ASA | SVV

Schweizerischer Versicherungsverband
Association Suisse d'Assurances
Associazione Svizzera d'Assicurazioni
Swiss Insurance Association

Grundlagenpapier

Fachstelle Ausschuss Rückversicherung
Gremium Arbeitsgruppe Cyber-Risk
Datum 22. Februar 2018
Thema **Grundlagenpapier des SVV zu Cyber-Risiken**

Zusammenfassung

Die jährlichen Kosten für Cyber-Risiken allein in der Schweiz belaufen sich schätzungsweise auf bis zu 9,5 Milliarden Schweizer Franken, Tendenz steigend. Im Kontext der Überarbeitung der Nationalen Cyber-Strategie der Schweiz beschreibt das vorliegende Grundlagenpapier die Rolle der Versicherungen zur Stärkung des Cyber-Risikomanagements. Ausserdem weist es auf die Voraussetzungen für die Versicherbarkeit von Cyber-Risiken hin und diskutiert die Rolle des Staates und der Politik für den Aufbau eines nachhaltigen Versicherungsmarktes für Cyber-Risiken.

Versicherer unterstützen Unternehmen im Risikomanagement und nehmen dabei eine Reihe volkswirtschaftlich wichtiger Aufgaben wahr. Cyber-Risiken weisen jedoch einige Herausforderungen für Versicherer auf:

– Akkumulation
– Mangel an Daten
– Informations-Asymmetrie
– Versicherungsobligatorien

Durch die zunehmende Interkonnektivität der Wirtschaft sowie durch Monokulturen von Hard- und Software kann ein Cyber-Vorfall viele Unternehmen gleichzeitig betreffen und einen beträchtlichen gesamtwirtschaftlichen Schaden anrichten. Fünf Akkumulationsszenarien wurden untersucht und ihr Schadenpotential für die Wirtschaft und die Versicherungswirtschaft abgeschätzt. Diese Schadenpotentiale liegen im Extremfall für das Szenario «Stromnetz» bei ca. 12 Milliarden CHF (ca. 2 Prozent des Schweizer Bruttoinlandproduktes BIP) und für die anderen Szenarien bei bis zu 2,5 Milliarden CHF bis 0,4 Prozent des BIPs).

Aufgrund der noch recht kleinen Marktdurchdringung für spezifische Cyber-Versicherungen und der im Markt bereit gestellten Kapazitäten durch Versicherer und Rückversicherer können derzeit auch

Schweizerischer Versicherungsverband SVV
Conrad-Ferdinand-Meyer-Strasse 14 – Postfach – CH-8022 Zürich – Zentrale +41 44 208 28 28 – Fax +41 44 208 28 00 – svv.ch
Gunthard Niederbäumer – gunthard.niederbaeumer@svv.ch – Direkt +41 44 208 28 57

Cyber-Grossschäden durch die Versicherungsindustrie getragen werden. Steigt die Marktdurchdringung allerdings weiterhin stark an, muss die Tragfähigkeit der Schäden durch die Versicherungsindustrie noch genauer untersucht werden.

Im Fall von Cyber-Angriffen auf kritische Infrastrukturen und daraus entstehenden Schäden an Sachwerten und möglicherweise auch Personen bietet die Versicherungsindustrie für Extremfälle keine vollumfänglichen Deckungen an, da solch gravierende Ereignisse schnell die Kapazitäten der Versicherungswirtschaft übertreffen können. Mögliche Lösungen, wie im Fall von Terrordeckungen oder Elementarschadenpools mit staatlicher Deckelfinanzierung, sind näher zu prüfen.

Der Mangel an Daten erschwert es der Versicherungsindustrie, adäquate Produkte zu risikobasierten Preisen anzubieten. Abhilfe schaffen könnte eine allgemeine Benachrichtigungspflicht für Cyber-Vorfälle, vor allem wenn diese nicht nur Datenschutzverletzungen umfassen, sondern auch andere Cyber-Vorfälle mit einbezieht. Allerdings zeigt die Erfahrung, dass eine freiwillige Meldung solcher Vorfälle unter Umständen einer staatlich auferlegten Pflicht vorzuziehen ist, weil die Meldestelle so im Allgemeinen bessere Daten erhält. Auf der anderen Seite sind die erhaltenen Daten dann nicht repräsentativ für die Gesamtwirtschaft. Es muss diskutiert werden, ob im Falle von Cyber-Vorfällen eine freiwillige Meldung oder eine Meldepflicht zu den gewünschten Ergebnissen der besseren Datengrundlage führt.

Auch der Datenaustauch spielt dabei eine wichtige Rolle. Für den Datenaustauch wird ein wettbewerbsrechtlicher Rahmen benötigt. Darüber hinaus kann sich die Versicherungsindustrie zusammen mit anderen Marktteilnehmern selbst organisieren.

Informations-Asymmetrien zwischen dem Versicherungsnehmer und der Versicherung können dazu führen, dass der Versicherungsnehmer die Versicherung über deren Zweck hinaus ausnutzt ('moral hazard'), oder die Antiselektion fördern. Beides sind Faktoren, die die Versicherbarkeit von Risiken stark einschränken. Einer möglichen Informations-Asymmetrie im Cyber-Bereich kann man mit Mindeststandards für Cyber-Security begegnen.

Solche Mindeststandards sollten prinzipienbasiert sein und dürfen die Unternehmen, welche sie implementieren sollten, nicht über alle Massen belasten und überfordern.

Dabei ist genau abzuwägen, wie solche Mindeststandards eingeführt und umgesetzt werden sollten:

– Gesetzliche vorgeschriebene Mindeststandards
– Eine gesetzliche Vorgabe für die Ausarbeitung von branchenspezifischen Mindeststandards
– Nicht gesetzlich vorgeschriebene branchenspezifische Mindeststandards, welche beispielsweise obligatorisch sind, um Versicherungsschutz zu erlangen oder an gewissen Lieferketten teilzunehmen

Ein wichtiger Bereich, der über die Einführung von Mindeststandards hinausgeht, ist das Bewusstsein von Unternehmen um ihre Cyber-Risiken. Dieses Bewusstsein kann z.B. durch Kampagnen und die Arbeit in «Public-Private-Partnerships» auch mit Einbezug der Versicherungsindustrie gefördert werden.

Versicherungsobligatorien gibt es insbesondere in Bereichen, wo eine Tätigkeit oder Anlage zu Schäden bei Dritten führen kann (z.B. für Berufsgruppen wie Ärzte, Fahrzeughalter, Atomkraftwerke, Stauanlagen). Andere Obligatorien – v.a. zur Absicherung gegen Naturgefahren – betreffen Eigenschäden der Versicherten. Das Obligatorium zwingt Marktteilnehmer ihr finanzielles Risiko (als potentielle Geschädigte oder Haftpflichtige) auf einen Dritten (den Versicherer) zu übertragen und setzt die vollumfängliche Versicherbarkeit des Risikos voraus. Da dies bei Cyber derzeit nur zum Teil gegeben ist und unter Umständen Anreize für Unternehmen resultieren könnten, Investitionen in Cyber-Security zu verringern, weil sie ja versichert sind, steht eine solche Massnahme dem Wunsch nach allgemein erhöhter Cyber-Sicherheit entgegen.

Aus Sicht des Schweizerischen Versicherungsverbandes sollte der Bund – gegebenenfalls gemeinsam mit der Wirtschaft – die folgenden acht Massnahmen umsetzen.

1 Das Bewusstsein bei den kleinen und mittleren Unternehmen (KMU) für die Gefahren durch Cyber-Risiken muss deutlich erhöht werden. Entsprechende Kampagnen sind zu führen oder zu unterstützen. Generell muss die Öffentlichkeit für Cyber-Risiken sensibilisiert werden (Awareness). Dazu ist u.a. die Erstellung und Umsetzung eines Kommunikationskonzeptes notwendig.
2 Der Kompetenz- und Wissensaufbau ist zu fördern. Dazu gehört auch der Ausbau der Fähigkeiten zur Beurteilung und Darstellung der Cyber-Bedrohungslage.
3 Das Resilienz-Management auf Unternehmensebene ist einzuführen bzw. auszubauen, insbesondere um das volkswirtschaftliche Akkumulationsrisiko zu vermindern und damit die Versicherbarkeit von Cyber-Risiken auch künftig zu ermöglichen.
4 Die Evaluierung und Einführung eines Minimalstandards ist zwingend und stösst grundsätzlich auf Zustimmung. Die Evaluierung eines (Bundesstandards) und/ oder mehrerer Standards (Branchenstandards) und die entsprechende Einführung ist deshalb voranzutreiben.
5 Eine Meldepflicht für Cyber-Vorfälle stösst eher auf Zustimmung als auf Ablehnung. Die Prüfung einer konkreten Meldepflicht sowie der Entscheid über die Einführung sind deshalb durch die zuständigen Bundesstellen an die Hand zu nehmen.
6 Der Aufbau von Dienstleistungen für alle Arten von Unternehmungen durch den Bund (z.B. Beratungen, Auskunftserteilung etc.) ist zu realisieren.
7 Die Strafverfolgung beim Vorliegen von Cyber-Kriminalität ist national und international konsequent anzuwenden und voranzutreiben, um so die Zahl der künftigen Schadenfälle zu reduzieren.
8 Eine nationale und internationale Kooperation (z.B. gemeinsame Schadenstatistik, Krisenmanagement, Bedrohungslage, etc.) ist zwingend, das gilt auch für den Versicherungsbereich.

Zusätzlich zu den oben genannten Massnahmen, bei welchen der Staat eine führende Rolle übernehmen muss, soll die Versicherungsindustrie folgende Initiativen prüfen:

9 Neben den Cyber-Bedrohungen für Industrie und Gewerbe, soll auch die Cyber-Bedrohung für Gemeindeinstitutionen analysiert werden, um möglichst gut Unterstützung für das Management der Cyber-Risiken auch auf dieser Ebene leisten zu können.

10 Die Entwicklung von Musterbedingungen für Cyber-Versicherungen ist zu prüfen und mit benachbarten Ländern zu koordinieren.

11 Die Versicherungsindustrie soll den Aufbau des Wissens im Bereich Cyber-Beratung und Schadenerledigung vorantreiben.

ASA | SVV

Inhaltsverzeichnis

1 Einleitung

Das derzeitige Bedrohungspotenzial von Cyber-Risiken ist hoch. Die durchschnittlichen jährlichen Kosten für Cyber-Risiken werden weltweit auf 445 Milliarden US-Dollar geschätzt (McAfee, 2014)[1]. Dies entspricht mindestens den Kosten für Naturkatastrophen weltweit, die 2015 bei rund 100 Milliarden US-Dollar lagen und im langjährigen Durchschnitt bei etwa 200 Milliarden US-Dollar liegen (Swiss Re, 2016). Für den Fall, dass sich das Basler Erdbeben von 1356 heute wiederholen sollte, rechnen Experten mit bis zu 2'000 Toten und Schäden bis zu 80 Milliarden Franken. Allein bei den Gebäuden entstünden laut einer Studie der Rückversicherungsgesellschaft Swiss Re Kosten von 13 bis 47 Milliarden Franken. Die jährlichen Kosten für Cyber-Risiken allein in der Schweiz belaufen sich schätzungsweise auf bis zu 9,5 Milliarden Schweizer Franken (diese Schätzung wurde von der bereits angeführten McAfee-Studie hergeleitet). Aufgrund der zunehmenden Digitalisierung einer alles in allem immer noch wachsenden Wirtschaft muss in Zukunft mit noch höheren Kosten gerechnet werden. Deshalb ist es notwendig, dass sich die Schweizer Gesellschaft, Wirtschaft, und Politik entsprechend vorbereitet. Dazu sind entsprechende Massnahmen in gesetzlich-politischer, organisatorischer, technischer und versicherungstechnischer Hinsicht wichtig und dringend.

Die Versicherungswirtschaft kann einen bedeutenden Beitrag zum Aufbau der Cyber-Resilienz in der Schweiz leisten. Das vorliegende Grundlagenpapier beschreibt die Voraussetzungen für die Versicherbarkeit von Cyber-Risiken und zeigt deren Grenzen auf. Ausserdem diskutiert es die Rolle des Staates und der Politik für den Aufbau eines nachhaltigen Versicherungsmarktes für Cyber-Risiken.

Dieses Grundlagenpapier deckt damit nur einen beschränkten Teil des Themenfelds ab. Nicht Gegenstand sind zum einen Angaben über die Ausgestaltung von Cyber-Versicherungsprodukte, zum anderen Aussagen zu konkreten Risikofeldern, wie das autonome Fahren in der Automobilindustrie oder Smartmeters in der Energieversorgung. Es wurde auch bewusst der Fokus auf die Risiken in den Bereichen Gewerbe und der Industrie gesetzt. Selbstverständlich gibt es weitere Bereiche die untersucht werden müssen, wie die kritische Infrastruktur, Armee oder der Bereich der Privatpersonen, resp. Smart Home. Diese Themen werden zum Teil durch den Bund bearbeitet oder müssen in künftigen Arbeiten vertieft werden.

[1] Die Schätzung der McAfee (2014) Studie ist die umfangreichste dieser Art und enthält sämtliche direkten und indirekten Kosten, inklusive dem Verlust von geistigem Eigentum, dem Diebstahl von Kapitalanlagen und sensitiven Geschäftsgeheimnissen, Opportunitätskosten, zusätzliche Kosten für Netzwerksicherheit sowie die Wiederherstellungskosten des Betriebs und Reputationsschäden. Eine aktuelle Überblicksstudie von ENISA (2016) kritisiert jedoch das Fehlen eines standardisierten Vorgehens und macht auf potentiell Überhöhte "echte" wirtschaftliche Schäden in Studien wie der von McAfee aufmerksam.

2 Begriffsdefinition

In der Literatur findet sich häufig folgende Definition von Cyber-Risiken (Cebula und Young, 2010): Cyber-Risiken sind jegliche Risiken, die durch den Gebrauch von Informations- und Kommunikationstechnologie entstehen und die Vertraulichkeit, die Verfügbarkeit und/oder die Unversehrtheit von Daten beeinträchtigen. Ergänzend dazu gehören auch die Folgen der Beeinträchtigung von Vertraulichkeit, Verfügbarkeit und Unversehrtheit von IT-Systemen zum Cyber-Risiko[2]. Cyber-Risiken sind das Produkt der Eintrittswahrscheinlichkeit eines Cyber-Vorfalls und des potentiellen Schadensausmasses im Ereignisfall. Entsprechend basiert die Einschätzung der Bedrohungslage durch Cyber-Risiken in der Schweiz auf der aktuellen und künftigen Eintrittswahrscheinlichkeit verschiedener Vorfälle und deren möglichen Schäden. Dabei muss zwischen Cyber-Vorfällen unterschieden werden, die durch beabsichtigte, unerlaubte Handlungen (Angriffe) herbeigeführt wurden, und solchen, die durch unbeabsichtigte Ereignisse ausgelöst wurden (Fehlmanipulationen, Fehlfunktionen).

Mit zunehmendem Einsatz von Informations- und Kommunikationstechnologie in allen geschäftlichen und sozialen Prozessen hat sich die Bedrohung durch Cyber-Angriffe in den letzten Jahren intensiviert. Angriffe im In- und Ausland mit teilweise gravierenden Konsequenzen haben gezeigt, dass nicht nur die Häufigkeit und Komplexität der Cyber-Angriffe steigen, sondern dass diese auch vermehrt zielgerichtet gegen Staaten oder Unternehmen eingesetzt werden.

Verschiedene Formen von Cyber-Angriffen und Cyber-Ereignissen werden nachfolgend beschrieben. Sie sind hier nach der Motivation der Täter gegliedert und basieren auf der provisorischen Auflistung der NCS 2.0 (Nationale Cyber Strategie).

2.1 Cyber-Spionage

Cyber-Spionage ist eine Tätigkeit, die es erlaubt, im Cyber-Raum an geschützte Informationen zu gelangen, um diese dann für kriminelle, politische, militärische oder wirtschaftliche Zwecke einzusetzen. Sie wird sowohl von staatlichen als auch nichtstaatlichen Akteuren ausgeübt. Im Fokus der Angreifer stehen sowohl Unternehmen wie auch staatliche, zivilgesellschaftliche oder internationale Institutionen. Die Schweizer Wirtschaft ist eine der innovativsten der Welt und viele internationale Konzerne haben hier ihren Hauptsitz. Zudem beherbergt die Schweiz viele wichtige internationale Organisationen und ist häufig Gastgeber von internationalen Verhandlungen. Dies macht die Schweiz zu einem attraktiven Ziel für Cyber-Spionage. Je nach Art und Umfang der gestohlenen Daten, können die Auswirkungen ein unterschiedliches Ausmass annehmen. Die Auswirkungen sind meist nicht unmittelbar bemerkbar, da politische und wirtschaftliche Nachteile erst dann entstehen, wenn die Angreifer ihr erlangtes Wissen einsetzen.

[2] Hier muss darauf hingewiesen werden, dass heutzutage nicht alle hier erwähnten Cyber-Risiken versicherbar sind

Cyber-Spionage wird weiter an Attraktivität gewinnen, da sie ein sehr effizienter Weg ist, Informationen zu beschaffen. Die Angreifer haben Methoden entwickelt, sich unauffällig zu verhalten, nachdem sie in Netzwerke eingedrungen sind und bleiben so oft lange Zeit unentdeckt.

2.2 Cyber-Sabotage / Cyber-Terror

Cyber-Sabotage bezeichnet jene Tätigkeit, die im Cyber-Raum Informations-, Steuerungs- und Kommunikationsinfrastrukturen stört oder zerstört, um deren Funktionsfähigkeit zu beeinträchtigen. Das kann je nach Art der Sabotage auch zu Personen und Sachschäden führen. Der Übergang zu Cyber-Terror ist fliessend. Währendem bei Cyber-Sabotage das Ziel ist, möglichst grosse Schäden zu erzielen, geht es bei Cyber-Terror besonders um politische Erpressung, um Machtdemonstration und Einschüchterung der Bevölkerung, verbunden mit der Absicht, die Gesellschaft zu destabilisieren. Während auf internationaler Ebene verschiedene Sabotageakte bekannt sind, kennen wir in der Schweiz bisher keine solche Fälle. Sollte die Schweiz oder Organisationen aus der Schweiz aber aus politischen Gründen in den Fokus von staatlichen oder nichtstaatlichen Akteuren mit den entsprechenden Fähigkeiten geraten, würde die Eintrittswahrscheinlichkeit eines solchen Ereignisses stark steigen. Die potentiellen Schäden einer Cyber-Sabotage könnten sehr gross sein.

Die Relevanz dieser Bedrohung wird mit der fortschreitenden Digitalisierung der Wirtschaft weiter steigen. Die zunehmende digitale Vernetzung von physischen Geräten über das Internet der Dinge lässt auch neue Formen der digitalen Manipulation zu – mit wiederum direkten Auswirkungen auf die physische Umwelt.

Als Cyber-Sabotage gelten auch bestimmte Aktionen von ehemaligen oder gegenwärtigen unzufriedenen Mitarbeitern, die sich an ihrem Unternehmen «rächen» wollen. Je nach Umgang dieser Aktionen kann eine solche Handlung auch unter Cyber-Kriminalität fallen, siehe Kap. 2.7.

2.3 Desinformation und Propaganda

Die Bedrohung, die von gezielter Verbreitung von Falschinformationen ausgeht, oder durch Verbreitung von Informationen, welche illegal durch Cyber-Spionage beschafft wurden, hat stark an Bedeutung zugenommen. Das Ziel dieser Aktionen ist es, bestimmte Personen, Organisationen oder Staaten zu schwächen oder zu diskreditieren. In verschiedenen Ländern wurden vor wichtigen Wahlen solche Aktivitäten beobachtet. Es ist gut möglich, dass staatliche oder nichtstaatliche Akteure auch in der Schweiz versuchen, das Vertrauen der Bürgerinnen und Bürger in den Staat zu unterminieren.

Da die Bedeutung von Sozialen Medien als Informationsquelle weiterhin zunimmt, muss damit gerechnet werden, dass auch diese Kanäle für Propaganda genutzt werden.

2.4 Cyber in Konflikten

Während ein ausschliesslich im Cyber-Raum geführter Krieg (Cyber-War) als unrealistisches Szenario betrachtet wird, hat sich gezeigt, dass Cyber-Angriffe als Mittel der Kriegsführung auch heute schon in verschiedenen Konflikten eingesetzt werden. Typischerweise handelt es sich dabei um hybride Konflikte, in welchen neben militärischen auch politische, wirtschaftliche und kriminelle Mittel verwendet werden. Der Zweck hybrider Konfliktführung ist es, die Verantwortlichkeiten unscharf zu machen. Cyber-Angriffe sind dafür ein geeignetes Instrument, da sie nur schwer eindeutig zugeordnet werden können und es erlauben, politisch-militärische Wirkung in der Grauzone unterhalb der Kriegsschwelle zu erzielen.

Die beträchtlichen Investitionen vieler Staaten zum Schutz und zur aktiven Abwehr von Cyber-Bedrohungen unterstreichen die Bedeutung von Cyber-Mitteln in der Sicherheitspolitik. Entsprechend ist zu erwarten, dass die Bedeutung von Cyber-Angriffen in Konflikten weiter zunehmen wird.

2.5 Hacktivismus

Verschiedene Interessengruppen können die Absicht haben, durch Cyber Attacken entweder auf sich aufmerksam zu machen oder sich an einer Firma oder an einer exponierten Person zu rächen, oft ohne, dass die Mitglieder dieser Interessengruppe selbst einen Nachteil oder Schaden erlitten haben. Man kann sich solche Aktionen unter anderem im politischen Umfeld, im sozialen/gesellschaftspolitischen Bereich oder auch in ideologischen Kreisen vorstellen.

2.6 Schadenfreude, Gruppendruck und «because I can»

Diese Art von Motivationen gehört üblicherweise zu den sogenannten Skript Kiddies. Wikipedia (2017) definiert Skript Kiddies folgendermassen:

«Der Begriff beschreibt vornehmlich jugendliche Computernutzer, die trotz mangelnder Grundlagenkenntnisse versuchen, in fremde Computersysteme einzudringen oder sonstigen Schaden anzurichten. Erfolgreiche Versuche sind dabei der Anwendung gebrauchsfertiger Lösungen geschuldet, also der Nutzung vorgefertigter Automatismen oder schriftlicher Anleitungen. Die Bezeichnung «Skript Kiddie» hat Anklänge von unreifem Verhalten und Vandalismus und wird oft abwertend verwendet».

In den letzten Jahren ist die Zahl von solchen Cyber-Attacken stabil geblieben, ihr relativer Anteil an der Gesamtheit der Cyber-Attacken hat eher abgenommen, dies besonders, weil die Anzahl bösartiger oder krimineller Aktionen im gleichen Zeitraum zugenommen hat.

2.7 Cyber-Kriminalität

Cyber-Kriminalität beschreibt die Gesamtheit aller strafbaren Handlungen und Unterlassungen im Cyber-Raum, die nicht schon oben erwähnt worden sind. Zweck der Cyber-Kriminalität ist oft die Bereicherung der Täter (Cyber-Fraud, Cyber-Betrug, Cyber-Erpressung, böswillige Datenschutzverletzungen), aber auch Mobbing und

illegaler Austausch oder Konsum auf dem Internet (e.g. Cyber-Pornographie) gehören dazu. Besonders Cyber-Betrug hat in den letzten Jahren stark zugenommen. Der Cyber-Raum eignet sich dafür gut, da das Risiko für die Täter gering ist und durch die grosse Zahl von leicht erreichbaren Opfern hohe Gewinne möglich sind.
Sie betrifft Unternehmen, Behörden und Bevölkerung gleichermassen und ist die Bedrohung mit der höchsten Eintrittswahrscheinlichkeit. Da es nicht das eigentliche Ziel der Angreifenden ist, das Funktionieren der Gesellschaft, Wirtschaft oder des Staates zu gefährden, beschränken sich die Auswirkungen oft auf die betroffenen Opfer. Cyber-Betrüger nehmen jedoch hohe Kollateralschäden in Kauf oder nutzen das Wissen über solche Auswirkungen sogar, um von den Opfern höhere Summen zu erpressen. Aus diesem Grund können Angriffe durch Cyber-Kriminelle zu einer nationalen Bedrohung eskalieren.

Im Umfeld der Cyber-Kriminalität entstehen Geschäftsfelder, in denen viel Geld verdient werden kann. Aufgrund der grossen Konkurrenz, aber auch getrieben durch schutzerhöhende Massnahmen ist der Innovationsdruck unter den kriminellen Akteuren hoch, weshalb die Angreifer laufend neue Geschäftsmodelle entwickeln. Entsprechend muss man mit zunehmender Frequenz und Spezialisierung der kriminellen Aktivitäten im Cyber-Raum rechnen.

Bestimmte kriminelle Cyber-Aktionen ehemaliger oder gegenwärtiger, aber unzufriedener Mitarbeiter, die sich an ihrem Unternehmen "rächen" wollen, können unter Cyber-Kriminalität statt unter Cyber-Sabotage fallen.

2.8 Fehlmanipulationen / Fehlfunktionen

Menschliche Fehler stehen bei vielen Cyber-Risiken am Ursprung. Auch Cyber-Angreifer nutzen Fehlverhalten ihrer Opfer oder Sicherheitslücken in der durch die Hersteller programmierten Software für ihre Attacken. Das Risiko der Fehlmanipulation bezieht sich aber im engeren Sinn auf unabsichtliche Fehler bei der Bereitstellung und Nutzung von Informations- und Kommunikationstechnologie. Solche Fehlmanipulationen passieren sehr häufig und gehören zum Alltag der IT-Abteilungen in Unternehmen und Behörden. Entsprechend sind die Auswirkungen dieser Fehler meist gut beherrschbar. Dennoch haben die Erfahrungen gezeigt, dass hinter vielen grossen Cyber-Vorfällen nicht Angriffe, sondern simple Fehlmanipulationen, verbunden mit einer unzureichenden Vorbereitung auf Fehlerereignisse, stehen.

Cyber-Risiken auf Grund von Fehlmanipulationen, Fehlprogrammierungen oder Fehlkonfigurationen werden weiterhin sehr wichtig bleiben. Die zunehmende Komplexität durch die Vernetzung verschiedenster Bereiche macht es zunehmend schwierig, die Auswirkungen von Fehlern abzuschätzen und einzugrenzen.

Auch Fehlfunktionen von Informations- und Kommunikationstechnik (IKT)-Systemen gehören in dieses Kapitel, unabhängig davon. ob sie durch die oben erwähnten Fehlkonfigurationen, manipulation oder -programmierungen entstehen oder aus externen unerwarteten Ereignissen, wie zum Beispiel aus Überhitzen von Computern oder anderen Hardwarefehlfunktionen resultieren.

3 Cyber Risiko Landschaft der Schweiz

3.1 Risikoverständnis

Trotz der beträchtlichen Bedrohung ist das Gefahrenbewusstsein in der Schweiz bezüglich Cyber-Risiken noch ungenügend. Eine repräsentative Umfrage des gfs-zürich im Herbst 2017 zeigt, dass nur jedes zehnte Unternehmen das Risiko durch einen Cyber-Angriff einen Tag ausser Kraft gesetzt zu werden als gross oder sehr gross einschätzt. In den strategischen Führungsgrundlagen der Unternehmungen wird dem Problem meist nur unzureichend Rechnung getragen. Die entsprechenden Richtlinien sind unklar. Die Verantwortlichkeit für Cyber-Risiken liegt sehr oft auf unterer Führungsebene und nicht, wie notwendig, bei der obersten Geschäftsleitung (CEO, CRO, CFO). Oft fehlen auch finanzielle und personelle Ressourcen für die IT- und Informationssicherheit und den Aufbau der Cyber-Resilienz.

3.2 Nationale Cyber-Strategie

Die Schweiz hat eine Nationale Cyber-Strategie (NCS), welche 2012 beschlossen wurde und bis Ende 2017 umgesetzt wird. Zurzeit ist diese Strategie in Überarbeitung und eine neue Fassung wird bis Frühling 2018 erwartet.

Die erreichten Ziele aus der ersten NCS und der strategische Kontext bilden die Grundlage für die Weiterentwicklung der NCS. Der Vergleich zwischen der aktuellen Bedrohungslage und ihrer erwarteten Entwicklung mit dem bestehenden Dispositiv zum Schutz der Schweiz vor Cyber-Risiken zeigt aber deutlich auf, dass eine Beibehaltung des Status quo nicht genügt, um ein ausreichendes Schutzniveau zu gewährleisten. Es besteht Handlungsbedarf auf verschiedenen Ebenen. Einerseits geht es darum, die vorhandenen Kapazitäten und Fähigkeiten weiter auszubauen und die geschaffenen Prozesse, Strukturen und Grundlagen für die Umsetzung der geplanten Massnahmen zu nutzen. Andererseits müssen aber auch strategische Anpassungen vorgenommen werden. Die NCS soll verstärkt als nationale Strategie über die Bundesverwaltung und die kritischen Infrastrukturen hinaus wirksam sein, um so der Tatsache gerecht zu werden, dass Cyber-Bedrohungen alle Bereiche der Wirtschaft, Gesellschaft und Politik betreffen. Dazu muss die Zielgruppe der NCS entsprechend erweitert werden. Schliesslich soll auch die dezentrale Organisationsstruktur mit einer stärkeren strategischen Führung ergänzt werden, damit angesichts der hohen Dynamik der Cyber-Risiken jederzeit auf neue Entwicklungen reagiert werden kann und damit die NCS in der Öffentlichkeit und der Politik klarer wahrgenommen wird.

4 Die Rolle der Versicherungsbranche

Geht es nun darum, die Anreize zur Investition in Cyber-Resilienz zu verbessern, um einen effizienteren Ressourceneinsatz zu erreichen, erscheint der Marktmechanismus des Risikotransfers (z.B. über Versicherung) grundsätzlich geeignet. Versicherer unterstützen Unternehmen im Risikomanagement und nehmen dabei eine Reihe volkswirtschaftlich wichtiger Aufgaben wahr. Im Rahmen der Prämienermittlung wird jedem Risiko ein

entsprechender Preis zugeordnet. So setzen Versicherer Anreize für risikoadäquates Verhalten. Sie unterstützen Unternehmen vor Abschluss und während der Laufzeit einer Police, insbesondere durch die Bewertung der Risiken. Hier stellen Versicherer ihre Expertise zur Verfügung und unterstützen die Unternehmen auch darin, das Verständnis für die entsprechenden Risiken zu schärfen und Massnahmen zur Prävention zu entwickeln. Im Falle eines Schadens finanzieren sie die Kosten des Schadens und unterstützen Unternehmen im Krisenmanagement zur Wiederherstellung der Betriebsfähigkeit.

Viele gängige Versicherungsprodukte, insbesondere solche, die nicht nur Personen- und Sachschäden, sondern rein finanzielle Schäden versichern, bieten schon seit langem in einem gewissen Umfang Versicherungsschutz für einige Schadenszenarien, die heute unter dem Begriff «Cyber» zusammengefasst werden. So werden beispielsweise durch konventionelle Berufshaftpflichtversicherungen für Rechtsanwälte oder Wirtschaftsprüfer auch solche Haftpflichtansprüche gedeckt, die ursächlich auf Informationssicherheitsverletzungen zurückzuführen sind.

Trotz der erwiesenen Bereitschaft der Versicherungswirtschaft, geeignete Lösungen zum Umgang mit Cyber-Risiken beizutragen, ist der Markt für Cyber-Versicherungen noch im Aufbau und einige der Teilrisiken sind schwer versicherbar.

Es müssen Lösungen gefunden werden, um die hohen Wachstumserwartungen an den Cyber-Versicherungsmarkt zu rechtfertigen und zu ermöglichen.

4.1 Versicherbarkeit von Cyber-Risiken

Sowohl die Schäden, die aus Cyber-Risiken resultieren, als auch der Wert von Cyber-Risikomanagement-Massnahmen sind für Unternehmen schwer zu bewerten. Dies liegt an der Komplexität des Risikos selbst, jedoch auch an der Unsicherheit bezüglich der Effektivität der Risikomanagement-Massnahmen. Cyber-Security Investitionen mit konkreten Kosten stehen folglich unklaren Resultaten gegenüber. Dies führt zu Anreizen für Unternehmen, nicht ausreichend in Cyber-Security zu investieren. Tatsächlich zeigt die Forschung auf der Grundlage von Experimenten ein tendenziell zu geringes Investitionsniveau, welches über die Zeit weiter sinkt (Laury und Holt, 2008). Dies ist insofern kritisch, da bereits ein Grossteil sämtlicher Cyber-Vorfälle vermieden werden könnte, wenn einfache IT-Hygiene Massnahmen beachtet würden.

Der Gruppe der Cyber-Risiken wird auch die Eigenschaft des Akkumulations-Risikos zugeschrieben. Ein Ereignis kann gleichzeitig bei vielen Marktteilnehmern Vorfälle auslösen. Die erhöhte Verletzlichkeit einzelner Marktteilnehmer ist daher für das ganze System relevant, bzw. hat einen negativen externen Effekt. Eine systematische Unterinvestition in das Management von Cyber-Risiken kann so zu einem äusserst grossen Risiko für die Schweizer Volkswirtschaft werden.

In einer ersten Bestandsaufnahme deutet vieles darauf hin, dass das Fehlen geeigneter staatlicher Rahmenbedingungen nicht zu einem optimalen Einsatz der Ressourcen – hier zu einer Unterinvestition in Cyber-Security – führen kann.

Tabelle: Kriterien der Versicherbarkeit nach Berliner (1982)

VERSICHERBARKEITSKRITERIEN	ANFORDERUNGEN
TEIL A: VERSICHERUNGSMATHEMATISCH	
ZUFÄLLIGKEIT DES SCHADENEREIGNISSES	UNABHÄNGIGKEIT UND SCHÄTZBARKEIT DES VERLUSTRISIKOS
MAXIMAL MÖGLICHER SCHADEN	MUSS FÜR VERSICHERER HANDHABBAR SEIN
MITTLERE SCHADENHÖHE	MODERAT (RELATIV GERINGES SCHADENAUSMASS)
MITTLERE SCHADENHÄUFIGKEIT	RELATIV GROSS
INFORMATIONSASYMMETRIE	GERINGE ROLLE VON ADVERSER SELEKTION UND MORAL HAZARD
TEIL B: MARKTBEZOGEN	
VERSICHERUNGSPRÄMIE	KOSTENDECKEND UND BEZAHLBAR
DECKUNGSABGRENZUNG	AKZEPTIERBAR
TEIL C: GESELLSCHAFTSBEZOGEN	
GESELLSCHAFTLICHE WERTE	IM EINKLANG MIT GESELLSCHAFTLICHEN WERTEN
GESETZLICHE SCHRANKEN	ERLAUBEN DIE DECKUNG

Eine systematische Kategorisierung von Risiken, die effizient über den Mechanismus der Versicherung abgesichert werden können und solchen, bei denen dies nicht möglich ist, erfolgt üblicherweise anhand von neun Kriterien der Versicherbarkeit (siehe Tabelle 1 nach Berliner, 1982). Neben objektiven Kriterien, die dem Risiko inhärent sind, hängt die Versicherbarkeit sehr stark von den individuellen Kapazitäten und Präferenzen der Marktteilnehmer ab. Folglich existieren keine allgemeinen Grenzen der Versicherbarkeit; die Diskussion hilft aber grundlegende Probleme und Tendenzen aufzuzeigen, die auf Marktebene relevant sind.

An dieser Stelle sollen einige der kritischen Aspekte aufgezeigt werden. Eine detaillierte Analyse aller Kriterien der Versicherbarkeit findet sich in Biener, Eling und Wirfs (2015a, b). Die wesentlichen Probleme lassen sich auf die Bereiche Zufälligkeit des Schadenereignisses und Informationsasymmetrien zurückführen.

Eine zentrale Anforderung für die Bereitstellung von Versicherung für ein spezielles Risiko ist die Unabhängigkeit der Risiken. Unabhängigkeit bedeutet, dass ein Schadenereignis nicht Folge eines anderen Schadenereignisses ist oder die gleiche Ursache hat. Nur wenn sich ein Versicherungsportfolio aus unabhängigen Risiken zusammenstellen lässt, konvergiert der durchschnittliche Gesamtschaden gegen den erwarteten Schaden bei zunehmender Portfoliogrösse (Böhme, 2005; Biener, 2013). Diese zentrale Unabhängigkeitsbedingung minimiert das sogenannte Akkumulations-Risiko, welches die Solvenz von Versicherungsunternehmen gefährdet. Für Cyber-Risiken stellen einige Studien fest, dass diese grundsätzliche Voraussetzung verletzt wird. So sind IT-Systeme vielfach in einer ähnlichen Weise aufgebaut und greifen auf die gleichen Komponenten (z.B. Hard- und Software) zurück und sind so ähnlich anfällig (Baer und Parkinson, 2007). Dies deutet darauf hin, dass Vorfälle in Firmen nicht unbedingt unabhängig sind.

Ein weiteres grundsätzliches Problem bei der Bewertung von Cyber-Risiken resultiert aus dem Mangel an Daten (ENISA, 2012; Herath und Herath, 2011; Baer und Parkinson, 2007; Gordon et al., 2003). Ungeachtet dessen, wie gut die Modellierungen für Cyber-Risiken sind, sind die Modelle von geringem Nutzen, wenn keine Daten zum Testen und Kalibrieren der Modelle vorhanden sind. Ein weiteres Problem in diesem Kontext ist das Änderungsrisiko, also die systematische Änderung wesentlicher Charakteristika des Risikos (Haas und Hofmann, 2013; ENISA, 2012). In diesem Fall ist eine Analyse historischer Daten für die Beschreibung des aktuellen und zukünftigen Risikos nicht aussagekräftig. Der Mangel an Daten, insbesondere zu Grossschäden, verstärkt zudem die Schwierigkeiten bei der Abschätzung der oben beschriebenen Kumulrisiken.

Bei vollkommener Symmetrie der Informationen führt der Versicherungsmechanismus dazu, dass Versicherungsnehmer ihre Ressourcen effizient zwischen Cyber-Security und Risikotransfer aufteilen und Prämien nach Risikotypen differenziert werden können. Eine besondere Problematik von Cyber-Risiken ist jedoch, dass hier ein hohes Mass an Informationsasymmetrie herrscht. Die schlechter informierten Marktteilnehmer – in diesem Zusammenhang oft die Versicherer – können die «schlechten» Risiken nicht von den «guten» unterscheiden und werden einen Preis setzen, zu dem nur noch die schlechten Risiken bereit sind, ihr Risiko zu transferieren. Es kommt zu einer negativen Auslese (Adverse Selektion) und in extremen Fällen zu einem vollständigen Marktzusammenbruch. Um diesem Problem zu begegnen, nehmen Versicherer zuvor eine intensive Überprüfung der Cyber-Security Architektur vor; solche Abklärungen sind aber aufgrund der Komplexität der heutigen Infrastruktur nur bedingt in der Lage, das tatsächliche Risiko zu identifizieren. Ein weiteres Problem von Informationsasymmetrien entsteht aus dem Mangel an Anreizen für die Versicherungsnehmer, Präventionsmassnahmen zu ergreifen, die die Schadenwahrscheinlichkeit verringern (moralisches Risiko oder Moral Hazard). Diese Problematik lässt sich klassischerweise mit Selbstbehalten adressieren, welche jedoch den Versicherungsnutzen mindern, wenn Versicherungsnehmer eine Präferenz für Vollversicherungen haben.

Die oben beschriebenen Probleme führen im Markt zudem dazu, dass Prämien zum Teil als zu hoch wahrgenommen werden und dass Versicherungsausschlüsse und Deckungsgrenzen für einige Kundengruppen nicht optimal ausgestaltet werden können. Es ist jedoch zu erwarten, dass Verbesserungen bei der Modellierung von

Cyber-Risiken und der Abbau von Informationsasymmetrien dazu führen, dass Cyber-Versicherungen einen stärker risikoadäquaten Preis bekommen.

4.2 Akkumulation

Die Versicherungsbranche befürchtet, dass aufgrund der zunehmenden Interkonnektivität sowie durch Monokulturen von Hard- und Software die Verwundbarkeit der IKT zunimmt. Es ist vorstellbar, dass diese Schwachstellen gleichzeitig und in grossem Umfang Ziele von Malware oder Logikbomben werden können und so für massive wirtschaftliche Verluste und Ausfälle sorgen könnten. Daher hat der Schweizerische Versicherungsverband eine Unter-Arbeitsgruppe zur Analyse der entsprechenden Cyber-Akkumulations-Szenarien und zur Quantifizierung ihrer wirtschaftlichen Folgen eingesetzt.

In dieser Arbeitsgruppe wurde untersucht, wie explizite Cyber-Deckungen auf spezifische Akkumulations-Szenarien reagieren und mit klassischen Versicherungsdeckungen interagieren. Klassische (stillschweigende) Versicherungsdeckungen können ebenfalls von Cyber-Akkumulations-Szenarien betroffen sein.

Während zweier halbtägiger Workshops im Mai und Juli 2017 evaluierten 17 IT-Sicherheitsexperten und 14 Versicherer die wirtschaftlichen Auswirkungen von fünf Cyber-Akkumulations-Szenarien auf die Schweiz.

Im Mai 2017 verschlüsselte das Erpressungs-Programm «WannaCry» Dateien weltweit auf rund 300’000 Computern. Zu diesem Zweck wurde eine Schwachstelle in nicht gepatchten Microsoft-Systemen und -Servern ausgenutzt. In Grossbritannien waren über 40 Institutionen des Gesundheitswesens betroffen. Glücklicherweise waren in Zusammenhang mit diesem Angriff keine Todesfälle zu beklagen. Der Zwischenfall dauerte 72 Stunden und hatte massive Auswirkungen auf die Routineprozesse der Krankenhäuser. Die kurze Dauer der Malwareverbreitung ist der Tatsache zu danken, dass die Urheber der Malware einen «kill-switch» eingerichtet hatten, der mehr oder weniger zufällig von einem IT Experten aktiviert wurde. Geht man von einem geschätzten dreitägigen Ereignis und einem durchschnittlichen wirtschaftlichen Nutzen von 500 US-Dollar pro Tag pro Computer aus, ergibt sich ein aggregierter wirtschaftlicher Verlust von 450 Millionen US-Dollar Bei einer konservativen Schätzung belaufen sich die Auswirkungen auf Dritte auf etwa denselben Betrag, sodass sich ein wirtschaftlicher Schaden von schätzungsweise unter 1 Milliarde US-Dollar ergibt. Dies entspricht weniger als 0,001 Prozente des weltweiten BIP von 75’000 Milliarde US-Dollar. Die im vorliegenden Bericht besprochenen Cyber-Akkumulations-Szenarien würden sich dagegen 200-mal stärker auf das BIP der Schweiz auswirken.

Ende Juni 2017 nutzte die Schadsoftware «NotPetya» eine ähnliche Windows-Schwachstelle aus und beeinträchtigte den Betrieb mehrerer global und regional tätiger Wirtschafts-Unternehmen aus verschiedensten Branchen. Der weltweite wirtschaftliche Schaden kann noch nicht genau beziffert werden, wird aber vermutlich relativ zum globalen Brutto-Welt-Produkt deutlich kleiner sein, als die hier analysierten Szenarien.

4.2.1 Analyse-Methode

Die untersuchten Szenarien werden als Prozentualer Schaden des Schweizer BIP für 2016 ausgedrückt, wobei 100 Prozent gleich 650 Milliarden CHF sind (SECO, 2017). Es sei angemerkt, dass nicht jedes der untersuchten Szenarien zwangsläufig einen Rückgang des BIP zur Folge hat. Dies liegt an möglichen Substitutions- und Erholungs-Effekten während des Cyber-Vorfalles und im Anschluss an diesen.

Für die Analyse wurde folgendes Vorgehen gewählt:

- Auswahl der gefährdeten volkswirtschaftlichen Segmente
- Durchdringungsgrad einer Angriffs-Methode oder eines Angriff-Vektors für gefährdete Segmente
- Dauer des Ereignisses und Zeit bis zur Wiederaufnahme des Normalbetriebes
- Schätzung von Aufwendungen und Kosten auf Seite der Angreifer
- Einschränkungen:
  - Die Resultate dieser Studie basieren auf Experteneinschätzungen
  - Alle Annahmen basieren auf dem aktuellen Wissensstand und dem derzeitigen Stand der Technologie
  - Die Eintritts-Wahrscheinlichkeiten der einzelnen Szenarien wurden zueinander in Bezug gesetzt. Auf Schätzungen zu Wiederkehrperioden wurde verzichtet
  - Wechselwirkungen von globalen oder überregionalen Cyber-Ereignissen wurden nicht berücksichtigt

Einige der wichtigsten Referenzstudien wurden vom Centre of Risk Studies der Universität Cambridge entwickelt:

- Integrierte Infrastruktur: Cyber Resiliency in Society (Cambridge Centre for Risk Studies, 2016)
- Business Blackout (Cambridge Centre for Risk Studies, 2015)
- Sybil Logic Bomb Cyber Catastrophe (Cambridge Centre for Risk Studies, 2014)

Folgende Szenarien wurden von der Arbeitsgruppe untersucht:

- Distributed-Denial-of-Service (DDoS) Angriff auf einen Cloud-Service-Anbieter
- Angriff auf industrielle Prozessleitsysteme (ICS/SCADA)
- Simultane Angriffe auf verschiedene Schweizer Spitäler
- Cyber-Angriff auf den grössten Telekomanbieter der Schweiz
- Cyber-Angriff auf das schweizerische Elektrizitätsnetz und/oder regionale Stromverteiler und -produzenten

4.2.2 Untersuchte Szenarien

DDoS-Angriff auf Cloud-Anbieter

DDoS-Angriffe treten in letzter Zeit gehäuft auf. Meistens handelt es sich um gezielte Angriffe mit der Absicht, die Dienste des Angriffsobjekts zu unterbrechen oder ihre Verfügbarkeit einzuschränken. Die Ausweitung eines DDoS-Angriffes auf ein Akkumulations-Niveau ist nur mit Hilfe einer aufwändigen Infrastruktur und entsprechendem Personal möglich, daher ist es wahrscheinlich, dass ein solches Szenario nur mit staatlicher Unterstützung vonstattengehen kann.

Kurzfristig könnten bei Angriffen auf die Clouds 62 Prozent des schweizerischen BIPS von einem Akkumulations-Szenario betroffen sein, wobei sich die daraus resultierenden Schäden in den meisten Branchen in engen Grenzen halten dürften. Nach den Annahmen der Expertengruppe dürften 20 bis 30 Prozent der Cloud-Service-Anbieter betroffen sein. Auswirkung auf die betroffenen Dienste sind mit 90 Prozent beziffert. Die Ausfälle dauern zwischen einem Tag und einer Woche. Alle 5 bis 12 Jahre passiert ein solches Szenario. Diese Beurteilung bezieht sich nur auf DDoS-Angriffe auf Finanzdienstleistungen und Handel.

Die wirtschaftlichen Folgeschäden für die Schweiz betragen in diesem Szenario zwischen CHF 0,2 und 1,3 Milliarden, was 0,03 bis 0,2 Prozent des Schweizer BIPs entspricht. Verursacht werden diese Schäden in erster Linie durch zusätzlichen Arbeitsaufwand und entsprechende Kosten. Die Umsätze der betroffenen Unternehmen wären nur marginal beeinträchtigt, da nach Behebung des Schadens ein Substitutions- und Erholungs-Effekt eintreten dürfte.

Prozessleitsysteme (SCADA/ICS)

Moderne SCADA/ICS-Standardprotokolle ermöglichen die Integration verschiedener Anbieter, so dass eine einzige Produktionsanlage mit Produkten von verschiedenen Anbietern bestückt sein kann. Bestimmte Schwachstellen werden so über verschiedene Anbieter hinweg geteilt.

Aus diesem Grund wurden zwei verschiedene Szenarien analysiert, in denen landesweit 10 Prozent der SCADA/ICS-Systeme während drei Wochen beeinträchtigt oder sicherheitshalber abgeschaltet würden.

Das erste Szenario basiert auf Industroyer/Crash Override-Derivaten (US-CERT, 2017). Der Durchdringungsgrad dieses Szenarios hängt von der Branche ab. Dieses Szenario und seine Umsetzung sind komplex, sodass nur Angreifer mit staatlicher Unterstützung oder grossen finanziellen und technischen Ressourcen zu seiner Ausführung imstande sein dürften. In erster Linie dürften folgende Wirtschaftszweige betroffen sein:

– Verarbeitendes Gewerbe
– Energie
– Verkehr
– Wasserversorgung

– Gesundheitswesen
– Landwirtschaft
– Bauwesen

Das zweite Szenario richtet sich vor allem gegen Pharma- oder Nahrungsmittelhersteller und ist als Erpressungsaktion angelegt. Dabei werden Prozess-Variablen so verändert, dass Endprodukte stark verändert werden.

Die jährlichen BIP Beiträge der Wirtschaftsbereiche, die durch Szenario 1 und 2 betroffen werden, belaufen sich auf 150 bis 370 Milliarden CHF, je nach angenommenem Durchdringungsgrad pro Branche. Die angenommene dreiwöchige Dauer der beiden Szenarien hat geschätzte wirtschaftliche Folgen zwischen 0,3 und 2,2 Milliarden CHF Dies entspricht 0,05 bis 0,3 Prozent des Schweizer BIPs. Die Kosten setzen sich aus Betriebsunterbrechungen, Ertragsausfällen, zusätzlichem Arbeitsaufwand und den damit verbundenen Kosten sowie physischer Schäden einschliesslich Unfällen und Todesfällen zusammen.

Gesundheitswesen und Spitäler

In diesem Szenario infiltriert ein Cyber-Angreifer gleichzeitig eine Reihe von Schweizer Spitälern. Das Ziel ist Erpressung entweder mittels Ransomware oder in Form eines DDoS-Angriffs, so dass die Spitäler für zwei bis drei Wochen ausfallen. Im Jahr 2015 beliefen sich die Erträge der 288 Schweizer Spitäler auf 24 Milliarden CHF (Bundesamt für Gesundheit, 2015). Anhand von unterschiedlichen Annahmen zur Dauer und Durchdringung der einzelnen Szenarien, wurde die folgende Bandbreite von möglichen wirtschaftlichen Schäden ermittelt:

– Vollständiger Ausfall sämtlicher Spitäler für drei Wochen: 1,4 Milliarden CHF, was 0,2 Prozent des Schweizer BIPs entspricht
– Ausfall von 10 Prozent der Spitäler während drei Wochen: 138 Millionen CHF
– Eine Woche Gesamtschaden 10 Prozent der Spitäler: 46 Millionen CHF

Die wirtschaftlichen Auswirkungen gehen in erster Linie auf Betriebsausfälle und Ertragsverlust, zusätzlichen Arbeitsaufwand und die damit verbundenen Kosten. Physische Schäden einschliesslich Unfälle und Todesfälle wie auch Haftpflichtansprüche sind nicht in diesen Zahlen berücksichtigt. Ein derartiges Akkumulations-Szenario ist komplexer Natur; zu seiner Konzeption und Umsetzung sind Know-how, Infrastrukturen und Spezialisten erforderlich. Daher geht die Expertengruppe davon aus, dass die Angreifer entweder über staatliche Unterstützung verfügen oder dass es sich um Terroristen bzw. Kriminelle handelt. Zahlreiche Spitäler arbeiten mit den gleichen Hard- und Software-Produkten. Dennoch sind Implementierung und Konfiguration dieser Produkte von Spital zu Spital unterschiedlich, so dass die Wahrscheinlichkeit eines erfolgreichen Akkumulations-Szenarios in mehr als 10 Prozent der Schweizer Spitäler als eher gering eingestuft wird.

Elektrizitätsnetz – Stromversorger

Dieses Szenario lehnt sich an den Cyber induzierten Stromausfall in der Ukraine von Dezember 2016 an. Die dort eingesetzte Industroyer Malware legte zahlreiche Umspannstationen lahm.

Die Elektrizitätsversorgung kommt zum Erliegen und in einer Kettenreaktion kann es zu Sachschäden innerhalb des Netzwerks kommen. Die potenzielle Dauer des Angriffs beträgt zwei bis sieben Tage bei einer Intensität von 100 Prozent. Nach zwei Tagen sind die Charakteristiken des Angriffs verstanden und es werden Gegenmassnahmen ergriffen, die nach und nach die Stromversorgung wiederherstellen. Je nach Umfang des Angriffs dürfte die Stromversorgungsinfrastruktur innerhalb von 5 bis 21 Tagen wieder vollumfänglich zur Verfügung stehen. Dies entspricht den Szenarien S1 und S2 der Lloyd's / Cambridge Business-Blackout-Studie.
Nach unserem konservativen Ansatz dürften die wirtschaftlichen Auswirkungen während zwei bis sieben Tagen auf 80 bis 100 Prozent des Schweizer BIPs betreffen. Je nach betroffenem Gebiet ist mit Schäden von bis zu CHF 12 Milliarden zu rechnen. Dies entspricht 2 Prozent des Schweizer BIPs.

Hinweis: In diesem Szenario richtet die betrachtete Malware keine grossen Sachschäden an Generatoren oder Transformatoren an. Grosse Sachschäden an der Kraftwerks-Infrastruktur und deren Reparaturen und Wiederbeschaffungen würden Auswirkung und Dauer des Szenarios wesentlich vergrössern. Solche Angriffe sind möglich, haben aber eine relative tiefe Wahrscheinlichkeit, da physische Schädigungen der genannten Hardware nur mit grossem Aufwand und Knowhow zu bewerkstelligen sind.

Telekommunikation

Drei Szenarien wurden analysiert:

– Eine Zero-Day-Malware richtet sich gegen weit verbreitete Router oder Modems und löscht die Firmware, sodass ein physischer Ersatz erforderlich wird.
– Ein DDoS-Angriff auf Basis eines IoT[3] -Botnetzes gegen DNS[4] -Anbieter an einem umsatzstarken Internet-Einkaufstag, z.B. vor Weihnachten.
– Ein führendes Schweizer Telekomunternehmen wird mittels Cryptolocker-Schadsoftware lahmgelegt

Die wirtschaftlichen Auswirkungen reichen von 200 Millionen CHF (DNS-Szenario) bis zu 2,5 Milliarden CHF im Rahmen des Routers/Modem und Cryptolocker-Szenarios. Dies entspricht 0,4 Prozent des jährlichen BIPs der Schweiz.

[3] Internet of Things

[4] Domain Name System

Extremszenarien

Costin Raiu von Kaspersky Lab schätzt die Entwicklungskosten für Stuxnet auf 100 Millionen US-Dollar Obwohl ein gegen ein individuelles ICS/SCADA[5] -System gerichteter Zero-Day-Exploit bereits für weniger als 10‘000 US-Dollar erworben werden kann, wie der CEO von www.gleg.net, Yuriy Gurkin, ausführt (Paganini, 2015), ist ein erfolgreicher, koordinierter Cyber-Angriff in grossem Stil nach wie vor ein äusserst komplexes und kostenintensives Unterfangen. Zudem stellt sich die Frage, ob es für Kriminelle wirklich attraktiv ist, solche Angriffe zu finanzieren, da sie sich im Gegensatz zu Ransomware oder DDoS kaum in Geld ummünzen lassen.

Daher wurde auf die Analyse von Extremszenarios wie einem Angriff auf den Sihlsee-Staudamm 35 Kilometer flussaufwärts von Zürich oder einem Angriff auf ein Kernkraftwerk verzichtet. Die Expertengruppe ist der Ansicht, dass derartige Szenarios eindeutig kriegerischer Natur sind, extrem komplex ausfallen und sich nur mit grosser Mühe erfolgreich umsetzen lassen. Man ist sich allerdings bewusst, dass zwischen Cyber-Kriegen und Cyber-Verbrechen keine eindeutige Trennlinie verläuft.

4.2.3 Überlegungen aus Versicherungssicht

In den hier vorliegenden Schweiz-bezogenen Szenarioanalysen werden die wirtschaftlichen Auswirkungen des Cyber Akkumulations-Szenarios «Stromnetz» auf weniger als 2 Prozent des BIPs geschätzt, während die übrigen Szenarien ein Ausmass von unter 0,5 Prozent des BIPs erreichen dürften. Im Vergleich dazu würden sich die ökonomischen Schäden einer Naturkatastrophe, wie das Basler Erdbeben auf ca. 15 Prozent des BIPs oder ein Pandemie-Szenario gemäss Bundesamt für Bevölkerungsschutz auf ca. 2,2 Prozent des BIPs belaufen.

Die oben dargestellten Cyber Akkumulations-Szenarien haben nicht nur Auswirkungen auf IT-Systeme und Daten, sondern auch auf Sach- und Vermögenswerte. Einige Szenarien könnten sogar Leben gefährden und wirtschaftliche Abläufe stören oder unterbrechen, Kettenreaktionen auslösen und Dritte schädigen. Neben expliziten Cyber-Deckungen können gewisse Szenarien auch Deckungen in Sach- und Haftpflicht-Policen auslösen. Die traditionellen Versicherungs- Klauseln berücksichtigen die besondere Problematik von Cyber-Risiken und deren Auswirkungen oft nicht. Das kann zu Vertragsunsicherheit führen (IMIA, 2016). Ein Beispiel hierfür stellen Cyber-Kriegshandlungen oder Akte Cyber-terroristischer Natur dar, bei denen sich die IT-Forensiker sehr schwertun dürften, sie klar von Cyber-Sabotage oder Cyber-Verbrechen abzugrenzen. Dementsprechend kann eine Anwendung der Ausschlussklauseln «Krieg» und «Terrorismus» mit erheblichen Schwierigkeiten verbunden sein. Zudem könnte der Versicherungsnehmer den Entscheid des Versicherers anfechten und vor Gericht ziehen, wodurch sich die Vertragsunsicherheit weiter verstärken würde.

KMU Sachversicherungen decken üblicherweise benannte Gefahren. Produktionsverluste durch Stromausfälle oder Unterbrüche der Telekommunikation würden meist keine Schadenzahlungen auslösen.

[5] Industrial Control Systems / Supervisory Control And Data Acquisition

Dahingegen decken sogenannte All-Risk-Policen, wie sie in den meisten technischen Versicherungssparten und für Grossunternehmen und multinationale Konzerne üblich sind, Sachschäden und hiervon ausgelöste Verluste aus Betriebs-Unterbrüchen, es sei denn, Stromausfall oder Nichtverfügbarkeit der Telekommunikation wären explizit ausgeschlossen.

Bei den Kühlgutversicherungen, die als Zusatzversicherung gekauft werden kann, ist der Stromausfall in der Regel versichert und die Ursache für den Ausfall der öffentlichen Stromversorgung spielt keine Rolle.

Bei Betrachtung der Cyber-Deckungen in klassischen Versicherungssparten lässt sich die verfügbare Versicherungs-Kapazität im Schweizer Markt in den Sparten Haftpflicht-, Sach-, Vermögensschaden-, Kranken- und Lebensversicherung nur mit grosser Mühe abschätzen. Staatsunternehmen und grosse Konzerne haben die Tendenz zur Selbstversicherung, was dazu führt, dass ein grosser Teil der möglichen Cyber-Schäden unversichert sein dürften. Mit anderen Worten: Die gesamte Schweizer Wirtschaft würde von derartigen Akkumulations-Szenarien wohl nicht in die Knie gezwungen werden, aber zahlreiche Unternehmen hätten keine oder keine ausreichende Versicherungsdeckung für diese Cyber-induzierten Schäden. Es lässt sich nicht ausschliessen, dass allenfalls eine staatliche Intervention erforderlich wäre, um den Zusammenbruch dieser Unternehmen zu verhindern.

Eine weitere Befürchtung der Versicherungswirtschaft besteht darin, dass stillschweigend übernommene Cyber-Risiken häufig nicht in die regulären Deckungen eingepreist sind. Wie oben erwähnt, besteht in Bezug auf Cyber-Risiken Vertrags-Unsicherheit. Versicherungsnehmer können sich nicht darauf verlassen, dass bei einer Nichterwähnung von Cyber-Risiken solche Schäden von der Versicherung gedeckt sind. In diesem Zusammenhang sei auf das Consultation Paper CP39/16 der britischen Aufsichtsbehörde zur Frage der stillschweigenden Cyber-Deckung verwiesen, in dem u.a. die Kapital-Unterlegung der Kapazitäten hinterfragt wird (Bank of England, 2016). Diese Mehrdeutigkeit nimmt Versicherte als auch die Versicherungsbranche in die Pflicht, in den Policen Vertrags-Sicherheit bezüglich Cyber herzustellen.

4.2.4 Schlussfolgerungen zur Akkumulation

4.2.4.1 Marktlösungen

Versicherungspools, Rückversicherung und Alternativer Risikotransfer am Kapitalmarkt (z.B. Cyber Cat Bonds) können die für einen Transfer von Cyber-Risiken verfügbaren Kapitalressourcen insbesondere in Bezug auf Extremereignisse erhöhen. Es ist noch weitgehend unklar, wie gross die Schäden aus einem weltweiten «erfolgreichen» Cyber-Ereignis sein können. Als Proxy kann man das globale Cyber-Prämienvolumen von ca. 3,5 Milliarden US-Dollar (KPMG, 2017) nehmen; damit bewegt sich der Markt noch in einem Bereich, der für die Versicherungsbranche zu bewältigen ist. Sollten die hohen Wachstumserwartungen, die einige Studien äussern (KPMG, 2017; PWC, 2015), jedoch gerechtfertigt sein, wird das Thema Risikotragfähigkeit weiter an Bedeutung

gewinnen. An dieser Stelle stellt sich dann auch die Frage nach den Grenzen der Versicherbarkeit in Bezug auf die maximale Risikotragfähigkeit der Assekuranz.

4.2.4.2 Staatliche Auffanglösung

Es stellt sich die Frage, ob es eine staatliche Auffanglösung für Cyber-Risiken geben sollte. Derartige staatliche Eingriffe finden sich heute insbesondere bei Risiken, die zu potenziell schwerwiegenden Schäden führen können und für die der Markt, aufgrund verschiedenster Probleme der Versicherbarkeit, keine genügende Absicherung anbietet. Beispiele hierfür sind Terror- (Terror Risk Insurance Act, Pool Re), Naturkatastrophen- (japanisches Erdbeben-Rückversicherungs-Programm) oder Atom-Risiken. Der Staat kann hier die entsprechenden Risiken entweder direkt (als Erstversicherer) selbst tragen, als Rückversicherer der Assekuranz für Gross-Schäden auftreten, als «lender of last resort» agieren und kurzfristig die Liquidität der Assekuranz sicherstellen oder die Herausbildung eines Versicherungsmarktes unterstützen, indem er ein Umfeld schafft, in dem der private Versicherungssektor sich entwickeln kann.

In vielen dieser Konstruktionen können das Wissen privatwirtschaftlicher Versicherer und Rückversicherer über die Risiken mit den finanziellen Ressourcen der öffentlichen Hand kombiniert werden. Hier lassen sich zwei Bereiche unterscheiden. Es gibt ein breites Spektrum an Cyber-Risiken und Industrien, für die die Assekuranz umfangreiche Deckungen anbietet bzw. durch Verbesserungen der Versicherbarkeit anbieten kann. Hier bedarf es aus heutiger Sicht keiner staatlichen Auffanglösung, da ausreichend Ressourcen auch für Extremszenarien vorhanden sind. Die Entwicklung der Frequenz von derartigen Extremszenarien bleibt aber kritisch zu beobachten. Darüber hinaus gibt es den Bereich der kritischen Infrastrukturen. Hier besteht typischerweise ein geringerer Appetit der Assekuranz, vollumfängliche Deckungen anzubieten (bzw. nur zu bestimmten Konditionen), insbesondere da Schäden aus einigen Extremszenarien die Kapazitäten der Versicherungswirtschaft übertreffen. Letztendlich geht eine staatliche Auffanglösung für gravierende Ereignisse im Bereich der kritischen Infrastrukturen implizit aus dem Staatszweck hervor (Nach Art. 2 der Bundesverfassung ist Aufgabe der Staatsorgane die Sicherheit des Landes zu gewährleisten).

4.3 Mangel an Daten

Im Gegensatz zu anderen versicherten Risiken wie Feuer oder Naturkatastrophen, für welche Daten seit Jahrzehnten oder sogar Jahrhunderten zur Verfügung stehen, fehlen bei Cyber-Risiken entsprechenden Statistiken und Daten. Um schnell und sauber eine brauchbare Menge an Daten zu besitzen, sollte der Regulator zusammen mit der Versicherungsindustrie und ihren Kunden einen entsprechenden Rahmen bestimmen.

4.3.1 Meldepflicht

Meldepflichten üben im Sinne der Marktdisziplin, insbesondere für Unternehmen, eine Wirkung aus, für die der Einfluss eines Cyber-Vorfalls bedeutsam ist. Meldepflichten könnten sich an entsprechende Vorschriften aus den USA und der EU im Bereich Datenschutzverletzungen orientieren. Das sind Verstösse gegen die Datensicherheit und den Datenschutz, bei denen personenbezogene Daten unberechtigten Dritten bekannt werden.

Die Wirksamkeit dieser Meldevorschriften in den USA wurde bereits in mehreren wissenschaftlichen Untersuchungen belegt und es ist wahrscheinlich, dass diese zur Marktentwicklung beigetragen haben. Auch in der Schweiz wird die Umsetzung eines derartigen Meldesystems im Rahmen der Revision des Bundesgesetzes über den Datenschutz (DSG) angestrebt und könnte entsprechend positive Effekte für den Schweizer Marktplatz bewirken. Datenschutzverletzungen als Teilmenge aller Cyber-Risiken ist derzeit das am besten dokumentierte Risiko, was zu einem grossen Teil den Meldevorschriften zuzuschreiben ist. Es bildet jedoch nur einen kleinen Teil der Gefahrenlandschaft ab.

Es stellt sich daher die Frage, ob es neben Meldepflichten zu Datenschutzverletzungen einer umfassenderen Pflicht zur Meldung von Cyber-Vorfällen bedarf. An dieser Stelle stehen sich verschiedene staatliche Interessen potenziell diametral entgegen. Geht es um Sicherheit, also den Schutz kritischer Infrastrukturen und der Volkswirtschaft als Ganzes, haben sich freiwillige Meldesysteme durchgesetzt (siehe Department of Homeland Security (DHS) in den USA sowie Melde- und Analysestelle Informationssicherung (MELANI) in der Schweiz), die darauf abzielen, die Gefahrenlandschaft, deren Ursachen und Hintergründe zu verstehen, um die Widerstandsfähigkeit des Gesamtsystems zu stärken. Die Freiwilligkeit dieser Systeme basiert auf der Erfahrung, dass eine Meldepflicht zu einer schlechten Datenqualität und zu keiner über die Meldung hinausgehenden Kooperation der Marktteilnehmer führt; es fehlt der Anreiz für eine Kooperation, die über das Mindestmass hinausgeht. Damit Marktteilnehmer in einem freiwilligen Meldesystem Anreize zur Kooperation und Meldung haben, wird auf verschiedene Art ein Nutzen erbracht. In erster Linie ist dies im Zugang zu Informationen über die Gefahrenlandschaft zu sehen, die nur eine übergeordnete staatliche Instanz liefern kann (z.B., weil sie Zugang zu nachrichtendienstlichen Informationen hat), aber auch in der Unterstützung bei der Gefahrenbewältigung. Zudem ist eine rechtliche Absicherung der Haftpflichtrisiken bei einer Datenweitergabe an solche offiziellen Stellen wichtig.

Besteht der Zweck einer Meldepflicht in der Förderung des gesamtwirtschaftlichen Nutzens und einer nachhaltigen Entwicklung, hat sie im Kontext der Entwicklung von Märkten für Risikotransfer (z.B. Versicherung) einen potenziellen Wert. Zum einen stärkt sie die Marktdisziplin und vermittelt Anreize zu Investition in Cyber-Security, wenn Cyber-Vorfälle publik werden und dadurch die Reputation tendenziell leidet. Dies erhöht die Versicherbarkeit durch den Abbau von Informationsasymmetrien. Zum anderen führt eine Meldepflicht dazu, dass erstmalig eine Datenbasis geschaffen würde, welche repräsentativ die Cyber-Gefahrenlandschaft in der Schweiz abbilden und Versicherer dabei unterstützten würde, Cyber-Risiken und deren Abhängigkeiten) besser zu verstehen. Die Bewertung der Risiken ist eine zentrale Voraussetzung, um Risikotransfer im Bereich-Cyber überhaupt nachhaltig anzubieten. Es ist demzufolge zu überlegen, ob es sinnvoll sein kann, neben dem bestehenden System für kritische Infrastrukturen ein identisches System für alle Industrien aufzubauen. Ob dies auf Basis freiwilliger oder verpflichtender Meldungen erfolgen soll, bleibt zu definieren. Sollte von einer Meldepflicht abgesehen werden, so ist es zentral, Anreize zur Erstattung solcher Meldungen zu schaffen und darauf hin zu arbeiten, schnellst möglich eine kritische Masse an Unternehmen zu gewinnen. Wichtig erscheint in diesem Kontext, eine zentrale Stelle zur Meldung zu definieren, die eine starke Aussenwirkung hat, z.B. durch den Ausbau von MELANI oder durch die Schaffung einer neuen Stelle (z.B. auf Basis von public-private-partnerships).

Die Analyse und Verarbeitung der Daten könnte, wenn nötig, an verschiedene Stakeholder ausgelagert werden (z.B. an MELANI für systemkritische Infrastrukturen sowie an weitere Stellen für andere Industrien). Zwei parallele Systeme aufzubauen erschient ineffizient, da Verantwortlichkeiten nach aussen möglicherweise nicht klar geregelt sind, was zu einer Zurückhaltung beim Melden führen kann, sollte dies freiwillig sein. Zu bemerken ist hier, dass die Europäische Zentralbank derzeit an der Umsetzung einer Meldepflicht für Cyber-Vorfälle innerhalb ihres Regulierungsbereiches arbeitet. Dies ist eine Einzellösung für den Bankenbereich, die wichtig für den Bankenregulierer ist, jedoch nicht für ein System taugt, das die Gesamtwirtschaft einschliesslich kleiner und mittlerer Betriebe in nichtregulierten Sektoren umfassen soll.

4.3.2 Datenaustausch

Um dem Mangel an Daten zur Bewertung und Modellierung von Cyber-Risiken zu begegnen, kann man Daten konzertiert sammeln und zur Verfügung stellen (Datenpooling). Ein Beispiel für einen wettbewerbsrechtlichen Rahmen, innerhalb dessen eine eingegrenzte Kooperation zwischen Versicherungsunternehmen stattfinden kann, ist die EU-Gruppenfreistellungsverordnung (GVO) 267/2010. Diese gestattete unter anderem eine Zusammenarbeit bei der «... Erstellung gemeinsamer, auf gegenseitig abgestimmten Statistiken oder dem Schadenverlauf beruhender Risikoprämientarife.» Nach dem Auslaufen der Verordnung im März 2017 hat die EU-Kommission deutlich gemacht, dass sie die Statistikarbeit in der Versicherungsbranche grundsätzlich für wettbewerbsfördernd hält und dass die in der GVO niedergelegten Grundsätze auch in Zukunft als Orientierung dienen können.

Sofern die gesetzlichen Rahmenbedingungen einen Austausch von Daten zwischen den Versicherern zulassen, liesse sich ein Datenpool im Markt realisieren; er bedarf nicht zwangsläufig einer staatlichen Organisation. So übernimmt zum Beispiel im deutschen Markt der Versicherungsverband GDV die Erhebung von versicherungstechnischen Daten bei den teilnehmenden Mitgliedsunternehmen, die Bereinigung und die statistische Auswertung sowie die Veröffentlichung der Ergebnisse und gewährleistet die Einhaltung der wettbewerbsrechtlichen Vorgaben.

4.4 Informationsasymmetrie

Informationsasymmetrie verursacht bekannter Weise ein moralisches Risiko («moral hazard») eines Geschäftspartners, oft des Versicherungsnehmers, und kann zu einer Antiselektion der Risiken in einem Versicherungsportfolio führen. Um dieser Informations-Asymmetrie zu begegnen, kann man auf Mindeststandards für IT- und Informations-Sicherheit wie auch – besonders um gegen die Antiselektion vorzugehen – auf Versicherungsobligatorien abstellen.

4.4.1 Mindeststandards

Mindeststandards für Cyber-Security könnten das Investitionsniveau in Cyber-Security erhöhen. Mindeststandards können allerdings bürokratisch und schwer umsetzbar sein. Bei gesetzlichen oder regulatorischen Mindeststandards besteht ausserdem die Gefahr, dass alle Marktteilnehmer unabhängig ihrer Grösse, Industrie,

Geographie, und der Art von Daten, die vorgehalten werden, und somit auch unabhängig ihres Beitrags zum Gesamtrisiko (ihrer Systemrelevanz, wenn man so will) gleichbehandelt werden. Wenn hingegen nicht alle Marktteilnehmer die Standards erfüllen müssen, entstehen Anreize, die Regeln durch gezielte Umgehungsmanöver auszuhöhlen. Es ist zudem zu erwarten, dass eine Art technischer Mindeststandard im Bereich Cyber-Security wenig effektiv ist, da die technologische Entwicklung zu dynamisch ist, als dass gesetzliche oder regulatorische Vorgaben, die man üblicherweise aus Gründen der Rechtsstabilität längerfristig ausrichtet, hier nützlich sein können. Aufgrund der internationalen Dimension von Cyber-Risiken wären regionale technische Mindeststandards insbesondere für internationale Firmen eine grosse Herausforderung und mit erheblichen Kosten verbunden, ohne dass es einen eindeutigen positiven Effekt auf Cyber-Security hätte.

Sinnvolle Mindeststandards im Bereich Cyber-Risiko können nur prinzipienbasiert ausgestaltet sein und erfordern ggf., dass die Verantwortung für Cyber-Security auf Vorstandsebene aufgehängt sein muss sowie ausreichend Ressourcen vorhanden sein müssen, um mit den aktuellen Herausforderungen adäquat umzugehen.

Eine Alternative wäre eine gesetzliche Verpflichtung Mindeststandards zu schaffen. Die Entwicklung und Ausformulierung der branchenspezifischen Mindeststandards könnte man dann an die entsprechenden Branchenverbände delegieren.

Eine weitere denkbare Marktalternative ist die Definition von branchenspezifischen technischen Mindestanforderungen, die zu erfüllen sind, um Versicherungsschutz zu erhalten. Hier könnten Versicherer einen wichtigen Beitrag leisten, gewisse Mindestanforderungen[6] am Markt zu forcieren – ähnlich der Verwendung von Winterreifen in der MF-Versicherung. Versicherer arbeiten schon heute eng mit IT-Security Unternehmen und ihren Kunden zusammen, um eine holistische Perspektive auf Cyber-Risiken zu bekommen und state-of-the-art Cyber-Security bei ihren Kunden zu unterstützen. Allerdings wirken diese Anforderungen allerdings nur auf solche Firmen, die ihre Cyber-Risiken versichern. Des Weiteren kann die Einhaltung dieser Mindeststandards als Basis einer möglichen Zertifizierung dienen, die es dann den Unternehmen erlaubt, mit dem Argument guter Cyber-Sicherheit im Wettbewerb teilzunehmen.

Gleichzeitig sollte auch das Thema der «Cyber-Awareness» aufgegriffen werden. Unternehmen in der Schweiz setzen sich nach wie vor nur geringfügig mit dem Thema Cyber-Risiko auseinander. Eine mögliche «Awareness Kampagne» könnte sinnvoll sein, um dem Thema die nötige Wichtigkeit beizumessen. Sowohl die Versicherungs- als auch die IT Security Branche stehen gerne zur Verfügung, um in «public-private partnerships» dieses

[6] Mindestanforderungen wie zum Beispiel die regelmässige Aktualisierung der Antiviren- und Firewallprogramme, die quasi sofortige Durchführung von "Patches" und Installation von neuen Versionen der Programme, saubere und aktuelle "governance" und Verantwortungsverteilung im IT- und Information-security.

Thema breiter zu adressieren und als Anlaufstelle für mögliche Lösungen und Aufklärung (Mindestanforderungen, Best Practices, Risk Management Wissen etc.) beigezogen zu werden.

4.5 Versicherungsobligatorien

Versicherungsobligatorien finden wir heute insbesondere im Bereich der Haftpflicht, dort wo eine Tätigkeit oder Anlage zu Schäden bei Dritten führen kann (z.B. für Berufsgruppen wie Ärzte, Fahrzeughalter, Atomkraftwerke, Stauanlagen). Andere Obligatorien – v.a. zur Absicherung gegen Naturgefahren – betreffen Eigenschäden der Versicherten. Die Versicherung von Cyber-Risiken betrifft sowohl Eigenschaden als auch Drittschäden. Während alle Unternehmen von Eigenschäden betroffen werden können, betrifft das Haftungspotential für Schäden Dritter vor allem IT-Dienstleister und andere Unternehmen, die sich als Verbreiter von schädlichem Software und Ähnlichem eignen oder grosse Mengen an Daten bewirtschaften.

Der Sinn eines Versicherungsobligatoriums liegt darin, finanzielle Mittel sicherzustellen, mit denen im Schadenfall der finanzielle Verlust des Versicherten kompensiert werden kann. Das Obligatorium zwingt Marktteilnehmer ihr finanzielles Risiko (als potentielle Geschädigte oder Haftpflichtige) auf einen Dritten (den Versicherer) zu übertragen. Hingegen kann ein Versicherungsobligatorium kein Ersatz für Sicherheitsvorkehrungen sein. Die Versicherung kann und soll nur einspringen, wenn zwar alle erforderlichen und zumutbaren Massnahmen getroffen wurden, aber versagen. Es ist zudem darauf hinzuweisen, dass auch eine Pflichtversicherung nicht alle volkswirtschaftlichen Schäden eines schweren Cyber-Vorfalles aufzuheben vermag.

Ein Versicherungsobligatorium setzt die Versicherbarkeit des Risikos voraus. Um Risiken versichern zu können, benötigt die Versicherungsindustrie genügend verlässliche Angaben und Daten, um die Höhe und Frequenz der zu erwartenden Schäden realistisch einschätzen zu können. Bei Cyber-Risken fehlen historische Erfahrungen weitgehend, was diese Einschätzung erschwert. Das hohe Mass an Informationsasymmetrie birgt in diesem Zusammenhang zusätzliche Gefahren.

Mit einem Versicherungsobligatorium könnte auch ein negativer Anreiz für pflichtversicherte Unternehmen geschaffen werden, ihre Investitionen in Cyber-Security zu reduzieren. Dies ist darauf zurückzuführen, dass die für die Beherrschung des Risikos notwendigen Investitionen die Versicherungsprämie nicht reduzieren. Somit würde der ökonomische Anstoss, in Sicherheit zu investieren, durch eine staatliche Vorschrift abgeschwächt. Dies steht dem Ziel einer erhöhten Cyber-Sicherheit entgegen.

Es ist deshalb sinnvoller, dass die Versicherungsindustrie im Dialog mit der Wirtschaft weiterhin an der Gestaltung von freiwilligen Versicherungslösungen arbeitet, die risiko- und marktorientiert sind.

5 Zusammenfassung und Handlungsempfehlungen

5.1 Zusammenfassung der wichtigsten Erkenntnisse

Cyber-Risiken stellen ein ökonomisch relevantes Thema für die Schweizer Volkswirtschaft dar. Es gibt Anzeichen dafür, dass das Fehlen geeigneter staatlicher Rahmenbedingungen und damit die alleinige Koordination über den Markt zu einer Unterinvestition in Cyber-Security führt. Dies kann zu einem erheblichen Risiko für die Schweizer Volkswirtschaft werden. Es ist daher essenziell, ein sinnvolles Rahmenwerk mit klaren Rollen und Verantwortlichkeiten zu definieren, um Wirtschaftswachstum, technischen Fortschritt, politische Stabilität und gesellschaftlichen Fortschritt zu fördern. Versicherung leistet dabei einen wichtigen Beitrag hinsichtlich Risikotransfer, Anreizen zur Prävention und Kompetenzen im Risikomanagement. Heute sind global, aber insbesondere in Europa und der Schweiz, nur ein geringer Teil der Cyber-Risiken versichert. Dies ist dadurch bedingt, dass der Versicherungsmarkt für Cyber-Risiken einige Friktionen aufweist, welche die Versicherbarkeit einschränken. Akkumulation der Risiken, Mangel an Daten und Informationsasymmetrien sind hier die zentralen Probleme, die adressiert werden müssen, um die Herausbildung eines effizienten und nachhaltigen Marktes zu ermöglichen. Es ergeben sich zahlreiche potenzielle Eingriffsmöglichkeiten, von denen hier einige diskutiert werden.

1 Prinzipienbasierte, gesetzliche oder implizite markt-basierte Cyber-Security Mindeststandards sind technischen, regelbasierten gesetzlichen Vorgaben vorzuziehen und können der Marktentwicklung dienen;
2 die Kombination aus freiwilliger Meldung und Meldepflicht könnte ein Weg sein, sowohl Sicherheit als auch den gesamtwirtschaftlichen Nutzen zu fördern. Unternehmen können sich in Datenpools zusammenschliessen, um die Bewertbarkeit und Modellierung insbesondere von Extremereignissen zu verbessern. Hierfür müssen die rechtlichen Rahmenbedingungen geschaffen werden.
3 Die Berechnung der Folgen von grossen Akkumulations-Szenarien für die Schweizer Wirtschaft hat gezeigt, dass zwischen den Auswirkungen auf ausdrückliche Cyber-Deckungen (insbesondere bei Datenverlusten, Beschädigung von Daten und unrechtmässiger Exposition von Daten, welche eine Haftpflicht gegenüber Dritten auslösen), sowie den Auswirkungen auf gängige Sachversicherungsdeckungen (so genannte «stillschweigende» Deckungen) aufgrund von cyber-induzierten Beschädigungen von Infrastrukturen oder gar Personenschäden zu unterscheiden ist.

Erstere hatten in den von einer Expertengruppe untersuchten Szenarien Auswirkungen im Umfang von weniger als 0,5 Prozent des BIPs zur Folge. Hier liesse sich im Schweizer Markt Versicherungskapazität in ausreichendem Umfang schaffen, sofern die Nachfrage seitens der Unternehmen und die wirtschaftliche Gestaltung der Versicherungsdeckungen in angemessenem Umfang zunehmen würden. Bei den letzteren Auswirkungen ist mit einem Umfang von bis 2 Prozent des BIPs zu rechnen. In diesem Fall stellt sich die Schätzung der verfügbaren Kapazität als äusserst schwierig heraus. Zudem haben staatliche Dienststellen und sehr grosse Unternehmen eine Tendenz zur Selbstversicherung, was dazu führt, dass ein grosser Teil allfälliger volkswirtschaftlicher Schäden unversichert sein dürfte. Man darf davon ausgehen, dass die gesamte Schweizer Wirtschaft in einem

solchen Szenario nicht zusammenbrechen würde. Es ist jedoch damit zu rechnen, dass zahlreiche KMU und andere Unternehmen nicht über eine (ausreichende) Versicherungsdeckung verfügen, sodass ihr Zusammenbruch allenfalls mit staatlichen Interventionen verhindert werden müsste.

5.2 Notwendige Massnahmen aus der Sicht der Assekuranz

Aufgrund der Diskussion in der Arbeitsgruppe des SVV, der Erkenntnisse im Vernehmlassungspapier NCS 2.0 und der Ergebnisse aus der Meinungsumfrage des gfs-zürich vom Herbst 2017 sind folgende Massnahmen zu realisieren:

Massnahmen die der Bund alleine oder gemeinsam mit der Wirtschaft umsetzen sollte.

1 Das Bewusstsein bei den KMU für die Gefahren durch Cyber-Risiken muss deutlich erhöht werden. Entsprechende Kampagnen sind zu führen oder zu unterstützen. Generell muss die Öffentlichkeit für Cyber-Risiken sensibilisiert werden (Awareness). Dazu ist u.a. die Erstellung und Umsetzung eines Kommunikationskonzeptes notwendig.
2 Der Kompetenz- und Wissensaufbau ist zu fördern. Dazu gehört auch der Ausbau der Fähigkeiten zur Beurteilung und Darstellung der Cyber-Bedrohungslage.
3 Das Resilienz-Management auf Unternehmensebene ist einzuführen bzw. auszubauen, insbesondere um das volkswirtschaftliche Akkumulationsrisiko zu vermindern und damit die Versicherbarkeit von Cyber-Risiken auch künftig zu ermöglichen.
4 Die Evaluierung und Einführung eines Minimalstandards ist zwingend und stösst grundsätzlich auf Zustimmung. Die Evaluierung eines (Bundesstandards) und/ oder mehrerer Standards (Branchenstandards) und die entsprechende Einführung ist deshalb voranzutreiben.
5 Eine Meldepflicht für Cyber-Vorfälle stösst eher auf Zustimmung als auf Ablehnung. Die Prüfung einer konkreten Meldepflicht sowie der Entscheid über die Einführung sind deshalb durch die zuständigen Bundesstellen an die Hand zu nehmen.
6 Der Aufbau von Dienstleistungen für alle Arten von Unternehmungen durch den Bund (z.B. Beratungen, Auskunftserteilung etc.) ist zu realisieren.
7 Die Strafverfolgung beim Vorliegen von Cyber-Kriminalität ist national und international konsequent anzuwenden und voranzutreiben, um so die Zahl der künftigen Schadenfälle zu reduzieren.
8 Eine nationale und internationale Kooperation (z.B. gemeinsame Schadenstatistik, Krisenmanagement, Bedrohungslage, etc.) ist zwingend, das gilt auch für den Versicherungsbereich.

Zusätzlich zu den oben genannten Massnahmen, bei welchen der Staat eine führende Rolle übernehmen muss, soll die Versicherungsindustrie folgende Initiativen prüfen:

9 Neben den Cyber-Bedrohungen für Industrie und Gewerbe, soll auch die Cyber-Bedrohung für Gemeindeinstitutionen analysiert werden, um möglichst gut Unterstützung für das Management der Cyber-Risiken auch auf dieser Ebene leisten zu können.

10 Die Entwicklung von Musterbedingungen für Cyber-Versicherungen ist zu prüfen und mit benachbarten Ländern zu koordinieren.

11 Die Versicherungsindustrie soll den Aufbau des Wissens im Bereich Cyber-Beratung und Schadenerledigung vorantreiben.

Referenzen

Baer, W. S. und A. Parkinson, 2007, Cyberinsurance in IT Security Management, *IEEE Security and Privacy*, 5(3): 50-56.

Bank of England, Prudential Regulation Authority, 2016, Cyber Insurance Underwriting Risk – CP39/16, http://www.bankofengland.co.uk/pra/Pages/publications/cp/2016/cp3916.aspx

, Zugriff am: 27.10.2017.

Berliner, B., 1982, *Limits of Insurability of Risks*. Englewood Cliffs, NJ: Prentice Hall.

Biener, C., 2013, Pricing in Microinsurance Markets, *World Development*, 41(1): 132-144.

Biener, C., M. Eling, und J. H. Wirfs, 2015a, Insurability of Cyber Risk: An Empirical Analysis, *Geneva Papers on Risk and Insurance*, 40(1): 131–158

Biener, C., Eling, M., und J. H. Wirfs, 2015b, Cyber Risk: Risikomanagement und Versicherbarkeit, *I.VW Schriftenreihe*, Band 54.

Böhme, R., 2005, Cyber-Insurance Revisited, Workshop on the Economics of Information Security (WEIS), Harvard University, Cambridge, MA.

Bundesamt für Gesundheit, 2015, https://www.bag.admin.ch/bag/de/home/service/zahlen-fakten/zahlen-fakten-zu-spitaelern/kennzahlen-der-schweizer-spitaeler.html

Cambridge Centre for Risk Studies, 2014, Sybil Logic Bomb Cyber Catastrophe, http://cambridgeriskframework.com/page/25, Zugriff am: 27.10.2017.

Cambridge Centre for Risk Studies, 2015, Business Blackout, http://cambridgeriskframework.com/page/20, Zugriff am: 27.10.2017.

Cambridge Centre for Risk Studies, 2016, Integrated Infrastructure: Cyber Resiliency in Society, http://cambridgeriskframework.com/page/20, Zugriff am: 27.10.2017.

Cebula, J. J. und L. R. Young, 2010, A Taxonomy of Operational Cyber Security Risks, *Technical Note CMU/SEI-2010-TN-028*, CERT Carnegie Mellon University.

European Network and Information Security Agency (ENISA), 2012, Incentives and Barriers of the Cyber Insurance Market in Europe. http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/incentives-and-barriers-of-the-cyber-insurance-market-in-europe, Zugriff am: 02.12.2013.

European Network and Information Security Agency (ENISA), 2016, The Cost of Incidents Affecting CIIs, https://www.enisa.europa.eu/publications/the-cost-of-incidents-affecting-ciis/, Zugriff am: 27.10.2017.

Gordon, L. A., Loeb, M. P. und T. Sohail, 2003, A Framework for Using Insurance for Cyber-Risk Management, *Communications of the ACM*, 44(9): 70-75.

Haas, A. und A. Hofmann, 2013, Risiken aus Cloud-Computing-Services: Fragen des Risikomanagements und Aspekte der Versicherbarkeit, *FZID Discussion Paper*, Nr. 74-2013.

Herath, H. und T. Herath, 2011, Copula Based Actuarial Model for Pricing Cyber, *Insurance Policies Insurance Markets and Companies – Analyses and Actuarial Computations*, 2(1): 7-20.

IMIA Working Group 98, 2016, Cyber Risks - Engineering Insurers Perspective, https://www.imia.com/wp-content/uploads/2016/09/IMIA-Working-Group-Paper-9816-Cyber-Risks-Rev-A002-16-09-20161.pdf, Zugriff am: 27.10.2017.

KPMG, 2017, Insurance Thinking Ahead: Versicherungen im Zeitalter von Digitalisierung und Cyber Studienteil B: Cyber.

Laury, S. K., und C. A. Holt, 2008, Chapter 84 Voluntary Provision of Public Goods: Experimental Results with Interior Nash Equilibria, in: *Handbook of Experimental Economics Results*, Volume 1: pp. 792–801.

McAfee, 2014, Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cyber-crime II, Center for Strategic and International Studies.

Paganini, P, 2015, How Much Cost a Zero-Day for an Industrial Control System? http://securityaffairs.co/wordpress/41385/cyber-crime/scada-zero-day-exploit-cost.html, Zugriff am: 27.10.2017.

PWC, 2015, Insurance 2020 & Beyond: Reaping the Dividends of Cyber Resilience.

SECO – Staatssekretariat für Wirtschaft, 2017, Gross Domestic Product Quarterly Data, https://www.seco.admin.ch/seco/en/home/wirtschaftslage---wirtschaftspolitik/Wirtschaftslage/bip-quartalsschaetzungen-/daten.html, Zugriff am: 27.10.2017.

Swiss Re, 2016, Sigma No 1/2016.

US-CERT, 2017, Alert (ICS-ALERT-17-206-01) CRASHOVERRIDE Malware, https://ics-cert.us-cert.gov/alerts/ICS-ALERT-17-206-01, Zugriff am: 27.10.2017.

Wikipedia (2017), Skriptkiddie, https://de.wikipedia.org/wiki/Scriptkiddie, Zugriff am: 27.10.2017.