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 03/2024

Erkenntnisse aus der Cyber-Risiko-Aufsichtstätigkeit, Präzisierung zur FINMA-Aufsichtsmitteilung 05/2020 und zu szenariobezogenen Cyber-Übungen

7. Juni 2024

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

Inhaltsverzeichnis

1 Einleitung

Seit mehreren Jahren zählen die Cyber-Risiken zu den Hauptrisiken, welche die FINMA in ihrem jährlich publizierten Risikomonitor aufführt. Die Anzahl der bei der FINMA eingegangenen Meldungen über erfolgreiche oder teilweise erfolgreiche Cyber-Attacken steigt dabei jährlich an.

Mit der FINMA-Aufsichtsmitteilung 05/2020 „Meldepflicht von Cyber-Attacken gemäss Art. 29 Abs. 2 FINMAG“ wurde die entsprechende Meldepflicht näher umschrieben. Die seither eingegangenen Meldungen zeigen unterschiedliche Entwicklungen in der Bedrohungslage, den Angriffsmethoden und den Zielen der Angriffe. Durch die Aufsichtstätigkeit erhält die FINMA ein detailliertes Bild über den Umgang der beaufsichtigten Institute mit Cyber-Risiken. Vor allem die cyberspezifischen Vor-Ort-Kontrollen ermöglichen es der FINMA, eine vertiefte Einschätzung der Maturität des Cyber-Abwehrdispositives der beaufsichtigten Institute vorzunehmen. Die Erkenntnisse daraus und die institutsspezifischen Feststellungen wurden jeweils im FINMA-Risikomonitor und im FINMA-Geschäftsbericht auf aggregierter Basis veröffentlicht.

In der vorliegenden Aufsichtsmitteilung vermittelt die FINMA den Beaufsichtigten anhand dieser Erkenntnisse spezifische Hinweise zum Umgang mit Cyber-Risiken. Diese Hinweise sind für alle von der FINMA beaufsichtigten Institute relevant. Bei gewissen Punkten wird explizit auf das FINMA-Rundschreiben 2023/1 „Operationelle Risiken und Resilienz – Banken“ eingegangen. Diese Hinweise richten sich primär an Institute, für welche dieses Rundschreiben zur Anwendung kommt, können jedoch auch den übrigen Instituten als Leitlinie dienen.

In diesem Zusammenhang werden auch wiederkehrende Fragestellungen zur FINMA-Aufsichtsmitteilung 05/2020 „Meldepflicht von Cyber-Attacken gemäss Art. 29 Abs. 2 FINMAG“ behandelt.

Abschliessend wird auf die Rz 70 des FINMA-RS 23/1 eingegangen und dieses präzisiert.

2 Erkenntnisse aus der Cyber-Risiko-Aufsichtstätigkeit

2.1 Auslagerungen

Bereits im FINMA-Risikomonitor 2020 berichtete die FINMA über eine Zunahme von erfolgreichen Angriffen auf die Lieferketten der beaufsichtigten Institute, was einen Anteil von rund 25% aller Attacken ausmachte. In den Folgejahren stieg diese Zahl bereits auf über 50% an und hielt sich stabil in diesem Bereich. Die FINMA hat sich deshalb intensiver mit dem Thema Cyber-Risiken bei Auslagerungen auseinandergesetzt[1] und dieses zu einem Aufsichtsschwerpunkt gemacht. Das Ziel der FINMA war es herauszufinden, aus welchem Grund Angriffe auf Dienstleister überdurchschnittlich häufig erfolgreich waren. Die Vor-Ort-Kontrollen zeigten, dass die Gründe u.a. in unklaren Anforderungen von den beaufsichtigten Instituten an die beauftragten Dienstleister hinsichtlich der Cyber-Sicherheit und in der fehlenden oder unregelmässigen Überprüfung dieser Anforderungen lagen:

- Nur sehr wenige Institute waren nach der Identifikation von schwerwiegenden Sicherheitslücken proaktiv im Austausch mit ihren wichtigsten Dienstleistern, um sicherzustellen, dass diese die Schwachstelle zügig und vor Eintritt eines Schadens schliessen.
- Die FINMA beobachtete häufig, dass die direkt beaufsichtigten Institute schwerwiegende Schwachstellen schnell unter Kontrolle brachten und so einen direkten Schaden abwenden konnten. Einige Dienstleister gingen jedoch oftmals nicht mit derselben Effektivität vor und waren nicht ausreichend auf erfolgreiche Cyber-Angriffe vorbereitet.
- Sehr oft verfügten die Institute über kein vollständiges Inventar ihrer Dienstleister: Es fehlten Informationen darüber, ob beim Dienstleister kritische Daten gespeichert sind oder dieser mit der Erbringung einer kritischen Funktion beauftragt ist. Deshalb fand bei solchen Dienstleistern oftmals eine lückenhafte oder gar keine regelmässige Kontrolle durch die beaufsichtigten Institute statt.
- Bei der Inventarisierung der wesentlichen Unterakkordanten bei Auslagerungen zeigten sich zwischen den untersuchten Instituten grosse Unterschiede im Reifegrad der Erfassung, Dokumentation und der Zugriffsmöglichkeiten auf kritische Daten[2].
- Die betroffenen Institute hatten grösstenteils nicht klar definiert, was für sie kritische Daten sind. Dies erschwerte nicht nur den internen Schutz dieser Daten, sondern auch die angemessene Klassifizierung der Dienstleister und die Bestimmung der erforderlichen Kontrollmassnahmen zur Reduktion der identifizierten Risiken.

[1] Siehe dazu auch das neue Hauptrisiko „Outsourcing“ im Risikomonitor 2023 und FINMA-Jahresbericht 2023.

[2] Siehe dazu auch Rz 14 FINMA-RS 18/3.

Weist ein Institut eine wesentliche Auslagerung an einen Dienstleister auf (insbesondere im Hinblick auf kritische Funktionen bzw. kritische Daten in relevantem Masse), müssen dort dieselben regulatorischen Anforderungen wie beim beaufsichtigten Institut sichergestellt werden. Gleichfalls sind diese Anforderungen auch anwendbar für allfällig involvierte Unterakkordanten. Darum erachtet die FINMA ein aktuelles Inventar ihrer wesentlichen Auslagerungen, inkl. der Unterakkordanten, als essenzielles Instrument.

Das Institut bleibt für die Einhaltung der aufsichtsrechtlichen Anforderungen jederzeit verantwortlich. Eine Auslagerung oder Übertragung dieser Verantwortung an einen Dienstleister ist nicht möglich.

2.2 Governance und Identifikation

Ein weiterer zentraler Bereich ist die Governance im Umgang mit Cyber-Risiken. In der Vergangenheit hat die FINMA häufig festgestellt, dass Cyber-Risiken als reines Technologie-Problem dargestellt wurden und dadurch nicht die notwendige Priorität in der Geschäftsleitung bzw. im Verwaltungsrat erhielten. Aus diesem Grund wurde z.B. für die Banken im neuen FINMA-RS 23/1 die Verantwortlichkeiten für das Oberleitungsorgan sowie die Geschäftsleitung klar definiert (vgl. Rz 61). Die FINMA stellte zudem bei vielen beaufsichtigten Instituten folgende weitere Schwachstellen im Bereich der Governance fest:

- Bei mittelgrossen Instituten bestand oftmals keine klare Abgrenzung zwischen dem operativen Umgang mit Cyber-Risiken und der unabhängigen Kontrollinstanz. Es ist wesentlich, dass der operative Umgang kontinuierlich von einer unabhängigen Kontrollinstanz auf ihre Effektivität überprüft wird[3].
- Die Identifizierung der institutsspezifischen Cyber-Risiko-Bedrohungspotenziale war häufig lückenhaft. Zudem war oft nicht bekannt, welche Mitarbeitenden Zugriff auf kritische Daten hatten, da ein zentrales Berechtigungstool fehlte. Dieser Umstand erschwerte es der Sicherheitsorganisation des jeweiligen Instituts, ein auf die kritischen Daten ausgerichtetes Schutzdispositiv zu erstellen.
- Etliche beaufsichtigte Institute integrierten die Cyber-Risiken nicht explizit in ihr übergreifendes Management der operationellen Risiken. Aufgrund dessen konnte kein systematisches und umfassendes Cyber-Risiko-Management gewährleistet werden.

[3] Siehe Abschnitte zu Kontrollfunktionen und unabhängigen Kontrollinstanzen in den FINMA-Rundschreiben 2017/1 „*Corporate Governance* – Banken“ und 2017/2 „*Corporate Governance* – Versicherer“.

- Zudem definierten einige beaufsichtigte Institute die Cyber-Risiken und ihren entsprechenden Risikoappetit und die Risikotoleranz ungenügend. Diese stellen jedoch zentrale Komponenten eines effektiven Schutzdispositivs vor Cyber-Risiken dar.

Gemäss dem FINMA-Risikomonitor gehören Cyber-Risiken seit Jahren zu den Hauptrisiken, weshalb es von zentraler Bedeutung ist, dass die beaufsichtigten Institute dieses Risiko als eigenständiges Risiko im Management der qualitativen operationellen Risiken erfassen und einen entsprechenden Risikoappetit sowie Risikotoleranzen definieren.

Ebenso ist unerlässlich, dass in Bezug auf Cyber-Risiken Schlüsselkontrollen nach international anerkannten Standards oder *Practices* in das interne Kontrollsystem (IKS) integriert werden und dass deren Wirksamkeit regelmässig durch eine unabhängige Kontrollstelle geprüft, bewertet und dokumentiert werden. Auch die Trennung der Aufgaben, Kompetenzen und Verantwortlichkeiten (AKV) zur Sicherstellung der Unabhängigkeit und Vorbeugung vor Interessenskonflikten ist regelmässig zu beurteilen.

2.3 Schutzdispositiv

Im Bereich des Schutzdispositivs konnte in der laufenden Aufsicht der vergangenen Jahre eine positive Tendenz beobachtet werden. Beispielsweise trafen die beaufsichtigten Institute im Bereich der Abwehr von *Distributed-Denial-of-Service*-Angriffen[4] immer bessere und effektivere Schutzmassnahmen. Allerdings gab es auch in diesem Bereich wesentliche Erkenntnisse zu vorhandenen Schwachstellen:

- Die Schutzmassnahmen zur *Data Loss Prevention*[5] (DLP) beschränkten sich oftmals nur auf Kundenidentifikationsmerkmale bzw. Kreditkartennummern. Weitere kritische Daten wie z.B. schützenswerte Personendaten, Geschäftsgeheimnisse, geistiges Eigentum, usw. wurden von DLP-Schutzmassnahmen nicht erfasst.
- Fast alle kontrollierten Institute hatten eine Richtlinie und Prozesse hinsichtlich Datensicherung (*Back-up*) sowie Wiederherstellungspläne definiert. Bei einigen Instituten fehlte aber ein Test dieser Prozesse im Falle eines schwerwiegenden Cyber-Angriffs, z.B. durch eine Verschlüsselungs-Schadsoftware (*Ransomware*).
- Bei einer grossen Anzahl von beaufsichtigten Instituten besteht auch Verbesserungspotenzial in den Bereichen Cyber-Training und -Bewusstsein. Für ein wirksames Schutzdispositiv ist es unerlässlich, dass Mitar-

[4] DDoS-Attacke: Durch hohe Anzahl von Anfragen, ausgehend von verteilter Rechenleistung, wird eine Überlastung der Systeme (z.B. einer Internetseite) bewirkt.

[5] DLP: Verhinderung von Datenabfluss

beitende auf allen Hierarchiestufen regelmässig über Cyber-Risiken informiert bzw. trainiert werden, die gängigsten Angriffsmethoden wie etwa *Phishing* kennen und wissen, an welche Stellen sie sich im Unternehmen wenden sollen, wenn sie Hinweise für einen Cyber-Angriff erkennen. Dieses Ziel kann insbesondere durch regelmässige Tests der Mitarbeitenden angestrebt werden.

Für Institute, für welche das FINMA-RS 23/1 zur Anwendung kommt, sind die Anforderungen betreffend Cyber-Risiko-Training und -Bewusstsein explizit im Rundschreiben enthalten (vgl. Rz 26).

Darüber hinaus ist es unerlässlich, dass sich alle Institute mit einem Szenario auseinandersetzen, in dem ihre Schutzvorkehrungen überwunden werden können und es einem Angreifer gelingen könnte, den grösstmöglichen Schaden im Unternehmen anzurichten. Es ist dabei wichtig, dass bestehende *Back-up*- und Wiederherstellungsstrategien dahingehend überprüft werden, ob bspw. im Rahmen einer Komplett-Verschlüsselung der (kritischen) Daten, diese innerhalb der gesetzten Fristen und gewünschten Aktualität, Integrität und Qualität sowie Vollständigkeit wiederhergestellt werden können. Für Banken wird in diesem Zusammenhang insbesondere auf die neuen aufsichtsrechtlichen Anforderungen zur Einhaltung der operationellen Resilienz gemäss FINMA-RS 23/1 verwiesen.

2.4 Detektion, Reaktion und Wiederherstellung

Die Fähigkeit, zeitnah Cyber-Attacken aufzuzeichnen, zu erkennen und darauf zu reagieren ist bei den meisten Cyber-Risiko Vor-Ort-Kontrollen der FINMA ein Schwerpunkt und oftmals auch das Thema von vertieften Prüfungen.

Während diesen Vor-Ort-Kontrollen beobachtete die FINMA insbesondere folgende wiederkehrenden Muster bei den beaufsichtigten Instituten:

- Einige der Institute hatten keine oder unvollständige Reaktionspläne für Cyber-Vorfälle oder überprüften diese nicht auf ihre Effektivität.
- Bei der Erkennung und Aufzeichnung von Cyber-Attacken zeigte sich zudem, dass einige Institute ihre Informations- und Kommunikationstechnologie nicht zeitnah und systematisch überwachten. Teilweise fehlte eine Auswertung von kritischen Log-Daten oder diese fand nur während der Bürozeiten statt.
- Die meisten Institute trafen Vorkehrungen, um eine zeitnahe Wiederherstellung des normalen Geschäftsbetriebs nach ausserordentlichen Ereignissen sicherzustellen. Dabei fehlten allerdings oftmals spezifische Wiederherstellungsmassnahmen nach Cyber-Attacken.

Die risikoorientierte und szenariobezogene Vorbereitung der beaufsichtigten Institute auf Cyber-Vorfälle und -Krisen ist zentral. Dabei stellt die Erstellung von realistischen bzw. getesteten Reaktionsplänen ein wesentlicher Erfolgsfaktor dar, um infolge Cyber-Attacken bedingte Stresssituationen effektiv meistern zu können. Insbesondere ist es nach einer erfolgreichen Cyber-Attacke äusserst wichtig, entsprechende Lehren zu ziehen und Verbesserungen umgehend umzusetzen.

3 Präzisierungen zur FINMA-Aufsichtsmitteilung 05/2020

Seit der Präzisierung der Meldepflicht für Cyber-Attacken aller beaufsichtigten Institute in der FINMA-Aufsichtsmitteilung 05/2020 hat die FINMA diverse Anfragen zu deren Auslegung erhalten.

Aufgrund dessen werden nachfolgend einige Punkte präzisiert:

- Ab dem Zeitpunkt der Entdeckung einer Cyber-Attacke hat das Institut 24 Stunden Zeit für eine Erstmeldung an die FINMA.
- Innerhalb dieser 24 Stunden wird von den beaufsichtigten Instituten erwartet, dass sie eine Erstbeurteilung über dessen Kritikalität vornehmen, um zu beurteilen, ob die Cyber-Attacke die Wesentlichkeit für eine Meldung an die FINMA erfüllt[6].
- Für die Erstmeldung innerhalb von 24 Stunden erwartet die FINMA eine formlose Meldung per E-Mail, Telefon usw. an den jeweiligen Aufsichts-*Key Account Manager* des betroffenen beaufsichtigten Instituts. Diese Erstmeldung soll eine Erstbeurteilung der Kritikalität enthalten und prägnant umschreiben, was bisher bekannt ist. Ein vollständig ausgefülltes Formular in der webbasierten Erhebungs- und Gesuchsplattform (EHP) ist zu diesem Zeitpunkt nicht erforderlich.
- Institute, welche ebenfalls der Meldepflicht gemäss Informationssicherheitsgesetz (ISG; SR *128*) unterstehen, können ihre 24 Stunden Meldung über das Meldeformular des Bundesamtes für Cybersicherheit (BACS) einreichen und die Option anwählen, die Meldung an die FINMA weiterzuleiten, sofern die Einhaltung der Frist sichergestellt werden kann. Die vollständige 72 Stunden Meldung muss weiterhin über die EHP eingegeben werden.
- Muss ein Institut abwägen, ob es die Ermittlung des Schweregrades für eine Erstbeurteilung abschliesst oder die Frist von 24 Stunden einhält, ist der Einhaltung der Frist Priorität einzuräumen.

[6] Siehe FINMA-Aufsichtsmitteilung 05/2020, Anhang 1.

- Eine bereits erfolgte Erstmeldung innerhalb von 24 Stunden an die FINMA kann jederzeit wieder zurückgezogen werden, falls das Institut im Rahmen der weiteren Ermittlungen des Schweregrades und dessen Beurteilung zum Schluss kommt, dass die Cyber-Attacke nicht die Wesentlichkeitsschwelle erreicht hat.
- Ist der Dienstleistungserbringer eines Instituts (z.B. Spital, Vermögensverwalter, Anwaltskanzlei) kein wesentlicher Outsourcing-Partner im Sinne des FINMA-Rundschreiben 18/3 „Outsourcing“, muss das Institut – gestützt insbesondere auf Art. 22 VAG, Rz 68 FINMA-RS 23/1, FINMA-Aufsichtsmitteilung 05/2020 – sicherstellen, dass es vom Dienstleistungserbringer über Cyber-Vorfälle bei diesem informiert wird. Stuft das Institut in einem solchen Fall einen ihm entsprechend gemeldeten Cyber-Vorfall als relevant im Sinne der FINMA-Aufsichtsmitteilung 05/2020 ein, so hat es auch die erforderlichen Meldungen an die FINMA vorzunehmen.
- Die Meldefristen von 24 bzw. 72 Stunden zählen nur an offiziellen Bankarbeitstagen. Eine Ausnahme bilden Cyber-Attacken mit dem Schweregrad „schwerwiegend“. Diese sind der FINMA auch ausserhalb von Bankarbeitstagen innert 24 Stunden zu melden.
- Die Meldepflicht bei Auslagerungen gestaltet sich folgendermassen: Gemäss Rz 23 FINMA-RS 18/3 tragen die Beaufsichtigten gegenüber der FINMA weiterhin dieselbe Verantwortung, wie wenn es die ausgelagerte Funktion selbst erbringen würde. Dies bedeutet im Umkehrschluss, dass die Meldefrist zu laufen beginnt, sobald das Institut, oder bei ausgelagerten Funktionen der Drittanbieter, einen Cyber-Vorfall entdeckt hat. Dies stellt auch die aufsichtsrechtliche Gleichbehandlung von Instituten sicher, welche keine Funktionen ausgelagert haben.
- Gemäss FINMA-Aufsichtsmitteilung 05/2020 wird für Meldungen für Cyber-Attacken mit dem Schweregrad „mittel“ ein abschliessender Ursachenbericht gefordert, welcher mindestens den internen oder externen Untersuchungs- bzw. forensischen Bericht umfasst. Bei Meldungen für Cyber-Attacken mit dem Schweregrad „hoch“ oder „schwerwiegend“ sollte dieser Ursachenbericht Folgendes umfassen:
  - Grund für den Erfolg der Cyber-Attacke;
  - Auswirkungen der Attacke auf die Einhaltung der aufsichtsrechtlichen Vorgaben, den Betrieb des Instituts und die Kunden;
  - eingeleitete Minderungsmassnahmen, um die Auswirkungen der Attacke zu adressieren.

  Für Cyber-Attacken mit dem Schweregrad „schwerwiegend“ sind zudem Nachweise und Analysen zur Funktionsfähigkeit der Krisenorganisation einzureichen.

4 Szenariobezogene Cyber-Übungen

Für Institute, für welche das FINMA-RS 23/1 zur Anwendung kommt, sind gemäss Rz 70 FINMA-RS 23/1 risikobasiert szenariobezogene Cyber-Übungen durchzuführen. Umfang und Inhalt dieser Übungen richten sich nach dem Proportionalitätsprinzip. Für systemrelevante Institute erachtet die FINMA *Red-Teaming*-Übungen[7] als erforderlichen Bestandteil der Cyber-Übungen. Nicht systemrelevante Institute sollten mindestens eine jährliche *Table-Top*-Übung[8] durchführen.

Mittels Teilnahme an den Übungen des Swiss Financial Sector Cyber Security Centre (Swiss FS-CSC)[9] können die Institute der Aufsichtskategorien 4 und 5 dieser Pflicht nachkommen. Dabei ist bei jedem teilnehmenden Institut sicherzustellen, dass das institutsspezifische Bedrohungspotenzial dieser Übungen nachvollziehbar dokumentiert wird sowie die institutsspezifischen Erkenntnisse aus diesen Übungen rapportiert werden. Wenn sich das institutsspezifische Bedrohungspotenzial aus der Cyber-Übung des Swiss FS-CSC nicht ableiten lässt, da bspw. das Übungsszenario keine ausgeprägte Relevanz für das Cyber-Risiko-Profil eines Instituts hat, dann hat dieses Institut zur Adressierung der Rz 70 trotzdem eine individuelle szenariobezogene Cyber-Übung durchzuführen.

Die FINMA behält sich vor, solche risikobasierte szenariobezogene Cyber-Übungen selektiv im Rahmen der aufsichtsrechtlichen Prüfung oder einer Zusatzprüfung durchführen zu lassen und eng zu begleiten. Es sollen dabei etablierte Rahmenwerke[10] als Grundlage verwendet werden.

[7] *Red Teaming*: Sicherheitsexperten übernehmen die Rolle eines Angreifers und versuchen, die Cybersicherheitsvorkehrungen eines Unternehmens anzugreifen und diese zu umgehen, indem die Angriffsweise eines „bösartigen" Hackers kopiert wird.

[8] *Table-Top*-Übung: Simulation und Durchspielen eines Szenarios auf dem Papier (Trockenübung)

[9] Vgl. https://fscsc.ch/

[10] Wie z.B. TIBER-EU, CBEST Threat Intelligence-Led Assessments