WILHELM

RECHTSANWÄLTE

Christian Drave, LL.M.

Versicherungspraxis, April 2016

Cyberversicherung

Cyberrisiken und Versicherung: Stand und Entwicklungen

Umfragen und Analysen bestätigen, dass Cyberrisiken aus Sicht der Unternehmen als „Top-Risiken“ einzuschätzen sind. Dazu beigetragen haben auch exponierte Cybervorfälle der jüngsten Vergangenheit. Verschärfte Anforderungen an Datensicherheit, potentiell existenzgefährdende Eigenschäden und Haftungsverlagerungen stellen Risikomanager wie auch Versicherer vor Herausforderungen.

Macht Ihnen das Thema Cyberrisiken Bauchschmerzen? Meinem Kollegen ganz sicher, und zwar physisch. Das liegt nicht etwa daran, dass er IT-Verantwortlicher wäre. Mein Kollege erlebte vielmehr am eigenen Leib, wie sich Bedrohungen aus dem Cyberraum auswirken können. Mit akuten Bauchschmerzen musste er sich kürzlich nachts in ein Klinikum im Rheinland begeben. Möglicherweise ahnen Sie es bereits: Dieses Klinikum gehörte zu den Krankenhäusern, die Opfer gezielter Cyberangriffe durch Verschlüsselungstrojaner (Ransomware) geworden waren. Die Folge war, dass die Ärzte keine Akutversorgung leisten konnten (wenngleich die medizinische Versorgung der Patienten nach Angaben der betroffenen Klinik zu keinem Zeitpunkt gefährdet war). Mein Kollege wurde in ein anderes Krankenhaus gebracht. Erfreulicherweise geht es ihm wieder gut – anders steht es jedoch Medienberichten zufolge mit der IT-Infrastruktur der betroffenen Kliniken. Das Bundesamt für Sicherheit in der Informationstechnik („BSI“) verweist im Zusammenhang mit den Cyberattacken auf Kliniken in einer Presseinformation vom 8. März 2016 auf die aktuelle Bedrohungslage für kritische Infrastrukturen, mithin Unternehmen und Einrichtungen der gesellschaftlichen Daseinsvorsorge:

„Krankenhäuser sind aufgrund ihrer herausragenden Bedeutung für das Wohlergehen der Bevölkerung ein wichtiger Teil der Kritischen Infrastrukturen. Sie haben daher eine besondere Verpflichtung, die Verfügbarkeit ihrer Dienstleistungen sicherzustellen…."

Nicht nur vor dem Hintergrund der Cyberangriffe auf Kliniken, den deutschen Bundestag oder Sony stellt sich die Frage nach Stand und Tendenzen in Sachen Cyberrisiken und ihrer Versicherung. Dieser Betrag beleuchtet die Gefährdungslage und das Risikobewusstsein im Zusammenhang mit Cyberrisiken und zeigt anhand von ausgewählten Einzelthemen Entwicklungen auf, die Versicherungsnehmer und Versicherer gleichermaßen vor Herausforderungen stellen.

Gefährdungslage und Risikobewusstsein

Experten stellen fest, dass einerseits Angriffe auf die Informationsinfrastrukturen im Cyber-Raum zunehmend komplexer und professioneller werden. Andererseits nimmt die IT-Abhängigkeit von Unternehmen, Staat und Bürgern und damit das Schadenspotenzial stetig zu.[1]

Die Risikolandschaft mit Blick auf Cyberrisiken verändert sich. Dies gilt auch für das rechtliche Umfeld. Das IT-Sicherheitsgesetz von 2015 verpflichtet Betreiber kritischer Infrastrukturen dazu, einen erhöhten Sicherheitsstandard ihrer IT-Systeme zu gewährleisten. Am 15. Dezember 2015 einigten sich das EU-Parlament, der Ministerrat und die EU-Kommission auf eine endgültige Fassung der EU-Datenschutz-Grundverordnung, um einen einheitlichen europaweiten Standard zum Datenschutz zu erreichen. Seit dem 24. Februar 2016 haben insbesondere Verbrauchschutzverbände ein Klagerecht im Fall von Datenschutzverstößen (geschaffen durch das Gesetz zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts). Damit drohen Unternehmen bei Verstößen gegen bestimmte datenschutzrechtliche Vorschriften nicht nur Sanktionen der Aufsichtsbehörde wie beispielsweise Bußgelder, sondern auch Unterlassungsklagen von Verbraucherschutzverbänden.

---

[1] Vgl. den Bericht zur Lage der IT-Sicherheit in Deutschland 2015 des Bundesamtes für die Sicherheit in der Informationstechnik, abgerufen am 10. März 2016 unter: https://www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html;jsessionid=551CE477F3D86D2703E97A41707F2B9D.2_cid294

Die gesetzgeberischen Initiativen schaffen für die Unternehmen nicht nur Risiken bei Verstößen, sondern verdeutlichen einen Wandel im allgemeinen Risikobewusstsein. Dieser Wandel führt auch dazu, dass Industrie und staatliche Institutionen vermehrt Standards der IT-Sicherheit herausbilden. Beispielsweise regelt die international führende Norm für Informationssicherheits-Managementsysteme ISO 27001 Anforderungen an die Einführung, Umsetzung, Überwachung und Verbesserung eines Informationssicherheits-Managementsystems. Derartige Standards können Auswirkungen auf die Definition von Sorgfalts- und Verkehrssicherungspflichten haben (etwa bei der Frage, wann ein Verhalten fahrlässig ist, also „die im Verkehr erforderliche Sorgfalt außer Acht lässt“ oder im Bereich der Produkthaftung im Rahmen der Frage, ob ein Produkt dem neuesten Stand der Wissenschaft und Technik entspricht).

Das Thema Cyberrisiken wird seit längerem gerne als „Chefsache“ bezeichnet und ist als solches angekommen: Anforderungen an die IT-Sicherheit betreffen die Unternehmensorganisation und insofern eine Leitungsaufgabe der Verantwortlichen. Der Vorstand ist verpflichtet, Risiken vom Unternehmen abzuwenden, die dessen Bestand bedrohen können (vgl. § 92 Absatz 2 AktG). Die Risikovorsorge erfasst auch den Fall, dass eine Risikoanalyse zu dem Schluss kommt, dass Cyberrisiken den Bestand des Unternehmens gefährden können. Der (Gesamt-)Vorstand ist für die Unternehmenscompliance verantwortlich – mit dem Risiko persönlicher Haftung im Fall von Verstößen. Unternehmenscompliance erfasst auch den Bereich des Datenschutzes und der Datensicherheit. Cyberrisiken festzustellen, zu analysieren und Maßnahmen zur Risikominderung oder zum Risikotransfer durch Versicherung zu treffen, ist somit zentrale Aufgabe des Risikomanagements. Einen Fokus setzen die Unternehmen in diesem Zusammenhang auf eine Risikominimierung durch Verbesserungen ihrer IT-Sicherheit und der Organisation.

Grenzen der Versicherbarkeit von Eigenschäden

Der Markt der Cyberversicherung entwickelt sich, ebenso wie Kapazitäten. Doch nicht alle Cyberrisiken sind versicherbar und der Versicherungsschutz hat Grenzen. Wegen ihrer wirtschaftlichen Bedeutung stehen mögliche Eigenschäden zu Recht im Fokus der Risikobetrachtungen.

Eigenschäden können das Unternehmen beispielsweise treffen, wenn es durch einen externen Cyberangriff oder Entwendungen durch Mitarbeiter Entwicklungsdaten (also geistiges Eigentum) verliert. Vor allem Betriebsunterbrechungen infolge von Systemaus-

fällen oder auch – wie im Beispiel attackierter Kliniken – durch das Sperren von Dateien/Systemen können gravierende Schäden verursachen. Übliche Deckungsbausteine von Cyberversicherungen decken Eigenschäden durch Betriebsunterbrechungen innerhalb bestimmter Haftzeiten und Limits ab.

An Bedeutung gewinnen dürfte das Risiko behördlich verhängter Bußen infolge von Datenschutzverletzungen durch Unternehmen. Bußen gehören schadenrechtlich zu möglichen Eigenschäden der Versicherungsnehmer, wenn auch Cyberpolicen teilweise Bußgelder systematisch als Haftpflichtfälle einordnen (und damit wie Drittschäden behandeln). Bezüglich der Versicherung von Bußen weichen Deckungsangebote der Versicherer teilweise stark voneinander ab.

Zu Recht gelangen Reputationsrisiken vermehrt in den Fokus der Unternehmen. Insbesondere wenn es um den Verlust von personenbezogenen Kundendaten geht, liegt das das Risiko von Reputationsschäden für Unternehmen auf der Hand. Aber auch für Unternehmensleiter können persönliche Risiken im Zusammenhang mit Cyberbedrohungen bestehen. So trat der Vorstandsvorsitzende des US-Einzelhändlers Target nach einem Hackerangriff zurück, der 2013 zum Verlust von über 40 Millionen Kredit- und Bezahlkartendaten von Kunden führte. Nach dem spektakulären Hackerangriff auf Sony-Pictures Ende 2014 verließ die Co-Chefin das Unternehmen. Cyberpolicen können über Assistance-Leistungen wie die Übernahme der Kosten der Krisenkommunikation einen Ausschnitt der finanziellen Beeinträchtigungen von Unternehmen ausgleichen, tun dies aber regelmäßig innerhalb überschaubarer Sublimits. Den häufig schwer zu quantifizierenden Schaden durch Umsatzeinbrüche etc. können möglicherweise gesonderte Reputations-Policen abbilden.[2]

Verlagerung von Haftungsrisiken: Cybersicherheit und Produkthaftung

Neben dem zuvor beschriebenen Risiko von Eigenschäden bestehen für Unternehmen vielfältige Haftungsrisiken. Die fortschreitende Digitalisierung und die Vernetzung im Cyberraum können dazu führen, dass sich Haftungsrisiken verlagern, insbesondere im Bereich der Produkthaftung. Die folgenden Beispiele aus dem Bereich der „digitalisierten Mobilität“ verdeutlichen diese Entwicklung.

---

[2] Siehe auch Klinkhammer, Versicherungspraxis 3/2016, S. 3 ff.

Flugverkehr:

Es wird damit gerechnet, dass sich die Verkehrsdichte im internationalen Luftverkehr innerhalb der kommenden 20 Jahre verdoppelt[3]. Mit den vorhandenen Managementsystemen sind die Herausforderungen einer zunehmenden Verkehrsdichte nicht zu bewältigen, darin sind sich Experten einig. Vermehrt gibt es daher Bestrebungen, das Luftverkehrsmanagement zu vereinheitlichen und zu synchronisieren (etwa im europäischen Raum durch eine Initiative der Europäischen Kommission). Ziel ist, über Echtzeitdaten alle Akteure des Luftverkehrs wie beispielsweise Piloten und Fluglotsen miteinander zu vernetzen und so ein sicheres und effizientes Luftverkehrsmanagement zu erreichen. Aber auch die Arbeitsbedingungen von Fluglosten könnten über eine Vernetzung optimiert werden. Üblicherweise arbeiten Fluglotsen in Schichtsystemen. Sind die Flughäfen vernetzt und die Luftraumüberwachung synchronisiert, könnte ein Fluglotse in Perth die Arbeit seiner Kollegen in einer anderen Zeitzone übernehmen – beispielsweise in England – und so eine Nachtarbeit vermeiden.

Das Risikopotenzial eines in Echtzeit vernetzten Luftraums liegt auf der Hand. Datensicherheit und Datenverfügbarkeit sind essentiell und durch externe Angriffe gefährdet. Unabhängig davon steigen durch eine zunehmende Digitalisierung aber Produkthaftungsrisiken von Systemherstellern. Eines der schwersten zivilen Flugunglücke im Jahr 2002 beruhte nach Einschätzung des damit befassten Zivilgerichts auf einem Produktfehler. Das Gericht führte die Kollision zweier Flugzeuge auf einen Konstruktions- und Instruktionsfehler des Herstellers des an Bord befindlichen Kollisionswarnsystems zurück. Dieser Fall verdeutlicht, dass eine Digitalisierung einerseits Schäden durch menschliches Versagen vermeiden und somit das Haftungsrisiko der Betreiber reduzieren kann (durch verbesserte Kollisionswarnsysteme). Andererseits verlagert sich das Haftungsrisiko vom Betreiber hin zu den Systemherstellern (deren Systeme einer immer komplexeren Risikolage begegnen müssen).[4] Dieser Risikoverlagerung müssen die Unternehmen und die Versicherer Rechnung tragen.

---

[3] Vgl. den Artikel im Schadenspiegel der Munich Re 2/2015, S. 6 ff., abgerufen am 10. März 2016 unter: http://www.munichre.com/site/touch-publications/get/documents_E-1212395301/mr/assetpool.shared/Documents/5_Touch/_Publications/08791_SSP_2_2015_de.pdf

[4] Vgl. wie vor, S. 12 mit weiteren Nachweisen.

Vernetztes Fahren und Big Data:

Auswirkungen auf Produkthaftungsrisiken hat auch die Entwicklung hin zu digitalisiertem Fahren.

Zunächst müssen Hersteller die (Daten)sicherheit auch im multidigitalen System Automobil sicherstellen. Dieser Aspekt gewinnt mit zunehmendem Digitalisierungsgrad an Bedeutung. Fälle von Hackern, die die Kontrolle über fahrende Autos übernahmen, sind bekannt und dürften auch zukünftig auftreten.

Zudem können Automobilhersteller eine Fülle von Daten im Zusammenhang mit dem Betrieb ihrer Produkte erheben und verarbeiten – auch möglicherweise sicherheitsrelevante. Damit stellt sich die Frage, welche Konsequenzen diese Verfügbarkeit von Datenmengen („Big Data“) mit Blick auf eine mögliche Produkthaftung der Hersteller hat. Hat er der Hersteller aufgrund umfangreicher Daten sicherheitsrelevante Erkenntnisse, z.B. über Systemschwächen eines Autos oder Unfallrisiken, muss er diese Informationen unter dem Gesichtspunkt der Produktsicherheit nutzen. Dies gilt bei der Produktentwicklung nach dem neuesten Stand der Wissenschaft und Technik, aber auch im Rahmen der Herstellerpflicht zur Beobachtung eigener Produkte, die sich bereits im Verkehr befinden. Möglicherweise ist ein Hersteller frühzeitiger zu einer Warnung oder einem Rückruf verpflichtet, weil ihm Erkenntnisse über Gefährdungen durch sein Produkt vorliegen – unter Umständen in Echtzeit aus vernetzen Fahrzeugen heraus übermittelt. Big Data stellt den Hersteller vor die Aufgabe, eine Unternehmensorganisation vorzuhalten, die es ihm erlaubt, die Fülle der Daten unter dem Gesichtspunkt der Produktsicherheit zu nutzen.[5] Eine zunehmende Digitalisierung kann das Fahren sicherer machen und insbesondere Schäden durch menschliches Versagen minimieren. Sie verlagert aber auch Verantwortlichkeiten auf die Hersteller. Die Anforderungen an die Sicherheit ihrer Produkte steigen, und damit letztlich auch die Risiken einer Produkthaftung.

Neue Ansätze und Deckungskonzepte gefordert

Ob das Thema tatsächlich Bauchschmerzen bereitet oder nicht – Cyberrisiken beschäftigen Unternehmen und Versicherer zu Recht. Gesetzgeberische Initiativen zum Datenschutz und Bestrebungen, einheitliche IT-Sicherheitsstandards zu schaffen, können hel-

[5] Vgl. instruktiv Hartmann, DAR 2015, 122 ff.

fen, Cyberrisiken zu begegnen. Allerdings steigen auch mögliche Haftungsrisiken für Unternehmen im Fall von Datenschutzverstößen. Haftungsrisiken und das Risiko gravierender Eigenschäden rücken die Themen IT-/Datensicherheit und Versicherungsschutz in den Fokus von Unternehmensleitern. Die fortschreitende Digitalisierung und damit verbundene Cyberrisiken haben auch auf „klassische“ Risiken und deren Versicherung Auswirkungen. Dies gilt insbesondere für den Bereich der Produkthaftung. Je höher der Digitalisierungsgrad der Produkte und Abläufe ist, desto höher ist auch eine mögliche Anfälligkeit. Beispiele des Flugverkehrs und des vernetzten Fahrens zeigen, dass sich Haftungsrisiken verlagern – vom Betreiber, Piloten oder Fahrer hin zu den Herstellern der Systeme, die das sicherere Fliegen oder Fahren gewährleisten sollen.

Versicherungsnehmer müssen die beschriebenen Entwicklungen im Rahmen ihres Risikomanagements berücksichtigen. Versicherer stehen vor der Herausforderung, bedarfsgerechten Versicherungsschutz bereitzustellen, der diesen Entwicklungen Rechnung trägt. Dies erfordert neue Ansätze und Deckungskonzepte.

Autor: Christian Drave, LL.M.

Für Rückfragen steht Ihnen der Leiter unserer Praxisgruppe Versicherungsrecht gern zur Verfügung:

Dr. Fabian Herdter, LL.M. Eur.
Rechtsanwalt und Partner

WILHELM Partnerschaft von Rechtsanwälten mbB
Tel: +49 211 687746 50
fabian.herdter@wilhelm-rae.de