DIE FINMA WARNT BEAUFSICHTIGTE FINANZDIENSTLEISTER VOR CYBERSECURITY-RISIKEN UND ERLÄSST EMPFEHLUNGEN

Die eidgenössische Finanzmarktaufsicht («FINMA») hat festgestellt, dass sowohl das Bewusstsein für Cyber-Risiken als auch die Umsetzung der entsprechenden regulatorischen Anforderungen durch die Finanzinstitute grosse Lücken aufweisen.

Wenger Vieli AG
Dufourstr. 56
Postfach
8034 Zürich
—
Metallstr. 9
Postfach
6302 Zug
—
+41 58 958 58 58
spotlight@
wengervieli.ch

Im Juni 2024 veröffentlichte die FINMA zwei neue Aufsichtsmitteilungen zu operationellen Risiken, mit besonderem Fokus auf Cyber-Risiken. Dieser Spotlight gibt einen Überblick über die rechtlichen Pflichten der beaufsichtigten Institute in Bezug auf Cyber-Risiken, stellt die neusten Erkenntnisse und Empfehlungen der FINMA in diesem Bereich vor und zeigt auf, wie Finanzinstitute ihre Cyber-Risiken effektiv managen und ihre Compliance mit den Aufsichtsmitteilungen sicherstellen können.

FINMA erlässt Aufsichtsmitteilungen zu Cyber-Risiken und zum Management von operationellem Risiko

Die FINMA weist auf die im Rahmen der Aufsichtstätigkeit festgestellten Mängel hin und publiziert Empfehlungen zum Umgang mit Cyber-Risiken und zum wirksamen Management von operationellen Risiken:

1. Die FINMA Aufsichtsmitteilung 03/2024 («**Cyber-Risiken**») fasst die Erkenntnisse der FINMA zu Cyber-Risiken aus ihrer Aufsichtstätigkeit zusammen. Sie umfasst Leitlinien zum Umgang mit Cyber-Attacken und konkretisiert, wie Cyber-Attacken zu melden und szenariobezogene Cyber-Übungen durchzuführen sind. Aufsichtsmitteilung 03/2024 ist auf alle von der FINMA beaufsichtigten Institute anwendbar.
2. Die FINMA Aufsichtsmitteilung 04/2024 («**Management der operationellen Risiken**») fasst die Erkenntnisse der FINMA zu operationellen Risiken zusammen. Sie unterstreicht die Bedeutung eines effektiven Risikomanagement, insbesondere von Cyber-Risiken, und präzisiert die Pflichten der Unternehmen in diesem Bereich. Obwohl primär an Fondsleitungen und Verwalter von Kollektivermögen gerichtet, kann Aufsichtsmitteilung 04/2024 auch anderen beaufsichtigten Instituten als Leitfaden dienen.

Anforderungen an Finanzdienstleister im Bereich Cyber-Risiken

Die regulatorischen Anforderungen an Finanzdienstleister im Bereich der Cyber-Risiken stützen sich auf die folgenden Grundsätze:

	Finanzmarktrecht	**Datenschutzrecht**	**Informationssicherheit**
Gesetzliche Anforderungen	Verschiedene Finanzmarktgesetze legen die übergreifenden Anforderungen an das Risikomanagement für die beaufsichtigten Institute fest. Cyber-Risiken sind innerhalb des operationellen Risikorahmen geregelt, der für Finanzinstitute vorgeschrieben ist.	Das Datenschutzgesetz («**DSG**») regelt die Nutzung von Personendaten, einschliesslich Vorschriften zur Reduzierung und Meldung und Bearbeitung von Cyber-Risiken.	Das revidierte Informationssicherheitsgesetz («**ISG**»), das voraussichtlich am 1. Januar 2025 in Kraft tritt, schreibt Betreibern kritischer Infrastrukturen vor, Cyber-Attacken an das Bundesamt für Cybersicherheit («**BACS**») zu melden. Dazu gehören Banken, Versicherungen und alle nach dem Finanzmarktinfrastrukturgesetz («**FinfraG**») beaufsichtigten Institute.
Rundschreiben/ Verordnung	FINMA RS zum Outsourcing Das FINMA Rundschreiben 2018/3 «Auslagerungen – Banken, Versicherungsunternehmen und ausgewählten Finanzinstituten nach FINIG» definiert die Anforderungen an Finanzdienstleister für das Outsourcing wesentlicher Funktionen, von deren ordnungsgemässer Ausführung die Einhaltung der Finanzmarktregulierung massgeblich abhängt. FINMA RS zu operationellen Risiken Das FINMA Rundschreiben 2023/1 «Operationelle Risiken und Resilienz – Banken» definiert Richtlinien für das Management von operationellen Risiken und Resilienz in Banken. Es umfasst dabei Aspekte wie Cyber-Risiken, den Schutz kritischer Daten und das Business Continuity Management.	Die Datenschutzverordnung («**DSV**») enthält detaillierte Bestimmungen zu Outsourcing, Datensicherheit und zur Meldung von Datenschutzverletzungen an den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten («**EDÖB**»).	
Aufsichtsmitteilungen	FINMA Aufsichtsmitteilung Cyber-Attacken Die FINMA Aufsichtsmitteilung 05/2020 «Meldepflicht von Cyber-Attacken gemäss Art. 29 Abs. 2 FINMAG» präzisiert das Verfahren für die Meldung von bedeutenden Cyber-Attacken.		

Erkenntnisse aus der FINMA Aufsichtspraxis

Die FINMA hat festgestellt, dass sich sowohl der Umfang als auch die Häufigkeit von Cyber-Attacken auf Finanzdienstleister in den letzten Jahren signifikant erhöht haben. Diese Entwicklung wurde durch gravierende Probleme bei der Einhaltung und Umsetzung regulatorischer Vorgaben bestärkt, was zu unzureichenden Reaktionen auf Cyber-Attacken führen könnte. Problematisch ist gemäss FINMA insbesondere das weit verbreitete Outsourcing, da mehr als 50 Prozent der Angriffe mittlerweile die Zulieferer betreffen.

Einige zentrale Probleme umfassen:

Mangelhafte Governance und Management von Cyber-Risiken

Viele Finanzdienstleister haben Cyber-Risiken nicht angemessen in ihr operationelles Risikomanagement integriert. Oft fehlen klare Definitionen der spezifischen Cyber-Risiken sowie der entsprechenden Risikotoleranz und es mangelt an einer klaren Trennung zwischen operativem Management und unabhängigen Kontrollfunktionen, was zu Interessenkonflikten führen kann.

Mangelhafte Schutzmassnahmen

Unberechtigte Dritte konnten wiederholt kritische Daten von beaufsichtigten Finanzdienstleistern erlangen, einschliesslich Zugangsdaten für wesentliche Applikationen. Schutzmassnahmen zur Verhinderung von Datenverlusten sind oft nur auf wenige Datenkategorien wie Kreditkartennummern beschränkt. Wichtige Kategorien wie Personendaten und Geschäftsgeheimnisse werden oft gar nicht erfasst.

Mangelhafte Erkennung, Reaktion und Wiederherstellung nach einer Attacke

Die FINMA hat festgestellt, dass Finanzinstitute oft über keine oder nur unvollständige Reaktionspläne auf Cyber-Attacken verfügen, was zu unklaren Zuständigkeiten führt. Business Continuity Pläne, die darauf ausgelegt sind, wesentliche Funktionen im Falle eines Angriffs zu sichern, umfassen vielfach nicht alle erforderlichen technischen und personellen Ressourcen, was die Wiederherstellung dieser Funktionen in Notfällen erschwert. Oft werden diese Pläne auch nicht regelmässig getestet, und viele Institutionen sind sich ihrer Meldepflichten im Falle von Cyber-Attacken nicht bewusst.

Outsourcing an IT-Dienstleister

Gemäss FINMA erhöht die Auslagerung an IT-Dienstleister die Verwundbarkeit von Finanzinstituten erheblich. Häufig wird zu wenig Wert auf die Auswahl und Kontrolle der Anbieter gelegt, insbesondere was ihre Erfahrung im Risikomanagement betrifft. IT-Dienstleister adressieren Sicherheitsprobleme tendenziell weniger effektiv als beaufsichtigte Finanzdienstleister. Die Kommunikation zwischen Finanzdienstleistern und IT-Dienstleistern ist zudem oft unzureichend und Sicherheitslücken werden selten gemeinsam behoben. Zudem gibt es vielfach nur unvollständige Dokumentationen über ausgelagerte Dienstleistungen und Subunternehmer, was Kontrolllücken verursacht.

Empfehlungen der FINMA zur Minimierung von Cyber-Risiken

Um die oben aufgeführten Missstände zu adressieren, erinnert die FINMA die beaufsichtigten Finanzinstitute an ihre Verpflichtungen zur Reduzierung von Cyber-Risiken:

Governance und Management von Cyber-Risiken

Finanzinstitute müssen Cyber-Risiken als eigenständige Risiken im Rahmen ihres operationellen Risikomanagements erfassen und in ihr internes Kontrollsystem («**IKS**») integrieren. Die Wirksamkeit der entsprechenden Kontrollen muss regelmässig unabhängig überprüft, bewertet und dokumentiert werden. Daten, insbesondere Kundendaten, müssen identifiziert und geschützt werden, um Verfügbarkeit, Vertraulichkeit und Integrität sicherzustellen. Sicherheitsmassnahmen sollten entsprechend der Risikotoleranz festgelegt werden. Zudem müssen alle verantwortlichen Funktionen, die damit beauftragten Personen und die Meldeprozesse klar definiert sein.

Schutzmassnahmen

Backup- und Wiederherstellungsstrategien sollten regelmässig überprüft werden und müssen Szenarien einschliessen, in denen Angreifer die Schutzmechanismen umgehen konnten. Zudem sollten Finanzinstitute regelmässige Schulungen durchführen, um das Bewusstsein für Cyber-Risiken bei den Mitarbeitenden zu schärfen.

Erkennung, Reaktion und Wiederherstellung

Finanzinstitute müssen realistische, regelmässig aktualisierte und getestete Reaktions- und Business Continuity Pläne haben, um wesentliche Prozesse während einer Krise aufrechtzuerhalten. Hierfür müssen Aufgaben, Verantwortlichkeiten und die Kommunikation mit Kunden und Partnern im Falle eines Cyber-Vorfalls klar definiert sein.

Darüber hinaus präzisiert die FINMA ihre Erwartungen hinsichtlich der Meldung von Cyber-Attacken. Eine Erstmeldung muss innerhalb von 24 Stunden nach Entdeckung erfolgen und eine erste Einschätzung der Schwere des Angriffs enthalten. Bei einer Bewertung als «mittel», «hoch» oder «schwerwiegend» hat innerhalb von 72 Stunden eine formelle Meldung mit Untersuchungsbericht zu erfolgen. Ist der Schweregrad «hoch» oder «schwerwiegend», müssen zudem die Gründe für den erfolgreichen Angriff, die Auswirkungen auf die regulatorischen Vorgaben und den Betrieb sowie die ergriffenen Abhilfemassnahmen dargelegt werden.

Outsourcing

Die FINMA betont, dass die beaufsichtigten Institute auch bei der Auslagerung ihrer Funktionen für die Einhaltung regulatorischer Anforderungen verantwortlich bleiben. Diese Pflicht kann nicht übertragen werden und erfordert eine sorgfältige Auswahl und Überwachung der IT-Dienstleister. Zudem müssen die detaillierten Anforderungen gemäss FINMA-Rundschreiben «Outsourcing» befolgt werden, sofern wesentliche Funktionen betroffen sind.

Wie geht es weiter?

Seit mehreren Jahren gehören Cyber-Risiken zu den Hauptrisiken, die die FINMA in ihrem jährlichen Risikomonitor erfasst. In diesem Zusammenhang erwartet die FINMA von beaufsichtigten Institutionen, einen integrierten und systematischen Ansatz zur Bewältigung von Cyber-Risiken umzusetzen. Dieser Ansatz muss spezifische Massnahmen für Governance, Identifikation, Schutz, Erkennung, Reaktion und Wiederherstellung von durch Cyber-Risiken bedrohten Systemen und Dienstleistungen umfassen.

Es besteht kein Zweifel daran, dass Cyber-Attacken auch in den kommenden Jahren eine zentrale Herausforderung für die Finanzindustrie bleiben und die FINMA wird die Bemühungen der beaufsichtigten Institutionen zur Risikominderung genau überwachen.

Wir empfehlen allen von der FINMA beaufsichtigten Institutionen, kontinuierlich ihre Massnahmen zur Cyber-Abwehr zu überprüfen und Cyber-Risiken explizit in ihr Gesamtmanagement der operationellen Risiken zu integrieren. Neben den finanziellen Verlusten, die durch Cyber-Attacken entstehen können, besteht auch die Gefahr eines Reputationsschadens, insbesondere im Finanzdienstleistungssektor.

In diesem Kontext können die folgenden Fragen dazu beitragen, Schwächen im Rahmen der Cyber-Abwehr und des Risikomanagements der Institutionen zu identifizieren:

- ☐ Haben wir Cyber-Risiken ausreichend in unser Gesamtmanagement der operationellen Risiken integriert?
- ☐ Haben wir Cyber-Risiken auf Management- oder Vorstandsebene angemessen priorisiert?
- ☐ Haben wir unsere institutionsbezogenen Cyber-Risiko-Bedrohungen identifiziert?
- ☐ Haben wir einen Prozess definiert, um Cyber-Attacken korrekt zu melden (z. B. Zeitpunkt, Form, Empfänger)?
- ☐ Führen wir risikobasierte und szenariobasierte Cyber-Übungen durch (wie etwa jährliche Table-top-Übungen, d.h. Simulation und Durchspielen eines Szenarios auf Papier)?
- ☐ Führen wir ein aktuelles Verzeichnis aller bedeutenden ausgelagerten Funktionen einschliesslich beteiligter Subunternehmer?
- ☐ Haben wir aktuelle Verträge mit unseren Outsourcing-Anbietern, die alle relevanten regulatorischen Anforderungen erfüllen?
- ☐ Haben wir ein System / Verfahren definiert, um unsere Outsourcing-Partner zu kontrollieren?
- ☐ Haben wir definiert, was für uns kritische Daten sind?
- ☐ Haben wir Schulungs- und Awareness-Programme für Cyber-Sicherheit für Mitarbeitende auf allen Ebenen unseres Unternehmens implementiert?
- ☐ Ist unsere Business Continuity Management Richtlinie auf dem neusten Stand und entsprechen die jeweiligen Prozesse dem aktuellen Bedrohungsniveau?
- ☐ Haben wir geprüft, ob wir ab dem 1. Januar 2025 den Meldepflichten des revidierten ISG unterliegen, und sind wir gegebenenfalls darauf vorbereitet, diese einzuhalten?

Keyfacts

01 **Im Juni 2024 veröffentlichte die FINMA zwei neue Aufsichtsmitteilungen, die sich auf Cyber-Risiken fokussieren und detaillierte Leitlinien für Finanzinstitute enthalten.**

02 **Die FINMA betont die Herausforderungen vieler Finanzdienstleister bei der Etablierung angemessener Governance-Strukturen für Cyber-Risiken und warnt vor erhöhten Verwundbarkeiten durch unzureichend berücksichtigte Sicherheitsaspekte beim Outsourcing.**

Martin Peyer
Partner
m.peyer@wengervieli.ch
+41 58 958 53 53

Claudia Keller
Partnerin
c.keller@wengervieli.ch
+41 58 958 53 15

Orlando Battaglia
Senior Associate
o.battaglia@wengervieli.ch
+41 58 958 53 69

Matthias Langenegger
Associate
m.langenegger@wengervieli.ch
+41 58 958 53 43