Beirat Zukunft Finanzplatz **Juni 2017**

Internationales Benchmarking der Schweiz im Bereich Cyber-Sicherheit im Finanzsektor

Inhaltsverzeichnis

Tabellenverzeichnis

1 Einleitung

Die globale digitale Vernetzung hat in den letzten Jahren stark zugenommen. Diese bietet grosses Potenzial, ist jedoch auch die Grundlage für gezielte Cyber-Angriffe, die anonym und ortsunabhängig durchgeführt werden können. Die Zahl solcher Cyber-Angriffe ist in den letzten Jahren stark angestiegen. Im Vergleich mit anderen Branchen ist die Finanzbranche für Cyber-Kriminelle mit Bereicherungsabsichten besonders interessant, was die Wahrscheinlichkeit von Cyber-Attacken auf die Finanzbranche gegenüber anderen Branchen erhöht.[1] Gleichzeitig steigt die Verwundbarkeit des Finanzsektors, da heute die meisten Finanzdienstleistungen über elektronische Kanäle angeboten und genutzt werden. Die Verwundbarkeit ist umso höher, als die digitale Vernetzung der Banken untereinander, aber auch die Vernetzung der Banken mit Unternehmen und Privatpersonen ausgeprägter ist, als in anderen Sektoren. Die Basis eines stabilen Finanzsystems ist das Vertrauen der Kunden. Grössere Vorfälle im Bereich der IT-Sicherheit können das Vertrauen von Unternehmen und Privatpersonen in den Schweizer Finanzplatz belasten. Ein entsprechender Vertrauensverlust birgt das Potenzial, die Stabilität des Finanzsystems zu gefährden. Zum Schutz der Finanzstabilität sowie der Bankkunden ist es daher angezeigt Rahmenbedingungen zu schaffen, die darauf abzielen, dass die Unternehmen ausreichend in die IT-Sicherheit investieren und dadurch die Sicherheit der Finanzinfrastruktur erhöhen.

2 Schutz des Schweizer Finanzsektors vor Cyber-Risiken

Die Gestaltung optimaler Rahmenbedingungen zur Erhöhung der Cyber-Sicherheit im Finanzsektor steht in direktem Zusammenhang mit der «Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS)». Dieser Zusammenhang sowie das der NCS zugrundeliegende Prinzip und die entsprechenden Zuständigkeiten werden im Weiteren erläutert. Anschliessend wird beschrieben wie die Schweizer Finanzbehörden und die Branche derzeit mit dem Thema Cyber-Sicherheit umgehen und jeweils ein direkter Vergleich mit ausgewählten Finanzplätzen vorgenommen. Der Fokus der internationalen Vergleiche liegt auf dem Teilsektor Banken. Die Details dazu sind dem Anhang zu entnehmen. In einem ersten Schritt werden die Zuständigkeiten im Schweizer Finanzsektor und die rechtlichen Grundlagen erläutert. Anschliessend wird beschrieben, welche Massnahmen in den Bereichen Prävention, Reaktion und Kontinuität in Planung oder Umsetzung sind. Letztlich wird der Informationsaustausch innerhalb des Schweizer Finanzsektors beschrieben. Zusammenfassend kann festgehalten werden, dass die Aktivitäten des Schweizer Bankensektors im Bereich Cyber-Sicherheit dem internationalen Vergleich Stand halten. Dennoch gibt es Bereiche in denen die bestehenden Rahmenbedingungen weiterentwickelt werden könnten.

2.1 Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken

Die «Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS)» wurde vom Bundesrat am 27. Juni 2012 für den Zeitraum 2012-2017 verabschiedet. Im Rahmen des Umsetzungsplans wurden 16 Massnahmen definiert und die Federführung für die einzelnen Massnahmen jeweils einem Bundesamt übertragen. Die 16 Massnahmen betreffen vier Bereiche: Prävention, Reaktion, Kontinuität und unterstützende Prozesse.[2] Die beiden kritischen Teilsektoren Banken und Versicherungen sind Teil der Massnahmen „Risiko- und Verwundbarkeitsanalyse“ und „Kontinuitätsmanagement zur Verbesserung der Resilienz der kritischen Teilsektoren“. Am 26. April 2017 hat der Bundesrat das Informatiksteuerungsorgan des Bundes (ISB) beauftragt, in Zusammenarbeit mit den betroffenen Stellen eine Nachfolgestrategie für die Jahre 2018-2023 bis Ende 2017 auszuarbeiten.

[1] Gemäss einer Studie des Ponemon Instituts verursachten Cyber-Angriffe in der Finanzbranche verglichen mit anderen Branchen die höchsten jährlichen Kosten.

[2] Internationale Zusammenarbeit, Forschung und Bildung und rechtliche Grundlagen.

2.1.1 Grundprinzip der Subsidiarität

Der dezentralen Wirtschafts- und Staatsstruktur der Schweiz entsprechend basiert die Nationale Cyber Strategie (NCS) auf dem Subsidiaritätsprinzip. Daher sind in erster Linie die einzelnen Akteure für die Aufrechterhaltung und Optimierung der Schutzmassnahmen zur Minimierung von Cyber-Risiken verantwortlich. Dies soll massgeschneiderte Lösungen für bereichs- oder branchenspezifische Probleme ermöglichen. Der Staat erbringt Leistungen zum Schutz vor Cyber-Risiken nur subsidiär z.B. durch Informationsaustausch und nachrichtendienstliche Erkenntnisse.

2.1.2 Zuständigkeiten für die NCS

2.1.2.1 Organisation auf Bundesebene

Die Gesamtverantwortung für die Umsetzung der Nationalen Cyber-Risiko-Strategie obliegt dem *EFD (ISB)*. Die Umsetzung erfolgt dezentral und basiert auf einer engen Zusammenarbeit mit den zuständigen Departementen der Bundesverwaltung, den Kantonen und der Wirtschaft. Der *Steuerungsausschuss STA NCS*, der sich aus Vertretern der Departemente mit federführender Verantwortung für die 16 Umsetzungsmassnahmen sowie aus Vertretern des Konsultations- und Koordinationsmechanismus Sicherheitsverbund Schweiz (KKM SVS) für die Kantone zusammensetzt, stellt die Umsetzung der NCS sicher. Für die Koordination und Überwachung des Umsetzungsstandes der 16 Massnahmen wurde zudem eine *Koordinationsstelle KS NCS* geschaffen, welche bei MELANI im ISB angesiedelt ist. Sie koordiniert auf operationeller und fachlicher Ebene die Umsetzung der NCS und ist die Geschäftsstelle des STA NCS.

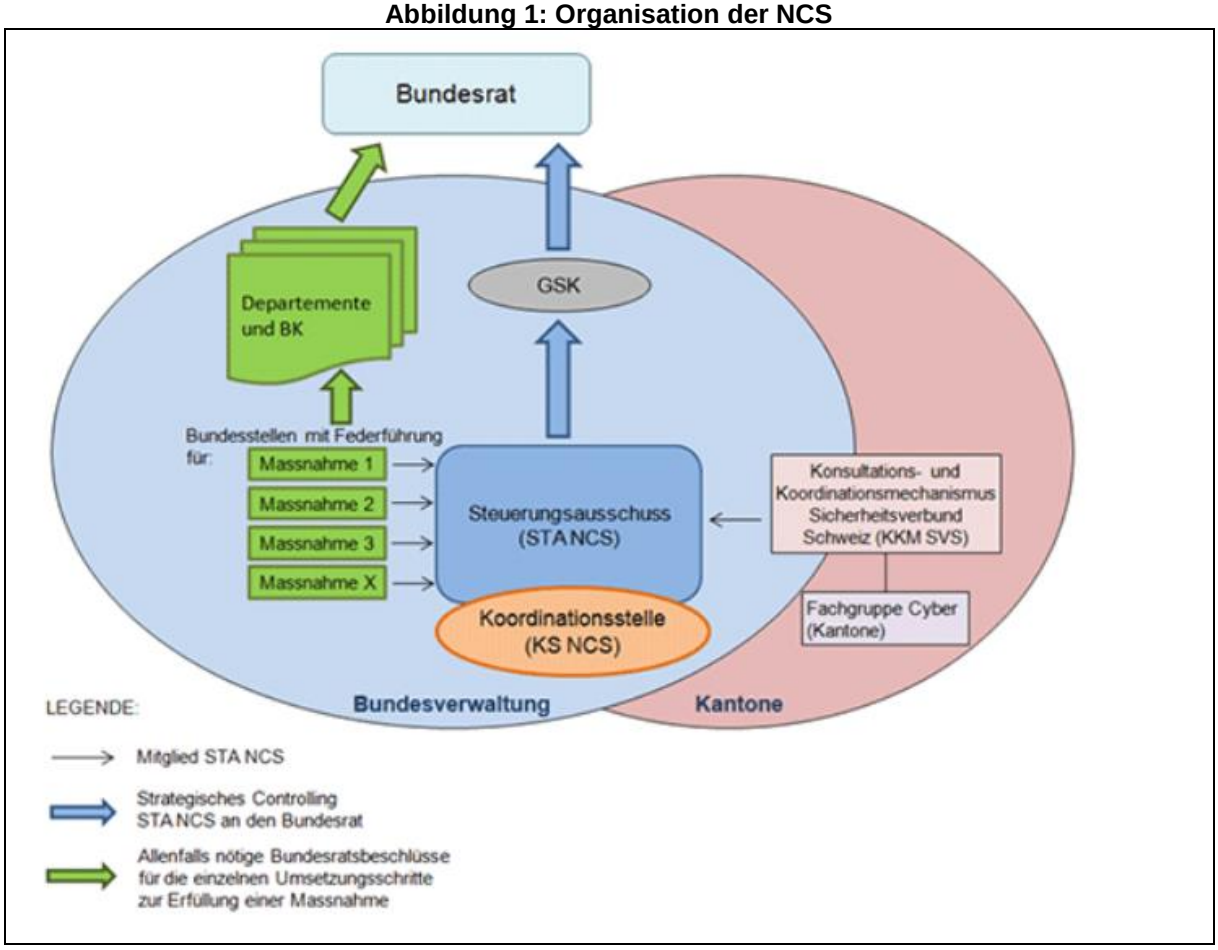
2.1.2.2 Zusammenarbeit Bund-Kantone

Auf ihrem Hoheitsgebiet sind in der Schweiz die Kantone für die Aufrechterhaltung der öffentlichen Sicherheit und Ordnung verantwortlich. Daher werden auch sie in die Umsetzung der NCS miteinbezogen. Die NCS-Umsetzung auf Stufe Kanton wird durch die Fachgruppe Cyber (FG-C) koordiniert, die die Kantone in sämtliche sie betreffenden Umsetzungsmassnahmen miteinbezieht. Für die kantonale Umsetzung der NCS bestehen vier Arbeitsgruppen: Risikoanalyse und Präventionsmassnahmen, Incident Management, Krisenmanagement und Übersicht Straffälle. Im Zusammenhang mit den Teilsektoren Banken[3] und Versicherungen[4] bestehen keine Berührungspunkte. Abbildung 1 gibt einen Überblick über die Organisation der NCS.

[3] Der Teilsektor Banken umfasst die Finanzinstitute, die Finanzmarktinfrastrukturbetreiber, die FINMA und die SNB.

[4] Der Teilsektor Versicherungen umfasst sowohl privatrechtliche als auch öffentlich-rechtliche Versicherungen.

Abbildung 1: Organisation der NCS



Quelle: ISB.

2.2 Zuständigkeiten im Schweizer Finanzsektor

Für den Teilsektor Banken und den Teilsektor Versicherungen wurden im Rahmen der NCS Risiko- und Verwundbarkeitsanalysen (siehe Kapitel 2.4.2) durchgeführt und basierend auf deren Ergebnisse entsprechende Massnahmenberichte erarbeitet. Der Massnahmenbericht zum Teilsektor Versicherungen ist derzeit in Erarbeitung. Die entsprechenden Arbeiten werden für durch das BSV, die FINMA, das ISB sowie Branchenvertreter durchgeführt und durch das BABS koordiniert. In die Arbeiten des Teilsektors Banken waren die FINMA, die SNB und das SIF sowie weitere Vertreter des Bankensektors involviert.[5] Die Verantwortung für die Optimierungen im Bereich der Prävention wurden der FINMA, im Bereich der Reaktion der SNB und im Bereich der Kontinuität dem SIF und dem BABS zugewiesen. Abgesehen von der Zusammenarbeit im Zusammenhang mit den Risiko- und Verwundbarkeitsanalysen und den Massnahmenberichten besteht jedoch derzeit kein institutionalisierter Austausch zwischen Behörden und Finanzsektor.

Im Teilsektor Banken gibt es branchenseitig ein Expertengremium der SBVg zu „Information Security & Cyber Defence“, das sich mit Cyber-Sicherheit befasst. Zudem besteht die Arbeitsgruppe Sicherheit in der Informationstechnologie der Schweizer Banken (ASIT), die als Kompetenzzentrum für Informationssicherheit der Schweizer Banken dient. Sie besteht aus Vertretern von 12 Banken, der SNB und der Finanzdienstleistungsbetreiber. Ansonsten besteht branchenseitig keine institutionalisierte Zusammenarbeit hinsichtlich Cyber-Sicherheit. Es besteht jedoch eine sektorinterne Zusammenarbeit im Rahmen der von der SBVg koordinierten

[5] In die Erarbeitung waren die folgenden Akteure involviert: Vertreter des SIF, der FINMA, der SNB, des ISB, des BAKOM, des BWL, der Verbände und Vertreter der Arbeitsgruppe BCM Banken.

Arbeitsgruppe BCM[6] Banken und der Expertengruppe Banken.[7] Diese beiden Gruppen befassen sich jedoch nicht spezifisch mit Cyber-Sicherheit. Zudem nehmen gewisse Finanzdienstleister an der branchenübergreifenden Partnerschaft von SISA (Swiss Internet Security Alliance) teil, die 2014 in Zusammenarbeit mit Internetanbietern, Finanzdienstleistern und weiteren Partnern gegründet wurde.

Im Teilsektor Versicherungen besteht die Arbeitsgruppe der Versicherer zur Förderung der Informationssicherheit in der Branche (AVIS). Diese dient dem Informationsaustausch zu Fragestellungen hinsichtlich IT-Sicherheit und entsprechenden Initiativen zwischen den Mitgliedern. Aktuell sind 13 Versicherungen Teil dieser Arbeitsgruppe.

Ein **internationaler Vergleich** (siehe Anhang) zeigt, dass insbesondere bei Singapur, Hong Kong und Deutschland die Hauptverantwortung für Regulierung und Aufsicht zu Cyber-Sicherheit bei der Monetary Authority of Singapore (MAS), der Hong Kong Monetary Authority (HKMA) respektive der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) und der Deutschen Bundesbank liegen, die eng mit den jeweiligen Bankenverbänden zusammenarbeiten. Demgegenüber gibt es sowohl in Australien als auch den USA sogenannte nationale Cyber Security Center, die als Hub für den Informationsaustausch mit den Behörden und zwischen den Sektoren dienen.[8] Diese stehen dem gesamten Privatsektor zur Verfügung. Im Vergleich zu Singapur, Hong Kong und Deutschland scheint die Herangehensweise von Australien und den USA zu grösserer Proaktivität der Finanzindustrie zu führen, was insgesamt zu einer starken Zusammenarbeit zwischen den Finanzinstituten führt.[9] Auch im UK wurde ein nationales Cyber Security Center errichtet. Es ist sowohl für den privaten wie auch für den öffentlichen Sektor Anlaufstelle im Bereich Cyber-Sicherheit und bündelt die Cyber-Kompetenz, die vorher über verschiedene Behörden verteilt war. Das UK verfügt als einziges Beispiel über eine institutionalisierte und regelmässige Zusammenarbeit zwischen den Behörden und den Finanzinstituten.[10] Diese findet im Rahmen von Arbeitsgruppen, die sich aus Behörden und Vertretern der Finanzinstitute zusammensetzen, statt.

2.3 Rechtliche Grundlagen

Analog zur dezentralen Umsetzung der NCS finden sich heute in der Schweiz rechtliche Grundlagen für den Cyber-Bereich in einer Vielzahl von Bundesgesetzen und Verordnungen. Eine Massnahme der NCS 2012-2017 war, dass die zuständigen Departemente bestehende Gesetzgebungslücken identifizieren und die nötigen rechtlichen Anpassungen vornehmen. Die Abklärungen haben ergeben, dass kein koordinierender Regelungsbedarf nötig ist.

2.3.1 Teilsektor Banken

Basierend auf der Massnahme „Prüfung von Möglichkeiten zur Reduktion von Cyber-Risiken“ des Massnahmenberichts für den Teilsektor Banken, die im Verantwortungsbereich der FINMA liegt, wurde für den Teilsektor Banken das FINMA-RS 2008/21 „Operationelle Risiken Banken“[11] revidiert und explizite Ausführungsbestimmungen zur Sicherstellung eines systematischen und ganzheitlichen Umgangs mit Cyber-Risiken integriert. Die Inkraftsetzung des revidierten FINMA-RS 2008/21 ist per 1.7.2017 geplant. Zudem wurde ebenfalls das FINMA-

6 Business Continuity Management.

7 Die Expertengruppe Banken besteht aus Vertretern der Behörden, der Verbände, der Finanzinstitute und der Finanzmarktinfrastrukturbetreiber. Sie wurde im Rahmen von Arbeiten zum Thema Schutz kritischer Infrastrukturen (SKI) gebildet und ihre Zusammenarbeit wurde im Kontext der Arbeiten betreffend NCS weiter vertieft.

8 Vergleichbar mit MELANI.

9 Die Regulierungs- und Aufsichtsbehörden spielen auch in Australien und den USA eine Rolle.

10 Auch im UK nimmt der Branchenverband eine aktive Rolle ein.

11 Das Rundschreiben konkretisiert die Art. 89–94 der Eigenmittelverordnung (ERV; SR 952.03) und definiert die qualitativen Grundanforderungen an das Management der operationellen Risiken beruhend auf Art. 12 BankV sowie Art. 19–20 BEHV.

RS 2008/7 „Outsourcing Banken“ revidiert, da auch Auslagerungen der IT und von Business Prozessen zu einer stärkeren Verwundbarkeit der Cyber-Sicherheit führen.[12]

2.3.2 Teilsektor Versicherungen

Für den Teilsektor Versicherungen gibt es keine expliziten Vorgaben im Bereich Cyber-Sicherheit. Es bestehen jedoch im Rahmen des Versicherungsaufsichtsgesetzes (Art. 22 und 27 VAG) und der –verordnung (Art. 98 AVO) sowie im FINMA-RS 2017/02 Vorgaben zum Risikomanagement sowie zum internen Kontrollsystem. Die entsprechenden Vorgaben haben ebenfalls für Cyber-Risiken Gültigkeit.

Der **internationale Vergleich** zeigt, dass es keine einheitliche Handhabung bzgl. rechtlichen Grundlagen gibt. Während die UK, Hong Kong, aber auch Australien über keine spezifische gesetzliche Grundlage im Bereich IT-Sicherheit verfügen, liegen in Singapur, den USA und Deutschland entsprechende branchenübergreifende Gesetze vor. Lediglich die UK und Australien machen keine verbindlichen Vorgaben zur IT-Sicherheit im Bankensektor, während die USA, Singapur, Hong Kong und Deutschland über entsprechende Richtlinien und Rundschreiben verfügen.

2.4 Prävention

2.4.1 Kritische Infrastrukturen

Da Angriffe auf Betreiber von kritischen Infrastrukturen fatale Kettenreaktionen auslösen können, kommt den (oft privaten) Betreibern von kritischen Infrastrukturen, als Erbringer von wichtigen Leistungen mit übergeordneter, sicherheitsrelevanter Bedeutung im Rahmen der NCS eine besondere Bedeutung zu. Basierend auf der Nationalen Cyber-Risiko-Strategie (NCS) und der nationalen Strategie zum Schutz kritischer Infrastrukturen (SKI) müssen daher für die 28 kritischen Teilsektoren (inkl. Teilsektor Banken und Teilsektor Versicherungen) bis Ende 2017 Risiko- und Verwundbarkeitsanalysen erstellt und basierend auf den jeweiligen Ergebnissen Vorschläge für Massnahmen zur Verbesserung der Resilienz erarbeitet werden.[13] Die Koordination dieser Arbeiten hat für die beiden kritischen Teilsektoren Banken und Versicherungen das Bundesamt für Bevölkerungsschutz inne. Die geltenden Aufgaben, Kompetenzen und Verantwortlichkeiten der zuständigen Akteure (Behörden, Verbände, Betreiber kritischer Infrastrukturen) bleiben bei allen Teilsektoren gewahrt. Insbesondere verbleibt die Regulations- und Vorgabekompetenz bei den zuständigen Fachbehörden. Sobald die Risiko- und Verwundbarkeitsanalysen aller 28 Teilsektoren vorliegen, werden diese konsolidiert und, wo nötig, weitere (beispielsweise auch sektorübergreifende) Massnahmen geprüft.

Aus dem **internationalen Vergleich** mit ausgewählten Finanzplätzen geht hervor, dass der Finanzsektor in allen Ländern zur kritischen Infrastruktur gehört und diese über entsprechende Pläne zur Stärkung der Widerstandsfähigkeit des Finanzsektors gegen Cyber-Attacken verfügen.

---

[12] Für Asset Manager gibt es keine expliziten Vorgaben im Bereich Cyber-Sicherheit. Es bestehen jedoch im Rahmen des Kollektivanlagengesetzes (Art. 13 und 14 KAG) und der –verordnung (Art. 12a KKV) sowie der Kollektivanlagenverordnung-FINMA (Art. 68 KKV-FINMA) Vorgaben zum Risikomanagement und zum internen Kontrollsystem. Asset Manager, deren Investoren gemäss Art. 10 Abs. 3, 3bis oder 3ter einzustufen sind und gewisse Kriterien erfüllen, sind von den Vorgaben ausgenommen.

[13] Das Bundesamt für Wirtschaftliche Landesversorgung und das Bundesamt für Bevölkerungsschutz sind jeweils für die Risiko- und Verwundbarkeitsanalysen von je 14 Teilsektoren zuständig und erarbeiten zusammen mit den zuständigen Akteuren Massnahmen zur Verbesserung deren Resilienz. Das BWL und das BABS haben ausschliesslich eine koordinierende Funktion inne.

2.4.2 Risiko- und Verwundbarkeitsanalysen und Massnahmenberichte

2.4.2.1 Teilsektor Banken

Die Risiko- und Verwundbarkeitsanalyse für den Teilsektor Banken wurde im März 2016 abgeschlossen. Daran beteiligt waren die folgenden Akteure: Vertreter der zuständigen Behörden, der Verbände und Vertreter der Arbeitsgruppe BCM Banken. Im Oktober 2016 wurde basierend darauf von derselben Gruppe ein Massnahmenbericht zum Kontinuitätsmanagement des Teilsektors Banken erstellt. Der Fokus lag auf IKT-Verwundbarkeiten und Cyber-Risiken, es wurden aber auch weitere relevante Schwachstellen und Gefährdungen wie beispielsweise ein grossflächiger Ausfall der Stromversorgung untersucht und Massnahmen zu deren Reduktion und zur Verbesserung der Resilienz im Teilsektor Banken erarbeitet.

2.4.2.2 Teilsektor Versicherungen

Die Risiko- und Verwundbarkeitsanalyse für den Teilsektor Versicherungen wurde im Februar 2017 abgeschlossen. In die entsprechenden Arbeiten für den Teilsektor Versicherungen waren das BABS, das BSV, die FINMA, das ISB sowie Branchenvertreter involviert. Basierend darauf wird derzeit von denselben Akteuren ein Massnahmenbericht zum Kontinuitätsmanagement des Teilsektors Versicherungen erstellt. Der Fokus liegt auf Massnahmen zur Verbesserung der Resilienz und Regenerationsfähigkeit insbesondere die Sensibilisierung und Schulung der Mitarbeitenden.

2.4.3 Präventionsmassnahmen

2.4.3.1 Teilsektor Banken

Als Teil der Massnahme „Prüfung von Möglichkeiten zur Reduktion von Cyber-Risiken“ des Massnahmenberichts für den Teilsektor Banken, die im Verantwortungsbereich der FINMA liegt, wurden die folgenden Massnahmen aufgesetzt oder sind derzeit in Planung. Bei den systemrelevanten Banken führten die aufsichtsrechtlichen Prüfgesellschaften spezifische Zusatzprüfungen zum Thema Cyber-Risiken durch und Banken der Kategorie 3 wurden aufgefordert Selbstbeurteilungen hinsichtlich Cyber-Sicherheit vorzunehmen. Banken der Kategorien 4 und 5 sowie Effektenhändler wurden mittels Brief auf die Notwendigkeit eines systematischen und ganzheitlichen Umgangs mit Cyber-Risiken sensibilisiert. Im Rahmen der Revision des FINMA-RS 2008/21 "Operationelle Risiken Banken" wurden Grundsätze zum Umgang mit Cyber-Risiken aufgenommen. Diese orientierten sich an dem international anerkannten NIST Cybersecurity Framework[14] und werden per 1.7.2017 in Kraft gesetzt. Diese Grundsätze verpflichten Banken auch zur periodischen Durchführung von Verwundbarkeitsanalysen und Penetration-Tests. Zudem wurde das FINMA-RS 2008/7 „Outsourcing Banken“ revidiert, da auch Auslagerungen der IT und der Business Prozesse zu einer stärkeren Verwundbarkeit für Cyber-Angriffe führen. Ebenfalls prüft die FINMA, ob auch in der Schweiz analog zu Singapur regelmässig (z.B. alle 18 bis 24 Monate) sektorweite Übungen durchgeführt werden sollen.

2.4.3.2 Teilsektor Versicherungen

Da der Massnahmenbericht im Teilsektor Versicherungen noch nicht erstellt wurde, wurden noch keine expliziten Präventionsmassnahmen definiert. Allerdings bestehen auch im Teilsektor Versicherungen Vorgaben zu Risikomanagement und zum internen Kontrollsystem (siehe Kapitel 2.3.2) sowie Vorgaben zum Business Continuity Management (BCM).

Der **internationale Vergleich** zeigt, dass Penetrationstests sowohl in Singapur, Hong Kong als auch Deutschland obligatorisch sind, während diese im UK, den USA und in Australien freiwillig durchgeführt werden können. Im UK werden bei den 34 grössten Finanzinstituten

[14] National Institute of Standards and Technology des US Department of Commerce.

durch externe Anbieter sogenannte CBEST-Tests durchgeführt. Der Lead liegt bei den Behörden, die eng mit den Finanzinstituten zusammenarbeiten. In Singapur finden alle 2-3 Jahre umfassende Echt-Zeit-Stresstests (Industrie-Wide Business Continuity Exercises) für den Bankensektor statt, die durch die Monetary Authority of Singapore (MAS) und den Bankenverband durchgeführt werden. In Hong Kong, Deutschland und in Singapur liegt die Verantwortung für die *regelmässigen* Penetrationstests bei den Finanzinstituten.

2.5 Reaktion

Im Bereich Reaktion der NCS wurden 2016 beim Informatiksteuerungsorgan des Bundes (ISB) und dem Eidgenössischen Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) insbesondere beim GovCERT die Fachkompetenzzentren zur Analyse von Schadsoftware weiter ausgebaut und die Detektions- und Reaktionsfähigkeit erhöht. In der Fachabteilung Cyber des Nachrichtendienstes des Bundes (NDB) konnten das Spezialwissen und Fähigkeiten aufgebaut werden, die es ihm erlauben, die Ziele, Methoden und Akteure eines Angriffs zu analysieren und so mögliche Täter zu identifizieren. Das entsprechende Knowhow wird dem Finanzsektor über MELANI zur Verfügung gestellt.

2.5.1 Teilsektor Banken

Im Schweizer Bankensektor besteht derzeit kein spezifisches Krisendispositiv für eine rasche Reaktion auf Cyber-Krisen. Allerdings besteht mit der Interbank Alarm- und Krisenorganisation (IAKO) eine Krisenorganisation mit vier Untergruppen (Kerngruppe, Gruppe Liquidität, Gruppe SIC/euroSIC, Gruppe IT). Diese Organisation wurde durch die Schweizerische Nationalbank (SNB) ins Leben gerufen und dient dazu, im Krisenfall schnell die Entscheidungsträger der systemrelevanten Banken und Institute im Rahmen einer institutsübergreifenden Telefonkonferenz zu verbinden.[15] Im Rahmen der Massnahme „Anbindung der Interbanken Alarm- und Krisenorganisation (IAKO) an ein ausfallsicheres Kommunikationssystem“ des Massnahmenberichts für den Teilsektor Banken wird derzeit geprüft, ob die IAKO – bestehend aus Vertretern der systemrelevanten Akteure des Teilsektors Banken – an ein ausfallsicheres Kommunikationssystem angeschlossen werden soll, damit sie auch bei grossflächigen und längerdauernden Ereignissen wie Stromausfällen und/oder Ausfällen der Telekommunikation einberufen werden kann. Die IAKO hat derzeit keine AKV im Zusammenhang mit Cyber-Sicherheit.

2.5.2 Teilsektor Versicherungen

Auch im Bereich der Reaktion wurden für den Teilsektor Versicherungen noch keine Massnahmen definiert.

Der **internationale Vergleich** zeigt, dass alle Länder über ein CERT verfügen, die sektorübergreifend tätig und mit dem bei MELANI angesiedelten GovCERT vergleichbar sind. Ein spezifisch für den Bankensektor verantwortliches Krisendispositiv für den Fall einer Cyber-Krise, gibt es lediglich im UK. Dieses kann von der Finanzmarktaufsicht (FCA/PRA) rund um die Uhr einberufen werden. Normalerweise sind nebst der Finanzmarktaufsicht die Bank of England und das Finanzministerium Teil des Dispositivs. Je nach Bedarf werden auch das nationale Cyber Security Center sowie die Sicherheitsdienste involviert.

2.6 Kontinuität

2.6.1 Teilsektor Banken

Im Rahmen der Risiko- und Verwundbarkeitsanalyse zum Teilsektor Banken wurden zwei Massnahmen definiert, die auf Kontinuität abzielen. Da bei einem grossflächigen und/oder langandauernden Ausfall der Telekommunikation oder der Stromversorgung die Leistungen,

[15] Die Versicherungswirtschaft ist hierbei nicht vertreten.

die von den Akteuren des Teilsektors Banken im Verbund erbracht werden (z. B. Bargeldversorgung, (bargeldloser) Zahlungsverkehr, Börsengeschäfte, Sicherstellung der Liquidität), stark beeinträchtigt werden, ist derzeit ein Notfallkonzept zur Sicherstellung der Bargeldversorgung und des (bargeldlosen) Zahlungsverkehrs in Erarbeitung. Der Lead dafür liegt beim SIF. Um die Auswirkungen zu reduzieren, die durch eine Beeinträchtigung von Leistungen im Teilsektor Banken infolge von grossflächigen und längerdauernden Ereignissen entstehen können, ist es denkbar, sogenannte Bankfeiertage einzuberufen. Es soll daher ein Konzept erarbeitet werden, das die Einberufung von Bankfeiertagen insbesondere die Rechtsgrundlagen und die Kompetenzen zur Einberufung respektive Aufhebung etc. klar definiert. Die Koordination dieser Massnahme liegt beim BABS, wobei die bestehenden Zuständigkeiten berücksichtigt und gewahrt bleiben.

2.6.2 Teilsektor Versicherungen

Auch im Bereich der Kontinuität wurden für den Teilsektor Versicherungen noch keine Massnahmen definiert.

2.7 Informationsaustausch

2.7.1 Informationsplattform

Die Melde- und Analysestelle Informationssicherung (MELANI) des Bundes betreibt eine Plattform namens MELANI-Net, auf welcher Informationen zu Cyber-Ereignissen publiziert und der Öffentlichkeit zur Verfügung gestellt werden. MELANI verfügt über einen offenen und einen geschlossenen Kundenkreis und ist sektorübergreifend tätig. Betreiber kritischer Infrastrukturen können dem geschlossenen Kundenkreis kostenlos beitreten. Dessen Mitglieder gewährt MELANI einen erweiterten Zugang zu detaillierteren und sehr zeitnahen Informationen vom Computer Emergency Response Team (GovCERT) der Schweiz. Aktuell sind lediglich die grossen Finanzinstitute Teil des geschlossenen Kundenkreises. Hingegen sind kleine Banken, Auslandbanken und relevante Drittparteien nicht Teil des geschlossenen Kundenkreises. Es könnte daher in Erwägung gezogen werden, ob auch diese Parteien Teil des geschlossenen Kundenkreises sein sollten. Auch die FINMA ist nicht Teil des geschlossenen Kundenkreises, obwohl dies im Rahmen ihrer Arbeit zielführend sein könnte. Es könnte daher ebenfalls abgeklärt werden, inwiefern ein zumindest partieller Zugang der FINMA zu den Informationen des geschlossenen Kundenkreises von MELANI möglich wäre.

Aus dem **internationalen Vergleich** geht hervor, dass Singapur, Deutschland und Australien über keine technische Informationsplattform verfügen. In Deutschland haben die Sektoren kritischer Infrastruktur jedoch über andere Kanäle Zugang zu Informationen des Bundesamtes für Informatiksicherheit. In Australien stehen für den Austausch zwischen Privatsektor und Regierung das nationale Cyber Security Center und die regionalen Joint Coordination Centers zur Verfügung. Das UK, die USA und Hong Kong verfügen jedoch analog zum schweizerischen MELANI über technische Informationsplattformen.

2.7.2 Meldung an Behörden

In der Schweiz gibt es derzeit keine Meldepflicht, die Unternehmen dazu verpflichtet, Cyber-Vorfälle an MELANI zu melden. Alle Meldungen erfolgen auf freiwilliger Basis. Jedoch besteht gemäss Finanzmarktaufsichtsgesetz sowohl für Banken als auch für Versicherer eine allgemeine Auskunfts- und Meldepflicht an die FINMA, die eine unverzügliche Meldung von Vorkommnissen vorsieht, die für die Aufsicht von wesentlicher Bedeutung sind. Dies umfasst auch wesentliche Cyber-Vorfälle. Zudem soll künftig gemäss Datenschutzgesetz bei Datenverlust eine Meldung ans EDÖB erfolgen.

Der **internationale Vergleich** zeigt, dass es keine einheitliche Handhabung bzgl. Meldepflicht gibt. In Singapur, Hong Kong und Deutschland ist die Meldung von Cyber-Vorfällen an die Behörden für Finanzinstitute obligatorisch, für alle übrigen Unternehmen jedoch freiwillig. Im UK, den USA und Australien hingegen ist die Meldung für alle Unternehmen freiwillig.

2.7.3 Information der Kunden

Das Rundschreiben „Operationelle Risiken“ (Anhang 3, Rz 46) sieht für Schweizer Finanzinstitute vor, dass deren Kunden bei schwerwiegenden Fällen in Bezug auf die Vertraulichkeit von Kundenidentifikationsdaten (bspw. durch Cyber-Vorfälle) informiert werden müssen. Für die Versicherer besteht aktuell keine analoge Regelung. Im **internationalen Vergleich** sind bis auf das UK, wo fallweise beurteilt wird, ob eine entsprechende Information nötig ist, in allen untersuchten Ländern die Kunden von Finanzinstituten obligatorisch über Cyber-Vorfälle zu informieren. In Singapur und Hong Kong muss es sich um folgenreiche Störfälle handeln.

2.8 Arbeiten zu Cyber-Sicherheit in den internationalen Finanzgremien

Auch auf internationaler Ebene steigt die Bedeutung von Cyber-Sicherheit im Finanzsektor.[16] Daher wurde das Financial Stability Board im März 2017 von der G20 beauftragt, eine Bestandesaufnahme der bestehenden Regulationen und Aufsichtspraktiken zu Cyber-Sicherheit der G20 Jurisdiktionen und zu internationalen Richtlinien zu tätigen. Damit wird das Ziel verfolgt die effektivsten Praktiken zu identifizieren. Ein erstes Update wird am G20 Gipfel im Juli 2017 erfolgen. Die Bestandesaufnahme wird im Oktober 2017 an die Finanzminister übergeben. Basierend auf dieser Bestandesaufnahme werden auf internationaler Ebene voraussichtlich weitere gemeinsame Arbeiten zum Thema Cyber-Sicherheit durchgeführt werden. Im Auftrag des Beirats Zukunft Finanzplatz hat das SIF im 4. Quartal 2016 eine eigene Bestandesaufnahme erstellt. Das Resultat dieser Bestandesaufnahme ist dem Anhang zu entnehmen.

[16] Das Thema Cyber-Sicherheit steht auch auf der Agenda der IOSCO und der IAIS.

3 Anhang

3.1 Einleitung

Der vorliegende Anhang soll einen Überblick über die Cyber Security Initiativen ausgewählter Finanzplätze schaffen. Er basiert auf den Rückmeldungen zu einem Fragebogen der entsprechenden Schweizer Botschaften. Zuerst werden die Einbettung des Finanzsektors in die nationalen Cyber Security Strategien sowie die rechtlichen Grundlagen der ausgewählten Länder erläutert. Anschliessend wird aufgezeigt, wie die Verantwortlichkeiten zwischen Behörden und Finanzsektor verteilt sind. Danach wird dargelegt, welche präventiven Massnahmen Teil der Cyber Security Initiativen sind, wie der Informationsaustausch zwischen Behörden und Finanzsektor, sowie finanzsektorintern funktioniert und welche Vorkehrungen für den Fall einer Cyber-Krise bestehen.

3.2 Sektorspezifische Cyber Security Schutzprogramme

Die Abklärungen der Botschaften zeigen, dass bis auf **Deutschland** keines der befragten Länder über eine auf den Finanzsektor ausgerichtete (Sub-)Strategie zur nationalen Cyber Security verfügt. Die deutsche Substrategie für den Finanzsektor wurde von den Banken selbst initiiert. Hingegen wurde der Finanzsektor in allen Ländern als kritische Infrastruktur definiert, weshalb bis auf **Australien** alle Länder über entsprechende Pläne zur Stärkung der Widerstandsfähigkeit des Finanzsektors gegen Cyber-Attacken verfügen. Im **UK** wird seit 2010 ein sogenannter Resilienz-Plan für den Finanzsektor erstellt und jährlich aktualisiert. In **Singapur** besteht für die 11 kritischen Infrastrukturen, zu welchen der Finanzsektor zählt, ein Schutzprogramm (CII Protection Programme) mit einem systematischen Cyber-Risikomanagement. In den **USA** gibt es den sogenannten Financial Services Sector-Specific Plan 2015, der Teil des nationalen Infrastrukturschutzplans (NIPP) ist. Als Teil der kritischen Infrastruktur wurde auch für den Finanzsektor **Hong Kongs** eine Cybersecurity Fortification Initiative (CFI) lanciert. Insgesamt messen alle befragten Staaten einer engen Zusammenarbeit zwischen Staat und Privatsektor einen hohen Stellenwert bei.[17]

Tabelle 1: Sektorspezifische Schutzprogramme

UK	USA	Singapur	Hong Kong	Deutschland	Australien	Schweiz
Resilienz-plan für den Finanzsektor	Financial Services Sector-Specific Plan 2015	CII Protection Programme	Cyber-security Fortification Initiative	Substrategie	Keine Substrategie	*Massnahmenpläne für die Teilsektoren Banken und Versicherungen*[18]

3.3 Rechtliche Grundlagen

Bis auf das **UK, Hong Kong und Australien** gibt es in allen befragten Ländern eine gesetzliche Grundlage für den Umgang mit Cyber Security oder entsprechende Gesetze sind in Erarbeitung.[19] In Hong Kong besteht die von der Hong Kong Monetary Authority (HKMA) erlassene Richtlinie zur generellen Handhabung von Technologie- und Cyber-Risiken.[20] In **Singapur** ist

[17] In Singapur sind für die Umsetzung der Nationalen Cyber Security Strategie auch die Zusammenarbeit mit der Wissenschaft und der Zivilbevölkerung relevant.

[18] Koordiniert durch das BABS.

[19] Erste Erkenntnisse aus den CBEST-Tests zeigen, dass das Wissen der Finanzinstitute zur Bedrohungslage im Bereich Cyber Security dürftig ist. Das UK befürwortet daher internationale Vorgaben. Die BIS/IOSCO-Richtlinien von Juni 2016 seien ein wichtiger Schritt in die richtige Richtung.

[20] Supervisory Policy Manuals on technology risk, business continuity and e-banking.

gegenwärtig ein neues Cyber Security Gesetz im Parlament, das im Verlaufe des Jahres 2017 verabschiedet werden dürfte. Dies ist ein nationales, sektorübergreifendes Rahmengesetz und wird auch für den Finanzsektor relevant sein. Es gibt Mindestanforderungen für Vorbeugemassnahmen vor und wird der seit 2015 existierenden Cyber Security Agency (CSA) die gesetzliche Grundlage geben. Zudem soll das neue Gesetz für alle Wirtschaftssektoren eine Berichterstattungspflicht bezüglich Cyber-Attacken enthalten. Nebst diesem Rahmengesetz legt die Monetary Authority of Singapore (MAS) – ähnlich wie in Hong Kong – Richtlinien[21] für den Finanzsektor zur generellen Handhabung von Technologie- und Cyber-Risiken fest.

Auch in den **USA** gibt es seit 2015 den Cybersecurity Act (CISA), der die rechtliche Grundlage für den Informationsaustausch im Privatsektor sowie zwischen Privatsektor und Behörden ist. Das Federal Reserve Board beabsichtigt zudem zusammen mit dem Office of the Comptroller of the Currency (OCC) und der Federal Deposit Insurance Corporation (FDIC) die Standards im Bereich Cyber Security Management für grosse Finanzinstitute, die unter ihrer Aufsicht stehen, zu verstärken. Im Gliedstaat New York gilt zudem ab 1.3.2017 eine spezifisch auf den Umgang von Finanzinstituten mit Cyber Security ausgerichtete Gliedstaatenregelung.

In **Deutschland** wurde im 2015 das nationale IT-Sicherheitsgesetz (IT-SiGes) verabschiedet. Dieses verpflichtet Betreiber kritischer Infrastrukturen (inkl. Finanzsektor) zu technischen Mindeststandards und Meldepflichten. Bei Nicht-Erfüllung werden die Betreiber mit Geldstrafen von zw. EUR 50‘000 – 100‘000 belangt. Zusätzlich gilt die Europäische Richtlinie für Netzwerk- und Informationssicherheit (NIS-Richtlinie). Diese ist teils zum IT-SiGes äquivalent, überträgt dem Bundesamt für Sicherheit in der Informationstechnik (BSI) jedoch zusätzliche Überwachungs- und Prüfbefugnisse. Spezifisch für den Finanzsektor sind im Kreditwesengesetz Schutzziele zur IT-Sicherheit festgelegt. Zudem definiert die BaFin im MaRisk-Rundschreiben Mindestanforderungen an das Risikomanagement. Die Einhaltung dieser Mindestanforderungen wird durch die BaFin überwacht. Seit 2016 regelt die EU-Zahlungsdienstleisterrichtlinie Standards zur IT-Sicherheit für Zahlungsdienstleister.

Tabelle 2: Rechtliche Grundlagen

UK	USA	Singapur	Hong Kong	Deutschland	Australien	Schweiz
Keine gesetzliche Grundlage	– Cyber Security Act – Standards des FED, OCC und FDIC	– Cyber Security Gesetz – Richtlinien der MAS	– Keine gesetzliche Grundlage – Richtlinien der HKMA	– IT-Sicherheitsgesetz – Kreditwesengesetz – MaRisk-Rundschreiben – Europäische Richtlinie für Netzwerk- und Informationssicherheit – EU Zahlungsdienstleisterrichtlinie	Keine gesetzliche Grundlage	– *FINMA-Rundschreiben: Operationelle Risiken Banken* – *FINMA-Rundschreiben: Corporate Governance – Versicherer*

[21] Technology Risk Management Guidelines.

3.4 Verantwortlichkeiten Staat / Finanzsektor

- Im UK besteht der institutionelle Aufbau im Bereich Cyber Security für den Finanzsektor aus zwei Pfeilern. Einerseits bestehen Arbeits- und Untergruppen in denen sowohl die Behörden (BoE, Finanzministerium, Finanzmarktaufsicht und NCSC) als auch der Finanzsektor vertreten sind. Andererseits bestehen Arbeits- und Untergruppen exkl. Beteiligung des Finanzsektors.
- In Hong Kong und in Singapur sind die Finanzmarktbehörden HKMA sowie die MAS federführend. Gleichzeitig leisten aber auch die Bankiervereinigungen einen massgeblichen Beitrag zur Erhöhung der Cyber-Resilienz.
- In den USA ist das National Cybersecurity and Communications Integration Center (NCCIC) für den sektorübergreifenden Informationsaustausch zuständig. Im Finanzsektor befassen sich die Regulierungsbehörden und das Treasury mit Cyber Security und bilden zusammen ein behördenseitiges Gremium. Diesem steht auf Seite des Finanzsektors das Gremium FSSCC gegenüber. Die beiden Gremien arbeiten eng zusammen. Der brancheninterne Informationsaustausch ist noch wenig ausgeprägt und es bestehen Bemühungen diesen zu verstärken.
- In Deutschland befassen sich hauptsächlich die Deutsche Bundesbank und das BaFin mit dem Thema Cyber Security im Finanzsektor. Der Informationsfluss zwischen dem Finanzsektor und den Behörden findet im Rahmen der UP KRITIS statt.
- In Australien besteht derzeit keine finanzsektorspezifische Zusammenarbeit zwischen Behörden und Finanzinstituten. Es besteht jedoch eine informelle Zusammenarbeit zwischen den Banken.

Der institutionelle Aufbau zur Cyber Security im Finanzsektor basiert im **UK** auf einem Mandat des Financial Policy Committee (FPC) der Bank of England. Das FPC hat Mitte 2013 Cyber Security als nicht-finanzielles Risiko für den Finanzsektor identifiziert und dem Finanzministerium den Auftrag erteilt, in diesem Bereich aktiv zu werden. Daraufhin wurden keine eigenen Cyber Security Institutionen, sondern auf das Thema ausgerichtete Arbeitsgruppen errichtet.[22]

Die Bank of England leitet den „Workstream Cyber Security". Darin vertreten sind das Finanzministerium, die Finanzmarktaufsicht, das Nationale Zentrum für Cyber Security (NCSC) und einzelne Unternehmen des Privatsektors. Diese Arbeitsgruppe trifft sich vierteljährlich und ist primär auf strategischer Ebene tätig. Sie kann als nationale Steuerungsgruppe betrachtet werden. Zusätzlich zu diesem Workstream besteht eine Strategiegruppe ohne Beteiligung des Privatsektors („Government-Regulator Strategy Group"). Diese trifft sich alle sechs Wochen, um strategisch relevante Themen im Bereich Cyber Security zu identifizieren. Sie bildet im Krisenfall das Krisendispositiv (siehe Kapitel 3.7). Sie ist für die Resilienzplanung des Finanzsektors insgesamt zuständig (inkl. operationale Resilienz etwa von Infrastruktur). Auf Stufe Sektionsleitung befasst sich eine Untergruppe nur mit Cyber Security. Auf operativer Ebene besteht unterhalb des Workstreams die sog. Cyber-Koordinationsgruppe in derselben Zusammensetzung wie der Workstream (hierarchisch etwa auf Stufe Sektionsleitung). Unterhalb der Cyber-Koordinationsgruppe gibt es zwei weitere Untergruppen, die die Resilienzplanung konkret umsetzen und üben. Die CMORG[23] Cyber Group (CCG) ist für das Monitoring des Cyber-Bedrohungsumfeldes zuständig und unterstützt den Privatsektor bei der Reaktion auf Bedrohungen. Die Sector Exercising Group (SEG) ist für ein regelmässiges Übungsprogramm zwischen Regierung und Firmen verantwortlich, das die Kapazitäten des Sektors testet.[24]

Im September 2016 wurde das Nationale Zentrum für Cyber Security (NCSC) eingerichtet. Es ist Teil der Behörde des Geheimdienstes, die für Kommunikationssicherheit zuständig ist (GCHQ). Sie ist sowohl für den privaten wie auch für den öffentlichen Sektor Anlaufstelle im

[22] Die Vertreter in den verschiedenen Arbeitsgruppen sind jeweils in ihrem spezifischen Aufgabenbereich tätig (Bank of England: Finanzstabilität, Finanzinfrastruktur; Finanzmarktaufsicht: Sicherheit der einzelnen Finanzinstitute, Konsumentenschutz; Finanzministerium: grundsätzliche Verantwortung für den Finanzsektor).

[23] Cross Market Operational Resilience Group (CMORG).

[24] Diese Übungen haben ihren Fokus auf dem Incident Response Management.

Bereich Cyber Security und bündelt die Cyber-Kompetenz, die vorher über verschiedene Behörden verteilt war. Auch das Computer Emergency Response Team (CERT-UK) wurde dabei in das NCSC integriert. Das NCSC[25] enthält für alle identifizierten Bereiche der kritischen Infrastruktur also auch für den Finanzsektor eigene Teams und arbeitet beim Cyber-Testing der Finanzinstitute eng mit der Bank of England zusammen.

Die Cyber Security Agency (CSA) ist **Singapurs** federführende Institution im Bereich Cyber-Sicherheit. Sie ist sektorübergreifend tätig und institutionell dem Büro des Premierministers angegliedert. Bislang waren 5% des nationalen Informations- und Technologiebudgets für Cyber-Sicherheit reserviert (2014: S$408.6 Mio. / ca. CHF 300 Mio.). Dieser Anteil wird ab 2017 auf 8% erhöht. Singapur verfügt über ein Computer Emergency Response Team (SingCERT), das 2015 dem CSA angegliedert wurde. Sein Auftrag ist die Erfassung, Bekämpfung und Vermeidung von Ereignissen im Zusammenhang mit Cyber-Sicherheit. Dem SingCERT sind diverse Cyber Security-Ereignisse zu melden.

Im Finanzsektor ist die MAS für die Aufsicht im Bereich Cyber-Sicherheitsrisiken zuständig. Sie überwacht die Finanzinstitute und führt Prüfungen bei Unternehmen vor Ort durch. Sie legt in den „Technology Risk Management Guidelines“ Richtlinien zur generellen Handhabung von Technologie- und Cyber-Risiken im Finanzsektor fest. Der Branchenverband Association of Banks in Singapore (ABS) verfügt über ein Standing Committee on Cyber Security, in dem die grossen Finanzinstitute vertreten sind. Dieses dient dem Informationsfluss zwischen den Finanzinstituten. Die kleineren Institute werden vom Committee separat informiert. Singapur verfügt zudem über diverse Public-Private-Partnerships im Bereich Bildung und Forschung.

In **Hong Kong** ist der institutionelle Aufbau bezüglich Cyber Security insbesondere im Finanzsektor sehr dezentral. Auch Hong Kong verfügt über ein Computer Emergency Response Team Coordination Centre (HKCERT), das vom Hong Kong Productivity Council (HKPC) betrieben wird. Es koordiniert Reaktionen auf Cyber-Vorfälle für lokale Unternehmen und Internetnutzer. Sein Auftrag ist die Aufklärung und Beratung zu präventiven Massnahmen im Bereich Cyber Security. Die HKMA ist verantwortlich für die Bankenaufsicht und -regulierung und ist in diesem Rahmen auch im Bereich Cyber Security im Finanzsektor tätig. Sie ist zuständig für die Cybersecurity Fortification Initiative (CFI), die sie in enger Zusammenarbeit mit dem Finanzsektor vorantreibt. Auch die Securities and Futures Commission (SFC) sensibilisiert in einem Rundschreiben auf Cyber Security Risiken und empfiehlt den durch sie lizenzierten Unternehmen acht spezifische Kontrollen. Der Branchenverband der Hong Konger Banken (HKAB) hat zudem eine Arbeitsgruppe zum Thema Cyber Security errichtet, die Cyber Security Themen zwischen den Banken koordiniert und als Informationskanal dient. Bislang besteht im Finanzsektor von Hong Kong kein koordinierter Ansatz zum Umgang mit Cyber Security Risiken.

In den **USA** ist das Department for Homeland Security (DHS) für die übergreifende Cyber Security-Strategie zuständig. Für die Erarbeitung der sektorspezifischen Pläne (SSP) werden die zuständigen Behörden, im Falle des Finanzsektors das Department of the Treasury, beauftragt. Es ist zusammen mit ausgewählten Finanzinstitutionen und dem Financial Services Information Sharing and Analysis Center (FS-ISAC) im National Cybersecurity and Communications Integration Center (NCCIC) vertreten. Dieses dient über alle Sektoren mit kritischer

[25] Das NCSC ist die Schnittstelle zwischen Geheimdienst und Finanzbehörden und ist primär für die Identifizierung der Bedrohungslage und für das Einspeisen dieses Wissens in die zuständigen Koordinationsgremien zuständig. Es fungiert als technisches Kompetenzzentrum für Cyber Security. Es ist für das Management von Sicherheitsvorfällen bis zu einer gewissen Schwelle zuständig. Es nimmt die Meldungen seitens Privatsektors entgegen. Es führt die CISP-Plattform, die dem Informationsaustausch mit dem Privatsektor bezüglich Cyber-Vorfällen dient. Ebenfalls führt es die Financial Services Information Exchange, ein regelmässiger technischer Austausch zwischen NCSC und dem Privatsektor (rund alle paar Monate).

Infrastruktur hinweg als Hub für den Informationsaustausch im Bereich Cyber Security. Die USA verfügt ebenfalls über ein Computer Emergency Response Team, das dem DHS angegliedert ist. Es reagiert auf technische Störungen, unterstützt Betreiber von Informationssystemen und sorgt für die rechtzeitige Benachrichtigung über aktuelle und potenzielle Bedrohungen. Es arbeitet zudem daran, Techniken zum weltweiten Informationsaustausch im Bereich Cyber Security (TAXII, STIX, CybOK)[26] zu automatisieren. Das Federal Reserve Board, das Office of the Comptroller of the Currency (OTC) und die Federal Deposit Insurance Corporation (FDIC) wollen ihrerseits die Cyber Risk Management Standards für grosse Institute in den folgenden Bereichen stärken: Cyber Risk Governance, Cyber Risk Management, Management von internen und externen Abhängigkeiten, Incident Response, Cyber Resilience und Situational Awareness. Die Financial Industry Regulatory Authority (FINRA) überprüft ihrerseits die Fähigkeit der Finanzinstitute, die Vertraulichkeit, Integrität und Verfügbarkeit sensibler Kundendaten zu schützen. Dazu gehört auch die Überprüfung der Einhaltung der SEC-Vorschriften[27] durch die einzelnen Unternehmen.

Für den Finanzsektor besteht als übergeordnete Organisation für den Schutz kritischer Infrastruktur auf Behördenseite ein Financial and Banking Information Infrastructure Committee (FBIIC). In diesem sind die Regulierungsbehörden und das US-Treasury vertreten. Das Gremium arbeitet eng mit dem DHS, dem US Secret Service, dem Department of Justice und den Federal Bureau of Investigation (FBI) sowie dem Department of Defense zusammen. Es setzt sich stark für Public-Private Partnerships im Finanzsektor ein. Auch seitens der Industrie besteht ein Gremium (FSSCC),[28] das sich unter anderem mit Cyber Security im Finanzsektor befasst. Das FSSCC arbeitet eng mit dem FBIIC, aber auch mit dem DHS zusammen. Seitens Finanzindustrie haben acht grosse US-Banken, die von der US-Regierung als kritische Infrastruktur definiert wurden, die Initiative für die Gründung eines strategisch orientierten Financial Systemic Analysis & Resilience Centers (FSARC) ergriffen. Dieses wird von der FS-ISAC, einer globalen nicht-gewinnorientierten Mitgliederorganisation des Finanzsektors, aufgebaut. Seit 2013 gibt es die vom Financial Services Roundtable organisierten Joint Financial Associations Cybersecurity Summits, an denen sich der Finanzsektor und Regierungsvertreter zweimal jährlich treffen, um über die Widerstandsfähigkeit des Finanzsektors gegenüber Cyber-Risiken zu diskutieren.

In **Australien** liegt die Gesamtverantwortung im Bereich Cyber Security beim Department of Prime Minister and Cabinet.[29] National wurden 250 Mio. australische Dollar (ca. 194 Mio. CHF) über fünf Jahre als Budget gesprochen. Es wurde sogar ein spezifischer Ministerposten für Cyber Security geschaffen. Auch Australien verfügt über ein CERT, das beim Attourney Generals Department angesiedelt ist. Für die Zusammenarbeit mit dem Privatsektor besteht keine Steuerungsgruppe, sondern es bestehen Strukturen, in welchen sich der Privatsektor auf freiwilliger Basis engagieren kann. Einerseits sind dies die sogenannten Joint Cyber Threat Sharing Centers, andererseits wurde auch ein nationales Cyber Security Center (ACSC) errichtet, über das die Zusammenarbeit von Behörden, Regulatoren und Privatsektor erfolgen soll. Das ACSC sammelt Informationen, evaluiert Bedrohungen und berät den Privatsektor entsprechend. Im Finanzsektor ist in Australien die Australian Securities and Investment Commission (ASIC) für die Regulierung insbesondere des Finanzsektors zuständig. Es gibt keine spezifische Regulierung zu Cyber Security, es wird jedoch erwartet, dass die Banken Cyber-Risiken

[26] Trusted Automated eXchange of Indicator Information (TAXII), Structured Threat Information eXpression (STIX) und Cyber Observable eXpression (CybOX) sind Applikationen, die einen automatisierten Informationsaustausch für das Bewusstsein bzgl. Cyber-Sicherheit, eine Echtzeit-Netzwerkverteidigung und eine ausgeklügelte Bedrohungsanalyse ermöglichen.

[27] Securities and Exchange Commission.

[28] Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security.

[29] Das Department of Foreign Affairs and Trade ist hinsichtlich internationaler Zusammenarbeit im Bereich Cyber Security zuständig, während das Australian Signals Directorate aus technischer Sicht zuständig ist.

angemessen in ihr Risikomanagement integrieren. Zwischen den vier grössten Banken gibt es eine informelle Zusammenarbeit.

In **Deutschland** ist das Bundesamt für Sicherheit in der Informationstechnik (BSI) dafür verantwortlich die Implementierung und Einhaltung des IT-Sicherheitsgesetzes sowie der NIS-Richtlinie, die auch für den Finanzsektor gelten, zu kontrollieren. Zudem unterstützt es die Bundesanstalt für Finanzdienstleistungsaufsicht (BAFin) bei der Ausgestaltung des IT-Sicherheitsgesetzes im Finanzbereich. Das BSI erstellt und zertifiziert zudem Normen (z.B. ISO 100-1). Bei IT-Angriffen auf kritische Infrastrukturen leistet das Computer Emergency Response Team für Bundesbehörden des BSI Nothilfe. Das CERT ist die zentrale Anlaufstelle für präventive und reaktive Massnahmen bei sicherheitsrelevanten Vorfällen in Computer-Systemen. Auch die deutsche Bundesbank ist im Bereich Cyber Security aktiv und erarbeitet zusammen mit der BaFin Prüfungsmodule zur IT-Prüfung, die auch im Rahmen der Europäischen Bankenaufsicht (EBA) weiterentwickelt und in den Single Supervisory Mechanism (SSM) eingebracht werden. Die BaFin führt diverse Aktivitäten im Rahmen der Aufsicht im Bereich Cyber-Sicherheit durch und überwacht die Mindestanforderungen an das Risikomanagement (MaRisk).

In Deutschland gibt es zudem Private-Public-Partnerships wie das UP KRITIS. Dies ist die Kooperation zwischen Betreibern kritischer Infrastrukturen (KRITIS) verschiedener Sektoren (inkl. Finanzsektor), deren Verbänden und den zuständigen staatlichen Stellen (BaFin). In sektorspezifischen Arbeitsgruppen werden Standards erarbeitet und es findet ein institutionalisierter Informationsaustausch statt. Neben seiner Mitarbeit in der UP KRITIS, behandelt der Bundesverband Deutscher Banken das Thema IT-Sicherheit in Arbeitsgruppen und Gremien der Mitglieder. Zudem besteht in Deutschland ein Cyber-Sicherheitsrat. Dies ist ein politisch neutraler Verein, der zum Zweck hat Unternehmen, Behörden und politische Entscheidungsträger im Bereich Cyber-Sicherheit zu beraten.

Auf **europäischer Ebene** arbeitet die Europäische Zentralbank (EZB) mit nationalen Banken und nationalen Bankenaufsichten sowie der European Banking Authority (EBA) zusammen, um Cyber-Resilienz bei wichtigen Banken in Europa aufzubauen. Seit November 2016 beaufsichtigt und überprüft sie die IT-Sicherheit bei 120 großen Banken in Europa. Die Schaffung einer zentralen Meldestelle für IT-Störfälle/-Angriffe ist in Planung, um den Austausch zwischen den Ländern zu gewährleisten. Die European Banking Authority (EBA) unterhält verschiedene Initiativen in Kooperationen mit nationalen Banken. Beispielsweise stellt sie mit der Task Force “IT-Risiken” neue Anforderungen an die IT-Organisation der Banken in Europa auf u.a. im Blick Vor-Ort-Prüfungen zur IT-Sicherheit.

Tabelle 3:Verantwortlichkeiten

UK	USA	Singapur	Hong Kong	Deutschland	Australien	Schweiz
Behördenseitig: – Nationales Zentrum für Cyber Security (sektorübergreifend) – Government-Regulator Strategy Group (Finanzsektor) – Untergruppe auf Stufe Sektionsleitung (Finanzsektor) Zusammenarbeit mit Finanzsektor: – Arbeitsgruppe Workstream Cyber Security (strategisch) – Cyber-Koordinationsgruppe (operativ) – Zwei weitere Untergruppen (operativ)	Behördenseitig: – Department for Homeland Security (DHS): sektorübergreifende Verantwortung – National Cybersecurity and Communications Integration Center (NCCIC): Hub für sektorübergreifenden Informationsaustausch – US-CERT (sektorübergreifend) – FBIIC: behördenseitiges Gremium des Finanzsektors – Department of the Treasury: Verantwortung Finanzsektor – FED, OCC und FDIC: Erstellung von Standards – FINRA: Aufsicht Branchenseitig: – FSSCC: Council das eng mit dem FBIIC zusammenarbeitet – FSARC: Center der acht grössten Banken – Ausgewählte Finanzinstitute und das FS-ISAC haben im NCCIC eine Präsenz	Behördenseitig: – Cyber Security Agency (CSA): sektorübergreifende Verantwortung – SingCERT (sektorübergreifend) – Monetary Authority of Singapore (MAS): Aufsicht und Regulierung Branchenseitig: – Standing Committee on Cyber Security der Association of Banks in Singapore (ABS) PPPs: – Public-Private-Partnerships im Bereich Bildung und Forschung	Behördenseitig: – Hong Kong Monetary Authority (HKMA): Aufsicht und Regulierung – HKCERT (sektorübergreifend) Branchenseitig: – Hong Kong Banking Association (HKBA): Koordinations- und Informationsfunktion zwischen den Banken	Behördenseitig: – Bundesamt für Sicherheit in der Informationstechnik (BSI): sektorübergreifende Verantwortung – CERT-Bund (sektorübergreifend) – Deutsche Bundesbank: Erarbeitung von Prüfungsmodulen – Bundesanstalt für Finanzdienstleitungsaufsicht (BaFin): Aufsicht und Regulierung Zusammenarbeit mit Finanzsektor: – UP KRITIS: Kooperation zwischen staatlichen Stellen und Betreibern kritischer Infrastruktur – Verbände Cyber-Sicherheitsrat: Beratung von Behörden und Unternehmen Europäische Ebene: – Europäische Zentralbank (EZB): Aufsicht und Prüfung – European Banking Authority (EBA): Erstellung von Anforderungen	Behördenseitig: – Department of Prime Minister and Cabinet (sektorübergreifend) – CERT (sektorübergreifend) – Australian Securities and Investment Commission (ASIC): Aufsicht und Regulierung Zusammenarbeit mit Privatsektor (inkl. Finanzsektor): – Cyber Security Center (ACSC) (sektorübergreifend) – Joint Cyber Threat Sharing Centers (sektorübergreifend) Branchenseitig: – Informelle Zusammenarbeit der vier grössten Banken	*Behördenseitig:* – *ISB: Steuerungsausschuss STA NCS und Koordinationsstelle KS NCS (sektorübergreifend)* – *MELANI: CERT* – *Expertengruppen: Risiko- und Verwundbarkeitsanalysen und Massnahmenberichte für die Teilsektoren Banken und Versicherungen* – *SNB und FINMA: Aufsicht und Regulierung* *Branchenseitig:* – *Expertengremium der SBVg zu „Information Security & Cyber Defence“* – *Arbeitsgruppe Sicherheit in der Informationstechnologie der Schweizer Banken (ASIT)* – *Arbeitsgruppe der Versicherer zur Förderung der Informations-Sicherheit in der Branche (AVIS)*

3.5 Penetrationstests

- Im UK werden bei den 34 grössten Finanzinstituten sogenannte CBEST-Tests durchgeführt. Der Lead liegt bei den Behörden, die eng mit den Finanzinstituten zusammenarbeiten. Die Tests werden durch externe Anbieter durchgeführt.
- In Singapur werden alle 2-3 Jahre umfassende Echt-Zeit-Stresstests für den Finanzsektor durchgeführt. Zusätzlich müssen die Finanzinstitute mindestens einmal jährlich Penetrationstests durchlaufen.
- Auch in Deutschland und in Hong Kong müssen die Finanzinstitute regelmässig Penetrationstests machen.
- In den USA steht es den Finanzinstituten auf nationaler Ebene offen, sich Penetrationstests durch das DHS zu unterziehen. Im Gliedstaat New York sind Penetrationstests ab 1.3.2017 obligatorisch.
- In Australien können sich Banken freiwillig Cyber Health Checks und Penetrationstests unterziehen.

Im **UK** hat das Financial Policy Committee (FPC) der Bank of England im Juni 2013 den Auftrag erteilt, die Cyber Security der kritischen Finanzinfrastruktur sicherzustellen. Es wurde definiert, welche Finanzinstitute zu dieser sogenannten „core group" gehören (34 Finanzinstitute (inkl. Bank of England und einer der beiden Schweizer Grossbanken).[30] Für diese 34 Institute wird seit Juni 2015 auf freiwilliger Basis ein Penetrationstest (CBEST) durchgeführt. Die Finanzinstitute tragen die Kosten des Tests in der Höhe von rund GBP 150'000-300'000 (ca. CHF 220'000-450'000) selbst. Die Bank of England verfügt über sechs Angestellte im Sector Cyber Team und über rund 35 in der IT-Sicherheitsabteilung. Sie stellt ihre eigenen Leistungen nicht in Rechnung.

Grundlage des Tests ist ein Fragebogen mit 100 Fragen zur Cyber Security. Um diesen auszufüllen, benötige ein Finanzinstitut rund vier Vollzeitstellen während sechs Monaten, während die Bank of England rund fünf Vollzeitstellen während einem Jahr zu dessen Auswertung beschäftige. In Zusammenarbeit mit dem Finanzinstitut werden die kritischen Funktionen des Instituts identifiziert. Externe Anbieter entwickeln in Zusammenarbeit mit NCSC und den Geheimdiensten die für das Institut relevanten Bedrohungsszenarien. Anschliessend wird ebenfalls von einem externen Anbieter der Penetrationstest durchgeführt (ethical hacking). Der Test erfolgt auf den „live"-Systemen und dauert in der Regel rund sechs Wochen. Es geht darum, alle technischen Schwächen im Detail zu erkennen. Die anschliessende Auswertung dauert mehrere Monate. Ziel ist, die Schwächen der Systeme zu erkennen und geeignete Massnahmen zur Erhöhung der Sicherheit zu definieren (Risk Mitigation Plan). Es gibt aber kein Bestehen oder Nichtbestehen des Tests. Die externen Anbieter unterliegen sehr strengen Anforderungen. Sowohl die „Threat Intelligence Providers" wie auch die Penetrationstester müssen in einem ersten Schritt von CREST (unabhängige Vereinigung für ethisches Hacking) und anschliessend von der Bank of England zertifiziert werden. Im März 2017 entscheidet die Bank of England über die Frequenz des CBEST-Tests. Voraussichtlich werden nicht alle Institute derselben Frequenz unterstellt. Ebenfalls werde evaluiert, ob ein CBEST „light" für kleinere Finanzinstitute entwickelt werden könne.[31]

[30] Die grössten Banken, Börsen, Clearing und Settlement-Institute sowie zwei Versicherungen (aufgrund ihres Angebots an Pensionen). Um sich genauer über die von UK durchgeführten Penetrationstests zu informieren, könnten die schweizerischen Behörden mit der schweizerischen Grossbank, die in den UK CBEST durchlaufen hat, Kontakt aufnehmen.

[31] Die niederländische Zentralbank hat für CBEST ein Secondment bei der Bank of England und auch mit Singapur und Hong Kong besteht ein enger Austausch betreffend Cyber-Tests. Die Bank of England und der FCA sind bereit auch mit den schweizerischen Behörden einen vertieften Austausch zu führen.

In **Singapur** werden seit 2006 alle 2-3 Jahre umfassende, über Cyber Security hinausgehende Echtzeit-Stresstests (Industry-Wide Business Continuity Exercise) für den Finanzsektor durchgeführt. Seit 2011 liegt der Fokus dieser Tests auf Cyber Security. Die Tests werden von der MAS zusammen mit der ABS organisiert, die die Tests sponsert. Gemäss der Bank of England steht Singapur bezüglich der Cyber-Tests 2018 in engem Austausch mit der BoE. Zusätzlich müssen die Banken mindestens einmal pro Jahr kleinere Tests (Penetration Testing Exercises) durchführen, die sich an den Industry Penetration Testing Guidelines[32] auszurichten haben. Die Guidelines werden vom ABS Standing Committee erstellt.[33]

In **Deutschland** sind die Banken gemäss dem Rundschreiben „Risikomanagement – MaRisk" der BaFin beauftragt regelmässig Penetrationstests durchzuführen. Zudem muss ein wirksames Patch-Management sicherstellen, dass sicherheitsrelevante Software-Updates und notwendige Konfigurationsänderungen rechtzeitig und sicher vorgenommen werden. Weiter müssen die Banken Sicherheitsmassnahmen in der Software-Entwicklung treffen und die IT-Sicherheit bei der Entscheidung über Auslagerung von Aktivitäten und Beschaffung von IT-Systemen berücksichtigen. Die BaFin überprüft ihrerseits die IT-Systeme und -Prozesse der Finanzinstitute auf Sicherheitslücken.

In **Hong Kong** wurde im Rahmen der Cybersecurity Fortification Initiative ein Cyber Resilience Assessment Framework (C-RAF) definiert. Im Rahmen von Penetrationstests wird in einem ersten Schritt das inhärente Cyber-Sicherheitsrisiko der Finanzinstitute definiert. Wird dieses als „durchschnittlich" oder „hoch" eingestuft, folgt anschliessend ein „intelligence-led cyber attack" Simultationstest (iCAST). Die Tests sind für alle unter der Aufsicht der HKMA stehenden Finanzinstitute obligatorisch und müssen durch eine anerkannte externe Firma durchgeführt werden. Die Testergebnisse werden der HKMA zugestellt. Die Frequenz der Tests ist noch nicht definiert.

In den **USA** bietet das DHS im Rahmen des Risk and Vulnerability Assessments (RVA) Penetrationstests an, die sowohl von den Behörden wie auch vom Privatsektor in Anspruch genommen werden können. Zudem lancierte der Federal Financial Institutions Examination Council (FFIEC)[34] im Juni 2015 ein Cyber Security Assessment Tool (CAT), das den Finanzinstituten dabei helfen soll Risiken zu identifizieren. Die Verwendung dieses Tools ist freiwillig. Das FBIIC stellt den Banken zudem ein Template zur Verfügung anhand dessen diese interne Cyber Security Übungen durchführen können.

In **Australien** wird den 100 grössten kotierten Unternehmen durch die australische Börse (ASX) und Australian Securities and Investment Commission (ASIC) empfohlen, sich auf freiwilliger Basis sogenannten „ASX 100 Cyber Health Checks" zu unterziehen. Diese bestehen aus dem Ausfüllen eines Online-Fragebogens, der sich am Fragebogen der UK orientiert. Die Australian Banking and Financial Services Group (BSFG) hat zudem mit Unterstützung der Regierung Cyber Simulations Tests unternommen.

---

[32] Diese Richtlinien zeigen den Finanzinstituten auf, worauf sie bei Stresstests der IT-Infrastruktur zu achten haben.

[33] Zudem hat die ABS mit dem „ABS Cloud Computing Implementation Guide" Empfehlungen im Zusammenhang mit Outsourcing auf eine Cloud herausgegeben.

[34] FFIEC is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Consumer Financial Protection Bureau (CFPB) and to make recommendations to promote uniformity in the supervision of financial institutions.

Tabelle 4:Penetrationstests

UK	USA	Singapur	Hong Kong	Deutschland	Australien	Schweiz
– Freiwillige CBEST Penetrationstests – Durch die Behörden koordiniert	– Freiwillige Penetrationstests durch das DHS – Freiwillige Verwendung des Cyber Security Assessment Tools (CAT) – Template für interne Cyber Security Übungen	– Industrie-Wide Business Continuity Exercises alle 2-3 Jahre durch die MAS und ABS organisiert (obligatorisch) – Min. 1 pro Jahr Penetration Testing Exercises durch die Banken	– Obligatorische Penetrationstests – Freiwillige Simulationstests gemäss C-RAF (Frequenz noch nicht definiert)	Obligatorische Penetrationstests durch die Banken	– Freiwillige Cyber-Simulations Tests durch die BSFG – Freiwillige Teilnahme an den ASX Cyber Health Checks für die grössten kotierten Unternehmen	*Ab 1.7.2017 Verwundbarkeitsanalysen und Penetrationstests für Banken obligatorisch*

3.6 Informationsaustausch

3.6.1 Meldung an Behörden

In den **UK** wird es jedem einzelnen Finanzinstitut überlassen, ab welchem Schweregrad es einen Cyber-Vorfall der zuständigen Finanzmarktaufsicht meldet. Wird ein Vorfall jedoch nicht gemeldet oder sogar vertuscht, kann die Aufsichtsbehörde das Verfehlen je nach Schweregrad bis hin zu strafrechtliche Massnahmen ahnden. Die NCSC hat sektorübergreifende Richtlinien zur freiwilligen Meldung von Cyber-Vorfällen veröffentlicht. Alle Firmen (inkl. Finanzinstitute) sind jedoch gemäss dem britischen Datenschutzgesetz dazu verpflichtet, Datenverluste im Rahmen von Cyber-Vorfällen ab einem bestimmten Schweregrad dem Information Commissioner's Office (ICO) zu melden. Das ICO hat diesbezüglich Richtlinien (Guidance) erlassen, welche den Schweregrad anhand von Beispielen erläutern.

Auch in **Australien** und den **USA** gibt es auf nationaler Ebene für Finanzinstitute keine Vorschriften, die Behörden über Cyber-Vorfälle zu informieren oder Informationen dazu zu teilen. Im Gliedstaat New York besteht jedoch ab 1.3.2017 eine Meldepflicht an das Department of Financial Services. In Australien gibt es für die freiwillige Meldung von Cyber-Vorfällen jedoch eine sektorübergreifende Meldestelle. Die Meldung, zu der die Behörden ermutigen, ist anonym und die Form der Meldung ist frei, so dass der Detaillierungsgrad variiert. Die **amerikanische** Rechtsgrundlage (CISA) verbietet der Regierung explizit Unternehmen zum Informationsaustausch zu zwingen. Versäumt es ein Unternehmen jedoch angemessen auf einen Cyber-Vorfall zu reagieren, kann dieses unter Umständen aufgrund fahrlässigen Handelns belangt werden. Das DHS ermutigt in seinem Merkblatt Cyber Incident Reporting Opfer von Cyber-Vorfällen der Regierung unter bestimmten Umständen Meldung zu erstatten.

Im Gegensatz zum UK und den USA haben die Finanzinstitute in **Singapur** gemäss dem „Securities and Futures Act (CAP. 289)" das MAS schnellstmöglich (spätestens nach Ablauf einer Stunde) mit einer kurzen Meldung über Cyber-Vorfälle zu unterrichten. In der ersten Meldung muss genannt werden was, wann, wie, wo passierte und was die Auswirkungen davon

sind. Zudem muss genannt werden, was das Unternehmen bereits unternommen hat. Ein ausführlicher Bericht muss innerhalb von 14 Tagen an die MAS geliefert werden.[35] Ähnlich wie in Singapur müssen Banken in **Hong Kong** Cyber-Vorfälle, die den Betrieb oder Bankkunden betreffen, unmittelbar der HKMA melden.[36] Dafür besteht zwar keine gesetzliche Grundlage, es bestehen jedoch entsprechende Richtlinien der HKMA.

In **Deutschland** sind bezüglich Meldepflichten die Vorgaben der BaFin und das IT-Sicherheitsgesetz des Bundes relevant. Aufgrund des IT-Sicherheitsgesetzes sind Unternehmen je nach Schwere des Vorfalles zur Meldung von IT-Vorfällen an das Bundesamt für Sicherheit in der Informationstechnik (BSI) verpflichtet. Das BSI teilt die Informationen zum Vorfall anschließend je nach Bewertung anonym mit anderen Betreibern des betroffenen Sektors kritischer Infrastruktur. Gemäss den Vorgaben der BaFin sind schwerwiegende Zahlungssicherheitsvorfälle sofort an die zuständigen Aufsichts- und Datenschutzbehörden[37] zu melden. Auf **europäischer Ebene** arbeitet die Europäische Zentralbank (EZB) an der Schaffung einer zentralen Meldestelle für IT-Störfälle/-Angriffe.

Tabelle 5: Meldung an Behörden

UK	USA	Singapur	Hong Kong	Deutschland	Australien	Schweiz
– Im Ermessen des Finanzinstituts – Sektorübergreifende Richtlinien der NCSC – Bei Datenverlust Meldung an ICO gemäss Datenschutzgesetz (inkl. Richtlinien)	– Freiwillige Meldung – Merkblatt des DHS	Obligatorisch gemäss „Securities and Futures Act“	Obligatorisch gemäss den Richtlinien der HKMA	– Obligatorische gemäss IT-SiGe und MaRisk-Rundschreiben (je nach Schwere)	Freiwillige Meldung an sektorübergreifende Meldestelle ACORN	– *Freiwillige Meldung an MELANI* – *Obligatorische Meldung an FINMA sofern von wesentlicher Bedeutung* – *Künftig soll bei Datenverlust gemäss DSG eine Meldung ans EDÖB erfolgen*

[35] Im diesem Cyber Incident Report müssen die Eckdaten des Ereignisses (Zeitpunkt des Vorfalls und des Entdeckens, Art des Ereignisses und betroffene Gebiete sowie Auflistung, was zur Behebung unternommen wurde) aufgelistet werden. Weiter muss eine Beurteilung über die Auswirkungen (auf den Betrieb und Stakeholders) sowie über die finanziellen, rechtlichen und regulatorischen Auswirkungen vorgenommen werden. Zudem werden ein detaillierter Beschrieb des Ereignishergangs in chronologischer Reihenfolge und eine detaillierte Ursachenanalyse gefordert. Zuletzt müssen die Massnahmen, die zukünftige Angriffe dieser Art vermeiden sollten, erläutert werden.

[36] Ausmass des Vorfalls, (finanzielle) Auswirkungen für die Bank oder ihre Kunden, eingeleitete Massnahmen, präventive Massnahmen, um die Ursache des Vorfalls zu beheben.

[37] BaFin, Deutsche Bundesbank sowie die zuständige Datenschutzbehörde.

3.6.2 Informationsplattform

- Sowohl UK, Hong Kong als auch die USA verfügen über eine Plattform, die dem Informationsaustausch zu Cyber-Risiken im Finanzsektor dient. Während die Plattformen im UK und in den USA sektorübergreifend sind, ist die Hong Konger Plattform finanzsektorspezifisch.
- Im UK bestehen für den institutionalisierten Informationsaustausch Arbeitsgruppen mit Vertretung der Behörden und des Finanzsektors.
- In Deutschland findet die Kommunikation der Behörden gegenüber dem Finanzsektor über die UP KRITIS statt.
- In Singapur und Hong Kong besteht eine enge Zusammenarbeit zwischen den Aufsichtsbehörden und den Bankiervereinigungen, die dem Informationsfluss dient.
- In den USA findet der Informationsfluss zwischen Behörden und Finanzindustrie über das NCCIC, aber auch über die Zusammenarbeit von FBIIC und FSSCC statt.
- In Australien findet die Kommunikation zwischen Behörden und Privatsektor im Allgemeinen über das Cyber Security Center und die Joint Cyber Treat Sharing Centers statt.

Im **UK** wurde im März 2013 die sektorübergreifende Cyber-Security Information Sharing Partnership (CISP) lanciert. Diese Plattform steht insbesondere den Finanzinstituten zum gegenseitigen Austausch zu Cyber Security-Themen (inkl. Vorfällen) zur Verfügung. Sie wird vom NCSC verwaltet. Die Aufsichtsbehörden haben keinen Zugang zur Plattform, was die Vertraulichkeit fördern soll. Als einzige Zulassungsbedingung gilt eine Empfehlung durch ein bestehendes Mitglied. Innerhalb von CISP gibt es thematische Untergruppen, welchen die Firmen je nach Interesse beitreten können. Bei einem Cyber-Vorfall kann eine Mitgliedsfirma von CISP die NCSC bitten, einen Notfallanruf zu initiieren, um den Fall mit anderen Finanzinstituten zu teilen. Zudem führt CityUK eine Cyber Taskforce, die sektorspezifische Themenberichte erstellt.

Als Teil der Cybersecurity Fortification Initiative (CFI) wurde eine Cyber Intelligence Sharing Platform (CISP) für den **Hong Konger** Finanzsektor entwickelt, der es ermöglicht Informationen über Cyber-Risiken zwischen den Banken auszutauschen und dadurch seine Widerstandsfähigkeit zu stärken. Der Zugang ist den Mitgliedern der Hong Konger Bankiervereinigung (HKAB) vorbehalten. Die CISP wurde von der HKMA und der HKAB in Zusammenarbeit mit dem Finanzsektor und dem staatlich-unterstützten Hong Kong Applied Science and Technology Research Institute entwickelt.

In den **USA** hat das DHS mehrere Information-Sharing-Programme geschaffen, mittels denen es Informationen mit dem Privatsektor[38] teilt. Für den Austausch von Public-Private-Informationen wurde beispielsweise das Cyber Information Sharing and Collaboration Program (CISCP) geschaffen. Um an diesem Programm teilzunehmen, müssen Unternehmen ein Cooperative Research and Development Agreement (CRADA) unterzeichnen. Dieses gewährt dem Unternehmen Zugang zum NCCIC Watch Floor und erlaubt den Unternehmen Zugang zu klassifizierten Bedrohungsinformationen. Da für viele Unternehmen die Errichtung effektiver Organisationen für den Informationsaustausch im Bereich Cyber Security schwierig war, erliess Präsident Obama 2015 ein Executive Order, der das DHS anwies die Entwicklung von sektorübergreifenden Information Sharing and Analysis Organizations (ISAOs) zu fördern. Das National Institute of Standards and Technology (NIST) hat zudem das sogenannte NIST Cybersecurity Framework entwickelt, um den Schutz kritischer Infrastruktur vor Cyber-Attacken zu verbessern. Das Framework wurde in Zusammenarbeit mit dem Privatsektor entwickelt und seine Einhaltung ist freiwillig. Es umfasst Industriestandards und Best Practice-Ansätze und zielt auf eine Erhöhung des Informationsflusses ab.

In **Deutschland, Australien und Singapur** gibt es keine technischen Informationsplattformen. Zum institutionalisierten Informationsaustausch wird in Deutschland die UP KRITIS verwendet.

[38] Eigentümer der Mehrheit der kritischen Infrastruktur.

In Singapur findet der Informationsaustausch zu Cyber Security über das Standing Committee der ABS, aber auch im Rahmen der jährlichen Technology Risk Conference, die von der Association of Banks Singapore (ABS) und der Monetary Authority of Singapore (MAS) organisiert wird, statt. In Australien stehen für den Austausch zwischen Privatsektor und Regierung das Cyber Security Center und die Joint Coordination Centers zur Verfügung.

Tabelle 6: Informationsplattformen

Technische Informationsplattform						
UK	**USA**	**Singapur**	**Hong Kong**	**Deutschland**	**Australien**	**Schweiz**
CISP: – BoE und FCA haben keinen Zugriff auf CISP – Bereitstellung durch die NCSC	CISCP: Betrieben durch das DHS	Keine technische Informationsplattform	CISP: – Zugang nur für Mitglieder der HKAB – Betrieben durch HKMA	Keine technische Informationsplattform	Keine technische Informationsplattform	*MELANI*
Institutionalisierter Informationsaustausch						
UK	**USA**	**Singapur**	**Hong Kong**	**Deutschland**	**Australien**	**Schweiz**
– Workstream Cyber Security – Cyber-Koordinationsgruppe inkl. Untergruppen – CityUK Cyber Taskforce	– Präsenz im NCCIC – Zusammenarbeit von FBIIC und FSSCC – FSARC – FS-ISAC – NIST Cybersecurity Framework (sektorüberfreifend) – ISAO (sektorübergreifend)	– Zusammenarbeit MAS / ABS – ABS Standing Committee – Technology Risk Conference – FS-ISAC	– Zusammenarbeit HKMA / HKAB – Arbeitsgruppe Cyber Security der HKAB	– Information durch BSI – UP KRITIS (sektorübergreifend)	– Cyber Security Center (sektorübergreifend) – Joint Coordination Centers (sektorübergreifend) – Informeller Austausch zwischen den vier grossen Banken	– *Expertengremium der SBVg zu „Information Security & Cyber Defence“* – *Arbeitsgruppe Sicherheit in der Informationstechnologie der Schweizer Banken (ASIT)* – *Arbeitsgruppe der Versicherer zur Förderung der Informations-Sicherheit in der Branche (AVIS)*

3.6.3 Information der Kunden

In **Singapur** gibt es die „Technology Risk Management Guidelines“ der MAS, gemäss denen Finanzinstitute ihre Kunden über alle folgenreichen Störfälle informieren sollten. Auch in **Hong Kong** müssen Banken betroffene Kunden, wenn nötig auch andere betroffene Banken sobald als möglich proaktiv informieren. In **Australien** liegt ein entsprechender Gesetzesentwurf vor,

gemäss welchem Kunden über Cyber-Vorfälle informiert werden müssen. In den **USA** müssen die betroffenen Kunden gemäss den geltenden Datenschutzregeln so schnell wie möglich über Cyber-Vorfälle informiert werden. Auch in **Deutschland** müssen die Banken ihre Kunden basierend auf den rechtlichen Grundlagen zum Datenschutz über Cyber-Vorfälle informieren. Im **UK** besteht hingegen keine rechtliche Grundlage für eine Informationspflicht betroffener Kunden. Bei einem Cyber-Vorfall legt die Finanzmarktaufsicht in Zusammenarbeit mit dem betroffenen Finanzinstitut fest, welche Kommunikation notwendig ist. Dabei werden auch die potenziellen Risiken (Sicherheit, Finanzstabilität) berücksichtigt. Bei börsenkotierten Unternehmen wird zudem mit der Unternehmensleitung diskutiert, welche Informationen mit der Börse geteilt werden müssen. Dabei werden vor allem die Konsequenzen (z.B. Aktienkurs) einer solchen Kommunikation beurteilt und von Fall zu Fall entschieden. Sind Kunden anderer Länder betroffen, ändert sich dieser Ansatz nicht. Allerdings sucht die Finanzmarktaufsicht unter Umständen den Kontakt mit den zuständigen Regulatoren.

Tabelle 7: Information der Kunden

UK	USA	Singapur	Hong Kong	Deutschland	Australien	Schweiz
Fallweise Beurteilung	Obligatorisch gemäss Datenschutzregeln	Bei folgenreichen Störfällen obligatorisch	Bei folgenreichen Störfällen obligatorisch	Obligatorisch gemäss Datenschutzregeln	Gesetzesentwurf	Bei folgenreichen Störfällen obligatorische Meldung an FINMA

3.6.4 Internationaler Austausch

Die **Bank of England** arbeitet eng mit anderen Staaten z.B. Singapur und Hong Kong zusammen und hat ein Secondment für CBEST mit der niederländischen Zentralbank. Zudem besteht eine enge Zusammenarbeit zwischen der britischen und der US-Regierung und global führenden Finanzinstituten, die die “Incident Response” und den Informationsaustausch zwischen den beiden Ländern fördern soll. Auch im Versicherungsbereich gibt es Anstrengungen Cyber Security im Rahmen des EU-US Insurance Project insbesondere hinsichtlich dem bilateralen Informations- und Wissensaustausch als Schlüsselinitiative zu definieren. Viele **US** Finanzinstitute engagieren sich zudem im Financial Services Information Sharing and Analysis Center (FS-ISAC) einer globalen nicht-gewinnorientierten Mitgliederorganisation des Finanzsektors. Deren hauptsächliche Funktion ist der Austausch von Informationen zu physischen und Cyber-Bedrohungen und -Vorfällen. Auch die Finanzindustrie **Singapurs** ist Teil dieser Organisation. In Zusammenarbeit mit dem MAS arbeitet das FS-ISAC derzeit an einer APAC Informationsplattform für die asiatisch-pazifische Region, die zum Ziel hat, die regionale Kooperation und den Datenaustausch im Bereich Cyber-Sicherheit in der Finanzbranche zu fördern. Für Singapur ist die Schaffung von ausreichenden Kapazitäten in allen ASEAN-Mitgliedern prioritär, um Cyber-Sicherheit in der Region bestmöglich gewährleisten zu können. In diesem Rahmen organisiert Singapur diverse Workshops, Seminare und Konferenzen. Zudem fand im Oktober 2016 erstmals die SICW (Singapore International Cyber Week) statt, die von der CSA organsiert wird. Diese wird in Zukunft einmal jährlich die nationale, regionale und globale Cyber-Sicherheitsbranche in Singapur zusammenbringen. In **Hong Kong** tauscht sich die HKMA regelmässig mit ausländischen Partnerorganisationen über Cyber Security aus. Auch **Deutschland** und **Lichtenstein** arbeiten im Bereich Cyber Security im Finanzbereich zusammen und werden dazu einen „Banking Hub“ gründen. Es besteht ebenfalls Interesse an einer DACHL-Kooperation.

3.7 Krisendispositiv

Lediglich im **UK** gibt es ein Krisendispositiv (Authorities Response Framework), das von der Finanzmarktaufsicht (FCA/PRA) rund um die Uhr einberufen werden kann. Normalerweise sind nebst der Finanzmarktaufsicht die Bank of England und das Finanzministerium Teil des Dispositivs. Je nach Bedarf werden das NCSC sowie die Sicherheitsdienste involviert. Die Führung liegt bei der Bank of England und der Finanzmarktaufsicht, ist jedoch vom Einzelfall abhängig (falls viele Kunden involviert sind, würde die FCA die Leitung übernehmen, falls es sich eher um eine Bedrohung der Finanzstabilität handelt, die PRA). Das Sekretariat / die Administration kann vom Finanzministerium geführt werden oder falls der Fall sehr technisch ist vom NCSC. Da für das Krisendispositiv keine separaten Strukturen bestehen, gibt es auch keine eigene Finanzierung für das Cyber Security Krisendispositiv. Die Form des Krisendispositivs ist nicht vordefiniert, sondern hängt vom Fall ab. Es bestehen vordefinierte Protokolle für unterschiedliche Krisenszenarien. Es gibt einen dreistufigen Prozess zur Lancierung des Krisendispositivs: (1) Beobachten / Bereitschaft auf working level, (2) Behörden verlangen eine Folgenabschätzung durch das Finanzinstitut, (3) formelle Einberufung des Krisendispositivs auf hoher Hierarchiestufe.