FMA

Finanzmarktaufsicht
Liechtenstein

FMA-Mitteilung 2018/3 – Umgang mit Cyber-Risiken

Mitteilung betreffend die Erwartungen der FMA zum Umgang mit Cyber-Risiken

Referenz:	FMA-M 2018/3
Adressaten:	- Banken nach BankG - Wertpapierfirmen nach BankG - E-Geld-Institute nach EGG - Zahlungsinstitute nach ZDG - Versicherungsunternehmen nach VersAG - Versicherungsvermittler nach VersVermG - Vorsorgeeinrichtungen nach BPVG - Pensionsfonds nach PFG - Verwaltungsgesellschaften und OGAW nach UCITSG - Verwaltungsgesellschaften und Investmentunternehmen nach IUG 2015 - Verwalter alternativer Investmentfonds nach AIFMG - Vermögensverwalter nach VVG - Treuhänder oder Treuhandgesellschaften nach TrHG
Anwendbarkeit:	Die Finanzintermediäre haben den Pflichten dieser Mitteilung ab dem 01.10.2018 nachzukommen
Publikation:	Webseite
Erlass:	25.09.2018
Inkraftsetzung:	01.10.2018
Letzte Änderung:	25.09.2018
Rechtliche Grundlagen:	Art. 4 FMAG

Landstrasse 109 • Postfach 279 • 9490 Vaduz • Liechtenstein
Telefon +423 236 73 73 • Telefax +423 236 73 74 • www.fma-li.li • info@fma-li.li

1. Ausgangspunkt und Zweck

Der liechtensteinische Finanzmarkt ist immer mehr auf den Einsatz von Technologien und IT-Systemen angewiesen. Daraus ergeben sich Chancen, zwangsläufig aber auch besondere Risiken. Dazu zählen vor allem Cyber-Risiken. Dabei handelt es sich um operationelle Risiken in Bezug auf mögliche Verluste durch Cyber-Attacken[1].

Vor diesem Hintergrund erachtet die FMA den Einbezug von Cyber-Risiken als zentralen Bestandteil des unternehmensinternen Risikomanagements. Die FMA erwartet deshalb, dass Cyber-Risiken in ein umfassendes unternehmensinternes Risikomanagement einbezogen werden. Die vorliegende Mitteilung hält die Erwartungen der FMA an die Finanzintermediäre im Umgang mit Cyber-Attacken fest. Die FMA betont, dass neben dem technischen Abwehrdispositiv auch geeignete organisatorische Vorkehrungen, die Mitarbeitenden und die Unternehmensführung zu einem umfassenden Management von Cyber-Risiken gehören.

2. Rechtliche Grundlagen

Die vorliegende Mitteilung wird gestützt auf Art. 4 FMAG erlassen. Sie bezweckt den Schutz des liechtensteinischen Finanzmarktes und der Kunden. Die FMA kann sektorspezifisch zusätzliche konkretisierende Regulierungen vorsehen oder europäische Leitlinien ergänzend für anwendbar erklären.

3. Anwendungsbereich

- Banken nach BankG
- Wertpapierfirmen nach BankG
- E-Geld-Institute nach EGG
- Zahlungsinstitute nach ZDG
- Versicherungsunternehmen nach VersAG
- Versicherungsvermittler nach VersVermG
- Vorsorgeeinrichtungen nach BPVG
- Pensionsfonds nach PFG
- Verwaltungsgesellschaften und OGAW nach UCITSG
- Verwaltungsgesellschaften und Investmentunternehmen nach IUG 2015
- Verwalter alternativer Investmentfonds nach AIFMG
- Vermögensverwalter nach VVG
- Treuhänder oder Treuhandgesellschaften nach TrHG

4. Erwartungen zum Umgang mit Cyber-Risiken

Konkret erwartet die FMA von den Finanzintermediären, Cyber-Risiken als Bestandteil des IT-Risikomanagements zu berücksichtigen. Finanzintermediäre haben die folgenden Aspekte durch ihr Risikomanagement abzudecken und diesbezüglich eine effektive Umsetzung durch geeignete Prozesse sowie eine eindeutige Verteilung von Aufgaben, Rollen und Verantwortlichkeiten sicherzustellen.

a. Die Finanzintermediäre gewährleisten die Identifikation der institutsspezifischen Bedrohungspotenziale durch Cyber-Attacken, insbesondere in Bezug auf kritische und/oder sensitive Daten und IT-Systeme. Dazu gehört die Durchführung regelmässiger Verwundbarkeitsanalysen[2] und Penetration

[1] Angriffe aus dem Internet und vergleichbaren Netzen, auf die Integrität, die Verfügbarkeit und die Vertraulichkeit der Technologieinfrastruktur, insbesondere in Bezug auf kritische und/oder sensitive Daten und IT-Systeme.
[2] Analysen zur Identifikation von derzeit bestehenden Software-Schwachstellen und Sicherheitslücken in der IT-Infrastruktur gegenüber Cyber-Attacken.

Testings[3] zur Überprüfung von Sicherheitslücken und zum Schutz kritischer und/oder sensitiver Daten und IT-Systeme.

b. Die Finanzintermediäre gewährleisten den Schutz der Geschäftsprozesse und der Technologieinfrastruktur vor Cyber-Attacken, insbesondere im Hinblick auf die Vertraulichkeit, Integrität und Verfügbarkeit der kritischen und/oder sensitiven Daten und IT-Systeme. Dazu gehören die rechtzeitige Vornahme sicherheitsrelevanter Software-Updates und notwendiger Konfigurationsänderungen.

c. Die Finanzintermediäre gewährleisten eine zeitnahe Erkennung und Aufzeichnung von Cyber-Attacken durch eine systematische Überwachung der Technologieinfrastruktur.

d. Die Finanzintermediäre gewährleisten eine Reaktion auf Cyber-Attacken durch zeitnahe und gezielte Massnahmen sowie bei wesentlichen Cyber-Attacken die Aufrechterhaltung des normalen Geschäftsbetriebs in Abstimmung mit dem Business Continuity Management.

e. Die Finanzintermediäre gewährleisten durch geeignete Massnahmen eine zeitnahe Wiederherstellung des normalen Geschäftsbetriebs nach Cyber-Attacken.

f. Die FMA erwartet ferner, dass die Finanzintermediäre die FMA innert 14 Tagen ab Kenntniserlangung über schwerwiegende oder betriebsstörende Cyber-Attacken informieren[4].

Die oben genannten Erwartungen gelten unabhängig davon, ob die Finanzintermediäre relevante Aktivitäten und Prozesse selbst ausüben oder ob sie diese auslagern oder auf andere Weise von externen Stellen beziehen.

5. Schlussbestimmungen und Inkrafttreten

Diese Mitteilung wurde von der Geschäftsleitung der FMA am 25.09.2018 genehmigt und tritt am 01.10.2018 in Kraft.

[3] Gezielte Prüfung und das Ausnützen von Software-Schwachstellen und Sicherheitslücken in der Technologieinfrastruktur, um unberechtigten Zugang zu dieser Technologieinfrastruktur zu erhalten.

[4] Schwerwiegende oder betriebsstörende Vorfälle einer Cyber-Attacke können beispielsweise der Verlust oder die ungewollte Veröffentlichung von Kundendaten oder finanzielle Schäden und Reputationsschäden nach einer Cyber-Attacke sein. Finanzielle Schäden beinhalten Zahlungen in Erpressungsfällen, nicht-autorisierte Transaktionen, Nicht-Verfügbarkeit der Verarbeitungs- und Transaktionsprozesse. Die Mitteilung sollte ausreichende Informationen zur vollständigen Nachvollziehbarkeit der Cyber-Attacke und dem Abschätzen der Folgen enthalten. Sind zum Zeitpunkt der Meldung nicht ausreichend Informationen vorhanden, können diese iterativ nachgereicht werden. Informationen zur Nachvollziehbarkeit beinhalten, sind aber nicht limitiert auf:

- Art und Ablauf des Angriffs
- Art und Anzahl betroffener Systeme und Daten
- Anzahl betroffener Mitarbeiter und Kunden
- Zeitpunkt des Angriffs und der Erkennung
- Klassifizierung und Priorisierung
- Potentielle Risiken für andere Finanzintermediäre
- Getroffene und geplante Massnahmen

Die Mitteilung ist nicht an eine bestimmte Form gebunden.