Empfehlung des Beirates Zukunft Finanzplatz an den Bundesrat

Cyber-Sicherheit des Schweizer Finanzplatzes

August 2017

Ausgangslage

Der Beirat Zukunft Finanzplatz wurde 2015 vom Bundesrat eingesetzt mit dem Auftrag, die strategischen Herausforderungen und Zukunftsperspektiven für das Finanzgeschäft in der Schweiz zu beurteilen und dem Bundesrat gegebenenfalls Empfehlungen zur Anpassung der Finanzmarktstrategie und zur Verbesserung der Rahmenbedingungen für den Finanzplatz zu unterbreiten.

Im Zuge der Digitalisierung und der Anpassung der Geschäftsmodelle der Finanzindustrie ist Cyber-Sicherheit zu einer zentralen Herausforderung für den Schweizer Finanzplatz geworden. Schwerwiegende Cyber-Vorfälle bergen grosse finanzielle, aber auch Reputationsrisiken und können das Vertrauen in den Schweizer Finanzplatz beeinträchtigen. Im Rahmen von drei Teilprojekten (Informationsaustausch und Krisenorganisation, Internationaler Benchmark und Versicherbarkeit von Cyber-Risiken) hat der Beirat geprüft, ob der Schutz des Schweizer Finanzplatzes vor Cyber-Risiken ausreichend ist und darauf basierend Handlungsempfehlungen erarbeitet.

Die Resultate der drei Teilprojekte liegen nun vor. Der Beirat beschloss auf Basis der Diskussion in der Sitzung vom 22. Juni 2017, dem Bundesrat drei Empfehlungen sowie zwei erläuternde Dokumente zu unterbreiten.

Empfehlungen

Die drei Empfehlungen des Beirats Zukunft Finanzplatz sollten angemessen in die gemäss Beschluss des Bundesrats vom 26. April 2017 auszuarbeitende, zweite NCS eingebettet werden. Mit Blick auf den strategischen Auftrag des Beirats und gestützt auf die Resultate der drei Teilprojekte, unterbreitet der Beirat Zukunft Finanzplatz dem Bundesrat folgende Empfehlungen:

Empfehlung 1: Verbesserter Zugang zu MELANI

MELANI verfügt über einen offenen und einen geschlossenen Kundenkreis. Dem geschlossenen Kundenkreis stellt MELANI Wissen und Mittel zur Verfügung, die nur ihr als staatlicher Stelle zur Verfügung stehen und der Wirtschaft nicht anderweitig zugänglich sind. Obwohl alle Finanzinstitute Teil des kritischen Teilsektors Banken sind, ist derzeit nur eine begrenzte Anzahl von Finanzinstituten (Dezember 2016: 63 Banken und 13 Versicherungen) Teil des geschlossenen Kundenkreises und profitiert von den vollen Dienstleistungen von MELANI. Der Beirat erachtet den Zugang zu relevanten Informationen für den gesamten Finanzsektor als wichtig. Daher sollte auch Finanzinstituten, die nicht Teil des geschlossenen Kundenkreises von MELANI sind, eine enge Zusammenarbeit mit MELANI ermöglicht werden.

Der Beirat empfiehlt dem Bundesrat, sicherzustellen, dass das MELANI-Serviceangebot im Bereich Cyberprävention und –Response von der gesamten Finanzindustrie genutzt wird. Zudem empfiehlt er, zu prüfen, ob auch relevanten Drittparteien Zugang zu Informationen, die über den offenen Kundenkreis von MELANI hinausgehen, gewährt werden kann. Mit dieser Empfehlung sind eine Anpassung des Mandats und der Ressourcen von MELANI verbunden.

Empfehlung 2: Institutionalisierte Zusammenarbeit zw. Finanzsektor und Behörden

Cyber-Sicherheit wird auch in Zukunft ein hochrelevantes Thema bleiben. In der Schweiz besteht jedoch derzeit zu diesem Thema keine institutionalisierte Zusammenarbeit zwischen den Fachleuten des Finanzsektors und der Behörden. Das Beispiel UK zeigt, dass eine entsprechende Zusammenarbeit es erlaubt sowohl strategische wie auch operative finanzsektorspezifische Fragestellungen zur Cyber-Sicherheit frühzeitig und proaktiv zu behandeln. Dadurch kann gewährleistet werden, dass der Finanzsektor sowohl im Bereich der Prävention, als auch im Bereich der Reaktion adäquat gegenüber Cyber-Angriffen gewappnet ist.

Der Beirat empfiehlt dem Bundesrat, ein Fachgremium zur institutionalisierten Zusammenarbeit zwischen den Fachleuten der Finanzindustrie und den Behörden zu Fragen der Cyber-Sicherheit einzusetzen. Ein entsprechendes Gremium könnte insbesondere die Grundlagen für eine finanzsektorspezifische Cyber-Sicherheits-Krisenorganisation erarbeiten (siehe Empfehlung 3).

Empfehlung 3: Finanzsektorspezifische Cyber-Sicherheits-Krisenorganisation

Derzeit gibt es keine finanzsektorspezifische Cyber-Sicherheits-Krisenorganisation, die im Falle einer sektorweiten Krise alarmiert, analysiert, eskaliert, koordiniert und mit Weisungsbefugnissen ausgestattet ist. Eine entsprechende Krisenorganisation könnte diese Aufgaben übernehmen und den spezifischen Risiken der Finanzbranche Rechnung tragen. Zudem könnte sie relevante Bedrohungs-Szenarien identifizieren und bewerten, allfällige Schutzmassnahmen empfehlen und in Zusammenarbeit mit den Behörden industrieweite Krisenübungen planen und durchführen. Entsprechende Tests würden Rückschlüsse auf und Verbesserungsmöglichkeiten für die Cyber-Resilienz des gesamten Schweizer Finanzplatzes ermöglichen. Eine finanzsektorspezifische Cyber-Sicherheits-Krisenorganisation könnte die Cyber-Resilienz des Schweizer Finanzplatzes nachhaltig stärken.

Der Beirat empfiehlt dem Bundesrat, gemeinsam mit der Finanzindustrie eine finanzsektorspezifische Cyber-Sicherheits-Krisenorganisation aufzubauen.

Erläuternde Dokumente

Beilage 1 «Internationales Benchmarking der Schweiz im Bereich Cyber-Sicherheit im Finanzsektor» enthält eine international vergleichende Einordnung der Situation der Schweiz, was den Schutz des Finanzsektors vor Cyber-Risiken betrifft. Der Vergleich basiert auf einer Umfrage bei den Schweizer Botschaften der Vergleichsländer. Dieser internationale Benchmark war ein wichtiges Element zur Beurteilung des Handlungsbedarfs, der schliesslich zu den Empfehlungen führte.

Beilage 2 «Rahmenbedingungen für die Versicherbarkeit und ein effizientes Management von Cyber Security Risiken» analysiert die Rahmenbedingungen, die notwendig sind, um Cyber Risiken versichern zu können und eruiert möglichen Anpassungsbedarf. Das Dokument kommt zum Schluss, dass zurzeit keine genügend wichtigen institutionellen Hindernisse bestehen, die eine Empfehlung an den Bundesrat rechtfertigen würden.