Rolf H. Weber
Prof. Dr. iur., Prof. an der Universität Zürich Rechtsanwalt
Konsulent
Telefon +41 58 258 10 00
rolf.weber@bratschi.ch

Cybersicherheits-Compliance in Finanzmarktunternehmen

Die Zahl verschiedenartiger Cybervorfälle hat sich in letzter Zeit nicht nur vermehrt, sondern die Angriffe sind auch immer ausgeklügelter geworden. Finanzinfrastrukturanbieter und Finanzdienstleister, deren Tagesgeschäft sich durch die Digitalisierung stark verändert hat, sind diesen Risiken besonders ausgesetzt. Spezifische Compliance-Vorkehren (Risikomanagement, Business-Continuity-Massnahmen) gewinnen deshalb an Bedeutung.

1. Rechtslage in der Schweiz

Cybervorfälle vermögen ganze Ökosysteme und Unternehmen lahmzulegen. Besondere Probleme entstehen, wenn die Akteure eines Sektors funktionsbedingt eng miteinander verknüpft sind, was auf die Finanzmarktteilnehmer zutrifft. Angesichts der weit fortgeschrittenen Digitalisierung der operativen Geschäftsabwicklungen und der Internationalisierung von Transaktionen besteht eine hohe Verletzbarkeit in der Finanzmarktbranche.

Die Schweiz kennt kein allgemeines Cybersicherheits-Gesetz (nur ein im Jahre 2022 in Kraft tretendes Informationssicherheitsgesetz für Infrastrukturen des Bundes). Abgesehen von der nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken, die strategische Ziele für die Jahre 2018-2022 formuliert hat, ist für Finanzmarktunternehmen insbesondere das FINMA-Rundschreiben 2008/21 von Bedeutung. Gemäss den anfangs 2020 in Kraft getretenen neuen Richtlinien in Rz. 135 ff. hat die Dokumentation zu den Cyberrisiken mindestens folgende Aspekte abzudecken:

- Identifikation der institutsspezifischen Bedrohungsziele durch Cybervorfälle;
- Schutz der Geschäftsprozesse und der Technologieinfrastruktur vor Cybervorfällen;
- Zeitnahe Erkennung und Aufzeichnung von Cybervorfällen;
- Reaktion auf Cybervorfälle mit kurzfristigen und gezielten Massnahmen;

- Gewährleistung der zeitnahen Wiederherstellung des Geschäftsbetriebs.

Die Finanzmarktunternehmen sind zudem verpflichtet, regelmässige Verwundbarkeitsanalysen und Penetrationstests durchzuführen, was qualifiziertes Personal und angemessene Ressourcen vorausgesetzt. Im Jahresbericht 2020 hat die FINMA festgestellt, die Abhängigkeit von den Informations- und Kommunikationstechnologien steige weiter an und die Verwundbarkeit der Finanzinstitute werde grösser. Deshalb beabsichtigt die FINMA, die Überwachung mittels Analysen der Bedrohungslage, laufender Aufsicht und Vorfallbewältigung (bzw. Krisenmanagement) zu verstärken.

Im Jahre 2016 hat die FINMA nur von sehr bedeutenden Marktteilnehmern eine Selbstbeurteilung verlangt, nicht von den anderen Finanzmarktunternehmen; dieser Ansatz wird aber der Tatsache nicht gerecht, dass die Risikoanfälligkeit bei der Finanzmarktstabilität vom schwächsten Glied der Transaktionskette abhängt. Auch die seit 2018 vorgenommenen Vor-Ort-Kontrollen erfolgen lediglich bei den grösseren Marktteilnehmern. Die Eidgenössische Finanzkontrolle (EFK) hat im Jahre 2020 die FINMA-Aufsicht zur Cybersicherheit geprüft und festgestellt, dass die FINMA nur einen lückenhaften Überblick über die Cybersicherheit der beaufsichtigten Institute habe; insbesondere die allgemeine Meldepflicht von Cybervorfällen nach Art. 29 Abs. 2 FinmaG funktioniere nicht ausreichend. Die FINMA hat die geäusserten Bedenken entgegengenommen und in Aussicht gestellt, die Cybersicherheits-Überwachung zu intensivieren.

Abgesehen vom FINMA-Rundschreiben bestehen auch Datensicherheitsvorgaben gemäss altem und neuem Datenschutzgesetz. Überdies hat der Bundesrat anfangs 2022 eine Vernehmlassung zur Einführung einer Meldepflicht für Cyberangriffe bei kritischen Infrastrukturen eröffnet (Anpassung von Art. 74*a* ff. des Informationssicherheitsgesetzes); mit einer solchen Meldepflicht wird eine verbesserte Übersicht über die Cyberangriffe in der Schweiz sowie die Unterstützung der Betroffenen bei deren Bewältigung angestrebt.

2. Risikomanagement

Finanzunternehmen haben ein den Geschäftstätigkeiten angemessenes Risikomanagement einzurichten. Das Risikomanagement umfasst «die organisatorischen Strukturen sowie die Methoden und Prozesse, die der Festlegung von Risikostrategien und Risikosteuerungsmassnahmen sowie der Identifikation, Analyse, Bewertung, Bewirtschaftung, Überwachung und Berichterstattung von Risiken dienen» (FINMA-Rundschreiben 2017/1, Rz. 3). Dabei kommt den Cyberbedrohungen eine besondere Bedeutung zu. Zu einem guten Risikomanagement im Rahmen der Cyberrisiken gehören funktionierende interne Governance- und Kontrollmechanismen, insbesondere:

- Identifizierung der cybersicherheitsbezogenen Unternehmensfunktionen;
- Massnahmen zum Schutz und zur Prävention vor Cyberattacken;

- Frühzeitige Erkennung von potentiellen Cyberrisiken zwecks Minimierung negativer Auswirkungen;
- Massnahmen zur Schaffung eines hohen «Situationsbewusstseins» beim Personal;
- Adäquate Vorkehren zur Realisierung eines optimalen Grades an Datensicherheit.

Als Teil der Bedrohungsanalyse ist die Einrichtung eines Prozesses zur Sammlung und Beurteilung relevanter Cyberbedrohungsinformationen angebracht, und zwar in Verbindung mit anderen internen und externen Informationsquellen, die einen geschäftsspezifischen Kontext schaffen. Die Finanzunternehmen haben zudem sicherzustellen, dass die gewonnenen Erkenntnisse den zuständigen Mitarbeitenden zur Verfügung gestellt werden, um die Prävention gegen Cyberrisiken auf strategischer, taktischer und operativer Ebene verwirklichen zu können.

3. Business-Continuity-Management

Auch das beste Risikomanagement mit sehr detailliertem Schutzkonzept vermag nicht zu garantieren, dass es nie zu einem Cybervorfall kommt. Aus diesem Grund ist es unabdingbar, das Vorgehen im Anschluss an einen Cybervorfall zu planen. Dazu gehören insbesondere eine kohärente und integrierte Überwachung, Handhabung und Weiterverfolgung solcher Vorfälle. Die FINMA hat für Banken und Versicherungen gewisse Mindeststandards und Empfehlungen der Branche für das Business-Continuity-Management als Selbstregulierung anerkannt; diese Mindeststandards sind angemessen mit Blick auf die Cyberbedrohungen anzupassen. Als mögliche Massnahmen fallen in Betracht:

- Klassifikation der Cyberrisiken und Festlegung von Wesentlichkeitsschwellen (z.B. Zahl der Betroffenen, Dauer des Vorfalls, Ausfallzeiten des Dienstes, geographische Ausbreitung, Ausmass der Datenverluste, Kritikalität der Dienste, wirtschaftliche Auswirkungen);
- Business-Continuity-Strategie (z.B. Aufzeichnung der Cybervorfälle, Sicherstellung der Kontinuität kritischer Funktionen, rasche und wirksame Reaktion auf einen Vorfall (Aktivierung von Schadenverhinderungsplänen);
- Vorbereitung von Gegenmassnahmen und Wiederherstellung der Funktionen (Notfallplan);
- Massnahmen zur Datensicherung und Datensicherheit;
- Kommunikationsplan und Erfüllung gesetzlicher Meldepflichten;
- Übungen und Tests, um Schwachstellen, Mängel oder Lücken zu ermitteln, einschliesslich Formulierung der Anforderungen an die Prüfer sowie Beschreibung der Methoden zur Schwachstellenbewertung und zu Penetrationstests.

Die Cybersicherheits-Massnahmen sollten nicht auf die Abwehr bereits bekannter Gefahren beschränkt sein, sondern sie müssen eine kontinuierliche Resilienz in einem sich schnell verändernden Bedrohungsumfeld gewährleisten. Finanzunternehmen sind verpflichtet, einen anpassungsfähigen Rahmen für die Cybersicherheit einzuführen, der sich mit der dynamischen Natur von Cyberrisiken weiterentwickelt, um Sicherheitsbedrohungen frühzeitig zu identifizieren, zu bewerten und geeignete Schutzmassnahmen zu implementieren. Ein Finanzunternehmen sollte folglich darauf abzielen, eine Kultur des Bewusstseins für Cyberrisiken und Cyber-Resilienz auf allen Betriebsstufen zu schaffen.

4. Ausblick

Im Vergleich zu ausländischen Rechtsordnungen sind in der Schweiz die ausdrücklichen Regelungen zu den Governance- und Kontrollmechanismen sowie zum Situationsbewusstsein mit Blick auf Cyberrisken noch nicht sehr weit entwickelt. Abgesehen von der derzeit laufenden Revision des Informationssicherheitsgesetzes (Meldepflicht im Falle von kritischen Infrastrukturen) ist aber zu erwarten, dass die FINMA die Anforderungen an geeignete Prozesse und Compliance-Massnahmen, um institutsspezifische Bedrohungspotentiale durch Cyberrisiken zu identifizieren, in den nächsten Jahren verschärfen wird.

Spezifikationen im Kontext des Business-Continuity-Management finden sich bisher lediglich in Selbstregulierungen, die sich zwar in der Praxis weitgehend bewährt haben. Die einzelnen Finanzunternehmen sind aber gut beraten, dem Bedrohungsumfeld durch Cyberattacken erhöhte Beachtung zu schenken und präventive Schutzvorkehren einzurichten. Eine Verstärkung der Compliance in diesem Bereich erscheint somit als ein Gebot der Stunde.

Weiterführende Literatur:

Rolf H. Weber/Okan Yildiz, Cybersicherheit und Cyber-Resilienz in den Finanzmärkten, Zürich 2022, EIZ Publishing *Open Access*

Basel
Lange Gasse 15
Postfach
CH-4052 Basel
T +41 58 258 19 00
F +41 58 258 19 99
basel@bratschi.ch

Bern
Bollwerk 15
Postfach
CH-3001 Bern
T +41 58 258 16 00
F +41 58 258 16 99
bern@bratschi.ch

Genf
Rue du Général-Dufour 20
1204 Genf
T +41 58 258 13 00
F +41 58 258 17 99
geneva@bratschi.ch

Lausanne
Avenue Mon-Repos 14
Postfach 5507
CH-1002 Lausanne
T +41 58 258 17 00
T +41 58 258 17 99
lausanne@bratschi.ch

St.Gallen
Vadianstrasse 44
Postfach 262
CH-9001 St. Gallen
T +41 58 258 14 00
F +41 58 258 14 99
stgallen@bratschi.ch

Zug
Gubelstrasse 11
Postfach 7106
CH-6302 Zug
T +41 58 258 18 00
F +41 58 258 18 99
zug@bratschi.ch

Zürich
Bahnhofstrasse 70
Postfach
CH-8021 Zürich
T +41 58 258 10 00
F +41 58 258 10 99
zuerich@bratschi.ch