CENTRE DE DROIT
BANCAIRE ET FINANCIER

FINMA Aufsicht

Ein neues Rundschreiben betreffend operationelle Risiken

Par Célian Hirsch le 19 Dezember 2022

Neue internationale Standards und starke Entwicklungen im Bereich der Digitalisierung. Dies sind die beiden Faktoren, die die FINMA als Gründe für die Überarbeitung ihres Rundschreibens 08/21 zu operationellen Risiken anführt. Das am 7. Dezember 2022 verabschiedete Rundschreiben 2023/1 wird am 1. Januar 2024 in Kraft treten.

Das neue Rundschreiben unterscheidet zwischen dem allgemeinen Management operationeller Risiken und dem Management spezifischer operationeller Risiken. Zu letzteren zählen insbesondere Risiken im Zusammenhang mit Informations- und Kommunikationstechnologien (IKT), Cyberrisiken, kritischen Daten und schließlich grenzüberschreitenden Dienstleistungstätigkeiten. Der vorliegende Kommentar konzentriert sich auf die ersten drei Risikoarten, bevor er kurz auf eine Neuerung des Rundschreibens eingeht : die betriebliche Widerstandsfähigkeit (Operational Resilience).

Operationelle Risiken entsprechen dem Risiko „finanzieller Verluste aufgrund der Unangemessenheit oder des Versagens interner Prozesse oder Systeme, unangemessener Handlungen von Personen oder von ihnen begangener Fehler oder aufgrund externer Ereignisse“. Die Definition entspricht derjenigen in Art. 89 der Eigenmittelverordnung und derjenigen des Basler Ausschusses für Bankenaufsicht (BCBS). Das zentrale Element ist das der finanziellen Verluste, das weit verstanden wird. Dazu gehören beispielsweise Cyberangriffe, die zu einem Vertrauensverlust bei den Kunden führen, auch wenn der finanzielle Verlust nicht direkt quantifizierbar ist.

Die digitale Entwicklung verlangt von den Steuerpflichtigen ein gutes Management der Veränderungen im Zusammenhang mit der IKT (Change Management), ihrem Betrieb (Run, Maintenance) und dem Management von Vorfällen. In Bezug auf den ersten Aspekt muss der Steuerpflichtige insbesondere die Trennung zwischen der Entwicklungs- oder Testumgebung einerseits und der IKT-Produktionsumgebung andererseits gewährleisten. In Bezug auf den zweiten Aspekt muss der Steuerpflichtige über ein Inventar verfügen, das die Hardware- und Softwarekomponenten sowie die Orte, an denen kritische Daten gesichert werden, umfasst. Schliesslich muss die beaufsichtigte Person im Falle eines bedeutenden IKT-Vorfalls unter anderem die FINMA unverzüglich darüber informieren.

Im Rahmen des Cyberrisikomanagements besteht auch die Pflicht, die FINMA über Cyberangriffe zu informieren, doch diese Pflicht ist nicht neu (und wird wahrscheinlich in Kürze überarbeitet, um sie an eine künftige, allgemeinere Meldepflicht für Cyberangriffe anzupassen).

Die Hauptpflicht besteht darin, eine Strategie gegen Cyberangriffe einzuführen. Diese Strategie muss Prozesse und Kontrollen umfassen, um (a) spezifische und potenzielle Bedrohungen durch Cyberangriffe zu identifizieren, (b) die Vertraulichkeit, Integrität und Verfügbarkeit kritischer elektronischer Daten und IKT-Komponenten zu schützen, (c) Cyberangriffe schnell zu erkennen und schließlich (d) auf Schwachstellen zu reagieren und (e) den Geschäftsbetrieb nach einem Cyberangriff schnell wiederherzustellen. Darüber hinaus muss der Steuerpflichtige Penetrationstests und Cyberübungen durchführen.

In Anhang 3 des Rundschreibens 08/21 schrieb die FINMA einen besonderen Schutz der „Kundenidentifikationsdaten“ (CID) vor. Der Schwerpunkt lag damals auf der Vertraulichkeit allein dieser Daten. In Übereinstimmung mit den technologischen Entwicklungen gilt der Schutz nun für alle wichtigen Daten sowohl unter dem Gesichtspunkt der Vertraulichkeit als auch der Integrität und Verfügbarkeit (nicht jedoch unter dem Aspekt der Rückverfolgbarkeit).

Das Rundschreiben 23/1 schreibt somit einen besonderen Schutz für sogenannte „kritische“ Daten vor („critical information assets“ in der Terminologie des BCBS). Während der Entwurf des Rundschreibens eine breite Definition der „kritischen Daten“ vorsah, wurde eine Definition gewählt, die der von der Schweizerischen Bankiervereinigung vorgeschlagenen Definition nahe kommt. Kritische Daten sind „Daten, die unter Berücksichtigung der Größe, der Komplexität, der Struktur, des Risikoprofils sowie des Geschäftsmodells des Instituts so wichtig sind, dass sie erhöhte Sicherheitsanforderungen erfordern“. Es obliegt jedem Steuerpflichtigen, seine kritischen Daten zu identifizieren.

Sobald diese Daten identifiziert sind, unterliegen sie besonderen Schutzmaßnahmen. Diese Maßnahmen umfassen nicht nur einen begrenzten Zugriff durch die Mitarbeiter (need to know-Prinzip) sowie deren Schulung und Überwachung, sondern auch den Schutz und die Überwachung der Daten, wenn sie außerhalb der Schweiz aufbewahrt werden, sowie eine Due Diligence der Dienstleister, die diese Daten verarbeiten. Schließlich muss jeder wichtige Vorfall im Zusammenhang mit kritischen Daten unverzüglich der FINMA gemeldet werden.

Das Rundschreiben 23/1 enthält schliesslich auch Anforderungen an die betriebliche Widerstandsfähigkeit. Die Aufnahme dieser Anforderungen wird mit der Zunahme von „operativen Schocks“ begründet, wie Pandemien, Cyberangriffen, systemischen Fehlern, Ausfällen in der Lieferkette, ausgedehnten oder lang anhaltenden Stromausfällen oder Naturkatastrophen.

Die betriebliche Widerstandsfähigkeit war auch Gegenstand neuer Regelungen auf internationaler Ebene. Der BCBS hat im März 2021 seine Principles for operational resilience verabschiedet. Zuletzt hat der Rat der Europäischen Union im November 2022 die Verordnung über die digitale betriebliche Widerstandsfähigkeit des Finanzsektors (DORA-Verordnung, siehe cdbf.ch/1164/) verabschiedet. Ihr Inkrafttreten wird schrittweise über zwei Jahre erfolgen, wie auch die Regeln zur Widerstandsfähigkeit in Rundschreiben 23/1. Anders als das Schweizer Recht gilt die DORA-Verordnung jedoch nicht nur für Finanzinstitute, sondern auch für Drittanbieter von IKT-Dienstleistungen, wie z. B. Cloud-Anbieter.