Auswirkungen der DSGVO auf die D&O- und Cyberversicherung: Teil II – Haftung des Managements bei Nichtabschluss einer Cyberversicherung

Eine Pflicht zum Abschluss einer Cyberversicherung besteht grundsätzlich nicht, sondern liegt zunächst im Ermessen des Managements. In Einzelfällen kann der Abschluss einer Cyberversicherung dennoch obligatorisch sein. Der zweite Teil des Beitrags befasst sich mit der Frage, ob, in welchen Fällen und aufgrund welcher Rechtsgrundlagen sich eine Haftung der Geschäftsleitung bei Nichtabschluss einer Cyberversicherung ergeben kann.

Cyberversicherung als Präventivmaßnahme?
Nach § 91 Abs. 2 AktG ist die Geschäftsleitung grundsätzlich verpflichtet, geeignete Maßnahmen zu treffen, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen frühzeitig erkannt werden. Diese Pflicht ist auch für andere Kapitalgesellschaften als die Aktiengesellschaft anerkannt. Unter bestandsgefährdenden Entwicklungen sind alle Entwicklungen zu verstehen, die in ihrer Konsequenz zu einer schwerwiegenden Beeinträchtigung der Vermögens-, Ertrags- oder Finanzlage des Unternehmens führen. Die gesamte Unternehmensleitung ist daher neben der Risikokontrolle auch zur Schadensprävention verpflichtet.

Wegweisend war insoweit das sogenannte „Siemens/Neubürger-Urteil“ des Landgerichts München I (Urt. v. 10.12.2013, 5 HKO 1387/10, LS 1). Danach gehört es zu den Pflichten der

gesamten Geschäftsleitung im Rahmen der Legalitätspflicht, das Unternehmen so zu organisieren, dass es zu keinen Gesetzesverstößen kommen kann und alle Verpflichtungen durch das Unternehmen erfüllt werden. Auch die Geschäftsführung einer GmbH ist dazu verpflichtet, ein Compliance Management System (CMS) einzuführen (OLG Nürnberg, Urt. v. 30.03.2022, Az. 12 U 1520/19). Die Geschäftsleitung muss durch geeignete organisatorische Maßnahmen verhindern, dass sich Risiken für die Informationssicherheit realisieren. Solche Risiken können intern, aber auch durch externe Einflüsse bestehen. Reduziert werden sie zum Beispiel durch die Implementierung eines effektiven Informationssicherheits-Managementsystems (ISMS).

Als präventive Maßnahme kann das Management eine Cyberversicherung abschließen. Hierbei ist jedoch zu beachten, dass es sich grundsätzlich nicht um eine Methode der Risikofrüherkennung, sondern primär um eine Maßnahme zur (nachträglichen) Risikobewältigung handelt. Eine Verpflichtung zum Abschluss einer Cyberversicherung besteht grundsätzlich nicht, sondern liegt zunächst im Ermessen der Geschäftsleitung.

DSGVO-Deckung in Cyberversicherungen

Generell bieten Cyber-Policen auch im Hinblick auf die DSGVO Versicherungsschutz. Während die Betriebshaftpflichtversicherung bei nicht-elektronischen Datenschutzverletzungen schützt, kann die Cyberversicherung die Lücke in Bezug auf die digitale Datenverarbeitung schließen. In vielen Cyber-Policen sind Bußgelder, die im Rahmen der DSGVO verhängt werden, mitversichert.

Die Cyberversicherung kann darüber hinaus weitere Leistungsbausteine enthalten, die im Falle einer Datenschutzverletzung sinnvoll sind. Je nach Bedingungswerk werden beispielsweise häufig auch die Rechtsanwaltskosten im Vorfeld eines möglichen DSGVO-Bußgeldverfahrens übernommen. Dies umfasst die Beratung zum weiteren rechtlichen Vorgehen, um negative Folgen abzumildern, sowie die anwaltliche

Unterstützung bei der Meldung eines Vorfalls an die Datenschutzbehörde. Denkbar ist auch, dass im Zuge eines öffentlichkeitswirksamen Bußgeldverfahrens ein Reputationsschaden für das versicherte Unternehmen droht. Hier sehen einige Cyberversicherungen Leistungen vor, um den Reputationsschaden abzumildern oder zu verhindern. Beispielsweise kann die Beauftragung eines externen Krisenberaters oder die Platzierung von Nachrichten, Darstellungen oder Anzeigen in verschiedenen Medien im Versicherungsschutz enthalten sein.

Haftung des Managements bei Nichtabschluss einer Cyberversicherung

Zwar besteht – wie dargestellt – grundsätzlich keine Pflicht zum Abschluss einer Cyberversicherung. Eine Pflichtverletzung könnte sich jedoch daraus ergeben, dass die Geschäftsführung es unterlassen hat, im Rahmen des Risikomanagements die Notwendigkeit einer solchen Versicherung überhaupt zu prüfen oder im Einzelfall bei einer „Ermessensreduzierung auf Null“ eine solche Versicherung abzuschließen. Gerade hoch digitalisierte und damit enorm exponierte Unternehmen könnten hier anders zu bewerten sein. Dies wäre vergleichbar mit dem Verzicht auf den Abschluss einer Feuerversicherung bei hochgradig brandgefährdeten Unternehmen.

Mit der neuen NIS2-Richtlinie soll auch eine besondere Haftung von Führungskräften für Verstöße gegen die erweiterten IT-Sicherheitspflichten eingeführt werden. Der Anwendungsbereich einer D&O-Versicherung könnte daher im Rahmen des Datenschutzes und der IT-Sicherheit in mehrfacher Hinsicht betroffen sein.

Dieser wäre eröffnet, wenn der Geschäftsführer gegen gesetzliche Vorschriften zur Cybersicherheit verstößt (zum Beispiel Art. 82 DSGVO) und haftbar gemacht wird. Die direkte Geldbuße gegen das Organmitglied ist in der D&O-Versicherung standardmäßig ausgeschlossen. Der Regress einer Unternehmensgeldbuße gegen das Management wegen mangelnder

Compliance ist jedoch in der Regel ausdrücklich mitversichert – vorausgesetzt, der Regress ist haftungsrechtlich zulässig und auch versicherbar.

In Umsetzung der NIS2-Richtlinie soll nach dem derzeit vorliegenden Referentenentwurf die persönliche Haftung der Leitungsebene deutlich verschärft werden. In wichtigen und besonders wichtigen Einrichtungen muss nach dem Entwurf die Geschäftsleitung die Risikomanagementmaßnahmen im Bereich der Cybersicherheit billigen und deren Umsetzung überwachen. Sie kann diese Aufgaben nicht delegieren, für Schäden aus Verstößen muss gehaftet werden, ein Haftungsverzicht des Unternehmens soll unwirksam sein. Dementsprechend könnte ein D&O-Schadensfall auch dann in Betracht kommen, wenn dem Vorstand im Einzelfall ausnahmsweise eine Pflichtverletzung vorzuwerfen ist, weil er keine Cyberversicherung abgeschlossen und insoweit eine ermessensfehlerhafte Entscheidung getroffen hat.

Um überhaupt eine Entscheidung treffen zu können, muss das Management eine ausreichende Faktenbasis schaffen. Dabei sind unter Abwägung von Kosten und Nutzen möglichst alle zur Verfügung stehenden Informationsquellen heranzuziehen. Die notwendigen Informationen für oder gegen den Abschluss einer Cyberversicherung beschränken sich keineswegs auf die Inhalte und Deckungssummen des Versicherungsvertrages, sondern gehen weit darüber hinaus. So muss sich die Geschäftsleitung zunächst einen Überblick darüber verschaffen, welche Schäden ein Cyberangriff überhaupt verursachen könnte. Darauf aufbauend muss sie beurteilen können, welche technischen und organisatorischen Maßnahmen zum Schutz vor solchen Angriffen bereits getroffen wurden oder noch getroffen werden können. Erst daraus lässt sich ableiten, ob und wenn ja, welches Restrisiko für die Gesellschaft besteht. Dieses Risiko wiederum ist einerseits dem gebotenen Versicherungsschutz gegenüberzustellen, andererseits aber auch in ein wirtschaftliches Verhältnis zur zu zahlenden

Versicherungsprämie zu setzen (vgl. Fortmann, r+s 2019, 688, 691).

Empfehlung: Um diese durchaus anspruchsvolle Prüfung durchführen und entsprechend dokumentieren zu können, empfiehlt es sich, externe Beratung in Anspruch zu nehmen, sei es durch spezielle Beratungsfirmen oder Versicherungsmakler, die den Prozess begleiten. Auch der Risikodialog mit dem Cyberversicherer kann bei der Entscheidungsfindung helfen.

Beitragsbild: Beautrium / Shutterstock

Autor:
Rechtsanwalt Dr. Stefan Steinkühler
Rechtsanwalt Dr. Stefan Steinkühler steht der VSMA GmbH seit Mitte des Jahres 2020 als juristischer Berater bei haftungs- und versicherungsrechtlichen Themen zur Seite. Er verfügt über langjährige Erfahrungen in der Versicherungswirtschaft. Seine Tätigkeitsschwerpunkte liegen neben der Bearbeitung von Sach-/BU- und Produkthaftungsschäden vor allem Fälle im Bereich der D&O- und VSV-Versicherung sowie der dazugehörigen Managerhaftung.

www.ra-steinkuehler.de