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

Meinungsartikel von FINMA-Direktor Mark Branson
Erschienen in der Finanz und Wirtschaft vom 15. Februar 2019

Cyber Security: Die Banken sind gefordert – aber nicht nur sie

Die Akteure auf dem Schweizer Finanzmarkt streben nach mehr Effizienz in der Wertschöpfungskette und Innovation bei Dienstleistungen. Die Digitalisierung in der Finanzindustrie birgt dafür enorme Chancen. Die Institute können ihren Kundinnen und Kunden dank digitalisierter Prozesse qualitativ bessere, günstigere oder schnellere Dienstleistungen anbieten. Logisch daher, dass wir uns zuerst auf die Vorteile der Digitalisierung konzentrieren, bevor wir uns den Kopf darüber zerbrechen, wie wir uns vor möglichen Risiken schützen können.

Aber die neuen Möglichkeiten der Digitalisierung zeigen auch unerwünschte Nebenwirkungen: die Cyberkriminalität. Es würde überraschen, wenn das Bankwesen davon verschont bliebe, denn ob analog oder digital: Bankräuber gehören seit jeher zum Bankwesen. Neu ist allerdings, dass es bei den unlauteren Machenschaften nicht einfach nur um Diebstahl gehen muss. So wurde 2017 beispielsweise der Internetverkehr von mehreren Finanzdienstleistern auf der ganzen Welt, darunter auch jener der Kreditkartenfirmen Visa und Mastercard, während knapp sieben Minuten über einen russischen Telekomanbieter umgeleitet. Dabei bestand die Möglichkeit, dass in der Zeit der Fehlleitung die Kommunikation analysiert oder schlimmstenfalls gar verändert wurde. In einem anderen Fall bei einer brasilianischen Bank übernahmen Angreifer den Internetverkehr während fünf Stunden komplett. Auf diese Wiese können potenziell Transaktionen ausgespäht, Zugangsdaten abgegriffen und Kundengeräte mit Malware infiziert werden. Digitale Attacken können also ganz andere Dimensionen annehmen, denn sie legen potenziell ganze Systeme von einzelnen Instituten oder gar das Finanzsystem lahm.

Vernetzung erhöht Anfälligkeit

Mit der Digitalisierung nimmt die Vernetzung der Finanzmarktakteure stetig zu. Das Internet verbindet die Banken mit der Welt. Die Institute sind auch viel stärker mit ihren Partnern, Lieferanten, Kundinnen und Kunden digital vernetzt. Dank der digitalen Möglichkeiten konzentrieren sich Finanzinstitute vermehrt auf ihre Kernkompetenzen wie die Einlagen- und Vermögensverwaltung oder Kreditvergabe und lagern Bereiche der Wertschöpfungskette aus, die als nicht strategisch erachtet werden. So bezieht bereits heute rund 85 Prozent der Banken in der Schweiz Kernfunktionen von Drittanbietern, wobei Dienstleistungen für den Betrieb von IT-Systemen klar dominieren.

Analoge Finanzdienstleistungen hingegen werden tendenziell immer weniger genutzt, da diese für die Institute teuer und damit weniger attraktiv sind. Teilweise verschwinden sie sogar ganz: Wer benutzt heute zum Beispiel noch ein Scheck-Buch? Weil mehr und mehr digital abläuft und analoge Alternativen fehlen, sind wir auch stärker denn je vom Funktionieren der digitalen Dienstleistungen abhängig. Damit steigen einerseits die Erwartungen an die Zuverlässigkeit und Verfügbarkeit der digitalen Systeme und andrerseits die Verletzlichkeit der Anbieter.

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

Banken: Cyber-Risiken gehören zu den bedeutendsten operationellen Risiken

Diese erhöhte Verletzlichkeit für Cyber-Attacken betrifft sowohl die Finanzinstitute als auch die Kundinnen und Kunden. Die Technologiesysteme von Finanzdienstleistern können aufgrund von böswilligen Attacken gefährdet werden. Pro Jahr werden beispielsweise rund tausend gefälschte Kopien von Internetseiten, so genannten Phishing-Seiten, von Schweizer Banken erstellt. Da die Technologieinfrastruktur mehr und mehr ausgelagert ist, zielen Cyber-Angriffe nicht mehr nur auf Banken, sondern vermehrt auf Drittparteien ab. So hätte beispielsweise ein Angriff auf eine der für den Zahlungsverkehr zentralen Infrastrukturen der Schweiz erhebliche Auswirkungen auf den Finanzmarkt und die Bevölkerung. Aber auch die Endgeräte von Kundinnen und Kunden werden Ziel von Cyber-Angriffen. Daher ist grundsätzlich das gesamte System in der Schweiz gefordert, die Bedrohungslage laufend zu beurteilen und Massnahmen koordiniert zu ergreifen.

Finanzmarktaufsicht gezielt verstärkt

In einer digitalisierten Welt sind Cyber-Risiken kein Hype-Thema oder punktuelles Problem. Sie stellen eine permanente Herausforderung und wahrscheinlich das wichtigste operationelle Risiko bei den Instituten der Finanzbranche dar. Entsprechend befasst sich die Eidgenössischen Finanzmarktaufsicht (FINMA) intensiv damit.

Zwar kann eine Aufsichtsbehörde nicht das gesamte Finanzsystem vor Cyber-Angriffen schützen. Es gehört aber zur Rolle der FINMA, für die nötige Sensibilisierung für die Problematik bei der Finanzbranche und ihren Partnern und Zulieferern zu sorgen. Für ihren Teil hat die FINMA daher Anforderungen für den Umgang mit Cyber-Risiken bei Banken in ihrer Regulierung kurz und prägnant festgelegt. Zudem hat sie gezielt die Aufsicht über diese Risiken verstärkt und Spezialisten mit dem nötigen Knowhow eingestellt. Denn die FINMA muss in der Lage sein, die richtigen Fragen zu stellen und die Antworten zu analysieren und beurteilen.

Banken müssen sich gegen Cyber-Risiken rüsten

Auch hat die FINMA 2018 zahlreiche Banken diesbezüglich Vorort kontrolliert. Die Ergebnisse der Aufsicht zeigen, dass die Banken den Umgang mit Cyber-Risiken in den letzten Jahren verbessert haben. Es liegt aus offensichtlichen Reputations- und finanziellen Gründen in ihrem ureigenen Interesse, diese Risiken im Griff zu haben. Für Finanzinstitute steht im Zentrum, dass Daten sicher gelagert oder transportiert werden.

Die FINMA erwartet von den Banken, dass sie sich systematisch mit Cyber-Risiken befassen und zielgerichtete Prozesse sowie interne Verantwortlichkeiten festlegen. Fünf Elemente stehen dabei im Vordergrund. Die Banken müssen erstens die potentiell gefährdeten Daten und Systeme identifizieren. Zweitens gilt es dann, die Vertraulichkeit, Integrität und Verfügbarkeit dieser Daten und Systeme bestmöglich zu schützen. Drittens sollen Banken in der Lage sein, Attacken auf ihre Technologieinfrastruktur mit einer systematischen Überwachung und Aufzeichnung frühzeitig zu erkennen. Viertens müssen Banken Reaktionsmassnahmen vorbereiten, damit sie während eines Vorfalls den Betrieb aufrechterhalten können. Letztlich brauchen die Institute einen Plan, wie der normale Geschäftsbetrieb rasch wiederhergestellt werden kann. Neben diesen fünf Punkten verlangt die FINMA von den Banken, dass sie ihr Dispositiv regelmässig testen. Sie lassen dafür ihr System probehalber angreifen (Penetration Testing). Auf diesem Weg lassen sich mögliche Schwachstellen ausfindig machen und korrigieren.

Systemische Fragen brauchen eine systemische Antwort

Neben den Massnahmen der einzelnen Institute ist für den Umgang mit Cyber-Risiken aufgrund der erwähnten systemischen Vernetzungen auch ein systemweites Abwehrdispositiv in der Schweiz gefragt. Die FINMA unterstützt explizit die Bestrebungen des Bundesrats: Es braucht nun rasch ein schweizerisches Cyber-Kompetenzzentrum als zentrale Ansprechstelle für die Anliegen der Wirtschaft. Ziel muss sein, dass alle Akteure sich einfach ein Bild über die aktuelle Bedrohungslage machen können, um umgehend darauf reagieren zu können. Zudem braucht es ein systemweites Krisenmanagement als Vorbereitung auf Angriffe, die auf die Finanzstabilität der Schweiz durchschlagen. Letztlich bietet nur ein Weg den besten Schutz vor Cyber-Attacken: Die enge Zusammenarbeit von Kundinnen und Kunden, Finanzdienstleistern, Zulieferern, Infrastrukturanbietern und Behörden.