

# Versicherungs wirtschaft

Magazin für Führungskräfte und Entscheider

75. Jahrgang | JULI 2020 | 22,- €

ISSN 0042-4358 | E 6945

## Eine Welt in Pixeln

Das System Versicherung am digitalen Wendepunkt

### HISTORISCH GEWACHSEN

Zeitgeschichte aus  
200 Jahren Gothaer

### KRAFTFAHRT IM UMBRUCH

Die wichtigsten  
Trends in der Analyse

### „CORONA-URTEIL“

Was das LG Mannheim  
nicht beachtet hat

# Von Fall zu Fall verschieden

Der Verzicht auf technische Obliegenheiten in der Cyberversicherung und seine Folgen

*Von Dr. Dan Schilbach*

Die Mehrzahl der auf dem Markt verfügbaren Deckungskonzepte zur Versicherung von Cyberrisiken enthält einen zum Teil umfangreichen Katalog technischer Obliegenheiten, die der Versicherungsnehmer erfüllen muss, um seinen Versicherungsschutz im Leistungsfall nicht zu gefährden. Bei diesen Obliegenheiten handelt es sich zumeist um solche technisch-organisatorischer Art. Sie sollen den Versicherungsnehmer dazu anhalten, für die Dauer des Versicherungsvertrags ein angemessenes IT-Sicherheitsniveau sicherzustellen. Dazu gehört insbesondere, die eigenen informationsverarbeitenden Systeme mit einem aktuell gehaltenen Schutz gegen Schadsoftware auszustatten, die Einrichtung eines Patch-Managementverfahrens, eines turnusmäßigen Datensicherungsprozesses sowie eines ausreichend komplexen Passwortmanagements.

Mitunter sind die vom Versicherungsnehmer zu erfüllenden Sicherheitsmaßnahmen nur im Rahmen generalklauselartiger Obliegenheiten umschrieben, wie z.B. die Verpflichtung des Versicherungsnehmers angemessene, dem „Stand der Technik“ entsprechende technische Einrichtungen und Verfahren zur Informationssicherheit zu unterhalten. Solche Vereinbarungen sind auf Kritik gestoßen, weil sie einen im Schadenfall gefährlichen Auslegungsspielraum aufweisen. Zwar darf hier nicht unberücksichtigt bleiben, dass dem Versicherer bei der Formulierung sicherheitstechnischer Obliegenheiten, angesichts der hohen Änderungsdynamik auf dem Gebiet der Informationstechnologie, ein gewisser Abstraktionsgrad zugestanden werden muss. Damit einher geht die Gefahr, dass die Frage nach der Einhaltung eines angemessenen IT-Sicherheitsniveaus nach einer Cyber-Attacke zur zentralen Streitfrage wird, wenn es darum geht, ob die Versicherung den Schaden übernimmt oder nicht. Interessant ist, dass Versicherer vereinzelt dazu übergegangen sind, überhaupt keine technischen Obliegenheiten in ihren Versicherungsverträgen zu formulieren. Es stellt sich die Frage, welche Folgen der Verzicht auf die Vereinbarung technischer Obliegenheiten für den Deckungsanspruch des Versicherungsnehmers hat, wenn sich im Schadenfall herausstellen sollte, dass wesentliche Sicherheitsstandards nicht eingehalten worden sind und der Schaden bei entsprechen-

der Umsetzung nicht oder jedenfalls nicht in selber Höhe eingetreten wäre. Die Antwort dürfte vom Einzelfall abhängen.

## GESETZLICHE OBLIEGENHEITEN

Das Versicherungsvertragsgesetz (VVG) enthält gesetzliche Obliegenheiten, die – jedenfalls soweit sie nicht in rechtlich zulässiger Weise vertraglich abbedungen sind – auch unabhängig von ihrer Regelung im Versicherungsvertrag gelten. Im hier interessierenden Kontext sind dabei insbesondere die vorvertragliche Anzeigepflicht des Versicherungsnehmers (§ 19 Abs. 1 VVG) sowie die Regelungen zur Gefahrerhöhung (§§ 23 ff. VVG) zu nennen.

*1. Vorvertragliche Anzeigepflicht:* Nach § 19 Abs. 1 VVG hat der Versicherungsnehmer bis zur Abgabe seiner Vertragserklärung die ihm bekannten Gefahrumstände, die für den Entschluss des Versicherers, den Vertrag mit dem vereinbarten Inhalt abzuschließen, erheblich sind und nach denen der Versicherer in Textform gefragt hat, dem Versicherer anzuzeigen. Dies soll dem Versicherer ermöglichen, das versicherte Risiko zutreffend einzuschätzen und eine risikoadäquate Prämie zu kalkulieren.<sup>1</sup> Die Anzahl der Fragen variiert in der Praxis sehr stark und hängt häufig von verschiedenen Risikofaktoren ab. Das Vorliegen bestimmter Risiko-Kategorien und Geschäftsfelder sowie jährliche Umsatzgrößen spielen dabei regelmäßig eine besondere Rolle.

Der Muster-Fragebogen des GDV zur Risikoerfassung bei Cyberversicherungen für KMU erfasst für das höchste Risikosegment bis zu 45 Fragen. Bemerkenswert ist, dass die Einhaltung zentraler IT-Sicherheitsmaßnahmen, wie z.B. die Verwendung aktueller Sicherheits- und Verschlüsselungstechnologien oder die Einrichtung eines Patch-Management-Verfahrens, üblicherweise von den meisten Anbietern von Cyberversicherungen im Rahmen der vorvertraglichen Risikoprüfung abgefragt wird. Macht der Versicherungsnehmer bei Abgabe seiner Vertragserklärung falsche oder unvollständige Angaben, stehen dem Versicherer unter den Voraussetzungen des § 19 Abs. 2 bis 5 VVG weitreichende Gestaltungsrechte zur Verfügung; davon unberührt bleibt auch das Recht des Versicherers, den Vertrag nach §§ 22 VVG i.V. mit § 123 BGB wegen arglistiger Täuschung anzufechten. Eine

wichtige Frage in diesem Kontext ist, welche Anforderungen an die inhaltliche Präzision vorvertraglicher Risikofragen zu stellen sind. Nicht selten sind diese nur sehr allgemein gehalten. Je allgemeiner die Fragestellung, desto weniger aussagekräftig fällt häufig allerdings auch die Antwort aus. Insoweit besteht das Risiko, dass die Anzeige gefahrerheblicher Umstände unterbleibt, weil dem Versicherungsnehmer die Reichweite der Fragestellung nicht hinreichend bewusst wird. Fehleinschätzungen aufgrund unklarer Fragestellungen gehen nach dem Sinn und Zweck des Frageerfordernisses zulasten des Versicherers. Hintergrund der Einführung des Frageerfordernisses war es gerade dem Versicherungsnehmer die Last zu nehmen, selbst beurteilen zu müssen, welche Umstände er in Bezug auf das versicherte Risiko als gefahrerblich zu offenbaren hat.<sup>2</sup> Pauschale Fragen eignen sich im Hinblick auf die Bewertung des IT-Sicherheitsniveaus regelmäßig nicht dazu, ein umfassendes Risikobild über das zu versichernde Unternehmen zu vermitteln. Etwaige daraus resultierende Fehlvorstellungen des Versicherers können dem Versicherungsnehmer im Schadenfall nicht unter Verweis auf dessen vorvertragliche Anzeigeobligiertheit zum Vorwurf gemacht werden.

**2. Gefahrerhöhung:** Die vorvertragliche Risikoprüfung bildet naturgemäß nur den Sicherheitsstandard zum Zeitpunkt der Vertragserklärung des Versicherungsnehmers ab. Ändert sich der Sicherheitsstandard nach diesem Zeitpunkt, so begründet dies regelmäßig eine Gefahrerhöhung i.S. von § 23 VVG. Nach der Rechtsprechung liegt eine Gefahrerhöhung vor, wenn ein Umstand unter Berücksichtigung möglicher Kausalverläufe die Wahrscheinlichkeit des Eintritts des Versicherungsfalls ex ante steigert.<sup>3</sup> In zeitlicher Hinsicht ist Bezugspunkt der Gefahrerhöhung gem. § 23 Abs. 1 VVG die Abgabe der Vertragserklärung des Versicherungsnehmers. Jener Zeitpunkt ist nämlich maßgeblich für die auf Grundlage der Anzeigen des Versicherungsnehmers vorzunehmende Risikokalkulation des Versicherers.<sup>4</sup> Umstände, nach denen der Versicherer vor Abgabe der Vertragserklärung des Versicherungsnehmers in Textform gefragt hat, sind deshalb regelmäßig auch gefahrerhebliche Umstände i.S. von § 23 VVG. Die Musterbedingungen des GDV für die Cyberrisiko-Versicherung (AVB-Cyber) definieren insoweit explizit in Ziffer B3-2.1.2, dass eine Gefahrerhöhung dann vorliegen kann, wenn sich ein gefahrerheblicher Umstand ändert, nach dem der Versicherer vor Vertragsschluss gefragt hat.

Die vom Versicherer vor Vertragsschluss gestellten Fragen zum IT-Sicherheitsniveau des Versicherungsnehmers erlangen damit auch über die vorvertragliche Risikoprüfung hinaus weiterhin an Bedeutung. Insoweit darf der Verzicht auf technische Obliegenheiten in Cyberversicherungsverträgen nicht zu der Fehlannahme verleiten, der Versicherungsnehmer

hätte über den versicherten Zeitraum überhaupt keine IT-sicherheitsrelevanten Obliegenheiten zu erfüllen. Fragt der Versicherer vor Vertragsschluss nach der Einhaltung technischer und organisatorischer Schutzmaßnahmen und stellt sich im Schadenfall heraus, dass der Versicherungsnehmer jene Schutzmaßnahmen nicht eingehalten hat, kann sich die Nichteinhaltung vielmehr ungeachtet einer korrespondierenden vertraglichen Obliegenheit nach den Grundsätzen über die Gefahrerhöhung deckungsschädlich auf den Versicherungsanspruch des Versicherungsnehmers auswirken. Es gibt freilich Deckungskonzepte, die den Begriff der Gefahrerhöhung zugunsten des Versicherungsnehmers modifizieren und auf bestimmte, vertraglich festgelegte Umstände reduzieren. Hier kann sich der Versicherer auf die Rechtsfolgen einer Gefahrerhöhung (§§ 24 ff. VVG) nur dann berufen, wenn der Versicherungsnehmer die Anzeige einer der vertraglich vereinbarten gefahrerhöhenden Umstände unterlässt. AGB-rechtlich sind derartige Modifizierungen wirksam, soweit sie für den Versicherungsnehmer günstig sind (vgl. § 32 Satz 1 VVG). Für den Versicherer begründen sie zum Teil eine erhebliche Risikoerhöhung, da im Schadenfall häufig keine rechtliche Handhabe besteht, die sich nach Vertragsschluss ändernde Gefahrenlage deckungsrechtlich einzuwenden.

Wie sich zeigt, bedeutet der Verzicht auf die Vereinbarung technischer Obliegenheiten in Cyberversicherungsverträgen nicht zwangsläufig auch, dass der Versicherungsnehmer überhaupt keine IT-sicherheitsrelevanten Maßnahmen mehr zu beachten hat. Je nachdem, in welchem Umfang der Versicherer das Vorhandensein technischer und organisatorischer Sicherheitsstandards zum Gegenstand seiner vorvertraglichen Risikoprüfung macht, können sich eine Vielzahl damit korrespondierender Verhaltensgebote für den Versicherungsnehmer auch ohne konkrete vertragliche Vereinbarung ergeben. Es ist deshalb auch Aufgabe von Maklern und Versicherern, im Rahmen ihrer gesetzlichen Beratungspflichten entsprechende Klarheit zu schaffen.

1 Armbrüster, in: Prölss/Martin, 30. Aufl. 2018, § 19 Rn. 1.

2 Armbrüster, Privatversicherungsrecht, 2. Aufl. 2020, Rn. 909; RegBegr., BT-Drs. 16/3945, S. 64.

3 BGH, Urt. v. 20.06.2012 – IV ZR 150/11, VersR 2012, 1300 Rn. 8.

4 Looschelders, in: Looschelders/Pohlmann, VVG, 3. Aufl. 2016, § 23 Rn. 9.



**Dr. Dan Schilbach**

Rechtsanwalt bei Noerr LLP in Düsseldorf