Eidgenössische Finanzmarktaufsicht FINMA
Autorité fédérale de surveillance des marchés financiers FINMA
Autorità federale di vigilanza sui mercati finanziari FINMA
Swiss Financial Market Supervisory Authority FINMA

FINMA-Aufsichtsmitteilung 05/2020

Meldepflicht von Cyber-Attacken gemäss Art. 29 Abs. 2 FINMAG

7. Mai 2020

Laupenstrasse 27
3003 Bern
Tel. +41 (0)31 327 91 00
Fax +41 (0)31 327 91 01
www.finma.ch

1 Einleitung

Die Gefahr von Cyber-Attacken[1] auf den Schweizer Finanzplatz erachtet die FINMA als weiterhin sehr hoch. Dabei stehen beaufsichtigte Institute der FINMA im Visier von Cyber-Kriminellen, die es nebst monetären Interessen auch auf die Beeinträchtigung der Verfügbarkeit, Vertraulichkeit und Integrität von kritischer Technologieinfrastruktur und sensitiven Informationen abgesehen haben. Vor allem in besonderen Stress-Situationen, wie die aktuelle COVID-19 Pandemie, besteht eine erhöhte Gefahr von Cyber-Attacken. Cyber-Kriminelle nutzen die Phase der Verunsicherung, passen Ihre Angriffsstrategien der aktuellen Situation an und belasten so die bereits geforderten Unternehmen zusätzlich.

Diese Aufsichtsmitteilung soll alle beaufsichtigten Institute der FINMA an die gemäss Art. 29 Abs. 2 FINMAG geltende gesetzliche Anforderung einer unverzüglichen Meldung von Vorkommnissen erinnern, die für die Aufsicht von wesentlicher Bedeutung sind. Dies umfasst wesentliche Vorkommnisse im Hinblick auf erfolgreiche oder teilweise erfolgreiche Cyber-Attacken.[2] Die FINMA wird nach den weiteren Erfahrungen mit dem Meldewesen die Überführung der nachstehenden Präzisierungen in ein Rundschreiben zum späteren Zeitpunkt prüfen.

2 Cyber-Attacken mit wesentlicher Bedeutung für die Aufsicht

Im Hinblick auf Cyber-Attacken ist die Wesentlichkeit dahingehend zu verstehen, dass durch eine Cyber-Attacke einerseits der Individualschutz, d. h. der Schutz der Gläubigerinnen und Gläubiger, der Anlegerinnen und Anleger sowie der Versicherten, und andererseits die Funktionsfähigkeit der Finanzmärkte direkt oder indirekt[3] beeinträchtigt wird.

Dabei stehen einerseits erfolgreiche oder teilweise erfolgreiche Cyber-Attacken auf kritische Funktionen[4] von Beaufsichtigten im Vordergrund, deren Ausfall oder Fehlfunktion erhebliche Auswirkungen auf den Individualschutz

[1] Sind 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] Für Versicherungsunternehmen erschliesst sich die Meldepflicht zudem aus der Medienwirksamkeit bzw. aufgrund des von Cyber-Attacken verursachten potentiellen Reputations- oder Solvenzschadens. Rz 1 und 5 FINMA-RS 08/25 „Auskunftspflicht Versicherer".

[3] Beispielsweise über Angriffe auf für die beaufsichtigten Institute der FINMA kritischen Infrastrukturen (z.B. *Internet Service Provider*, Stromerzeuger usw.).

[4] Produkte bzw. Dienstleistungen von Beaufsichtigten und ihre zugrundliegenden Geschäftsprozesse (bspw. Zahlungsverkehr, Bargeldversorgung, Börsenhandel, Erstellung und Verwaltung von Versicherungsverträgen, Schaden- und Leistungsbearbeitung, Datenverwaltung von besonders schützenswerte Personendaten im Kranken- und Lebensversicherungsbereich; Verwaltung von Wertpapieren und Anlagen usw.) sowie ihren kritischen Aktiven.

hätten und diese stark beeinträchtigen würden. Dies umfasst insbesondere das Schutzziel Verfügbarkeit. Andererseits können bei solchen Attacken aber auch die Schutzziele Integrität und Vertraulichkeit von Informationen bzw. Daten gefährdet sein. Sind dabei systemrelevante Institute bzw. mehrere Institute gleichzeitig oder Institute, die kritische Verbundleistungen erbringen, betroffen, wäre unter Umständen gar die Funktionsfähigkeit der Finanzmärkte in der Schweiz gefährdet.

Die Cyber-Attacken zielen in der Regel direkt auf die unterstützenden Ressourcen dieser kritischen Funktionen ab. Als unterstützende Ressourcen, die als kritische Aktiven bezeichnet werden, gelten insbesondere Personal, Technologieinfrastruktur, Informationen und Gebäude wie auch kritische Dienstleister[5], die die Geschäftsprozesse dieser kritischen Funktionen unterstützen. Jeder Beaufsichtigte hat dabei selbständig seine kritischen Funktionen, die entsprechenden Geschäftsprozesse sowie die unterstützenden kritischen Aktiven zu identifizieren[6].

Führt eine Cyber-Attacke auf kritische Aktiven dazu, dass ein bzw. mehrere Schutzziele von kritischen Funktionen und ihrer Geschäftsprozesse gefährdet sind, ist dies der FINMA unverzüglich zu melden.

[5] Gliedert ein Institut wesentliche Funktionen auf andere natürliche oder juristische Personen aus, ist das beaufsichtigte Institut ebenfalls verantwortlich für Meldungen über Cyber-Vorfälle von ihren Dienstleistern, sofern ein Bezug auf die ausgelagerten wesentlichen Funktionen besteht. Vgl. dazu Art. 47 Abs. 2 Versicherungsaufsichtsgesetz (VAG; SR 961.01)

[6] Beispielsweise Rz 135.2 bzw. Rz 135.7 ff. FINMA-RS 2008/21 „Operationelle Risiken – Banken“ bzw. SVV Mindeststandards Business Continuity Management, Rz 28 ff. FINMA-RS 2017/2 „Corporate Governance – Versicherer“

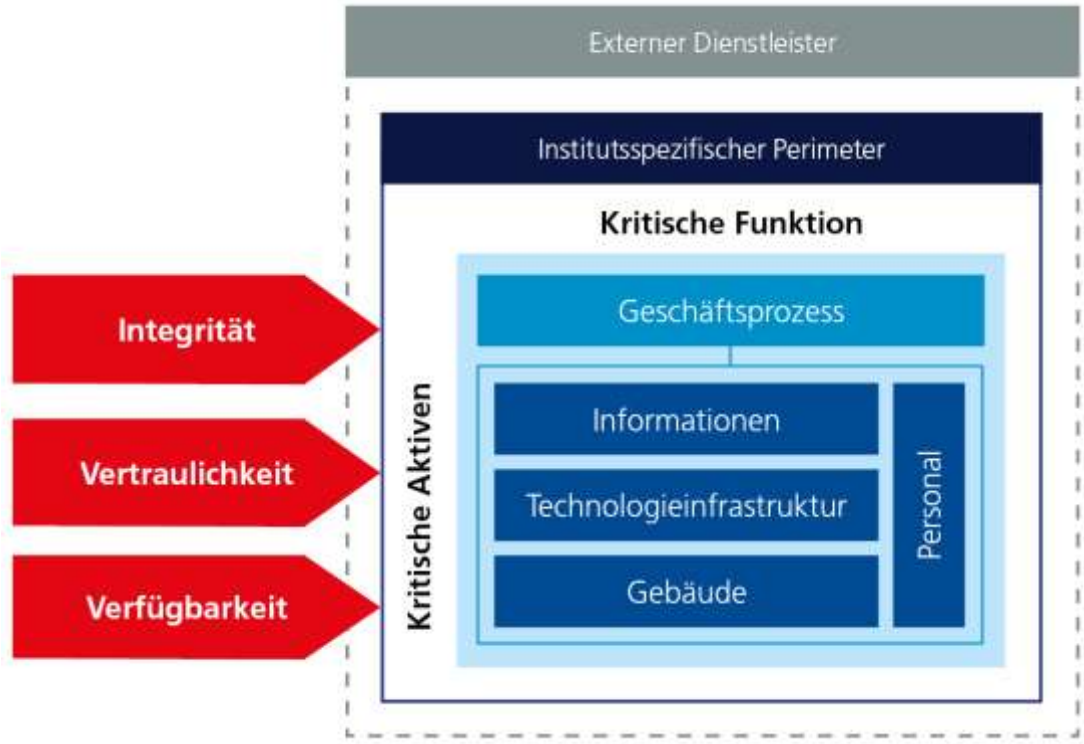

Abbildung 1: Schematische Darstellung einer Cyber-Attacke auf die kritische Funktion eines Beaufsichtigten.

Nicht abschliessende Beispiele für kritische Aktiven und mögliche Cyber-Attacken auf diese sind in Anhang 2 aufgeführt.

3 Unverzügliche Meldung an die FINMA

Eine unverzügliche Meldung an die FINMA bedeutet, dass der betroffene Beaufsichtigte bei Feststellung einer solchen Cyber-Attacke, und einer Erstbeurteilung über dessen Kritikalität, innerhalb von 24 Stunden die FINMA über den zuständigen *(Key)-Account Manager* vororientiert. Die eigentliche Meldung soll entlang der folgenden Liste innerhalb von 72 Stunden über die webbasierten Erhebungs- und Gesuchsplattform (EHP) der FINMA erfolgen[7,8].

Die folgende Liste beinhaltet Anhaltspunkte für den Inhalt einer solchen Meldung an die FINMA:

- Name des Instituts

[7] https://www.finma.ch/de/finma/extranet/erhebungs--und-gesuchsplattform/ (verfügbar ab dem 1. Juni 2020)

[8] Auf der EHP Plattform: "EHP" – "Meldungen" – Schaltfläche: "Neue Meldung" – Meldungsvorlage: "Meldung Cyber-Attacke"

- Kontaktperson inkl. Kontaktdaten (Telefon & E-Mail Adresse)
- Datum / Uhrzeit Meldung an FINMA
- Datum / Uhrzeit Feststellung Angriff
- Datum / Uhrzeit Angriffszeitpunkt (sofern bereits bekannt)
- Beschreibung der Cyber-Attacke und aktueller Status
- Erstbeurteilung Schweregrad der Cyber-Attacke (Siehe Anhang 1) *(Einfachauswahl: mittel, hoch, schwerwiegend)*
- Trend des Schweregrads *(Einfachauswahl: abnehmend, stabil, erhöhend)*
- Betroffene Entitäten (Betroffene Organisationseinheit(en) im Institut bzw. Dienstleister)
- Betroffene Schutzziele (*Mehrfachauswahl: Vertraulichkeit, Integrität, Verfügbarkeit)*
- Betroffene kritische Funktionen, Geschäftsprozesse bzw. Aktiven (Betroffene Informationen, Technologieinfrastruktur, Gebäude oder Personal)
- Betroffene Anzahl Kunden (aktueller Stand)
- Angriffsvektoren (*Mehrfachauswahl: E-Mail, Web-basierter Angriff, Brute-Force-Angriff, Identitätsdiebstahl, externe Wechselmedien, Verlust/Diebstahl von Geräten, Ausnutzung von Software-Schwachstelle, Ausnutzung von Hardware-Schwachstelle, Andere [Bitte definieren]*)
- Typus des Angriffs (Beschreibung) (z.B. DDoS, Unautorisierter Zugriff, Schadsoftware, Missbrauch / unsachgemässe Benutzung von Technologieinfrastruktur usw.)
- Administrative, operative und/oder technische Gegenmassnahmen mit erwarteter Fristigkeit
- Kommunikationsmassnahmen (was, an wen, wann)

Ergeben sich nach vollständig erfüllter Meldepflicht neue Entwicklungen oder Einschätzungen zur selben Attacke, ist wiederum innert der erwähnten Frist von 72 Stunden eine erneute Meldung zu erstatten.

Für Cyber-Attacken mit Schweregrad Hoch und Schwerwiegend (vgl. Anhang 1) erwartet die FINMA nach Abschluss der institutsseitigen Fallbearbeitung einen abschliessenden Ursachenbericht (*Root-Cause*-Analyse) inklusive einer Analyse, Grund für den Erfolg der Attacke, Auswirkungen der Attacke für die Einhaltung von regulatorischen Vorgaben, den Betrieb und die Kunden sowie mindernde Massnahmen, um die Konsequenzen der Attacke zu adressieren. Für Cyber-Attacken mit Schweregrad Schwerwiegend (vgl. Anhang 1) sind zudem Nachweise und Analysen zur Funktionsfähigkeit der Krisenorganisation einzureichen.

Für Cyber-Attacken mit dem Schweregrad Mittel (vgl. Anhang 1) reicht ein abschliessenden Ursachenbericht.

Die FINMA erwartet die Umsetzung der Konkretisierung aus der Aufsichtsmitteilung zur Meldung von Cyber-Attacken bis spätestens per 1. September 2020 oder auf *Best-Effort*-Basis bereits früher.

Anhang 1: Ermittlung des Schweregrades einer Cyber-Attacke

Als Erstbeurteilung für die Ermittlung des Schweregrades einer Cyber-Attacke können folgende Kriterien angewandt werden:

Schweregrad	Definition	Kriterien
Schwerwiegend	Umfangreiche und länger anhaltende Schäden an Schutzzielen (Verfügbarkeit, Integrität, Vertraulichkeit) kritischer Aktiven vorhanden bzw. erwartet.	– Verfügbarkeit: Kritische Aktiven sind mittel- bis langfristig nicht verfügbar (Ausfall > 200 % des RTO[9]) – Vertraulichkeit / Integrität: Sensitive Informationen in (fast) vollumfänglichen Ausmass betroffen – Existenzbedrohende finanzielle Auswirkungen bzw. Reputationsschäden – Die Bewältigung der Cyber-Attacke bedingt die Aktivierung der Krisenorganisation (BCM).
Hoch	Schutzziele (Verfügbarkeit, Integrität, Vertraulichkeit) kritischer Aktiven sind erheblich geschädigt bzw. bedroht.	– Verfügbarkeit: Kritische Aktiven sind mittelfristig nicht verfügbar (Ausfall >= RTO) – Vertraulichkeit / Integrität: Sensitive Informationen im umfangreichen Ausmass und / oder für den Geschäftsprozess kritische Informationen betroffen – Erhebliche finanzielle Auswirkungen bzw. Reputationsschäden – Die Bewältigung der Cyber-Attacke bedingt den Beizug von externen Ressourcen.
Mittel	Unmittelbare Schädigung bzw. Bedrohung von Schutzzielen (Verfügbarkeit, Integrität, Vertraulichkeit) kritischer Aktiven.	– Verfügbarkeit: Kritische Aktiven sind kurzfristig nicht verfügbar (Ausfall > 50 % des RTO) – Vertraulichkeit / Integrität: Sensitive Informationen massgeblich[10] betroffen – Wahrnehmbare finanzielle Auswirkungen bzw. Reputationsschäden – Die Cyber-Attacke kann intern mit den zur Verfügung stehenden Ressourcen bewältigt werden.

[9] *Recovery Time Objective* – Festgesetzte Sollzeit für die Wiederinbetriebnahme von kritischen Aktiven

[10] Ausserhalb des normalen Geschäftszustandes (*Business as Usual*)

Anhang 2: Beispiele für kritische Aktiven und Cyber-Attacken auf dessen Schutzziele

	Beispiele für kritische Aktiven	Beispiele für Cyber-Attacken
Informationen	Sensitive / vertrauliche Informationen wie z.B. Kundenidentifikationsdaten, Versicherungsverträge, Daten in Zusammenhang mit der Schadenregulierung bzw. Leistungsbearbeitung, VR- bzw. Geschäftsleitungsprotokolle, Strategieinformationen, HR-Daten usw.	Angriffe auf Schutzziele mittels unautorisiertem Datenzugriff unternehmensintern oder auch von extern, Datenabflüsse, Datendiebstahl, Daten-Veränderung usw.
Technologieinfrastruktur	Für das Ausführen einer kritischen Funktion notwendige Technologieinfrastruktur (z.B. *Hardware*, *Software*, Netzwerkinfrastruktur usw.)	Angriffe auf Schutzziele mittels (D)DoS, Verlust / Diebstahl von Speichermedien mit vertraulichen Informationen, *Ransomware* usw.
Gebäude	Essenzielle Gebäude für das Erbringen von kritischen Funktionen (z.B. Rechenzentren, Filialen, *Backoffice* Büroräumlichkeiten usw.)	Angriffe auf Schutzziele mittels Störung oder Deaktivierung der Schutzmassnahmen zur Regelung des autorisierten Zugangs zu sensitiven Bereichen usw.
Personal	Mitarbeitende, die kritischen Funktionen ausführen oder wesentlich dazu beitragen wie z.B. Geschäftsleitung, Händler, Kundenberater usw. sowie auch Schlüsselmitarbeitende (z.B. Mitarbeitende mit erhöhten Rechten, Systemadministratoren, Sicherheitspersonal, Buchhaltung usw.)	Angriffe auf Schutzziele mittels Social Engineering (wie z.B. *Spear Phishing*), Insider-Bedrohungen, Identitätsdiebstahl, Erpressung usw.