FMA

Finanzmarktaufsicht
Liechtenstein

FMA-Merkblatt 2019/1 – Orientierungshilfe Cyber-Security

Orientierungshilfe zur Umsetzung der Anforderungen der FMA-Mitteilung 2018/3 betreffend den Umgang mit Cyber-Risiken.

Durch diese Orientierungshilfe werden keine neuen Anforderungen gestellt. Es handelt sich um eine Auslegungshilfe. Sie verfolgt insbesondere das Ziel, für die beaufsichtigten Unternehmen ein Problembewusstsein im Umgang mit Cyber-Risiken zu schaffen und mögliche Umsetzungskontrollen und -massnahmen aufzuzeigen, um den einzelnen Aspekten der FMA-Mitteilung 2018/3 gerecht zu werden. Die Orientierungshilfe ist weder rechtlich bindend noch ist sie abschliessend.

Referenz:	FMA-MB 2019/1
Adressaten:	- Banken nach BankG
	- Wertpapierfirmen nach BankG
	- E-Geld-Institute nach EGG
	- Zahlungsinstitute nach ZDG
	- Versicherungsunternehmen nach VersAG
	- Versicherungsvermittler nach VersVertG
	- 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
Betrifft:	FMA-M 2018/3
Publikationsort:	Webseite
Publikationsdatum:	20. Februar 2019
Letzte Änderung:	20. Februar 2019

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

In der FMA-Mitteilung 2018/3 „Umgang mit Cyber-Risiken“ werden die Erwartungen der FMA zum Umgang mit Cyber-Risiken bei Finanzintermediären festgelegt. Das Risikomanagement jedes Finanzintermediärs soll die in der Mitteilung festgehaltenen Aspekte (Ziffer 4 Absatz a bis f) abdecken und die Umsetzung soll durch geeignete Prozesse sowie eine eindeutige Zuordnung von Aufgaben, Rollen und Verantwortlichkeiten sichergestellt werden.

Die hier folgenden Absätze beschreiben mögliche Umsetzungskontrollen und -massnahmen, um den einzelnen Aspekten der FMA-Mitteilung gerecht zu werden. Zu jeder Kontrolle ist ein Umsetzungsleitfaden beschrieben, der Aktivitäten, Methoden und Beispiele beinhaltet. Sowohl die Kontrollen als auch die Umsetzungsleitfäden basieren auf etablierten, international anerkannten Industriestandards und Good Practices – insbesondere auf der Standard-Reihe ISO/IEC 27002 (für Informationssicherheits-Managementsysteme) und den Standards des National Institute of Standards and Technology (NIST) für Cyber Security und Informationssicherheit. Referenzen zu relevanten Passagen der Standards sind jeweils vermerkt.

Die Kontrollen sollen die Cyber-Risiken der Finanzintermediäre auf ein adäquates Risikoniveau reduzieren. Hierzu werden die möglichen Angriffsarten berücksichtigt. In Anhang 1 dieser Orientierungshilfe ist eine Auswahl relevanter Angriffsarten beschrieben und es ist dargestellt, durch welche Kontrollen diese abgedeckt werden.

a. Identifikation

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[1] und Penetration Testings[2] zur Überprüfung von Sicherheitslücken und zum Schutz kritischer und/oder sensitiver Daten und IT-Systeme.

Kontrolle	Umsetzungsleitfaden
A1. Kritische und/oder sensitive Daten und IT-Systeme werden durch die Etablierung einer Kritikalitätsanalyse identifiziert.	- Eine Methode zur Analyse der Kritikalität von Daten und IT-Systemen sollte entwickelt und implementiert werden, unter Berücksichtigung von Vertraulichkeit, Verfügbarkeit und Integrität. - Eine Kritikalitätsanalyse sollte bei signifikanter Änderung oder Neuentwicklung eines Systems durchgeführt werden. - Ergebnisse der Kritikalitätsanalyse sollten dokumentiert werden. Beispiel: Ein Beispiel-Schema zur Kritikalitätseinstufung kann in Anhang 2 gefunden werden.

Referenz Beispiel:
NIST Special Publication 800-53 Rev. 4: SA-14

[1] Analysen zur Identifikation von derzeit bestehenden Software-Schwachstellen und Sicherheitslücken in der IT-Infrastruktur gegenüber Cyber-Attacken.
[2] Gezielte Prüfung und das Ausnützen von Software-Schwachstellen und Sicherheitslücken in der Technologieinfrastruktur, um unberechtigten Zugang zu dieser Technologieinfrastruktur zu erhalten.

A2. Eine Risikoanalyse gewährleistet die Identifikation der institutionsspezifischen Bedrohungspotenziale.	- Eine Methode zur Analyse des Risikos in Bezug auf die unautorisierte Löschung, Modifikation, Einsehung oder Veröffentlichung der Daten eines Informationssystems sollte entwickelt und implementiert werden. Diese sollte Faktoren wie die Bedrohung, Schwachstellen, Wahrscheinlichkeit und Auswirkung einbeziehen. - Ergebnisse der Risikoanalyse sollten dokumentiert werden. Beispiel: Ein Risiko-Bewertungsschema kann in Anhang 3 gefunden werden.

Referenz Beispiel:
ISO/IEC 27002: 12.6.1
NIST Special Publication 800-53 Rev. 4: RA-3

A3. Verwundbarkeitsanalysen und Penetration Testings werden auf regelmässiger Basis durchgeführt.	- Verwundbarkeitsanalysen und Penetration Testings sollten in regelmässigen Intervallen durchgeführt werden. Die Festlegung der Intervalle kann auf Grundlage der Kritikalitätsanalyse (siehe A1) vorgenommen werden. Bei Änderungen mit erhöhtem Risiko sind anlassbezogen Verwundbarkeitsanalysen und Penetration Testings durchzuführen. - Verwundbarkeitsanalysen und Penetration Testings sollten zur Vermeidung negativer Auswirkungen vorher geplant und in einer solchen Weise dokumentiert werden, dass sie wiederholbar sind. - Eine Verwundbarkeitsanalyse bzw. ein Penetrationstest sollte die Phasen (a) eines Pre-Tests zur Identifikation der Systeme, (b) die Identifikation von Schwachstellen und – bei Penetration Testings – (c) Tests zur Ausnutzung der identifizierten Schwachstellen umfassen. - Verwundbarkeitsanalysen und Penetration Testings können auch von damit beauftragten externen Experten durchgeführt werden. - Die Ergebnisse der Verwundbarkeitsanalyse und des Penetration Testings sollten dokumentiert werden; bei Feststellung von Sicherheitslücken muss denen nachgegangen werden. Beispiel: Eine Verwundbarkeitsanalyse für Internet-exponierte Systeme kann halbjährlich und Penetration Testings sowie interne Verwundbarkeitsanalysen einmal jährlich stattfinden. Für risikobehaftete Systeme wie eBanking können Penetration Testings je nach Komplexität und durchgeführter Änderungen halbjährlich oder öfter durchgeführt werden.

Referenz Beispiel:
ISO/IEC 27002: 18.2.3
NIST Special Publication 800-53 Rev. 4: RA-5, CA-8

b. Schutz

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.

Kontrolle	Umsetzungsleitfaden
B1. Eine Sicherheitsrichtlinie für die Organisation der Informationssicherheit ist etabliert und dokumentiert.	- Eine in Abstimmung mit der Leitung genehmigte Informationssicherheitsrichtlinie sollte erarbeitet und dokumentiert werden. Diese sollte die Strategie und aktuelle Vorschriften und Gesetze der Organisation reflektieren, sowie Informationssicherheitsziele, Grundsätze und Verantwortlichkeiten definieren. - Die Sicherheitsrichtlinie kann durch themenspezifische Richtlinien ergänzt werden. - Es sollten Zuständige für die regelmässige Nachhaltung der Richtlinien ernannt werden. - Vorgaben hinsichtlich Informationssicherheit sollten – wo anwendbar – auch von externen Dienstleistern und Lieferanten entsprechend umgesetzt werden, um die Daten und IT-Systeme des Finanzintermediärs nicht zu gefährden. Diese Vorgaben sollten in einer Vereinbarung mit dem Dritten verbindlich kommuniziert und die Einhaltung nachgewiesen bzw. überprüft werden. Beispiel: Beispiele für themenspezifische Richtlinien können im ISO/IEC 27002 in Kapitel 5.1.1 gefunden werden. Zuständige Personen sollten die Richtlinien nach Erstellung hinsichtlich ihrer Aktualität und Angemessenheit überprüfen.

Referenz Beispiel:
ISO/IEC 27002: 5.1.1
NIST Special Publication 800-53 Rev. 4: PL-1

B2. Daten und Informationen werden in einer solchen Art und Weise geschützt und verwaltet, dass die Vertraulichkeit, Integrität und Verfügbarkeit gewährleistet ist.	- Daten und Informationen sollten während der Speicherung (‚Data-at-Rest') ausreichend geschützt sein. - Daten und Informationen sollten während der Übertragung (‚Data-in-Transit') ausreichend geschützt sein. Dies sollte sowohl physische als auch logische Schutzmassnahmen umfassen. - Wechseldatenträger sollten formell gemanagt und

über ihren gesamten Einsatzzyklus geschützt werden.

Beispiel: Schutzmassnahmen für Daten und Information während der Speicherung können den folgenden Kontrollen entnommen werden und umfassen beispielsweise sichere Grundkonfigurationen, die Handhabung von Regeln für Firewalls und den Zugriffsschutz auf diese.
Schutzmassnahmen für Daten und Informationen während der Übertragung können beispielsweise den physischen Zugriffsschutz auf Datenträger, sowie die Verschlüsselung dieser und der Kommunikation von Daten und Informationen umfassen.
Die Sicherheit von Daten und Informationen auf Datenträgern kann beispielsweise durch die sichere Übertragung beim Wechsel von Datenträgern, die Löschung von Daten in einer solchen Art und Weise, dass sie nicht wiederherstellbar sind, sowie die sichere Entsorgung der Datenträger gewährleistet werden.

Referenz Beispiel:
ISO/IEC 27002: 12.5.1
NIST Special Publication 800-53 Rev. 4: SC-8, SC-28

B3. Zur Härtung kritischer Systeme werden sichere Grundkonfigurationen dokumentiert und gepflegt.	- Grundkonfigurationen sollten dokumentiert, formell kontrolliert und intern akzeptiert werden. - Die Grundkonfiguration eines Systems sollte mindestens die Informationssystem-Komponenten, Netzwerktopologie und die Einordnung der Komponenten in die Systemarchitektur enthalten. - Die Grundkonfiguration sollte bei Änderung des Systems neu erstellt werden. - Grundkonfigurationen sollten auf technischen Sicherheitsrichtlinien der Hersteller bzw. anerkannter Herausgeber beruhen. Beispiel: Empfohlene Konfigurations- und Sicherheitseinstellungen werden häufig von Herstellern (beispielsweise Microsofts Windows Security Baselines) oder auch von anderen Organisationen (z.B. vom Center of Internet Security „CIS“ oder der United States Defense Information Systems Agency „DISA“) veröffentlicht.

Referenz Beispiel:
ISO/IEC 27002: 12.5.1
NIST Special Publication 800-53 Rev. 4: CM-2

B4. Zum Schutz vor Attacken, die auf das Fehlverhalten von Mitarbei-	- Zur Minderung der Bedrohung sollte ein Sensibilisierungsprogramm in Einklang mit internen Richtlinien

tern (und Kunden) abzielen, werden Mitarbeitende (und Kunden) regelmässig für Cyber-Bedrohungen sensibilisiert.	entwickelt, aktualisiert und regelmässig durchgeführt werden. - Informationen zu neuen Attacken und Angriffsmustern und deren effektive Behandlung können sowohl mit Mitarbeitenden als auch in anwendbaren Fällen mit Kunden geteilt werden. - Relevante Verfahren zur Prävention und Behandlung von Cyber-Attacken sollten regelmässig mit allen involvierten Parteien geübt werden. Beispiel: Informationen zu aktuellen Attacken und Angriffsmustern können über öffentliche und private, sogenannte Threat Intelligence Feeds bezogen werden. Relevante Informationen, beispielsweise zu neuen Betrüger-Vorgehen im eBanking-Bereich, können zu Sensibilisierungszwecken unter Berücksichtigung gängiger Datenschutzverordnungen auch den e-Banking-Kunden mitgeteilt werden.

Referenz Beispiel:
ISO/IEC 27002: 6.2.2, 7.2.2
NIST Special Publication 800-53 Rev. 4: PM-16

B5. Änderungen an Geschäftsprozessen, Software und Systemen werden, zum Schutz vor negativen Auswirkungen, gemanagt.	- Verfahren und Verantwortlichkeiten für Änderungen sollten etabliert und dokumentiert werden.
	- Änderungen sollten entsprechend ihrer Kritikalität und unter Berücksichtigung der Risiken behandelt werden. Signifikante Änderungen sollten geplant, geprüft und protokolliert werden:
	  - Die Planung sollte mögliche negative Auswirkungen der Änderungen und deren Behandlung berücksichtigen.
	  - Die Anforderungen an die Informationssicherheit sollten geprüft und erfüllt werden.
	  - Änderungen sollten dokumentiert und an relevante Personen kommuniziert werden.
	- Die Durchführung einer Änderung sollte von geschulten Personen vorgenommen werden.
	- Wo möglich sollten Änderungen zunächst an Testsystemen und/oder unkritischen Systemen vorgenommen werden.
	- Geschäftskritische Anwendungen sollten nach Änderung an Betriebs- oder Produktionsplattformen überprüft und getestet werden.

Referenz Beispiel:
ISO/IEC 27002: 12.1.2, 12.5.1, 14.2.3

B6. Zur Handhabung von technischen Schwachstellen ist ein Patchmanagement etabliert und dokumentiert.	- Sicherheits-Patches sollten grundsätzlich zeitnah installiert werden. Werden in begründeten Einzelfällen Sicherheits-Patches nicht installiert, sollte der jeweilige Entscheid dokumentiert werden; kompensierende Massnahmen zur Risikoreduzierung sind zu ergreifen. - Zeiträume zur Aktualisierung durch Patches und Updates von technischen Systemen sollten definiert und dokumentiert werden. - Patches sollten von autorisierten und vertrauenswürdigen Quellen bezogen und getestet werden. Die Art und Weise und Ausführlichkeit der Tests kann je nach zu aktualisierenden System variieren. Zudem sollten mit der Installation verbundene Risiken beurteilt und entsprechend behandelt werden. Beispiel: Sicherheits-Updates sollten für alle IT-Systeme angewandt werden, die in der Umgebung des Finanzintermediärs betrieben werden bzw. Daten des Finanzintermediärs bearbeitet. Dazu gehören neben Server-, Netzwerk- und Workstation-Systeme auch mobile Geräte (Laptops, Tablets, Smartphones) sowie andere verbundene Geräte wie etwa Überwachungskameras, Videokonferenz-Systeme, Gebäudesteuerungssyteme, oder andere „Internet-der-Dinge“-Geräte.

Referenz Beispiel:
ISO/IEC 27002: 12.6.1
NIST Special Publication 800-53 Rev. 4: SI-2

B7. Der Zugriff auf und Zugang zu Daten und Systeme ist geschützt, dokumentiert und gemanagt.	- Ein sogenanntes ‚Identity and Access Management (IAM)‘ sollte die Gesamtheit der Identitäten und Zugriffe der Mitarbeitenden, basierend den Rollen und Anforderungen des entsprechenden Geschäftsbereichs, auf Assets über die gesamte Anstellungslaufzeit (Eintritt, Wechsel, Kündigung) steuern. Dies betrifft sowohl den logischen als auch physischen Zugang zu Assets. - Benutzer sollten lediglich über solche Zugriffe verfügen, welche sie zur Erledigung ihrer täglichen Arbeit benötigen. Zugriffe, die sie auf unregelmässiger oder anlassbezogener Basis darüber hinaus benötigen, sollten angefordert und nach Erledigung der damit verbundenen Tätigkeit wieder entzogen werden. - Physische Sicherheitsperimeter sollten für kritische Bereiche festgelegt und dokumentiert werden. Der Sicherheitsumfang kann auf Grundlage der Risikoeinschätzung der sich darin befindenden Assets erfolgen. - Der Zutritt für unbefugte Personen sollte durch physische Barrieren verhindert werden.

- Zugriffe und Zugänge sollten protokolliert und überwacht werden.

Beispiel: Vordefinierte Regeln geben vor, welche Zugriffsrechte und Zugänge Mitarbeitenden entsprechend ihrer Rolle und ihrem Geschäftsbereich bei Eintritt zugewiesen, bei Wechsel geändert und bei Austritt unverzüglich entzogen werden.
Gebäude oder Bereiche, in denen sensible Daten verarbeitet werden, können durch zusätzliche Zugangssperren gesichert werden.
Besucher oder externe Lieferanten erhalten nur Zutritt durch die Anmeldung am Empfang, welcher Informationen zu Zeitpunkt, Dauer und Besucher dokumentiert.

Referenz Beispiel:
ISO/IEC 27002: 9.1, 11.1
NIST Special Publication 800-53 Rev. 4: PE-3

c. Erkennung

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

Kontrolle	Umsetzungsleitfaden

C1. Zur zeitnahen Erkennung von Cyber-Attacken ist eine systematische Überwachung der Technologieinfrastruktur und Alarmierung bei verdächtigen Ereignissen etabliert.	- Die Technologieinfrastruktur sollte auf (potentielle) Attacken und unautorisierte Zugriffe, insbesondere bei Internet-exponierten Systemen und Fernzugriffen, überwacht werden.
	  - Unautorisierter Zugriff oder Eindringen in die Technologieinfrastruktur kann durch ein sogenanntes „Intrusion Detection System“/“IDS“ erkannt werden.
	  - Die Systeme der Technologieinfrastruktur können an ein zentrales Logging- und Monitoring-System für sicherheitsrelevante Ereignisse angeschlossen werden. So können durch Mustererkennung und Korrelationen der Ereignisse Angriffe und Angriffsversuche erkannt werden.
	- Regeln und Kanäle für die Alarmierung sollten definiert, etabliert und dokumentiert werden. Zudem sollten diese regelmässig überprüft und an neue Systeme und Anforderungen angepasst werden.
	
	Beispiele: Ein Intrusion Detection System der exponierten Infrastruktur in Kombination mit der Überwachung von Schadsoftware-Ausbrüchen sollte grundsätzlich eingesetzt werden und die Alarmierung an entsprechende Stellen sichergestellt werden, sodass entsprechend reagiert werden kann.

	Finanzintermediäre mit komplexer Technologieinfrastruktur und grösseren Risiken sollten die Etablierung eines Security Information and Event Managements (SIEM) zur effektiven, automatischen Auswertung von Ereignissen nahe Echtzeit erwägen.

Referenz Beispiel:
ISO/IEC 27002: 8.3, 12.1.3
NIST Special Publication 800-53 Rev. 4: SI-4, SI-5, CA-7

C2. Technische und organisatorische Massnahmen zur Erkennung und zum Schutz vor Schadsoftware und bösartigen Code sind etabliert und dokumentiert.	- Ein Mechanismus zum Schutz vor bösartigem Code sollte etabliert und so konfiguriert sein, dass regelmässig nach bösartigem Code gescannt, dieser erkannt und beseitigt wird. Zudem sollte der Mechanismus regelmässig auf neue Erkenntnisse und Veröffentlichungen hin aktualisiert werden. - Für Benutzergeräte, insbesondere Mobilgeräte sollte entschieden werden, welcher Code ausgeführt und benutzt werden darf und die Entscheidung in einer Policy festgehalten werden. - Eine Richtlinie zur Nutzung von (nicht zentral verwalteter) Software sollte etabliert sein. - Es sollten Verfahren etabliert werden, die das sichere Ausführen von Code oder Öffnen von Dateien mit unbekannter Vertrauenswürdigkeit zulassen. Beispiele: Eine Anti-Virensoftware gewährleistet einen Basisschutz vor bösartigem Code. Manche Anti-Virensoftware bietet zudem die Funktion vor dem Öffnen verdächtiger Anhänge zu warnen. Ein weiteres Verfahren zur sicheren Ausführung von Code und dem Öffnen von Dateien mit potentiellem Sicherheitsrisiko sind virtuelle Umgebungen, die als ‚Detonationskammern' dienen, sodass der potentiell bösartige Code keinen Zugriff auf kritische Systeme und Daten hat. Eine Ausbreitung kann so vermieden werden. In zentral verwalteten, standardisierten Umgebungen eignen sich auch Mechanismen, die die Ausführung von nicht freigegebener Software technisch unterbindet, wie beispielsweise durch den „Microsoft AppLocker" oder vergleichbaren Produkten.

Referenz Beispiel:
ISO/IEC 27002: 12.2.1
NIST Special Publication 800-53 Rev. 4: SI-3, SC-18, SC-44

d. Reaktion

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.

Kontrolle	Umsetzungsleitfaden
D1. Ein Vorgehen zur Reaktion und Handhabung einer Cyber-Attacke ist etabliert und dokumentiert.	- Eine interne Vorgabe zur Handhabung von Cyber-Attacken sollte die Vorbereitung, Ermittlung und Analyse, Eindämmung, Beseitigung und Wiederherstellung beinhalten. Zudem sollten Verantwortlichkeiten und Ansprechpartner dokumentiert sein. - Ein konkreter Plan zur Reaktion auf Cyber-Attacken sollte erstellt und regelmässig auf Aktualität überprüft werden, um die Fähigkeit zur Reaktion auf Cyber-Attacken zu gewährleisten. - Die Einhaltung und Anwendbarkeit der internen Vorgaben und Pläne sollte regelmässig überprüft bzw. mit Hilfe von Übungen getestet werden. Beispiel: International anerkannte Standards und Frameworks können zur Entwicklung eines Vorgehens hinzugezogen werden. So beschreibt beispielsweise NIST 800-61 die benötigten organisatorischen Aspekte zur Reaktion auf Vorfälle, die Handhabung von Vorfällen sowie die Koordination und der Austausch von Informationen.
Referenz Beispiel: ISO/IEC 27002: 16.1.5 NIST Special Publication 800-53 Rev. 4: IR-3, IR-4, IR-8 NIST Special Publication 800-61 Rev. 2: 3.5	
D2. Ein Business Continuity Management (BCM) Plan unter Berücksichtigung von Cyber-Attacken ist etabliert und dokumentiert.	- Es sollten Prozesse, Verfahren, Massnahmen und Verantwortlichkeiten zur Aufrechterhaltung des Geschäftsbetriebs im Falle einer Cyber-Attacke etabliert und dokumentiert werden. Dabei sollten interne und externe Abhängigkeiten sowie die Aufrechterhaltung eines definierten Informationssicherheitsniveaus berücksichtigt werden. - Die Einhaltung und Effektivität der Pläne sollte regelmässig getestet werden. Beispiel: Externe Abhängigkeiten, die in einem Business Continuity Management Plan zu berücksichtigen sind, können beispielsweise zu Stellen bestehen, welche Finanzinformationen versenden oder Finanzservices (bspw. Internetbanking, Bargeld Management oder Verarbeitung von Kreditkarten) bereitstellen.

Referenz Beispiel:
ISO/IEC 27002: 17.1.1
ISO/IEC TR 27015: 14.1.3
NIST Special Publication 800-53 Rev. 4: CP-2

e. Wiederherstellung

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

Kontrolle	Umsetzungsleitfaden
E1. Schritte zur Wiederherstellung des normalen Geschäftsbetriebes nach dokumentierten Wiederherstellungsprozessen werden nach einer Cyber-Attacke eingeleitet.	- In einem dokumentierten Wiederherstellungsplan (Desaster Recovery Plan oder Notfallplan) sollten die Aktivitäten, Mittel und Verantwortlichkeiten zur Wiederherstellung der IT-Systeme und des Geschäftsbetriebes definiert sein. Dies umfasst die vorherige Ermittlung der essentiellen Business Funktionen, Wiederherstellungspunkte und -ziele sowie Prioritäten. - Zur Wiederherstellung des normalen Geschäftsbetriebes sollte auf geeignete Wiederherstellungsmittel zurückgegriffen werden, die zur Verfügung stehen müssen. - Die Einhaltung und Effektivität der Pläne sollte regelmässig getestet werden. - Zur Wiederherstellung vorgesehene Mittel sollten durch adäquate physische und technische Mittel geschützt sein. Beispiel: Die unter dem Wiederherstellungsplan definierten Mittel können beispielsweise Backups, Snapshots, physische Kopien und andere Redundanzen sowie die notwendige Hardware umfassen.

Referenz Beispiel:
ISO/IEC 27002: 16.1.5, 17.2.1
NIST Special Publication 800-53 Rev. 4: CP-10

f. Meldung

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

Kontrolle	Umsetzungsleitfaden

F1. Schwerwiegende oder betriebsstörende Vorfälle aufgrund einer Cyber-Attacke sind der FMA zu melden.	- Eine schwerwiegende oder betriebsstörende Cyber-Attacke hat negative Auswirkungen auf kritische Systeme, wichtige Betriebsprozesse oder auf den Schutz sensibler Daten.
	- Die Meldung über eine schwerwiegende oder betriebsstörende Cyber-Attacke sollte so bald als möglich, jedoch spätestens innert 14 Tage nach Kenntniserlangung an die zuständige Aufsichtsabteilung der FMA erfolgen.
	- Die Meldung 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 nachgemeldet 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 Meldung an die FMA entbindet die Finanzintermediäre nicht von den sonstigen Meldepflichten nach geltendem Gesetz, Richtlinien, Verordnungen und Standards.
	
	Beispiel: 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.

Referenz Beispiel:
ISO/IEC 27002: 16.1.4
NIST Special Publication 800-53 Rev. 4: IR-6

F2. Verfahren zur Meldung einer Cyber-Attacke sind etabliert.	Verfahren, die Zeitpunkt und Zuständigkeit der Meldung innerhalb der Finanzintermediäre festlegen, sollten dokumentiert, vorbereitet und den zuständigen Personen bekannt sein.

Referenz Beispiel:
ISO/IEC 27002: 6.1.3

Anhang

Anhang 1: Beispielszenarien anhand von Angriffsvektoren

Beispielhaft werden nachfolgend relevante Angriffsvektoren beschrieben:

Distributed Denial of Service (DDoS)
Unter Verwendung von technischen Hilfsmitteln wird gezielt die Verfügbarkeit von Internetservices beeinträchtigt. DDoS-Attacken werden mithilfe einer Vielzahl von verteilten Rechnern durchgeführt, die bei dem Angriff ein hohes Datenvolumen auf dem Ziel generieren und das System überlasten.

DDoS-Attacken und die damit verbundene Nicht-Verfügbarkeit können für Finanzintermediäre je nach Angriffsdauer und Zielsystem ein tiefes bis sehr hohes Schadensausmass für Reputation und Finanzen darstellen.

Siehe auch MELANI DDoS Attacken und NIST Special Publication 800-53 Rev. 4, SC-5.

Insider Bedrohungen
Eine der grössten Bedrohungen geht von den Mitarbeitenden des Finanzintermediärs aus. Dabei kann die Insider-Bedrohung viele Ausprägungen aufweisen und muss weder technischer noch böswilliger Natur sein. Einer der erfolgreichsten Attacken, das sogenannte ‚Social Engineering', macht sich beispielsweise die Unwissenheit oder die fehlende Sensibilisierung von Mitarbeitenden zu Nutze, um diese zu bestimmten Aktionen zu bewegen. Beispielsweise kann sich bei einem solchen Angriff der Angreifer als CEO, sonstiger Vorgesetzter, Mitarbeiter der IT oder externer Partner ausgeben und via E-Mail oder Telefon die Mitarbeitenden zum Einschleusen und Ausführen von bösartiger Software, Übermittlung von Informationen, Preisgabe von Passwörtern oder das Ausführen von nicht autorisierten Transaktionen bewegen.

Die zahlreichen Insider-Bedrohungen können tiefe bis sehr hohe finanzielle Schadensausmasse für den Finanzintermediär annehmen. Ein Datenverlust kann zudem einen sehr hohen Schaden für die Reputation und Gesetzeskonformität bedeuten.

Siehe auch MELANI Social Engineering, MELANI CEO-Fraud, NIST Special Publication 800-53 Rev. 4, PM-12, NIST Special Publication 800-53 Rev. 4, SC-5 und ISO/IEC 27015, 8.1.2.

Bösartiger Code in E-Mail Anhängen
Über das Öffnen von Anhängen oder dem Klick auf Links zu Internetseiten kann bösartiger Code, beziehungsweise Schadsoftware auf die Rechner der Mitarbeitenden gelangen. Hierzu werden Dateien und Internetseiten so präpariert, dass beim Öffnen der Code zur Infizierung automatisch ausgeführt wird. Im Falle mancher Schadsoftware kann sich diese darüber hinaus im Netzwerk verteilen um eine weitere Verbreitung zu ermöglichen. Ziel der Attacke kann der Spam-Versand weiterer E-Mails, die Nutzung der infizierten Rechner in einem Netz für DDoS-Attacken (siehe Distributed Denial of Service (DDoS)) oder die Zerstörung von oder die Erpressung mit verschlüsselten Daten (siehe Ransomware (Cryptolocker)) sein.

Ein daraus resultierender Datenverlust kann einen sehr hohen Schaden in Sachen Reputation und

Gesetzeskonformität darstellen.

Siehe auch MELANI Schadsoftware in E-Mail, NIST Special Publication 800-53 Rev. 4, SC-44, NIST Special Publication 800-53 Rev. 4, PM-16, ISO/IEC 27002, 7.2.2 und ISO/IEC 27015, 6.2.2.

Ransomware (Krypto Trojaner)
Bei Infizierung eines Systems, beispielsweise über das Öffnen eines präparierten E-Mail Anhangs (siehe Bösartiger Code in E-Mail Anhängen), mit einem Krypto Trojaner werden Daten auf dem Laufwerk und auf verbundenen Netzwerklaufwerken verschlüsselt. Häufig werden Betroffene anschliessend zu einer Zahlung aufgefordert, um den Schlüssel zur Entschlüsselung der Daten zu erhalten.

Bei Zahlung des Lösegeldes oder der Nicht-Verfügbarkeit der Daten und Systeme kann für den Finanzintermediär ein tiefes bis sehr hohes finanzielles Schadensausmass entstehen.

Siehe auch MELANI Verschlüsselungstrojaner

Die in diese Orientierungshilfe beschriebenen Kontrollen und Leitfäden decken die wichtigen Cyber-Angriffsszenarien ab, um das Risiko eines Vorfalls bzw. den resultierenden Schaden zu reduzieren:

Angriffsvektor	Identifikation			Schutz							Erkennung		Reaktion		Wiederherstellung	Meldung	
	A1	**A2**	**A3**	**B1**	**B2**	**B3**	**B4**	**B5**	**B6**	**B7**	**C1**	**C2**	**D1**	**D2**	**E1**	**F1**	**F2**
DDoS	(x)	(x)	(x)	(x)		(x)		(x)	(x)		(x)		(x)	(x)	(x)	(x)	(x)
Insider	(x)	(x)	(x)	(x)	X		X			X	X	(x)	(x)	(x)	(x)	(x)	(x)
E-Mail Anhänge	(x)	(x)	(x)	(x)	(x)	(x)	X	(x)	(x)		(x)	X	(x)	(x)	(x)	(x)	(x)
Ransom ware	(x)	(x)	(x)	(x)	X	(x)	X	(x)	(x)	(x)	(x)	X	(x)	(x)	X	(x)	(x)

X Dedizierte Abdeckung
(x) Allgemeine Abdeckung

Anhang 2: Beispiel-Schema zur Kritikalitätseinstufung

Schadensausmass (Business Impact)					
Schadens-szenarien		**klein [1]**	**wesentlich [2]**	**kritisch [3]**	**bedrohlich [4]**
1	**Verletzung der Vertraulichkeit**	Öffentliche Informationen (keine Zugriffseinschränkungen) z.B.: Informationen auf Webseite, Wegweisungen, Publikationen etc.	Interne Informationen (Nur der Finanzintermediär hat Zugriff) z.B.: interne Verzeichnisse (Telefonbuch), Organigramme, interne Memos, Protokolle etc.	Vertraulich (Zugriff innerhalb des Finanzintermediärs ist eingeschränkt) z.B.: Persönlichkeitsinformationen (DSG), Kundeninformationen, Provisorische Rechnungslegungsinformationen	Streng vertraulich (Zugriff innerhalb des Finanzintermediärs ist stark eingeschränkt, z.B. auf die Geschäftsleitung) z.B.: besonders schützenswerte Persönlichkeitsinformationen (DSG), streng vertrauliche Strategiedokumente, besonders vertrauliche Kundeninformationen etc.
2	**Verletzung der Integrität**	Der Verlust der Integrität hat marginale Auswirkungen auf die Rechnungslegung, die Entscheidungsfindung, das Einhalten rechtlicher Vorschriften oder die Kontrolle über Geschäftsprozesse.	Der Verlust der Integrität hat mässige Auswirkungen auf die Rechnungslegung, die Entscheidungsfindung, das Einhalten rechtlicher Vorschriften oder die Kontrolle über Geschäftsprozesse.	Der Verlust der Integrität hat kritische Auswirkungen auf die Rechnungslegung, die Entscheidungsfindung, das Einhalten rechtlicher Vorschriften oder die Kontrolle über Geschäftsprozesse.	Der Verlust der Integrität hat bedrohliche Auswirkungen auf die Rechnungslegung, die Entscheidungsfindung, das Einhalten rechtlicher Vorschriften oder die Kontrolle über Geschäftsprozesse.
3	**Verletzung der Verfügbarkeit**	Ausfall: < 0.5 Tage	Ausfall: > 0.5 Tage < 3 Tage	Ausfall: > 3 Tage < 10 Tage	Ausfall: > 10 Tage
4	**Finanzielle Auswirkungen**	Der finanzielle Schaden bleibt für die Institution gering und tolerabel. Betrag: < CHF 10'000.-	Der finanzielle Schaden ist für die Institution empfindlich, jedoch verkraftbar. Betrag:CHF 10'000.- > < CHF 150'000.-	Der Schaden bewirkt beachtliche finanzielle Verluste, ist jedoch nicht existenzbedrohend. Betrag: CHF 150'000.- > < CHF 5'000'000.-	Der finanzielle Schaden ist für die Institution existenzbedrohend. Betrag: > CHF 5'000'000.-

Anhang 3: Beispiel – Risikobewertungsschema

Schadensausmass (Business Impact)		Eintretenswahrscheinlichkeit			
		unwahrscheinlich	**selten**	**gelegentlich**	**wahrscheinlich**
	bedrohlich [4]	mittel	mittel	hoch	hoch
	kritisch [3]	mittel	mittel	mittel	hoch
	wesentlich [2]	tief	mittel	mittel	mittel
	klein [1]	tief	tief	mittel	mittel

Klassifikation	**Kriterien (Basis ein Jahr)**
wahrscheinlich	50 % <= Eintretenswahrscheinlichkeit < 100 % (1 x in 2 Jahren bis 1 x in 1 Jahr).
gelegentlich	20 % <= Eintretenswahrscheinlichkeit < 50 % (1 x in 5 bis 1 x in 2 Jahren).
selten	5 % <= Eintretenswahrscheinlichkeit < 20 % (1 x in 20 bis 1 x in 5 Jahren).
unwahrscheinlich	Eintretenswahrscheinlichkeit < 5 % (1 x in 20 Jahren).

Risikobewertung	**Richtlinie für die Risikoverminderung / -überwachung**
Hoch	Das Risiko ist nicht akzeptierbar. Es muss im Rahmen der Risikosteuerung umgehend und mit allen erforderlichen Ressourcen vermieden, vermindert, übertragen bzw. abgesichert werden.
Mittel	Das Risiko ist nicht akzeptierbar. Kurzfristig ist es bei entsprechender Überwachung (erhöhte Management-Attention) tragbar, mittelfristig muss es aber im Rahmen der Risikosteuerung vermieden, vermindert, übertragen bzw. abgesichert werden.
Tief	Das Risiko ist akzeptierbar. Es ist mit geeigneten Mitteln zu überwachen.