Rückblick: 5. Cyberversicherungstag am 12. Oktober 2023 an der FU Berlin

Am 12. Oktober 2023 fand am Fachbereich Rechtswissenschaft der FU Berlin in Zusammenarbeit mit dem Deutschen Verein für Versicherungswissenschaft e.V. (DVfVW) und dem Berliner Verein zur Förderung der Versicherungswissenschaft bereits zum fünften Mal der Cyberversicherungstag statt. Rund 100 Interessierte verfolgten die Vorträge aus Wissenschaft und Praxis zu aktuellen Themen zur Cyberversicherung teilweise vor Ort, teilweise online. Die Veranstaltungsreihe wurde initiiert und wird inhaltlich koordiniert von Thomas Pache (Aon Hamburg) und Dr. Dan Schilbach (Kanzlei Noerr, Düsseldorf) als Vertreter der Praxis sowie von Univ.-Prof. Dr. Christian Armbrüster als Vertreter der Wissenschaft, der die Tagung auch moderierte.

Zum ersten Mal gab es in diesem Jahr einen informellen Vorabend in der Hotelbar des Seminaris CampusHotel Berlin, bei dem die Teilnehmenden bereits im Vorlauf der Veranstaltung die Möglichkeit zu einem ersten Austausch in informeller Atmosphäre hatten.

Die Veranstaltung begann am folgenden Tag nach einer Begrüßung sowie kurzen Einleitung in das Thema der Cyberversicherung durch Prof. Armbrüster mit dem ersten Vortrag zu aktuellen Entwicklungen bei Cyber-Schadenfällen von Christian Taube (Beazley Cyber Services, München). Untermauert von einigen echten Fallbeispielen, die aufzeigten, wie Cyberangriffe üblicherweise ablaufen, wies er auf klassische Schwachpunkte der Cybersicherheit hin. Besonders bemerkenswert sei eine Tendenz dazu, dass Cyberkriminelle Daten zwar zunehmend exfiltrieren, aber nicht mehr verschlüsseln. Auf Nachfrage aus dem Publikum gab er an, diese Tendenz sei wahrscheinlich auf die steigende Bedeutung einer Rufschädigung bei Datenverlust sowie den Erfahrungen der Hacker zurückzuführen. So würden Unternehmen bei einer reinen Exfiltration häufiger und schneller zahlen, als wenn ihre Infrastruktur vollständig verschlüsselt wurde. Letztlich kam er auch mit Blick auf den Sachverhalt der aktuellen Entscheidung des LG Tübingen (4 O 193/21) zu dem Schluss, dass die Anforderungen an die Cybersicherheit entgegen gängiger Auffassung nicht ständig steigen. Vielmehr scheitere Cybersicherheit immer noch oft an einer mangelnden Umsetzung grundlegender Maßnahmen.

Alexander Welter (Aon, Mülheim an der Ruhr) und Dr. Dan Schilbach befassten sich anschließend mit Herausforderungen in der Regulierung von Cyberschadenfällen. Dabei ging es zum einen um Herausforderungen im Schadenhandling, welche die Referenten insbesondere in den vorvertraglichen Anzeigeobliegenheiten sowie Auskunfts- und Mitwirkungsobliegenheiten im Schadenfall sahen. Hier sei ein häufiger Streitpunkt beispielsweise die Herausgabe von sogenannten Pentests oder Audit-Berichten, die der regelmäßigen Prüfung der Systemsicherheit dienen und Rückschlüsse auf mögliche Sicherheitslücken des Versicherungsnehmers zulassen.

Zum anderen befassten sich die Referenten mit häufigen Streitpunkten in der Regulierung von Cyberschäden. Nach einer kurzen Übersicht zu deckungsrechtlichen Einwendungen ging es erneut um die aktuelle Entscheidung des LG Tübingen, diesmal jedoch unter dem Gesichtspunkt einer Herbeiführung des Versicherungsfalls, die – so das Gericht – dem Versicherer als Einwand versperrt ist, wenn die betreffende Gefahrenlage bereits bei

Vertragsschluss bestand und bereits Grundlage der Risikoprüfung des Versicherers war bzw. hätte sein müssen. Die Referenten betonten vor diesem Hintergrund die Bedeutung vorvertraglicher Risikoermittlung. Auf die Rückfrage, ob immer mehr technische Obliegenheiten eingeführt würden, wurde von den Vortragenden entgegnet, dass weniger eine Zunahme der technischen Obliegenheiten, sondern viel eher eine Zunahme der Risikofragen zu beobachten sei.

Nach einer Kaffeepause, die von den Teilnehmenden zum regen Austausch genutzt wurde, befasste sich Roman Dickmann (Rechtsanwalt, Frankfurt a.M.) mit dem IT-Schwachstellenmanagement in der Cyberversicherung. Hierfür warf er zunächst einen Blick auf die Historie der Regulierung und Versicherung von Cyberrisiken. Letztlich schlussfolgerte er, dass es trotz der exponentiellen Entwicklung bisher keinen Sockel an IT-Sicherheit gebe, der – ähnlich den Sicherheitsstandards in der Feuerversicherung – zum Erreichen eines Mindestmaßes an IT-Sicherheit aber dringend nötig wäre. Dies würde beispielsweise dazu führen, dass bereits unsichere Produkte angeboten werden und Cyberkriminelle Handel mit den Schwachstellen betreiben. In neuer EU-Gesetzgebung sah er jedoch positive Impulse. Im Schwerpunkt folgte eine detaillierte Darstellung eines optimalen Schwachstellenmanagements. In diesem Zusammenhang bemerkte Herr Dickmann, dass die Reaktion von Unternehmen auf Hinweise Dritter häufig von wenig Dankbarkeit geprägt sei, obwohl diese Hinweise als Bereicherung verstanden werden müssten. Der Vortrag schloss unter anderem mit der These ab, dass vor diesem Hintergrund der Umgang mit Schwachstellen Eingang in das Underwriting finden sollte.

Den Abschluss des Vormittagsprogramms machte Peter Graß (GDV, Berlin), der digital zugeschaltet über die überarbeiteten GDV-Musterbedingungen zur Cyberversicherung referierte. Die Veröffentlichung der Neufassung sei zum Ende des Jahres 2023 zu erwarten. Darin seien nach Abstimmung mit den Marktteilnehmern wichtige Anpassungen vorgenommen werden. Einige dieser Neuerungen stellte der Referent unter dem Vorbehalt ihrer Finalität vor. So werde unter anderem die viel umstrittene Kriegsausschlussklausel neu gefasst. Auf Nachfrage aus dem Publikum bemerkte Herr Graß, dass bei der Kriegsausschlussklausel künftig auch eine staatliche Billigung von Angriffshandlungen erfasst sein soll. Er wies in diesem Zusammenhang auf eine aktuelle GDV-Initiative zur Cybersicherheit hin. In Reaktion auf das bereits erwähnte Urteil des LG Tübingen solle aller Voraussicht nach auch die Einwendung nach § 81 Abs. 2 VVG ausdrücklich ausgeschlossen werden, wenngleich sich dies aus Sicht des Referenten bereits aus der bislang geltenden Fassung der AVB ergebe.

Nach einem ausgiebigen Mittagessen und der Möglichkeit zu weiterem Austausch hielt Volker Pulskamp (FleishmanHillard, Frankfurt a.M.) einen Vortrag zur professionellen Krisenkommunikation in den Phasen vor, während und nach einem Cybervorfall. Dabei präsentierte er die hierfür aus seiner Sicht wichtigsten Grundregeln. Zum einen sei es entscheidend, die Kommunikation den Experten zu überlassen. Zum anderen sollte dies nicht erst im Schadenfall passieren. Ein präventives Netzwerk für den Ernstfall könne oft dabei helfen, schwerwiegende Fehler zu vermeiden. „Undisziplinierte“ Sprache solle durch vorbereitete Botschaften und Textbausteine verhindert werden. Insbesondere unabhängige Kommunikationskanäle zu den Stakeholdern sollten existieren, damit diese von einem Vorfall nicht aus anderer Quelle erfahren und so wichtiges Vertrauen erhalten bleibt.

Im Folgenden ging es um Kumulrisiken. Die Referenten Thomas Pache, Sebastian Scholz (PPI AG/cysmo Cyber Risk GmbH, Köln) und Daniel Kasper (Qualrisk Cyber Insurance Center, Köln) warfen nacheinander jeweils einen eigenen, kurzen Blick auf dieses für die Cyberversicherung brisante Thema. Zunächst referierte Herr Pache dazu, ab wann Cyber-Kumule grundsätzlich nicht mehr versicherbar seien und welche Maßnahmen Versicherer ergreifen könnten. Hier sei es möglich, Ausschlüsse wie etwa die Kriegsausschlussklausel zu vereinbaren sowie Risiken genau zu selektieren und zu überwachen. Er stellte auch Überlegungen zu einem staatlich gelenkten Rückversicherungspool für die Cyber-Kumulrisiken an. Sebastian Scholz widmete sich der Identifikation von Kumulen in der Cyberversicherung. Nach Darstellung einiger potentieller Kumulszenarien präsentierte er ein IT-Tool, dass der Identifzierung von Kumulrisiken in einem Risikoportfolio dienen kann. Daniel Kasper resümierte zuletzt, dass niemand genau wissen könne, wann Kumulrisiken eintreten. Vor allem das stete Bewusstsein für diese Risiken sei entscheidend. Er wies auf die erste Cyber-Katastrophen-Anleihe von Beazleys hin, mit der sich eine neue spannende Entwicklung auf dem Versicherungsmarkt abzeichne.

Die Tagung wurde mit einem Vortrag von Isabelle Brams (Lathan&Watkins, Frankfurt a.M.) abgerundet, die sich Schadensersatz und Bußgeldern wegen DSGVO-Verstößen nach einem Cyberangriff widmete. Nach einem Überblick über die rechtlichen Rahmenbedingungen referierte sie zu den typischen Konsequenzen mit Blick auf einen Verstoß gegen Art. 32 DSGVO. Hier könne es für das Unternehmen Meldepflichten geben, gleichzeitig drohten Behördenverfahren und Bußgelder sowie Schadensersatz und Kündigungsrechte von Vertragspartnern. Diese Konsequenzen wurden anschließend detailliert referiert. Als vorbereitende Maßnahmen sollte grundsätzlich eine gerichtsfeste Dokumentation der für den Datenschutz relevanten Strukturen und Prozesse erfolgen. Außerdem seien selbstverständlich die üblichen Anforderungen an die IT-Sicherheit einzuhalten. Korrespondierend zu ihren Vorrednern wies die Referentin auf die Notwendigkeit eines sogenannten Cybersecurity Incident Response Plan hin, also einem Plan, der dem Unternehmen im Ernstfall hilft, die richtigen Schritte einzuleiten. Abschließend erläuterte Frau Brams, auch Manager würden sich bei einem Datenschutzverstoß regelmäßig Haftungsrisiken ausgesetzt sehen. Als Fazit hielt sie fest, dass ein Datenleck allein nie die Katastrophe sei. Vielmehr würde die Katastrophe erst bei einem unprofessionellen Umgang mit dem Problem entstehen.

Die Veranstaltung wurde von Prof. Armbrüster mit einer Danksagung an die Vortragenden und Diskutanden, das Publikum und die an der Organisation Beteiligten beendet. Dabei kamen noch weiterführende Fragen zur Sprache, die in den Vorträgen aufgeworfen wurden und Anlass für eine Fortsetzung des Formats im kommenden Jahr bieten würden. Wie jedes Jahr lud er die Teilnehmenden dazu ein, auch künftig eigene Themenvorschläge einzubringen, um auch weiterhin eine große Praxisnähe des Berliner Cyberversicherungstags zu gewährleisten.

Der nächste Berliner Cyberversicherungstag soll am Freitag, dem 11. Oktober 2024 stattfinden. Nähere Informationen werden auf den homepages der beteiligten Institutionen zu finden sein.

Dominik Schürger/Markus Hoffmann

Wissenschaftliche Mitarbeiter

Lehrstuhl Univ.-Prof. Dr. Christian Armbrüster

Freie Universität Berlin