Bericht vom 40. Versicherungswissenschaftlichen Fachgespräch
am 17. September 2018

„Absicherung von IT-Risiken durch moderne Cyber-Versicherungen?“

Der Begriff der Digitalisierung ist derzeit in aller Munde. Moderne Technologien haben inzwischen in nahezu allen Bereichen des Wirtschaftslebens Einzug gehalten. Welche Chancen und Risiken diese Entwicklung auch für den Versicherungssektor mit sich bringt, war bereits Gegenstand mehrerer Fachgespräche des Vereins zur Förderung der Versicherungswissenschaft in Berlin e. V., unter anderem der 25. und 26. Öffentlichen Veranstaltung 2016 und 2017. Das 40. Versicherungswissenschaftliche Fachgespräch, das von der Funk-Gruppe im DIN-Gebäude ausgerichtet wurde, knüpfte hieran an, allerdings mit einer anderen Akzentuierung. So ging es diesmal um Fragen der Cyberrisiko-Versicherung, mit der Wirtschaftsunternehmen sich gegen IT-Sicherheitsrisiken absichern können.

Im Anschluss an die Begrüßung durch den Vorstandsvorsitzenden des Vereins **Olaf Dilge** führte der Moderator **Prof. Dr. Hans-Peter Schwintowski** am Beispiel von fehlerhaften Warenbestellungen über Cloud-Softwares in die Problematik des digitalen und vernetzten Vertriebs ein, aus dem sich für die Industrie mitunter schwierige Haftungsfragen ergeben. Um welche Risiken es sich dabei im Einzelnen handelt und inwieweit hierfür Versicherungsprodukte Lösungen anbieten können, wurde von Vertretern aus verschiedenen Bereichen der Versicherungswirtschaft erläutert.

Als erster Redner legte Herr **John Philipp Seebohm**, Berater und Auditor bei Funk im Bereich Cyber-Risiken und IT-Sicherheit, zunächst dar, was unter dem Begriff „Cyber“ überhaupt zu verstehen ist. Dabei zeigte er anhand von Beispielen aus der Praxis auf, dass IT-Sicherheitsrisiken keineswegs ausschließlich in Hackerangriffen liegen, sondern ganz unterschiedliche Ursachen haben können, wie etwa organisatorische Mängel, technisches Versagen oder höhere Gewalt. Insoweit stelle sich die Frage, ob diese heterogenen IT-Sicherheitsrisiken, die auch in ihren Auswirkungen sehr verschieden seien, über eine Cyber-Versicherung versichert werden können. Vor diesem Hintergrund weist er auf die Schwierigkeit hin, den

Begriff „Cyber“ einheitlich und zugleich präzise zu definieren. Darüber hinaus sei ein Problem bei der Entwicklung von Cyber-Versicherungsprodukte in einem besonderen Risikowachstum und einer entsprechenden Risikokumulierung zu erblicken. So bestehe eine jährliche Steigerung der Datensicherheitsvorfälle von 27 %. Gleichzeitig sei ein jährlicher Zuwachs von 33 % von Geräten feststellen, die mit dem Internet verbunden werden. Eine weitere Herausforderung sah Herr Seebohm in einer Diskrepanz zwischen den versicherbaren Risiken und den tatsächlichen Risiken. Insbesondere gebe es bedeutsame Schadenspositionen, wie den Reputationsverlust eines Unternehmens und den Verlust von Datensätzen, die im Rahmen einer Cyber-Versicherung entweder nicht versichert seien oder sich jedenfalls nur schwer beziffern ließen. Sodann ging Herr Seebohm auf die Auswirkungen auf das IT-Sicherheitsniveau ein. Dabei nannte er Faktoren, die zur Reduzierung des IT-Sicherheitsniveaus aufgrund von Cyber-Versicherungen beitragen können, namentlich das moralische Risiko, die adverse Selektion sowie Budget-Verschiebungen. Problematisch sei schließlich auch die Beweisbarkeit des Eintritts des Versicherungsfalls sowie die Nachweisbarkeit von Obliegenheitsverletzungen, da erhebliche forensische Schwierigkeiten im Zusammenhang mit IT-Sicherheitsverletzungen bestünden.

Frau **Alexandra Köttgen**, Unternehmensjuristin bei Funk im Bereich Cyber-Versicherung, griff die Thesen von Herrn Seebohm in ihrem Vortrag auf. Es sei zwar zutreffend, dass der Begriff „Cyber“ keiner allgemeingültigen Definition zugeführt werden könne, jedoch legt der GDV seinen Musterbedingungen zur Cyberrisiko-Versicherung ein einheitliches Risikoverständnis zugrunde. Das Bedingungswerk spreche insoweit nicht von „Cyber“, sondern definiere den Versicherungsfall dahingehend, dass die Schutzziele der Verfügbarkeit, Vertraulichkeit und Integrität der IT-Sicherheit durch bestimmte Gefahren verletzt werden. Frau Köttgen legte überdies dar, dass das klassische Spartendenken durch die moderne Cyberrisiko-Versicherung stark aufgeweicht werde. So seien IT-Sicherheitsrisiken auch über die Vertrauensschaden- sowie über Elektronikversicherungen versicherbar, wobei etwaige Überschneidungen etwa auch durch Subsidiaritätsklauseln gelöst werden können. Richtig sei auch, dass das exponentielle Wachstum von Cyberrisiken ein erhebliches Problem im Hinblick auf die Kalkulation derartiger Risiken darstellt. Ein Blick auf die US-amerikanische Marktlage zeige jedoch, dass eine kurz- und

mittelfristige Kalkulation durchaus möglich sei. Auch führe das steigende Risikowachstum zu einer stärkeren Sensibilisierung von Unternehmen für die Notwendigkeit von Investitionen in die IT-Sicherheit. Sodann bezog sich Frau Köttgen auf das von Herrn Seebohm angesprochene Auseinanderfallen von versicherbaren und tatsächlichen Risiken. Hierbei weist sie darauf hin, dass lediglich ca. 40 % der in Betracht kommenden Schäden nicht versichert seien. Darüber hinaus können bestimmte Schäden auch über den Kostenersatz abgedeckt werden, wobei die Bemessung von einzelnen Schadenspositionen vielfach kein spezifisches Problem der Cyber-Versicherung, sondern ein generelles Problem darstelle. Entgegen der Auffassung von Herrn Seebohm seien Cyberrisiko-Versicherungen zudem sehr wohl geeignet, das IT-Sicherheitsniveau zu erhöhen, indem sie Investitionsanreize für Versicherungsnehmer setzen und diese dazu motivieren, sich auf wirksame IT-Sicherheitsmaßnahmen zu fokussieren. Auf diesem Wege könne auch das Problem der adversen Selektion abgeschwächt werden. Zum Schluss ihres Vortrags räumte Frau Köttgen ein, dass die Beweisbarkeit des Eintritts des Versicherungsfalls durchaus problematisch sei. Gleichwohl könne diesem Problem etwa durch Mitwirkungsobliegenheiten des Versicherungsnehmers nach Eintritt des Versicherungsfalls, durch Kostenpositionen für Schadensermittlungskosten sowie durch Beweiserleichterungen begegnet werden.

Als kurzfristigen Ersatz für Frau Kress-Happel vom Versicherer CHUBB, die ihren Vortrag leider krankheitsbedingt absagen musste, konnte Herr **Roman Potyka** gewonnen werden, der zum Abschluss als Underwriter beim internationalen Versicherer Hiscox dem Publikum einen Überblick über die bisherige und gegenwärtige Marktsituation im Bereich von Cyberversicherungen verschaffte. Es lasse sich insoweit der Befund erheben, dass es eine breite Gemengelage aus unterschiedlichen Cyberrisiken gebe. Klassische „Trends“ ließen sich insoweit nicht ausmachen, wobei man immerhin feststellen könne, dass Verschlüsselungstrojanern immer besser beizukommen sei. Auf dem Vormarsch seien stattdessen sogenannte Krypto-Miner, bei denen es sich um virtuelle Viren zur Erzeugung von Bitcoins handele. Angesichts des Facettenreichtums und der Dynamik von Cyberrisiken plädierte Herr Potyka dafür, die überkommene Funktionsweise von Versicherung im Bereich der Cyberversicherung aufzugeben und stattdessen den Fokus von Versicherern auf (vorbereitende) technische und organisatorische Maßnahmen zu

legen. So müsse durch Prävention und Assistance, z.B. durch die Erstellung eines Krisenplans, die Einrichtung einer Notfallhotline oder durch Schulung von Mitarbeitern, auch von Versicherungsunternehmen ein wichtiger und notwendiger Beitrag zur Reduzierung von Cyberrisken geleistet werden. Demgegenüber fungiere eine Cyberversicherung nur noch als „letzte Mauer“.

Im Rahmen der anschließenden Aussprache ist neben Fragen des technischen Know-how bei Cyberangriffen und der Versicherbarkeit von Reputationsschäden unter anderem auch die Frage erörtert worden, ob der Vorstand einer AG den Abschluss einer Cyberrisiko-Versicherung in Erwägung ziehen muss. Die Diskussion erinnert an die aus dem Bereich der D&O-Versicherung bekannte – und überwiegend verneinte – Frage, ob der Vorstand nach § 91 Abs. 2 AktG verpflichtet ist, für einen angemessenen Versicherungsschutz der Organmitglieder zu sorgen. So bestand auch hinsichtlich der Cyberrisiko-Versicherung Konsens darin, dass die Pflichten des Vorstandes sich unter dem Gesichtspunkt des Risikomanagements lediglich auf eine Prüfung geeigneter Maßnahmen beschränken. Kritisiert wurden darüber hinaus die bestehenden Beweisschwierigkeiten bei Eintritt des Versicherungsfalls und bei Obliegenheitsverletzungen. Zur Lösung des Problems sprach sich Herr Potyka dafür aus, überhaupt keine vertraglichen Obliegenheiten in Cyberversicherungsverträgen aufzunehmen.

Prof. Schwintowski schloss die Diskussion und dankte den Referenten für die Vorträge und dem Publikum für die lebhafte Diskussion.

Berlin, den 7. Oktober 2018
Dr. Vincent Schreier