Cyber-Kumulrisiko

11

Frank Cremer und Stefan Materne

Zusammenfassung

Während die Frequenz und die finanziellen Auswirkungen von Cyber-Schäden immer größere Dimensionen annehmen, haben Versicherer das volle Ausmaß dieses Risikos noch nicht verstanden. Für die Versicherungsbranche nimmt der Aspekt des Kumulrisikos eine zentrale Rolle ein. Aus diesem Grund werden die Bedeutung und Besonderheiten des Cyber-Kumulrisikos erarbeitet und der Status quo gemäß der Diskussion in der Literatur sowie der Erfahrungen aus der Praxis analysiert. Abschließend werden die Grenzen der Versicherbarkeit von Cyber-Kumulrisiken diskutiert, wie auch Möglichkeiten des versicherungstechnischen Risikotransfers.

11.1 Einleitung

Cyber-Risiken sind eine wachsende globale Herausforderung, die Regierungen, Unternehmen und Privatpersonen betrifft. Die steigende Frequenz und die wirtschaftlichen Auswirkungen verdeutlichen die Tragweite von diesen Risiken und zeigen, dass Cyber-Risiken Einfluss auf alle Bereiche unseres täglichen Lebens nehmen können. Begünstigt wird die Entwicklung dieser Risiken unter anderem durch die fortschreitende digitale Transforma-

F. Cremer (✉)
TH Köln, Institut für Versicherungswesen, Forschungsstelle Rückversicherung, Köln, Deutschland
E-Mail: frank.cremer@th-koeln.de

S. Materne
TH Köln, Institut für Versicherungswesen, Köln, Deutschland
E-Mail: stefan.materne@th-koeln.de

R. Arnold et al. (Hrsg.), *Risiko im Wandel*,
https://doi.org/10.1007/978-3-658-37071-8_11

tion, den technologischen Innovationen sowie die immer stärkere Vernetzung von Geräten mit dem Internet.

Ein Beispiel für ein realisiertes übergreifendes Cyber-Risiko ist der Cyber-Angriff im Jahre 2021 auf die Colonial Pipeline, welche schätzungsweise 45 Prozent aller verbrauchten Kraftstoffe an die US-Ostküste liefert. Der Angriff hatte zur Folge, dass das Unternehmen für mehrere Tage keinen Treibstoff über seine Pipelines liefern konnte. Aufgrund von Versorgungsengpässen und Panikkäufen stieg der Benzinpreis auf den höchsten Stand seit 2014 (vgl. Brower und McCormick 2021).

Ein ähnlicher Cyber-Angriff mit Lösegeldforderung ereignete sich im selben Jahr nur wenige Wochen später auf die irische Gesundheitsbehörde. Durch den Angriff wurden die Systeme und Dateien des Gesundheitsdienstes verschlüsselt und waren damit nicht zugänglich. Die Cyber-Kriminellen verlangten ein Lösegeld von 20 Millionen Euro von der irischen Regierung für die Übermittlung eines Codes, mit dem die betroffenen Systeme wieder hergestellt werden würden (vgl. Tidy 2021).

Diese prominenten Beispiele zeigen, welche wirtschaftlichen Auswirkungen Cyber-Risiken annehmen können. Für das Jahr 2020 wurde geschätzt, dass unzureichende Maßnahmen im Rahmen der Cyber-Sicherheit die Weltwirtschaft 945 Milliarden Dollar gekostet haben (vgl. Maleks Smith et al. 2020, S. 3).

Vor diesem Hintergrund sind insbesondere Unternehmen dazu angehalten, sich intensiv mit Cyber-Risiken auseinanderzusetzen. Je nach Ausrichtung der Geschäftstätigkeit sind sie immer mehr von Technologie abhängig. Damit einhergehend sind sie ebenfalls anfällig für Cyber-Schwachstellen, welche erhebliche Unternehmensrisiken darstellen können, wie zum Beispiel Betriebsunterbrechung (BU) und finanzielle Verluste durch Vertraulichkeitsverletzungen und Integritätsverletzungen. Im Rahmen des Risikomanagement nimmt die Cyber-Versicherung daher eine wichtige Risikotransferrolle ein.

Die steigende Gefahr und eine Veränderung des Risikobewusstseins sehen Erst- und Rückversicherer als gute Wachstums- und Investitionsmöglichen in der Absicherung von Cyber-Risiken. Durch die dynamische Entwicklung, fehlende Schadenhistorie und weitere Faktoren sind die Versicherer jedoch mit unterschiedlichen Herausforderungen bei der Bereitstellung von Versicherungsschutz konfrontiert. Als ein Teil dieser Herausforderung gilt das Cyber-Kumulrisiko.

Das Cyber-Kumulrisiko soll nachfolgend näher erläutert und seine Besonderheiten analysiert werden mit dem Ziel einer Darstellung des Status quo dieses Risikos. Durch die Berücksichtigung von Literatur und Praxis eignet sich dieses Kapitel für unterschiedliche Stakeholder der Versicherungsbranche, welche einen tiefer gehenden Einblick in die Cyber-Kumulrisiken erhalten möchten. Darüber hinaus werden die derzeitigen Geschehnisse und Entwicklungen von Cyber-Kumulen im Rahmen des versicherungstechnischen Risikotransfers berücksichtigt.

Um ein allgemeines Verständnis des Cyber-Kumulrisikos zu geben, erfolgt zunächst eine eingehende Betrachtung dieses Risikos. Hierzu wird auf die Begriffe *Cyber-Risiko* und *Kumulrisiko* genauer eingegangen. Darauf aufbauend erfolgt eine Darstellung des *Cyber-Kumulrisikos* und seiner Aspekte. Im Anschluss werden ausgewählte Möglichkei-

ten des *versicherungstechnischen Risikotransfers* zur Bewältigung dieses Risikos aufgezeigt und erläutert. Abschließend werden die *Grenzen der Versicherbarkeit* von Cyber-Kumulrisiken und die aktuellen *Trends in der Praxis* behandelt.

11.2 Betrachtung des Cyber-Kumulrisiko

Der Begriff **Cyber-Kumulrisiko** ist die Komposition der Begriffe *Cyber-Risiko* und *Kumulrisiko*. Aufgrund der relativen Neuartigkeit dieses Begriffs hat sich eine eindeutige Begriffsbestimmung noch nicht etabliert. Um eine klare Vorstellung des Begriffs Cyber-Kumulrisiko zu vermitteln, erfolgt im nächsten Abschnitt die Definition und kurze Erläuterung des Cyber-Risikos sowie des Kumulrisikos.

11.2.1 Cyber-Risiko

Für den Begriff **Cyber-Risiko** finden sich in der wissenschaftlichen sowie in der praxisbezogenen Literatur unterschiedliche Auslegungen. Diese können in der Regel mal eng oder breit gefasst sein, wobei der Trend hin zu einer breit gefassten Definition verläuft. Die Gründe liegen u. a. in der Neuartigkeit dieses Begriffes sowie in der fortlaufenden Digitalisierung und dem damit einhergehenden, sich verändernden Risikoverständnis. Nachfolgend wird die häufig zitierte Definition von Cebula und Young verwendet, bei der Cyber-Risiken beschrieben werden als

> *„operational risks to information and technology assets that have consequences affecting the confidentiality, availability, and/or integrity of information or information systems“.* (Cebula und Young 2010, S. 1)

Die Ursachen für Cyber-Risiken sind vielfältig, weswegen mit Abb. 11.1 eine Taxonomie zur Verfügung gestellt wird, die die Komplexität dieses Risiko verdeutlichen soll.

Den höchsten Anteil der Ursachen von Cyber-Risiken belegt das *menschliche Verhalten*. Dieses beinhaltet insbesondere ein bewusstes Handeln, welches zur Cyber-Kriminalität und deren Cyber-Angriffe zugerechnet wird. Ein Cyber-Angriff verfolgt meist das Ziel, die informationstechnischen Systeme des betroffenen Unternehmens („Targets“) ganz oder teilweise zu beeinträchtigen oder sogar komplett außer Betrieb zu setzen. Weitere Ziele von Cyber-Angriffen sind die Spionage oder Korrumpierung von Daten. Darüber hinaus verschaffen sich Cyber-Kriminelle u. a. über andere Hilfsmittel Zugang zu den Systemen der Targets. Zum Beispiel kann durch das Anklicken von infizierten Emails oder Webseiten Software heruntergeladen werden, mit deren Hilfe die Kriminellen die Systeme verschlüsseln und die Benutzer dadurch aussperren. Im weiteren Verlauf werden die Targets kontaktiert und mit Lösegeldforderungen erpresst. Häufig beinhalten diese Erpressungen zwei Drohungen – zum einen wird gedroht die Systeme weiterhin verschlüsselt zu

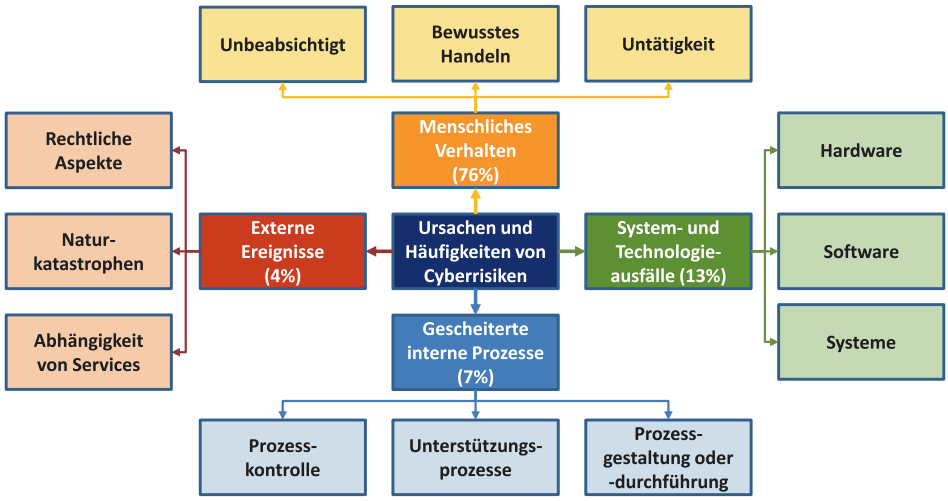

Abb. 11.1 Ursachen und Häufigkeiten von Cyber-Risiken. (Quelle: eigene Darstellung; vgl. Cebula und Young 2010, S. 1 sowie Eling und Wirfs 2019, S. 1113) (Die relativen Häufigkeiten aus den zitierten Quellen beziehen sich auf eine Gesamtzahl von 1579 Cyber-Schäden)

Tab. 11.1 Finanzielle Auswirkungen von Cyber-Risiken. (Quelle: eigene Darstellung)

Kategorie	Finanzielle Auswirkungen
Eigenschäden	• Betriebsunterbrechung. • Kosten für Ermittlungs- und Ersatzmaßnahmen. • Wiederherstellungskosten. • Kosten für die Hinzuziehung eines Krisenmanagements. • Kosten für die Kommunikation mit Stakeholdern.
Drittschäden	• Schadenersatzansprüche von Dritten. durch aus der Verletzung von Datenschutzbestimmungen. • Kosten für Rechtsstreitigkeiten. • Datenschutzrechtliche Maßnahmen (z. B. Informationen von Kunden). • Kosten für die Wiederherstellung von Daten.

lassen, was einer Betriebsunterbrechung oder Störung gleichkäme – zum anderen wird insbesondere Unternehmen gedroht, die Kundendaten im Darknet zu veröffentlichen, was weitere negative Konsequenzen für das Unternehmen nach sich ziehen könnte.

So vielfältig wie Cyber-Risiken sind, so differenzierbar sind ebenfalls deren Auswirkungen. In der versicherungsbezogenen Literatur werden die Cyber-Schäden in zwei Kategorien eingeteilt. So können Schäden, die dem Unternehmen selbst entstanden sind, in die Kategorie *Eigenschäden* zugeordnet werden. Cyber-Schäden, welche eine Haftung gegenüber Dritten hervorrufen, können in die zweite Kategorie *Drittschäden* eingeordnet werden.

Tab. 11.1 zeigt eine Auswahl an Eigen- und Drittschäden, welche durch ein realisiertes Cyber-Risiko entstehen können.

11.2.2 Kumulrisiko

Der Begriff **Kumulrisiko** wird in der Literatur als Art des Zufallsrisiko beschrieben, welches wiederum eine Ausprägung des versicherungstechnischen Risikos darstellt. Im Rahmen der Kernleistung eines Versicherers – dem Risikotransfer – ergibt sich das versicherungstechnische Risiko

> „*aus der Streuung der Gesamtschadenverteilung eines Kollektivs, d. h. der potenziellen bzw. tatsächlichen Abweichung vom Erwartungswert*". (von der Schulenburg und Lohse 2014, S. 62)

Für Versicherungsunternehmen besteht in diesem Kontext die Gefahr eines Restrisikos, welches für die betrachtete Periode einen technischen Ruin bedeuten könnte. Unterteilt wird das versicherungstechnische Risiko in drei verschiedene Ausprägungen: das *Änderungsrisiko*, das *Irrtumsrisiko* sowie das *Zufallsrisiko*. Für das Verständnis in den nachfolgenden Ausführungen ist das Irrtumsrisiko relevant. Das Zufallsrisiko beschreibt die zufällige Abweichung des tatsächlichen Gesamtwertes der Schäden vom Erwartungswert.

Das *Kumulrisiko* bezeichnet den zufälligen Umstand, dass mehrere Risiken nicht unabhängig voneinander sind und ein einzelnes Schadenereignis zu einer Vielzahl an Schäden bei versicherten Risiken gleichzeitig führt (vgl. Farny 2011, S. 85).

Für die Versicherungsbranche bedeuten Kumulrisiken eine große Herausforderung, da sie erkannt und richtig eingeschätzt werden müssen. Diese Risiken haben zwar in der Regel eine niedrige Eintrittswahrscheinlichkeit, können jedoch im Eintrittsfall zu einem massiven Schadenaufwand führen durch die Vielzahl der betroffenen Risiken.

Die Gründe für das Entstehen von Kumulrisiken sind vielseitig und können je nach Blickwinkel andere Formen annehmen. Erstversicherer können diesem Risiko unterliegen, wenn sie zum Beispiel viele Risiken in einer Region zeichnen. Die Realisierung des Kumulrisiko spiegelt sich zudem in der jeweiligen Gefahr wider. So können ein Erdbeben oder ein Hagelschaden in der jeweiligen Region dazu führen, dass viele Risiken gleichzeitig von demselben Ereignis betroffen sind. Erstversicherer können im Rahmen ihres Risikomanagement unterschiedliche Maßnahmen ergreifen, um dieses Risiko zu minimieren. Ein risikopolitisches Tool ist der versicherungstechnischen Risikotransfer mithilfe der Rückversicherung. Durch die Bereitstellung entsprechender Kapazitäten müssen Rückversicherer darauf achten, dass ihre Risiko-Portfolien eine möglichst breite Diversifizierung (zum Beispiel geografisch, nach Sparten etc.) aufweisen.

11.2.3 Cyber-Kumulrisiko

Nachdem zuvor die Grundlagen erläutert und dargestellt wurden, erfolgt nun die tiefer gehende Einführung in das Cyber-Kumulrisiko. Aufbauend auf den vorherigen Begriffen bezeichnet das **Cyber-Kumulrisiko** ein einzelnes Schadenereignis, bei dem sich das

Cyber-Risiko realisiert und eine große Anzahl an versicherten Risiken gleichzeitig betroffen ist.

Im Gegensatz zu den traditionellen Kumulrisiken (Hagel, Sturm, Erdbeben etc.) weist das Cyber-Kumulrisiko einige Besonderheiten auf. So werden bei der Kumul-Modellierung der traditionellen Gefahren die Abhängigkeiten der unterschiedlichen Risiken zu einem sogenannten „Footprint" erfasst, welcher die räumliche Ausdehnung eines Szenarios erfasst und das Ausmaß eines Schadenereignisses einschätzt (vgl. Glaab 2018).

Für das Cyber-Kumulrisiko gestaltet sich eine solche Einschätzung von Footprints als Herausforderung. Die Gründe hierfür liegen u. a. in dem stetig wachsenden privaten Gebrauch von *Internet of Things Geräten*, in der übergreifenden Nutzung *homogener Hard-* und *Softwarekomponenten*, in der fortschreitenden Digitalisierung von *Wertschöpfungsketten* sowie in einer kontinuierliche Vernetzung der Industrie mithilfe der *Cloud* und des *Internets* (vgl. Hofmann und Wilson 2018, S. 15 ff.).

Diese weitreichende Vernetzung führt dazu, dass Cyber-Kumulrisiken sich nicht auf bestimmte Regionen beschränken, sondern global und übergreifend zwischen unterschiedlichen Branchen und Bereichen verbunden sind. Diese Komplexität der Vernetzung zeigt, dass diese Verbindungen weder offensichtlich noch leicht nachvollziehbar sind. Ein Beispiel für ein solchen übergreifenden Schaden ist der Ransomware-Angriff „Wannacry" im Jahre 2017. Die Erpressungssoftware nutzte eine Schwachstelle von nicht gepatchten Microsoft-Systemen und -Servern aus und verschlüsselte global rund 230.000 Computer in ca. 150 Ländern. Laut dem Sicherheitssoftwareanbieter Kaspersky betrug der Schaden schätzungsweise vier Milliarden Dollar (vgl. Kaspersky 2018).

Ein weiterer Aspekt ist die Unklarheit der Realisation von Schäden. So kann es sein, dass bereits ein Cyber-Ereignis eingetreten ist, jedoch noch nicht bemerkt wurde. Vor diesem Hintergrund steigt im zeitlichen Verlauf der Gesamtschaden durch die weitere Verbreiterung, bis dieser erkannt wird.

Eine weitere Herausforderung stellt die unklare und fehlende einheitliche Definition von Cyber-Risiken in Versicherungsprodukten dar. Derzeit verwenden die Cyber-Versicherer unterschiedliche Begriffsbestimmungen in ihren Versicherungsbedingungen, um den Versicherungsfall zu bestimmen. Dies führt dazu, dass die Versicherungsnehmer oft im Unklaren sind, ob gewisse Cyber-Schäden überhaupt versichert sind. Im Jahre 2017 wurden nur 28 Prozent der gemeldeten Schadenansprüche anerkannt (vgl. Bermuda:Re+ILS 2021).

Als weiterer Aspekt im Rahmen des Cyber-Kumulrisikos gilt *Silent Cyber*. Da diese Problematik eine eigenständige Abhandlung rechtfertigen würde, wird an dieser Stelle der Vollständigkeit halber nur auf sie verwiesen. Bei Silent Cyber besteht die Gefahr, dass bereits das Cyber-Risiko in anderen herkömmlichen Versicherungsverträgen (zum Beispiel Sach) unbewusst mitversichert und nicht als Stand-Alone Cyber-Versicherung versichert ist. Diese Exponierung führt dazu, dass die Prämien der betroffenen Versicherungsverträge viel zu niedrig kalkuliert wurden und sich das in einem Schadenfall entsprechend negativ für die betroffenen Versicherer auswirken kann. Diese genannten Besonderheiten von Cyber-Kumulrisiken erschweren eine korrekte Einschätzung durch die Versicherer im Vergleich zu den traditionellen Kumulrisiken.

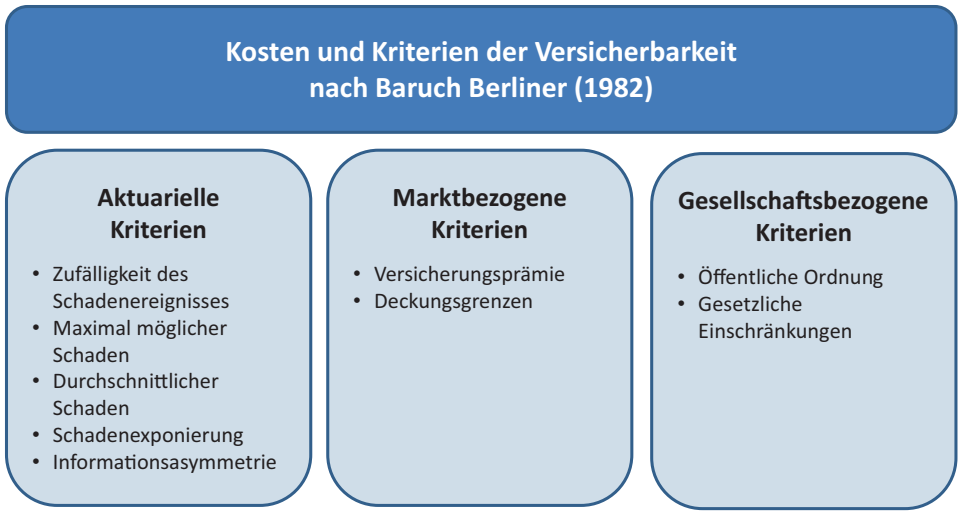

Abb. 11.2 Kriterien der Versicherbarkeit. (Quelle: eigene Darstellung; vgl. Berliner 1982, S. 325 sowie Biener et al. 2015, S. 138)

11.2.4 Unterteilung der Cyber-Kumulrisiken

Derzeit lassen sich die wesentlichen Cyber-Kumulrisiken in zwei große Kategorien einteilen. Die erste Kategorie betrifft diejenigen Kumule, welche modellierbar und somit *versicherbar* sind. Die andere Kategorie betrifft Kumulrisiken, welche sich derzeit nicht konkret in Modellen abbilden lassen und damit für Versicherer noch *nicht versicherbar* sind. Für den weitere Verlauf werden zuerst nur die versicherbaren Cyber-Kumulrisiken behandelt und im Rahmen des versicherungstechnischen Risikotransfers betrachtet. Eine gesonderte Betrachtung der nicht versicherbaren Cyber-Kumulrisiken erfolgt im Abschnitt zu den Grenzen der Versicherbarkeit.

Bevor eine Erläuterung zu den Arten von Cyber-Kumulrisiken erfolgt, sollen in Abb. 11.2 die Kriterien der Versicherbarkeit nach Baruch Berliner aufgezeigt werden (vgl. Berliner 1982).

Aufgrund der fehlenden Historie von Cyber-Schäden orientieren sich die Versicherer am Beispiel von bekannten und erprobten Modellierungen. So verwenden sie die Erkenntnisse der Risikomodellierung von Naturkatastrophen oder kombinierte Ansätze aus anderen Versicherungssparten (vgl. Sigma 2017, S. 38).

Zwar können im Laufe der Zeit die Daten zu Cyber-Schäden gesammelt und ausgewertet werden, jedoch unterliegen diese Daten ständigen Änderungen aufgrund der schnellen Entwicklung von Cyber-Risiken.

11.2.4.1 Malware Bedrohungen und Sicherheitslücken

Der Begriff **Malware** ist eine Zusammensetzung der englischen Begriffe „malicious“ und „Software“ und wird als Abkürzung für schädliche Software oder Software, die in einen Computer einzudringen versucht, verwendet. Unter diesem Oberbegriff werden in der Li-

teratur verschiedenste Arten von schädlichen Programmen bezeichnet. Bekannte Beispiele hierfür sind beispielsweise

- *Ransomware* (das heißt Schadenprogramme, die Systemzugriffe beschränken, und für deren Abschaltung Lösegeldforderungen erfüllt werden müssen),
- *Spyware* (das heißt Spähprogramme bzw. Spionagesoftware),
- *Trojaner* (das heißt Programme, die unbemerkt andere Programme installieren),
- *Viren* (das heißt sich selbst verbreitende Programme, die sich in andere Programme einschleusen) sowie
- *Würmer* (das heißt Schadenprogramme, die sich selbstständig verbreiten).

Durch die Verwendung von identischer Soft- und Hardware der Unternehmen können dieselben Sicherheitslücken bei unterschiedlichen Industrie- und Branchensektoren gefunden werden. In diesem Kontext können die Cyber-Kriminellen diese Schwachstellen bei anderen Unternehmen, welche die gleiche Soft- und/oder Hardware verwenden, für ihre Zwecke ausnutzen. Dadurch ist es möglich, dass die Kriminellen in einem geplanten Cyber-Angriff viele Unternehmen gleichzeitig an dieser Schwachstelle attackieren und mit der entsprechenden Malware für eine große Verbreitung sorgen. Dadurch ist es möglich, dass unter Umständen weitere Unternehmen durch die Malware in der Lieferkette betroffen sind.

Für dieses Cyber-Kumulrisiko können unterschiedliche Szenarien in Frage kommen. Ein erfolgreicher Ransomware-Angriff wie „NotPetya“ oder „WannaCry“ kann dazu führen, dass durch eine Sicherheitslücke eine große Anzahl an Unternehmen gleichzeitig betroffen ist. Neben Ransomware können andere Malware Attacken ähnliche wirtschaftliche Auswirkungen erreichen. Für Unternehmen bedeutet dies meist eine Betriebsunterbrechung mit entsprechender Leistung für den Versicherer. Der Versicherer kann aber auch aufgrund von Drittschäden – zum Beispiel Schadenersatzansprüche von Dritten aufgrund des Cyber-Vorfalls – herangezogen werden.

11.2.4.2 Ausfall von IT-Service Providern

Das hohe Maß an Interkonnektivität der Unternehmen wird als eines der größten Cyber-Kumulrisiken eingestuft (vgl. Hofmann und Wilson 2018, S. 14–15).

Unterstützt wird diese Vernetzung der Unternehmen insbesondere durch die Cloud Service Provider (CSPs), welche im Rahmen ihrer Geschäftstätigkeiten meist identische Produkte wie *Software as a Service*, *Plattform as a Servie* und *Infrastructure as a Service* umfassen. Eine steigende Anzahl an Unternehmen nutzen diese Services, indem sie u. a. Teile ihrer Datenspeicherung, -verarbeitung und -analyse sowie der IT-Infrastruktur auslagern. Je nach gewähltem Service und Modell sind diese skalierbar und passen sich den jeweiligen Bedürfnissen der Unternehmen an.

Mit Blick auf das Cyber-Kumulrisiko wird deutlich, dass sich Unternehmen mit anderen Unternehmen durch CSPs verbinden, die in ihren herkömmlichen Geschäftsbereichen keine Verbindungen beziehungsweise Überschneidungen hätten. So kann ein Kumul bereits dadurch entstehen, dass mehrere per se unabhängige Unternehmen beispielsweise die IT-Infrastruktur von CSPs nutzen und dadurch abhängig werden (vgl. Cambridge Centre for Risk Studies 2020, S. 40 ff.).

Die Abhängigkeit der Unternehmen ergibt sich durch die Verfügbarkeit der Services von CSPs. Diese können jedoch auch von Ausfällen oder Beeinträchtigungen betroffen sein. Beispiele hierfür sind:

- Beschädigung von Server-Standorten durch Naturkatastrophen oder physische Einwirkung,
- Ausfall von Versorgungsleistungen wie zum Beispiel Strom oder Kühlsysteme,
- Ausfall oder Beeinträchtigung der Cloud Systeme aufgrund eines Cyber-Angriffs sowie
- Ausfall des internen Softwaresystems durch Unfälle.

Folgen für die Unternehmen wären in diesem Zusammenhang Eigenschäden wie zum Beispiel *Betriebsunterbrechung*, der *Verlust von Daten* oder *Imageschäden* aufgrund fehlender Verfügbarkeit der angebotenen Dienstleistungen. Im Hinblick auf Drittschäden können Schadenersatzansprüche von Dritten durch unterschiedliche Konstellationen erfolgen.

Ein übergeordnetes Cyber-Kumulrisiko besteht zudem bei der Auswahl von CSPs. Im Juli 2021 hatten allein die drei größten Anbieter Amazon, Microsoft und Google einen Marktanteil von ca. 63 Prozent in diesem Segment (vgl. Synergy Research Group 2021).

Auch wenn diese Cloud Zentren über höchste Sicherheitsstandards verfügen, besteht jedoch immer ein Restrisiko, welches ein immenses Schadenpotenzial beinhaltet.

11.2.4.3 Data Breach

Im englischsprachigen Gebrauch bezeichnet **Data Breach** einen Cyber-Vorfall, bei dem sensible, vertrauliche oder geschützte Daten ohne Autorisierung kopiert, übertragen, gestohlen, eingesehen oder verwendet wurden.

In Tab. 11.2 sollen ausgewählte Arten von Daten Aufschluss darüber geben, welche Daten bei einem Data Breach betroffen sein könnten.

Tab. 11.2 Betroffene Daten bei einem Data Breach. (Quelle: eigene Darstellung; vgl. Cambridge Centre for Risk Studies 2020, S. 25)

Arten von Daten	Beispiele
Persönliche Identitätsdaten	• Vollständiger Name • Kontaktdaten • Ausweisdaten • Sozialversicherungsnummer
Zahlungs- und Kreditkarteninformationen	• Kontodaten • Zugangsdaten • PIN
Gesundheitsdaten	• Krankenakte • Biometrische Identifikationen
Kommerzielle Daten	• Geschützte Geschäftsinformationen • Daten zu Geschäftspartnern • Patente

Ein Data Breach kann sich auf unterschiedliche Weisen ereignen. So können die Daten durch fehlerhaftes menschliches Verhalten in den Einflussbereich von nicht autorisierten Empfängern gelangen. In den letzten Jahren haben jedoch Kriminelle Lukrativität und den Wert von Daten für sich entdeckt. So versuchen Cyber-Kriminelle sich mithilfe von Malware Zugang zu den Daten von Unternehmen zu beschaffen und diese für ihre kriminellen Zwecken zu nutzen (zum Beispiel Verkauf der Daten im Darknet). Für betroffene Unternehmen kann dies unterschiedliche und starke finanzielle Auswirkungen haben, welche nachfolgend beispielhaft aufgeführt sind:

- Kosten für Kreditmonitoring, Forensik, PR-Agenturen und Benachrichtigungen der betroffenen Personen,
- Entschädigungszahlungen an alle Stakeholder, deren Daten kompromittiert wurden (Kunden, Mitarbeiter, Lieferanten etc.),
- Lösegeldzahlungen sowie
- Bußgelder und Kosten für Rechtsstreitigkeiten.

Das Cyber-Kumulrisiko bei Data Breaches setzt sich aus unterschiedlichen Komponenten zusammen. Hierzu gehört der stetig wachsende Umfang an Daten, welche das Unternehmen während seiner Geschäftstätigkeit sammelt und benötigt. Die Zunahme kann zwar geschätzt werden, liefert jedoch keine genauen Angaben, wie viele Datensätze bei einem Data Breach betroffen sein könnten. Eine weitere Komponente ist die kriminelle Weiterverwendung der erbeuteten Daten. Diese Unklarheit führt zu mehreren Szenarien, mit denen ein Versicherer konfrontiert ist.

11.3 Ausgewählte Möglichkeiten des VT-Risikotransfers von Cyber-Kumulrisiken

Nachfolgend werden ausgewählte Möglichkeiten des versicherungstechnischen Risikotransfers hinsichtlich des Cyber-Kumulrisikos erläutert. Als Ausgangspunkt für eine Betrachtung kann ein Cyber-Portfolio eines Erstversicherers herangezogen werden. Durch die Gewährung von Versicherungsschutz gegenüber seinem Versicherungsnehmer nimmt der Erstversicherer eine Vielzahl von Cyber-Risiken in sein Risiko-Portfolio auf. Durch die schwer einschätzbaren Cyber-Risiken und die Anhäufung dieser Risiken steigt die Gefahr von Cyber-Kumulrisiken beim Erstversicherer. Vorab hat der Cyber-Versicherer bereits die Möglichkeit, mithilfe von risikopolitischen Maßnahmen wie zum Beispiel einer restriktiven *Zeichnungspolitik*, *Gestaltung des Versicherungsproduktes*, *Selbstbehalte* sowie *Begrenzungen der Versicherungsleistungen* Einfluss auf das Cyber-Kumulrisiko zu nehmen; dies ist jedoch nicht Gegenstand der vorliegenden Betrachtung.

Vor dem Hintergrund der bisher gezeigten Beispiele wird für den Erstversicherer deutlich, dass die alleinige Tragung des Cyber-Kumulrisikos eine existenzielle Gefährdung für den Geschäftsbetrieb darstellt.

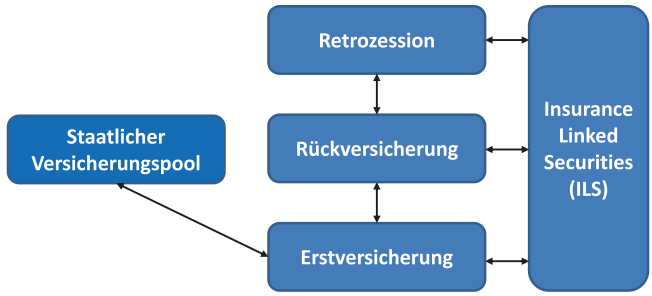

Abb. 11.3 Möglichkeiten des versicherungstechnischen Risikotransfers. (Quelle: eigene Darstellung)

Um dieses versicherungstechnische Risiko zu reduzieren bzw. zu teilen, stehen unterschiedliche Möglichkeiten des Risikotransfers zur Verfügung, die in Abb. 11.3 dargestellt sind.

11.3.1 Rückversicherung

Eine klassische Form des versicherungstechnischen Risikotransfers ist die **Rückversicherung**. Dabei gibt der Erstversicherer einen Teil seiner Risiken an einen Rückversicherer weiter. Der Rückversicherer erhält für die Bereitstellung seiner Versicherungskapazitäten vom Erstversicherer eine Prämie. In der Rückversicherung gibt es unterschiedliche Formen und Techniken, um Risiken zu (rück)versichern. Mit dem Fokus auf Cyber-Kumulrisiken sollen zwei ausgewählte Beispiele vorgestellt werden, wie ein Erstversicherer sein Kumulrisiko begrenzen kann.

11.3.1.1 Summenexzedent

In dieser Form der *proportionalen Rückversicherung* wird die Aufteilung des Risikos nicht anhand einer festen Quote bestimmt, sondern obliegt in der Entscheidung des Erstversicherers (im Hinblick auf die Gestaltung des Rückversicherungsvertrages), bis zu welcher Versicherungssumme er pro Risiko maximal haften möchte. Der Selbstbehalt des Erstversicherer wird in einer absoluten Summe vereinbart. Die Aufteilung der Risiken erfolgt im Verhältnis von Selbstbehalt zu hinausgehender Versicherungssumme (vgl. Liebwein 2018, S. 77).

Durch diese Vertragskonstellation erreicht der Erstversicherer eine stärkere Homogenisierung seines Risiko-Portfolios nach Rückversicherungsnahme („Netto-Risiko-Portfolio“) und entlastet sich bis zu einem gewissen Grad von Haftungsspitzen.

11.3.1.2 Kumulschadenexzedent

Der Kumulschadenexzedent zählt zu den Formen der *nicht-proportionalen Rückversicherung*. Diese Form der Rückversicherung deckt ein Schadenereignis, bei dem die kumulierten Schäden des Erstversicherers den vorher vereinbarten Selbstbehalt überstei-

gen. Der Rückversicherer übernimmt den Anteil des Schadenaggregats, der oberhalb des Selbstbehaltes des rückversicherten Erstversicherers liegt. Begrenzen kann der Rückversicherer seine Haftung mit der Festlegung einer Haftstrecke. Wenn dieses Limit überschritten wird, geht der überschießende Schadenanteil wieder auf den Erstversicherer zurück. Für den Erstversicherer bietet diese Form eine effektive Absicherung seines Kumulrisikos (vgl. Schwepcke und Vetter 2017, S. 190–191).

11.3.2 Retrozession

Ausgehend vom Rückversicherer können die Risiken weiter transferiert werden. Unter dem Begriff **Retrozession** wird der Vorgang bezeichnet, bei dem ein Rückversicherer einen Teil des Risikos weitergibt. Begründet wird dieser Ablauf mit dem Bedarf der Absicherung aufgrund des versicherungstechnischen Risikos, welchem der Rückversicherer ausgesetzt ist (vgl. Liebwein 2018, S. 365).

Beispiele für die Motivation zur Retrozessionsnahme sind erhöhte Kumulgefahren oder auch Limitierungen der Haftung des Rückversicherers. Der Retrozessionär – also der Risikoträger, der Teile des Risikos des Rückversicherers übernommen hat, kann wiederum das Risiko oder Teile davon an weitere Versicherer transferieren. Dieser Vorgang trägt die gleiche Bezeichnung, kann jedoch als Retrozession höherer Art angesehen werden. Beachtet werden sollte in diesem Zusammenhang, dass ein Risikoträger im Rahmen eines Schadenfalls durch die Retrozession möglicherweise in größerer Weise beteiligt ist als ursprünglich angenommen.

11.3.3 Insurance Linked Securites

Neben der Rückversicherung gibt es die Möglichkeit, den Kapitalmarkt in den versicherungstechnischen Risikotransfer einzubinden. Unter der Bezeichnung **Insurance Linked Securites** (ILS) werden versicherungsbezogene Risiken an den Kapitalmarkt abgetreten. Als Schnittstelle für den Kapitalmarkt und den Erst- oder Rückversicherer wird häufig ein Special Purpose Vehicle (SPV) eingesetzt. Am Beispiel eines Insurance Linked Bonds soll dieser Vorgang näher erläutert werden. Zu Beginn emittiert das SPV an Investoren originäre Finanztitel, die eine verbriefte Bindung an versicherungstechnische Risikoereignisse beinhalten (vgl. Liebwein 2018, S. 499).

Dabei ist das Schadenereignis durch Trigger definiert. Am Beispiel von Cyber-Risiken sind parametrische Trigger mit folgenden Definitionen denkbar:

- Anzahl an gestohlenen Datensätzen,
- Schweregrade an infizierten Systemen durch Malware,
- Bußgelder im Rahmen von Datenschutzverletzungen sowie
- Dauer von Cyber-bedingten Betriebsunterbrechungen.

Das SPV finanziert sich durch Ausgabe der Insurance Linked Bonds und investiert die Erlöse in Wertpapiere. Diese werden wiederum in einem besicherten Fonds verwaltet. Sollte das Schadenereignis mithilfe des Triggers eintreten, erhält der Versicherer die finanziellen Mittel vom SPV gemäß eines vorher vereinbarten Rückversicherungsvertrags. Das verbleibende Kapital wird am Ende der Laufzeit vom SPV an die Investoren ausgeschüttet (je nach Form inkl. eines jährlichen Kupons). Für Versicherer und Kapitalmarkt besteht eine hohe Motivation an der Einbindung von ILS in den versicherungstechnischen Risikotransfer. Die Versicherer können durch ILS die eigene Risikotragfähigkeit erhöhen. Die Motivation des Kapitalmarktes liegt in dem Abschluss eines profitablen Geschäfts, welches zudem die Diversifikation des Portfolios aufgrund von niedrig korrelierten Assets („Markowitz-Effekt“) verbessert.

11.3.4 Staatlicher Versicherungspool

In Anlehnung an andere Kumulrisiken wie zum Beispiel Terror (Terror Risk Insurance Act 2005, Pool Re im Vereinigten Königreich) oder Naturkatastrophen (japanisches Erdbebenrückversicherungsprogramm) ist es möglich, den Staat als Versicherungspool im Hinblick auf den versicherungstechnischen Risikotransfer zu betrachten. Der Staat kann dadurch als eventuelle Übergangslösung die Bildung eines Cyber-Versicherungsmarktes unterstützen, indem er eine Entwicklungsumgebung von Cyber-Versicherung für die Versicherungswirtschaft schafft (vgl. Schweizerischer Versicherungsverband 2018, S. 22).

11.4 Grenzen der Versicherbarkeit

Wie bereits vorab beschrieben lassen sich Cyber-Kumulrisiken derzeit in nicht versicherbare und versicherbare Kumule unterscheiden.[1] Letztere wurden bereits eingehend beschrieben. In diesem Abschnitt soll nun die Grenzen der Versicherbarkeit von Cyber-Kumulrisiken aufgegriffen werden. Diese Grenzen werden von den Versicherern selbst gesetzt. Durch nicht-kalkulierbare bzw. nicht-modellierbare Risiken gehen Versicherer das Risiko eines versicherungstechnischen Verlusts bis hin zu einem Ruin ein. Als beispielhafte Cyber-Ausschlüsse werden die Allgemeinen Ausschlüsse der Allgemeinen Versicherungsbedingungen für die Cyber-Risiko-Versicherung (AVB Cyber) des Gesamtverbandes der Deutschen Versicherungswirtschaft e. V. (GDV) herangezogen. Vorab sei jedoch darauf hingewiesen, dass es sich hierbei um Musterbedingungen handelt und die Bedingungswerke in der Praxis auch untereinander große Unterschiede in allen Bereichen aufweisen.

Für ein besseres Verständnis erfolgt eine kurze Aufstellung der Cyber-Ausschlüsse ohne weitere Beschreibungen in Tab. 11.3.

[1] Für eine weitergehende Diskussion zu den Grenzen der Versicherbarkeit vgl. auch Kap. 8 in diesem Band.

Tab. 11.3 Allgemeine Cyber-Ausschlüsse. (Quelle: eigene Darstellung; vgl. GDV 2017, S. 11 ff.)

Vorvertragliche Informationssicherheitsverletzung	Krieg
Politische Gefahren	Terrorakte
Ausfall von Infrastruktur	Fahrzeuge
Löse-/Erpressungsgeld	Finanzmarkttransaktionen
Abfluss von Vermögenswerten	Vorsatz und wissentliche Pflichtverletzung
Behördliche Maßnahmen, Strafen/Bußgelder	Verletzung von Immaterialgüterrechten
Kernenergie	Diskriminierung

Ein Großteil der gezeigten Cyber-Ausschlüsse ist deckungsgleich mit Ausschlüssen anderer Versicherungssparten. Mit dem Abgleich von anderen Bedingungswerken aus der Praxis wird ersichtlich, dass *Krieg* (Cyberwar) und *Terrorakte* (Cyberterror) sowie der Ausfall von Infrastruktur nicht versicherbar bzw. ausgeschlossen waren. Die ersten beiden Beispiele verdeutlichen die Grenzen der Versicherbarkeit,

> *„weil sie einen potenziellen existenzgefährdenden Einfluss auf ein Unternehmen haben und darüber hinaus gesamtwirtschaftliche Auswirkungen haben können“*. (Baban et al. 2018, S. 4)

Durch die Beschaffenheit des Cyber-Risikos besteht Unklarheit, inwiefern sich das Risiko realisiert hat. So kann ein erfolgreicher Cyber-Angriff durch einen anderen Staat finanziell unterstützt sein und somit unter den Kriegsausschluss fallen. Somit wäre dieser Cyber-Schaden nicht gedeckt.

Als Beispiel für einen solchen Versicherungsfall ist die Cyber-Angriffsserie der „Petya“ Ransomware. Die Urheber der Software verschlüsselten die Systeme der Unternehmen und verursachten dadurch Schäden in Milliardenhöhe. Zudem forderten sie ein Lösegeld der Targets. Im Zuge dieses Angriffes in Jahre 2017 wurden beim Unternehmen Mondolez 1700 Server sowie zehntausende Laptops unwiederbringlich zerstört. Der damalige Cyber-Versicherer Zurich verweigerte die Zahlung der Versicherungsleistung mit der Begründung, dass es sich um feindliche und kriegerische Handlungen gehandelt habe (vgl. Ferland 2019, S. 1).

Als letzter Cyber-Ausschluss wird der Ausfall von Infrastruktur behandelt. Ein **Ausfall der Infrastruktur** liegt vor, wenn

- Gebietskörperschaften bzw. wesentliche Teile hiervon wie *Stadtteile*, *Gemeinden*, *Städte* und *Kreise* oder
- Netzstrukturen, die der überregionalen Informationsvermittlung dienen – insbesondere *Telefon-*, *Internet-* oder *Funknetze* – oder
- bestimmte Einrichtungen der Daseinsvorsorge (*Abfallbeseitigung*, *Trinkwasserversorgung*, *Abwasserentsorgung*, *Gas-* und *Stromversorgung* sowie der Betrieb des *öffentlichen Personennah-* und *Fernverkehrs*) oder
- sonstige Infrastrukturbetriebe

vom Ausfall betroffen sind. Der Ausfall von Infrastruktur bleibt vorerst für Erst- sowie Rückversicherer nicht konkret modellierbar und damit nicht versicherbar, da derzeit Unklarheit hinsichtlich der Wahrscheinlichkeit sowie des Gesamtausmaßes eines solchen Ereignisses herrscht (vgl. Sigma 2017, S. 17).

Am Beispiel eines Ausfalls von Netzwerkstrukturen oder des Internets hätte dies weltweite nicht absehbare finanzielle Auswirkungen. In Gesprächen mit Praktikern wurde ebenfalls bekräftigt, dass die Tragweite eines Ausfalls von Infrastrukturen als Cyber-Kumulschaden zu erheblichen Schäden führen würde. Das Ausmaß des Kumulschadens kann nicht in versicherungsbezogenen Modellen abgebildet werden.

11.5 Aktuelle Trends für den VT-Risikotransfer

Nachfolgend werden die aktuellen Trends (Stand Oktober 2021) bei dem Risikotransfer des Cyber-Kumulrisikos beschrieben, soweit diese den Autoren bekannt sind. Zudem bieten sich Analogieschlüsse aus den Lehren der Covid-19-Pandemie an.

Während der Covid-19-Pandemie kam es zu zahlreichen und umfangreichen Diskussionen – bis hin zu gerichtlichen Auseinandersetzungen – zwischen Risikoträgern und deren Kunden über den tatsächlichen Deckungsumfang von erworbenen Risikotransfer-Produkten und durchgeführten Risikotransfer-Transaktionen.

Von besonderem Interesse waren dabei die unterschiedlichen Interpretationen von Kumulschadenexzedenten (*Property Cat XL*), durch die sich anschließende Betriebsunterbrechungsschaden (BU-Schaden) abgedeckt waren. Häufig wurde seitens der rückversicherten Erstversicherer behauptet, dass die Covid-19-Pandemie den für das Ziehen der BU-Deckung notwendigen vorangegangenen Sachschaden darstelle.

Ein extremes Beispiel war die Class Action zur Durchsetzung des Deckungsanspruchs von Versicherungsnehmern unter Betriebsunterbrechungspolicen, die sich auf den Urteilsspruch in „Danny de Vito vs Governor of Pennsylvania“ gründete. Der Pennsylvania Supreme Court hatte die Klage auf Untersagung der Schließung eines Wahlkampfbüros durch den Governor infolge einer Covid-19 Lockdown-Maßnahme abgewiesen mit der Begründung

> *„[…] reduce vulnerability of people […] to damage, injury and loss of life and property resulting from disasters […]“.* (Justia US Law 2020, S. 25)

Die Erwähnung des Begriffs „property“ ist in diesem Zusammenhang wichtig sowie der entscheidende Zusatz

> *„[…] the Covid-19 pandemic is of the same general nature or class as those specifically enumerated, and thus is included, rather than excluded, as a type of natural disaster*“. (Justia US Law 2020, S. 24)

In den Class Actions zur Durchsetzung des Deckungsanspruchs von Versicherungsnehmern unter Betriebsunterbrechungspolicen wurde argumentiert, dass Covid-19 – unter Berufung auf die Urteilsbegründung des Pennsylvania Supreme Court – offensichtlich eine Naturkatastrophe oder einer Naturkatastrophe gleichzusetzen sei, die Sachschäden verursache. Rechtsanwälte von Erstversicherern sahen hierin die Begründung für den Deckungsanspruch ihrer Mandanten unter Property Cat XLs.

Aus diesen Erfahrungen heraus ist der Trend gut nachzuvollziehen, dass Risikoträger ihre Deckungszusage auf eine strikte „*Named Perils*" Schadenereignisdefinition (das heißt eine abschließende Aufzählung der gedeckten Gefahren) basieren wollen. Diese Vorgehensweise ist insbesondere auch in dem ILS-Bereich zu beobachten – sowohl für Cat-Bonds als auch verstärkt für Collateralized Reinsurance (das heißt Rückversicherungsverträge, bei denen die Haftungsstrecke vollständig mit Kapital hinterlegt ist). Die betreffenden Investoren einschlägiger ILS-Transaktionen wurden in 2020 ebenfalls mit der oben geschilderten Sichtweise von Covid-19 als einer Naturkatastrophe konfrontiert, die Sachschäden verursacht. Damit ist über die Anpassung der Schadenereignisdefinition hinaus auch das generell beobachte nachlassende Interesse an Collateralized Reinsurance zu begründen, zumindest teilweise.

Die Anpassung der Contract Wordings hin zu einer abschließenden, expliziten Auflistung der gedeckten Gefahren wird durch die häufig konstatierte Vorgehensweise begleitet, zusätzlich Cyber-Sachverhalte auszuschließen. Dieses ausgeschlossene Cyber-Exposure wird dann in separaten (Rück-) Versicherungsverträgen explizit („affirmative") abgesichert. Auf diese Weise wird insbesondere auch der bekannten Silent Cyber-Problematik begegnet.

Eine weitere Lehre aus Covid-19, die von den Risikoträgern bezüglich angebotener Cyber-Kumuldeckungen adaptiert wurde, ist die angestrebte Beschränkung auf lokale oder regionale Kumulschadenfälle. Weltweit exponierte Cyber-Kumulrisiken werden dagegen als nicht-versicherbar angesehen. Dabei wird es interessant sein zu beobachten, wie die für Pandemien betriebene Abgrenzung – griffig formuliert als „Salmonellen" vs. „Covid-19-artige weltweite Virusinfektion" – auf Cyber-Schadenfälle übertragen werden wird. Nicht zuletzt unter diesem Bezug auf die eingeschränkte Versicherbarkeit wurde das Schlagwort

> *„die nächste Pandemie wird wahrscheinlich von einem Computervirus ausgelöst"* (Lauer 2020)

geprägt. Die Risikoträger führen als Gründe für die Unversicherbarkeit unbeschränkter Cyber-Kumule dieselben Argumente an wie bezüglich einer Pandemie: die unzureichende Kapitalisierung des Rückversicherungs-, Retrozessions- und ILS-Marktes sowie die mangelnde Möglichkeit, die für die Risikotragung notwendige Diversifizierung der Risiko-Portfolien sicherzustellen.

Als weiterer Trend setzt sich der seit wenigen Jahren konstatierte Rückgang von Aggregate XLs fort. Letztere werden weiterhin zunehmend durch Kumulschadenexzedenten ersetzt. Es ist zu erwarten, dass diese Präferenz der Risikoträger sich auch in der Cyber-Sparte zeigen wird.

Allgemein verstetigt sich im Cyber-Einzelschadenversicherungsmarkt der Trend zu geringeren Vertragslimiten und höheren Prämien. Gleiches gilt auch für den Risikotransfer höherer Ordnung in Rückversicherung, Retrozession und ILS. Daraus erklärt sich wohl auch die Zurückhaltung bei expliziten Deckungen für das Cyber-Kumulrisiko. Für letztere Entwicklung sind noch zwei weitere Gründe zu nennen. Zum einen erfolgt die Deckung von Rückversicherern und Retrozessionären ganz überwiegend auf *proportionaler Vertragsbasis* – und in der Regel auch nur dann, wenn auf die Produktgestaltung der Erstversicherer Einfluss genommen werden kann. Nicht-proportionale Deckungsverträge – als die grundsätzlich bessere Form für die Absicherungen des Kumulrisikos – werden daher nur in geringem Maße angeboten. Zum anderen gesellt sich bei Rückversicherungs- oder Retrozessionsdeckungen zu dem Policen-Kumulrisiko eines Erstversicherers zusätzlich noch das *Zedentenkumulrisiko*, das zu einer wesentlich höheren Kumulexponierung der betreffenden Risikoträgern führt. Gleiches gilt für ILS-Transaktionen, sofern die Emittenten Versicherer oder Rückversicherer sind.

Die Zurückhaltung von Risikoträgern – insbesondere gegenüber dem Risikotransfer des expliziten Cyber-Kumulrisikos – erklärt sich unter anderem daraus, dass sich das Cyber-Bedrohungspotenzial dynamisch und substanziell verändert. Somit mutieren die möglichen Cyber-Kumulschadenbilder in starker Weise und mit ihnen die notwendigen Konsequenzen für das Underwriting und Pricing, vgl. dazu die nachfolgenden Beispiele:

- In den vergangenen Jahren war die *Schädigung* der Infrastruktur sowie der Diebstahl oder der Missbrauch der Daten von Unternehmen die eigentliche Bedrohung. Nunmehr verlagert sich das Exposure massiv hin zu der *Sperrung* von Daten und deren Back-Ups mit dem Ziel einer Lösegeldzahlung (ransom). Hierbei kann das Vorhandensein einer Versicherung – oder genauer die Kenntnis um das Vorhandensein – sich gefahrerhöhend auswirken und ist bei dem Underwriting und der Strukturierung der (Rück-)Versicherungsdeckung beziehungsweise der ILS-Transaktion zu berücksichtigen.
- Auch wurden die früher vornehmlich *direkt geführten Angriffe* auf Unternehmen um *indirekt durchgeführte Attacken* erweitert: so manipulierten Hacker die Produkte eines Software-Herstellers, um über diesen Weg in mehrere Stromversorger eindringen zu können. Auf diese Weise konnte das eigentliche Ziel erreicht werden, die Vielzahl der Kunden jedes dieser Stromversorger angreifen zu können. Somit haben sich die „Ultimate Targets" der Attacken sowie deren Einfallstore und daraus abgeleitet die Analyse, die Beurteilung, das Underwriting und das Pricing des betreffenden Exposures durch die Risikoträger nachhaltig geändert. Dies gilt für eine Cyber-Einzeldeckung und in besonderem Maße natürlich für die Absicherung des Cyber-Kumulrisikos.

Das Vorgehen der Risikoträger ist also vorsichtiger geworden. Einzelne (Rück-)Versicherungsunternehmen sehen die Cyber-Sparte jedoch unverändert als eine attraktive Wachstumsmöglichkeit an. Eindrucksvoll ist deren Aufbietung an Ressourcen bzw. Exposures – insbesondere die Anzahl an spezialisierten Aktuaren und Datenanalysten.

11.6 Ausblick

Für die Versicherungsbranche bleibt das Cyber-Kumulrisiko vorerst eine große Herausforderung. Die rasche Geschwindigkeit, mit der sich unsere Technologie entwickelt, treibt das Cyber-Risiko und mit ihm das Cyber-Kumulrisiko. Große Trends wie *Deep-Fake-Video-* und *Audioaufzeichnungen*, Verbreitung von *Big Data*, Nutzung von *Cloud Computing*, die globale Einführung von *5G-Netzwerken* und die vermehrte *Nutzung des Homeoffices* werden dazu führen, dass sich die Cyber-Kumulrisiken weiter ausbreiten und im schlimmsten Fall erst bei konkreten Cyber-Schäden sichtbar werden. Die Technologisierung bedeutet jedoch für die Versicherer im Hinblick auf die Cyber-Kumule nicht nur Negatives. Die wachsende Verfügbarkeit und Historie von Cyber-Schäden sowie die stärkere Nutzung von künstlicher Intelligenz zur Berechnung und Modellierung in der Versicherungswirtschaft kann ebenfalls als Chance für die Absicherung dieses Risiko aufgefasst werden. Neben dem Fokus auf der Versicherungsbranche können sowohl der Staat als auch die Unternehmen zu einer besseren Absicherung von Cyber-Kumulen beitragen.

Der Staat kann zusätzlich zu einem Versicherungspool allgemeine gesetzliche Mindestanforderung zur Cyber-Sicherheit festlegen und Unternehmen verpflichten, jegliche Cybervorfälle zu melden. Die gewonnenen Daten sollten Versicherern und akademischen Zwecken zur Verfügung gestellt werden. Mit Blick auf die Unternehmen können die steigenden Frequenzen von Cyber-Schäden zu einem Wandel der Wahrnehmung hinsichtlich des Cyber-Risikos führen. Eine positive Folge hiervon wäre eine bessere Absicherung des Cyber-Risikos sowie zusätzliche Investitionen in die Cyber-Sicherheit. Die kontinuierlichen Bemühungen aller Parteien in diesem Segment haben das Potenzial, die finanziellen Auswirkungen von Cyber-Kumulrisiken besser einzuschätzen und zu begrenzen.

Literatur

Baban, C./Gruchmann, Y./Paun, C./Peters, A./Stuchtey, T. (2018): Die Grenzen von Cyberversicherungen – Handlungsalternativen zur Verbesserung von Cybersicherheit, Potsdam, Brandenburgisches Institut für Gesellschaft und Sicherheit gGmbH.

Berliner, Baruch (1982): Limits of insurability of risks, New Jersey, Prentice Hall.

Bermuda:Re+ILS (2021): Cyber: still small for its age, in: bermudareinsurancemagazine.com, https://www.bermudareinsurancemagazine.com/contributed-article/cyber-still-small-for-its-age, zugegriffen am 07.09.2021.

Biener, C., M. Eling, and J. H. Wirfs. 2015. "Insurability of cyber risk: An empirical analysis." *Geneva Papers on Risk and Insurance: Issues and Practice* 40 (1):131–158. doi: https://doi.org/10.1057/gpp.2014.19.

Brower, D./McCormick, M. (2021): Colonial pipeline resumes operations following ransomware attack, ft.com, https://www.ft.com/content/b6ac99ea-d7c6-49dd-b7d7-1284ce2e85c0?accessToken=zwAAAXl0_VTwkdO2rJnq18ZJ3dO31xKEzi6FwA.MEUCIQCBNk5FIgf3-SHq42qwwsVhKIyy-3KpApm6lgqnpj7X0QIgSFK067wNsAr86GM3v8jy_WkQPUvvr690F86D05H-1OM&sharetype=gift?token=f8b1ac18-1d38-4f2c-bf72-a08297843eb3, zugegriffen am 07.09.2021.

Cebula, J. J./Young, L. R. (2010): A taxonomy of operational cyber security risks, in cmu.edu, https://resources.sei.cmu.edu/asset_files/TechnicalNote/2010_004_001_15200.pdf, zugegriffen am 23.10.2021.

Cambridge Centre for Risk Studies und Risk Management Solutions, Inc. (2020): Managing Cyber Insurance Accumulation Risk, in: jbs.caam.ac.uk, https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-rms-managing-cyber-insurance-accumulation-risk.pdf, zugegriffen am 24.10.2021.

Eling, M./Wirfs, J. (2019): What are the actual costs of cyber risk events? European Journal of Operational Research 272, S. 1109–1119.

Farny, D. (2011): Versicherungsbetriebslehre, 5. Auflage, Karlsruhe, Verlag Versicherungswirtschaft.

Ferland, J. (2019): Cyber-Insurance – What coverage in case of an alleged act of War? Questions raised by the Mondolez v. Zurich case, Computer Law & Security 35, S. 369–376.

GDV – Gesamtverband der Deutschen Versicherungswirtschaft e. V. (2017): Allgemeine Versicherungsbedingungen für die Cyberrisiko-Versicherung, in gdv.de, https://www.gdv.de/resource/blob/6100/d4c013232e8b0a5722b7655b8c0cc207/01-allgemeine-versicherungsbedingungen-fuer-die-cyberrisiko-versicherung%2D%2Davb-cyber%2D%2Ddata.pdf, zugegriffen am 26.10.2021.

Glaab, H. (2018): Cyber-Kumulrisiken, in: munichre.com, https://www.munichre.com/topics-online/de/digitalisation/cyber/dealing-with-cyber-accumulation-risk.html, zugegriffen am 27.10.2021.

Hofmann, D./Wilson, S. (2018): Advancing accumulation risk management in cyber insurance, in: genevaassociation.org, https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public/report_advancing_accumulation_risk_management_in_cyber_insurance_0.pdf, zugegriffen am 27.10.2021.

Justia US Law (2020): Friends of Danny DeVito, et al. v. Wolf (majority), in: law.justia.com, https://law.justia.com/cases/pennsylvania/supreme-court/2020/68-mm-2020.html, zugegriffen am 30.10.2021.

Kaspersky (2018): Was ist die WannaCry-Ransomware?, in: kaspersky.de, https://www.kaspersky.de/resource-center/threats/ransomware-wannacry, zugegriffen am 25.10.2021.

Lauer, B. (2020): Die nächste Pandemie wird die virtuelle sein, in: onlinepc.ch, https://www.onlinepc.ch/internet/sicherheit/naechste-pandemie-virtuelle-2617686.html, zugegriffen am 31.10.2021.

Liebwein, P. (2018): Klasische und moderne Formen der Rückversicherung, 3. Auflage, Karlsruhe, Verlag Versicherungswirtschaft.

Malekos Smith, Z./Lostri, E./Lewis, J. A. (2020): Hidden Cost of Cybercrime, in: mcafee.com, https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf, zugegriffen am 20.10.2021.

Schweizerischer Versicherungsverband (2018): Grundlagenpapier des SVV zu Cyber-Risiken, in: svv.ch, https://www.svv.ch/sites/default/files/2018-04/Grundlagenpapier%20CyberRisiken_DE.pdf, zugegriffen am 26.10.2021.

Schwepcke, A./Vetter, A. (2017): Praxishandbuch Rückversicherung, Karlsruhe, Verlag Versicherungswirtschaft.

Sigma (2017): Cyber: Bewältigung eines komplexen Risikos, in: swissre.com, https://www.swissre.com/institute/research/sigma-research/sigma-2017-01.html, zugegriffen am 25.10.2021.

Synergy Research Group (2021): Quaterly Cloud Markets, in: srgresearch.com, https://www.srgresearch.com/articles/quarterly-cloud-market-leaps-to-42b-amazon-microsoft-google-pocket-63-of-dollars-spent, zugegriffen am 28.10.2021.

Tidy, J. (2021): Irish cyber-attack: Hackers bail out Irish health service for free, in: bbc.com, https://www.bbc.com/news/world-europe-57197688, zugegriffen am 25.10.2021.

Von der Schulenburg, J. M. G./Lohse, U. (2014): Versicherungsökonomik: Ein Leitfaden für Studium und Praxis, Karlsruhe, Verlag Versicheurngswirtschaft.

Frank Cremer studierte Versicherungswesen mit den Schwerpunkten Rückversicherung, Bilanzierung von Versicherungsunternehmen und Sachversicherung am Institut für Versicherungswesen der Technischen Hochschule Köln. Im Anschluss absolvierte er dort auch das Masterstudium Risk & Insurance. Während des Studiums erwarb er den Titel des Fellow of the Chartered Insurance Institute in London (FCII). Neben seiner beruflichen Tätigkeit als wissenschaftlicher Mitarbeiter der Kölner Forschungsstelle Rückversicherung promoviert Herr Cremer seit dem 01.01.2021 unter der Betreuung von Prof. Michael Fortmann in Kooperation mit der University of Limerick und der Technischen Hochschule Köln.

Prof. Stefan Materne (FCII) ist seit 1998 Inhaber des Lehrstuhls für Rückversicherung an dem Institut für Versicherungswesen der TH Köln mit den Schwerpunkten Effizienz von Rückversicherung, Industrieversicherung und Alternative Risk Transfer (ART). Er studierte Mathematik und Informatik mit dem Schwerpunkt Künstliche Intelligenz und forschte von 1988 bis 1991 am Fraunhofer Institut für Autonome intelligente Systeme (AiS) in Schloß Birlinghoven. Von 1991 bis 2004 war Prof. Materne für die Gen Re (vormals Kölnische Rück) in verschiedenen Managementfunktionen im In- und Ausland tätig, von 2001 bis 2003 fungierte er als General Manager der Cologne Re of Dublin in Irland. In 2008 gründete Prof. Materne die Kölner Forschungsstelle Rückversicherung, deren Direktor er ist und in der aktuelle Fragestellungen der Rückversicherung und angrenzender Gebiete analysiert und mit der Praxis diskutiert werden, wobei die Praxiskontakte durch den Förderkreis Rückversicherung und die Ausrichtung des jährlichen Kölner Rückversicherungs-Symposiums gewährleistet werden. Prof. Materne übt verschiedene internationale Aufsichtsrats-, Verwaltungsrats- und Beiratsmandate bei Erst- und Rückversicherungsunternehmen, Captives, InsurTechs, der Europäischen Versicherungsaufsicht EIOPA sowie bei versicherungswissenschaftlichen Einrichtungen aus. Zudem fungiert er als Schiedsrichter und Parteivertreter in Schiedsgerichtsverfahren.