digitalen Betriebsstabilität von Finanzunternehmen. Ziel ist es, sicherzustellen, dass Banken, Versicherer und andere Finanzdienstleister auch bei IT-Ausfällen, Cyberangriffen oder Störungen bei Dienstleistern handlungsfähig bleiben. DORA betrachtet digitale Resilienz nicht nur als IT-Thema, sondern als Bestandteil der Unternehmenssteuerung.

Warum stehen Drittanbieter unter DORA plötzlich so stark im Fokus?

Der erste gemeinsame DORA-Bericht der europäischen Aufsichtsbehörden zeigt, dass viele schwere IKT-Vorfälle nicht durch Hackerangriffe, sondern durch Systemausfälle und externe Dienstleister verursacht wurden. Fällt ein kritischer Anbieter aus, können gleichzeitig zahlreiche Finanzunternehmen betroffen sein. Deshalb bewertet die Aufsicht heute nicht nur die Stabilität eines Instituts, sondern zunehmend auch dessen Abhängigkeiten entlang der digitalen Lieferkette.

Sind Cyberangriffe nicht mehr das größte Risiko?

Cyberangriffe bleiben ein erhebliches Risiko. Der DORA-Bericht zeigt jedoch, dass sie lediglich rund zehn Prozent der gemeldeten schweren IKT-Vorfälle ausmachten. Häufiger waren Systemfehler, technische Störungen oder externe Ereignisse. Die Aufsicht erkennt deshalb, dass die größte Verwundbarkeit oft in gemeinsamen Infrastrukturen und Dienstleisterabhängigkeiten liegt.

Betrifft DORA auch Versicherungsmakler und Vermittler?

Direkt oder indirekt ja. Selbst wenn kleinere Vermittler nicht denselben regulatorischen Pflichten wie große Versicherer oder Banken unterliegen, sind sie heute stark von Maklerverwaltungsprogrammen, Vergleichsrechnern, Kundenportalen oder Cloud-Diensten abhängig. Fällt ein solcher Anbieter aus, kann der Geschäftsbetrieb schnell zum Stillstand kommen. Die Frage lautet daher weniger, ob DORA unmittelbar gilt, sondern wie resilient das eigene Unternehmen gegenüber Dienstleisterausfällen ist.

Was erwartet die Aufsicht künftig konkret?

Die Aufsicht möchte wissen, welche Dienstleister geschäftskritisch sind, welche Prozesse von ihnen abhängen und wie Unternehmen auf einen Ausfall reagieren würden. Gefragt wird nach Notfallplänen, Wiederanlaufzeiten, Exit-Strategien, Datensicherungen und regelmäßigen Tests. Ein Vertrag mit einem Dienstleister reicht künftig nicht mehr aus. Entscheidend ist der Nachweis, dass ein Unternehmen auch dann funktionsfähig bleibt, wenn ein zentraler Anbieter ausfällt.

Versicherungs- und Finanznachrichten

expertenReport

https://www.experten.de/id/4950196/DORA-nach-dem-ersten-Stresstest-Warum-Drittanbieter-zum-Aufsichtsrisiko-werden/