Prüfung der Aufsicht über die Cybersicherheit bei Finanzdienstleistern

Eidgenössische Finanzmarktaufsicht

Das Wesentliche in Kürze

Die Eidgenössische Finanzkontrolle (EFK) hat eine Prüfung bei der Eidgenössischen Finanzmarktaufsicht (FINMA) durchgeführt, mit dem Ziel, die Effizienz und Wirksamkeit der Aufsicht im Bereich der Cybersicherheit bei Finanzdienstleistern zu untersuchen.

Der Bundesrat hat am 8. Dezember 2017 die nationale Strategie zum Schutz kritischer Infrastrukturen (SKI) für den Zeitraum 2018–2022 verabschiedet. Zwei der 27 definierten Teilsektoren werden von der FINMA beaufsichtigt: die Finanz- und die Versicherungsdienstleistungen.

Das Gesamtdispositiv in der Schweiz kommt nur zögerlich voran

Die 2017 von der FINMA erlassenen verpflichtenden Vorgaben für Banken und Effektenhändler sind angemessen. Jedoch bestehen seit Jahren Lücken im Gesamtdispositiv der Cyberrisiken. Konkrete Massnahmen kommen aufgrund unklarer Verantwortungen und Kompetenzen allerdings nur zögerlich voran. So befindet sich eine funktionierende Krisenorganisation nach wie vor im Aufbau und auch regelmässige sektorübergreifende Übungen zu Cyberangriffen wurden erst einmal durchgeführt.

Aufsicht richtet sich nach den vorhandenen Mitteln

Die Aufsicht über Cyberrisiken, eines von sechs Hauptrisiken für die FINMA, wurde mit den zur Verfügung stehenden Ressourcen stetig weiterentwickelt. Alle geplanten Aktivitäten in dem Bereich konnten noch nicht durchgeführt bzw. umgesetzt werden. Die FINMA hat dies erkannt und organisatorische sowie formelle Anpassungen Anfang 2020 vorgenommen. Es besteht aber weiterhin das Risiko, dass die Aufsicht nicht den geplanten Aktivitäten folgt, sondern sich an den vorhandenen Ressourcen ausrichtet. Effizienzgewinne könnten bei der Erhebung und Auswertung der Prüfergebnisse erzielt werden.

Meldepflicht der Banken zu Cybervorfällen nur ungenügend eingehalten

Die Meldepflicht in Bezug auf Cybervorfälle haben die Banken nur ungenügend befolgt. Eine Nicht-Meldung hatte keine Konsequenzen für die Beaufsichtigten, obwohl entsprechende Instrumente dafür bestünden. Der FINMA fehlt somit eine wesentliche Quelle zu Cyberrisiken auf Institutsebene.

Dieser Umstand wird dadurch akzentuiert, dass die Banken einen direkten Zugriff der FINMA auf MELANI (Analyse- und Meldestelle des Bundes zur Informationssicherheit) ablehnen. Die von der EFK empfohlene Intensivierung der Vor-Ort-Kontrollen könnte diese Lücken teilweise beheben.