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

Jahresmedienkonferenz vom 27. März 2018

Mark Branson, Direktor

Technologie und die Finanzbranche – die Chancen und Risiken

Sehr geehrte Damen und Herren

Ich widme mich heute dem Thema Technologie und möchte dabei sowohl Chancen wie auch Risiken beleuchten. Die Schlagworte sind bekannt: Blockchain, ICO, Big Data, Cyberrisiko u.ä. Aber was steht hinter den Schlagzeilen dazu?

Angesichts tiefer Zinsen, schwacher Profitabilität und neuem Kundenverhalten ist Innovation eine wichtige, vielleicht sogar existenzielle Frage für die Finanzindustrie.

Innovation kann nicht staatlich verordnet werden; die Industrie selbst ist gefordert. Als Aufsichtsbehörde möchten wir jedoch sicherstellen, dass das regulatorische Rahmenwerk Innovation ermöglicht. Dies nicht als verkappte Strukturpolitik – vielmehr geht es darum, bestehende Markteintrittshürden abzubauen, um gesunden Wettbewerb zu ermöglichen.

Innovationsfreundlichkeit bedeutet aber nicht Blauäugigkeit. Digitalisierung und Finanzinnovation führen zu neuen Risiken oder zu alten Risiken in neuen Kleidern. Als Aufsichtsbehörde ist es unsere Aufgabe, diese Risiken zu kennen, zu beobachten und bei Bedarf einzuschränken. Ich denke dabei an Geldwäschereirisiken im Blockchain-System, an Verlustrisiken für Investoren bei ICOs und besonders auch an die Bedrohung aufgrund von Cyberrisiken.

Das Versprechen von Fintech

Doch lassen Sie mich zuerst auf die Chancen von Fintech eingehen. Eine Vielzahl neuer Produkte und Anwendungen kommen auf den Markt. Projekte finanzieren sich über die Crowd, Geld wird per Smartphone übermittelt, neue Bevölkerungsschichten in Entwicklungsländern erhalten Zugang zu Finanzdienstleistungen und "Roboter" treffen Anlageentscheide.

Wir anerkennen das grosse Potenzial, das Fintech und die Blockchain-Technologie dem Finanzplatz bieten. Wir sehen uns als Aufsichtsbehörde hier auch in einer Rolle: Wir wollen Innovation ermöglichen. Den Tatbeweis haben wir mehr als einmal erbracht. So gestalten wir unsere nachgelagerte Regulierung konsequent technologieneutral, unterscheiden also nicht zwischen digitalem und analogem Kanal. Die FINMA hat zudem ursprünglich die Idee der Sandbox und jene der Fintech-Lizenz lanciert. Und wir haben im Rahmen des Möglichen den ICO-Betreibern auch eine Orientierungshilfe gegeben.

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

Unser Ziel ist, dass Innovatoren für einen gesunden Wettbewerb sorgen und zugleich die Integrität des Finanzplatzes geschützt ist. Denn so "pro Innovation" wir sind, so entschlossen sind wir "anti Finanzkriminalität".

Blockchain: Hype oder Innovationsmotor?

Blockchain ist eine spannende Technologie. Man kann sich zum Beispiel vorstellen, dass Teile der heutigen Finanzmarktinfrastruktur eines Tages obsolet werden – man erinnert sich an die Prophezeiung von Bill Gates aus dem Jahr 1994: "Banking is necessary, banks are not".

Stark genutzt wird die Blockchain-Technologie bereits im Kontext von Kryptowährungen und ICOs. ICOs haben sich in kurzer Zeit von einer unbekannten Methode der Geldbeschaffung zu einem regelrechten Magneten entwickelt, der allein im Jahr 2017 weltweit über sechs Milliarden Dollar angezogen hat. Vier der sechs grössten ICOs fanden dabei in der Schweiz statt. Die Schweiz hat sich zu einem wichtigen ICO-Hub entwickelt. Kein Wunder, wurde und wird die FINMA mit Dutzenden von Anfragen konfrontiert. Wir haben dies zum Anlass genommen, in einer Wegleitung transparent zu machen, wie wir entsprechende Gesuche auf Basis der bestehenden Finanzmarktgesetze behandeln werden. Die ersten Rückmeldungen zu diesem Vorgehen waren positiv. Die seriösen Anbieter begrüssen es. Sie wissen, dass eine grossflächige anarchische Spielwiese Utopie bleiben wird.

Bei all der Begeisterung, die teilweise herrscht, sollte nicht vergessen werden: Kryptowährungen sind riskant. Ein völlig libertärer Ansatz ist deshalb verfehlt. Die Wertschwankungen sind extrem. Die Risiken werden den Kunden von ICOs zudem häufig nicht transparent vermittelt. Vielfach gibt es nur rudimentäre Informationen über die oft noch jungen Projekte. Das Ausfallrisiko ist – wie bei anderen Start-up-Investitionen – erheblich. Zudem besteht Potenzial für Geldwäscherei. Viele Anbieter von Kryptowährungen werben ja gerade mit deren Intransparenz und Anonymität. Und nicht zuletzt waren Handelsbörsen von Kryptowährungen Ziel von Hackerangriffen mit Schäden von Hunderten Millionen Dollar. Deswegen unser einfacher Ansatz: ICOs von Zahlungstoken oder von Kryptowährungen sind dem Geldwäschereigesetz unterstellt; ICOs, die Investitionsmöglichkeiten bieten, sind wie Effektengeschäfte zu behandeln.

Cyberrisiken: Erwartungen der FINMA

Lassen Sie mich mit dem Stichwort "Hackerangriff" überleiten auf die Thematik der Cyberrisiken. Finanzinstitute sind ein Lieblingsziel von Hackerangriffen und anderen Cyberattacken. Dies zeigen die jüngsten Statistiken der Melde- und Analysestelle Informationssicherung MELANI: Zwei Drittel der Angriffe auf kritische Infrastrukturen betreffen den Finanzsektor.

Das Risiko für solche Attacken steigt mit der zunehmenden Digitalisierung. Cyberangriffe sind inzwischen das grösste operationelle Risiko für das Finanzsystem. Wir – und damit meine ich sowohl den privaten Sektor als auch die Behörden – sollten das Thema daher todernst nehmen. Grundsätzlich sehen wir, dass die Sensibilität für dieses Thema bei unseren Beaufsichtigten hoch ist und sie im Schnitt gut gerüstet scheinen. Eine Vielzahl von Attacken wird täglich abgewehrt. Beispielsweise werden im Zusammenhang mit der Schadsoftware "Retefe" zurzeit pro Tag bis zu 100 Angriffe auf E-Banking-Lösungen in der Schweiz festgestellt.

Aber das beste Abwehrsystem ist nur so gut wie das schwächste Glied. So konnten sich Hacker erfolgreich Zugang zum internationalen Zahlungssystem Swift verschaffen, nachdem sie bei der Zentralbank in Bangladesh eingedrungen waren. In der Schweiz wurden jüngst umfangreiche Kundendaten bei einer Krankenversicherung entwendet.

Was erwartet die FINMA angesichts dieser Risiken? Zentral ist es, dass die Finanzinstitute ihre eigene Verwundbarkeit kennen. Ein wichtiges Instrument ist hier Penetration-Testing. Ebenso bedeutend ist die Reaktionsfähigkeit, sollte es zu einem Cyberangriff kommen. Im Falle eines Angriffs muss der Geschäftsbetrieb so schnell wie möglich wiederhergestellt werden. Jedes Institut muss hier für sich ein funktionierendes Krisendispositiv aufbauen und unterhalten.

Die Risiken gehen aber weit über einfache Diebstähle von Geld oder Daten hinaus. Gezielte Angriffe, vielleicht sogar von terroristischen, staatlichen oder halbstaatlichen Stellen, könnten systemische Dimension annehmen. Scheinen die Schweizer Finanzinstitute im internationalen Vergleich gut aufgestellt, so sehen wir, dass die Schweiz als Land weniger tut als andere Länder, um das System als Ganzes zu schützen. Andere Länder mit bedeutenden Finanzplätzen unternehmen mehr, beispielsweise mit der Sicherstellung einer zentralen Cyberkompetenz oder mit systemweiten Penetration-Tests. Ein systemweites Monitoring und entsprechende Prozesse sollte auch die Schweiz umsetzen – und die FINMA ist bereit, hier eine starke Rolle zu spielen. Wir haben auf diesem Gebiet gezielt Spezialisten rekrutiert und scheuen uns nicht vor weiteren Investitionen.

Der Beirat Zukunft Finanzplatz unter der Leitung von Prof. Brunetti hat zur Cybersicherheit des Schweizer Finanzplatzes drei wichtige Empfehlungen erarbeitet. Diese erhielten wenig öffentliche Aufmerksamkeit – zu Unrecht.

Erstens soll der Zugang zu MELANI erweitert werden, auch für kleine Finanzinstitute in der Schweiz. Zweitens gilt es, die Arbeit zwischen Fachleuten aus Finanzindustrie und Behörden zu institutionalisieren und zu stärken. Es gibt wohl kaum einen Bereich, in welchem die Interessen von Privatindustrie und Aufsicht so gleich gelagert sind wie bei der Bekämpfung von Cyberrisiken. Drittens gilt es, ein finanzsektorspezifisches Cybersicherheits-Krisendispositiv zu gestalten und zu testen.

Die FINMA begrüsst die Empfehlungen des Beirats Zukunft Finanzplatz ausdrücklich. Und wir arbeiten aktiv mit. Gemeinsam erreichen wir hier mehr als jeder für sich. Die Schweiz tut hier zwar einiges. Aber andere Länder tun deutlich mehr.

Konzentrationen durch Outsourcing

Die Cyberbedrohung wird durch ein Phänomen teilweise verstärkt: die zunehmende Auslagerung von Geschäftsprozessen und IT-Infrastruktur. Eine deutliche Mehrheit der Schweizer Banken hat wesentliche Geschäftsbereiche ausgelagert. Zum Teil lagern Banken ihre gesamten Backoffice-Prozesse aus. Diese Entwicklung stellt auch die Aufsicht vor Herausforderungen.

Wir beobachten insbesondere eine starke Konzentration bei bestimmten Anbietern in der Schweiz. Viele Banken haben ihre Dienstleistungen an diese ausgelagert. Wir setzen hier die gleichen Massstäbe an wie bei den Finanzinstituten selbst. Wir verfügen seit 2016 über die rechtliche Grundlage, selbst vor Ort zu gehen und die Outsourcing-Partner der Finanzinstitute zu prüfen. Wir haben

denn auch bei solchen Dienstleistern bereits Vor-Ort-Kontrollen durchgeführt und werden diese systematisch weiterverfolgen.

Chancen wahrnehmen, Risiken erkennen

Fintech hat grosses Potenzial. Als Aufsichtsbehörde werden wir unser Möglichstes tun, seriöse Innovation im Finanzsektor zu ermöglichen. Ob die Anwendungen ihr Versprechen halten können, sollen der Markt und die Kunden entscheiden, nicht die regulatorischen Rahmenbedingungen. Dies ist unser Leitmotiv.

Es tummeln sich sowohl Innovatoren als auch Trittbrettfahrer, regulatorische Arbitrageure und Betrüger in der Kryptowelt. Unsere Aufgabe ist es, zusammen mit unseren Partnerbehörden den seriösen Innovatoren die Möglichkeit zu geben, zu reüssieren, Arbitrage zu verunmöglichen und Betrüger dorthin zu bringen, wo alle Betrüger hingehören.

Sowohl die Chancen als auch die Risiken der neuen Technologien brauchen unsere Aufmerksamkeit und unser Engagement.

Besten Dank für Ihre Aufmerksamkeit.