Zeitschrift für die gesamte Versicherungswissenschaft, 113 (2024), 11 – 53
https://doi.org/10.3790/zverswiss.2024.1430501

Aktuelle Entwicklungen in der Cyberversicherung

Robert Koch

Zusammenfassung

Die heutige Cyberversicherung markiert das Ende einer Entwicklung, die zu Beginn der 1970er Jahre ihren Anfang genommen hat. Der Umfang der Deckung hat sich seit der Einführung der Cyberversicherung zu Beginn der 2010er Jahre kontinuierlich erweitert. Neu und insoweit innovativ ist die Aufnahme zahlreicher Assistance-Leistungen in das Leistungsangebot, die insbesondere die Bedürfnisse von KMUs befriedigt. Dieser Beitrag gibt einen Abriss über die Ursprünge bzw. die Entwicklung der Cyberversicherung und einen Überblick über den Umfang des Versicherungsschutzes in ihrer aktuellen Ausgestaltung. Zudem werden werden ausgewählte cyberversicherungsspezifische Inhalte näher betrachtet (z. B. Erstattung von Lösegeldzahlungen).

Abstract

Todays's cyber insurance marks the end of a development that began in the early 1970s. Since the introduction of cyber insurance in the early 2010s, the scope of cover has continuously expanded. A new and innovative feature is the inclusion of numerous assistance services in the insurance cover, which meet the needs of SMEs in particular. This article provides an outline of the origins and development of cyber insurance and an overview of the scope of insurance cover in its current form. It also takes a closer look at selected cyber insurance-specific content (e. g. coverage for ransom payments).

1. Einleitung

Die Cyberversicherung hat sich mittlerweile als eigenständiges Versicherungsprodukt etabliert. Die Bundesanstalt für Finanzdienstleistungsaufsicht beschreibt die charakteristischen Merkmale der Cyberversicherung wie folgt:[1]

Der Autor, Prof. Dr. Robert Koch, LL.M. (McGill), ist Inhaber des Lehrstuhls für Bürgerliches Recht und Versicherungsrecht an der Universität Hamburg und Geschäftsführender Direktor des Seminars für Versicherungswissenschaft.
Universität Hamburg
Mail: robert.koch@uni-hamburg.de

[1] Mitteilung vom 15.9.2017, https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Meldung/2017/meldung_170915_loesegeldversicherung.html; vgl. auch BaFin Jour-

Duncker & Humblot · Berlin

„Cyberversicherungen sichern gegen die Folgen von Cyberrisiken ab. Darunter fallen alle Arten von Informationssicherheitsverletzungen aufgrund unbefugter oder fehlerhafter Nutzung von informationsverarbeitenden Systemen, also die Beeinträchtigung der Verfügbarkeit, der Vertraulichkeit, der Integrität und der Authentizität elektronischer Daten."

Nach Angaben des Gesamtverbands der Deutschen Versicherungswirtschaft e.V. (GDV) hatten Ende 2021 knapp 243.000 Kunden eine Cyberversicherung abgeschlossen – ein Viertel mehr als ein Jahr zuvor. Ähnlich stark würden die Vertragszahlen auch im ersten Halbjahr 2022 zunehmen.[2] Ungeachtet dieses Anstiegs bleibt die wirtschaftliche Entwicklung jedoch hinter den Erwartungen der Versicherer zurück. 2017 rechneten Allianz und AXA für den deutschen Unternehmensbereich im Jahr 2021 bereits mit einem Prämienvolumen von bis zu 300 Mio. EUR. KPMG ging sogar von Prämieneinnahmen zwischen 420 und 880 Mio. Euro für 2021 aus.[3] Tatsächlich beliefen sich die Einnahmen nach Angaben des GDV auf 178 Mio. Euro.[4]

Als Hauptgründe für die Zurückhaltung werden eine noch immer mangelnde Risikowahrnehmung und ein mangelndes Risikobewusstsein auf der Nachfrageseite genannt.[5] Vertriebsseitig dürften die Komplexität des Produkts und die Vielfalt der Bedingungswerke, die einen direkten Vergleich erschweren, ein Hindernis für ein schnelleres Wachstum sein. Die Komplexität der Cyberversicherung resultiert vor allem daraus, dass sie in Form einer verbundenen Versicherung angeboten wird, bei der mehrere Versicherungssparten (verschiedene finanziellen Verluste (Eigenschäden), Haftpflicht, Kredit) in einem Vertrag zusammengeführt werden. Abweichend von z. B. der Kfz-Versicherung, in der Haftpflicht-, Kasko-, Autoschutzbrief-, Unfall- und Fahrerschutzversicherung

---

nal, September 2021, S. 6, https://www.bafin.de/SharedDocs/Downloads/DE/BaFinJournal/2021/bj_2109.pdf?__blob=publicationFile&v=3 (zuletzt abgerufen am: 21.4.2023): „Eigener Versicherungszweig denkbar".

[2] https://www.gdv.de/gdv/medien/medieninformationen/cyber-ver-si-che-rer-machen-erst-mals-ver-luste-markt-legt-wei-ter-zu-89766 (zuletzt abgerufen am: 21.4.2023).

[3] Baban/Barker/Gruchmann/Paun/Peters/Stuchtey: Cyberversicherungen als Beitrag zum IT-Risikomanagement – Eine Analyse der Märkte für Cyberversicherungen in Deutschland, der Schweiz, den USA und Großbritannien, BIGS Standpunkt Nr. 8, September 2017, S. 28 f., https://www.bigs-potsdam.org/publikationen/cyberversicherungen-als-beitrag-zum-it-risikomanagement-eine-analyse-der-maerkte-fuer-cyberversicherungen-in-deutschland-der-schweiz-den-usa-und-grossbritannien/ (zuletzt abgerufen am: 21.4.2023).

[4] https://www.gdv.de/gdv/medien/medieninformationen/cyber-ver-si-che-rer-machen-erst-mals-ver-luste-markt-legt-wei-ter-zu-89766 (zuletzt abgerufen am: 21.4.2023).

[5] *Heinrichsmeier*, in: Hartung, Versicherbarkeit von Cyber-Risiken? (2020), S. 16; https://www.unibw.de/insurance/reader_2020_cyber_risiken.pdf (zuletzt abgerufen am: 21.4.2023).

ebenfalls in einem Bedingungswerk integriert sind,[6] handelt es sich bei der Cyberversicherung nicht um jeweils rechtlich selbstständige Verträge.

Die Bündelung verschiedener Sparten stellt die Versicherer vor besondere Herausforderungen bei der Ausgestaltung der Versicherungsbedingungen, da sich die versicherungsvertraglichen Rahmenbedingungen für diese Sparten unterscheiden. Die Versicherer müssen deshalb bei der Abfassung der Klauseln darauf achten, nicht Begriffe zu verwenden, die kennzeichnend nur für eine Sparte sind. Um diesbezüglich Unklarheiten zu vermeiden, müssen sie ggf. eigene Definitionen aufnehmen. Es verwundert deshalb nicht, dass die Bedingungswerke im Durchschnitt weit mehr als 20 Seiten umfassen, was wiederum Versicherungsvermittler und erst recht Versicherungsnehmer vor Herausforderungen stellt. In jedem Fall besteht ein erhöhter Beratungsbedarf für (potentielle) Versicherungsnehmer.

Im Folgenden soll zunächst ein Abriss über die Ursprünge bzw. die Entwicklung der Cyberversicherung (sub 2.) und ein Überblick über den Umfang des Versicherungsschutzes (sub 3.) gegeben werden. Sodann werden ausgewählte cyberversicherungsspezifische Fragestellungen wie die Prioritätsklausel und die Erstattungsfähigkeit von Lösegeldzahlungen näher betrachtet (sub 4.).

2. Entwicklung der Cyberversicherung

Die Cyberversicherung, die in ihrer aktuellen Erscheinungsform Drittschäden und Eigenschäden versichert, markiert den vorläufigen Endpunkt einer Entwicklung, die sich grob in drei Phasen unterteilen lässt.

2.1 Phase 1970 bis 2000

2.1.1 Computer-Missbrauch-/Datenmissbrauch-Versicherung

Die Anfänge der Cyberversicherung in Deutschland gehen auf die Computer-Missbrauch-Versicherung (Absicherung gegen Computerkriminalität der eigenen Mitarbeiter)[7] sowie die Datenmissbrauch-Versicherung (Absicherung gegen Computerkriminalität externer Dritter)[8] zurück, die als Ausschnittsdeckungen zur Vertrauensschadensversicherung im Hinblick auf EDV-Delikte in den

[6] Vgl. *Koch*, in: Bruck/Möller, VVG, 9. Aufl. 2018, Band 12 (Kraftfahrtversicherung), Präambel AKB 2015 Rn. 3.

[7] *Mucksch*, Datenschutz und Datensicherung in Klein- und Mittelbetrieben, 1988, S. 189.

[8] *Ihlas*, VersR 1994, 898 ff.; Kersten, VersR 1987, 1172 ff.

1970er und 1980er Jahren eingeführt wurden.[9] Das Risiko des Datenmissbrauchs durch externe Dritte gehört an sich nicht zur Vertrauensschadensversicherung, weil es gerade nicht Mitarbeiter sind, die diese Schäden verursachen. Zudem wird eine Identifizierung der Täter nur selten möglich sein. Die sich aus dem Nebeneinander der verschiedenen Bedingungswerke ergebende Redundanz veranlasste die Vertrauensschadenversicherer jedoch dazu, diese unter Aufgabe des bis dato bestehenden Erfordernisses der Identifizierung des Täters zum Nachweis über den Versicherungsfall in einem einheitlichen Bedingungswerk zusammenzuführen.[10]

2.1.2 Daten-/-träger- und Softwareversicherung

In der Sachversicherung fand die Datenträgerversicherung bereits 1976 als Klausel 638 Eingang in die Allgemeinen Versicherungsbedingungen für Fernmelde- und sonstige elektrotechnische Anlagen 1976 (AVFE 76).[11] Voraussetzung für den Versicherungsschutz war ein Sachschaden an dem Datenträger. Versichert waren die Kosten beschädigter und entwendeter Datenträger einschließlich der Wiederherstellungskosten darauf gespeicherter Daten. Die Datenverluste mussten in zeitlichem Zusammenhang mit dem Schaden am Datenträger stehen.[12] Im Jahr 1989 bot die TELA Versicherung AG erstmalig die Software-Versicherung im deutschen Markt an, bei der ein Sachschaden am Datenträger nicht mehr Voraussetzung für die Deckung war.[13]

Im Jahre 1997 veröffentlichte der GDV die Musterbedingungen zur Datenträger- und Datenversicherung (Klausel 010 zu den ABE) und zur Softwareversicherung (Klausel 028 zu den ABE) als Zusatzbausteine zur Elektronikversicherung. Abgesehen von dem Datenverlust infolge einer Blitzeinwirkung war Voraussetzung für den Versicherungsschutz in der Datenträger- und Datenversicherung, dass die eingetretenen Schäden auf einem Sachschaden an dem betroffenen Datenträger zurückzuführen waren und die Daten dadurch nicht mehr gelesen werden konnten. Das bloße versehentliche Löschen von Daten war nicht versichert. In der Softwareversicherung wurden weitergehend auch nachteilige Datenveränderungen/-verluste versichert, die nicht aus einem Sachschaden am Datenträger resultierten, sondern durch Schadprogramme verursacht wurden. Auch der Verlust durch Bedienungsfehler war versichert.[14] Für Schäden infolge von Denial-of-Service-Attacken (DoS) bestand kein Versiche-

[9] *Kersten*, VersR 1987, 1172; Ihlas, VersR 1994, 898 ff.
[10] *Koch*, VersR 2005, 1192.
[11] Vgl. LG Aachen v. 11.3.1987 – 4 O 38/86, CR 1987, 857.
[12] Vgl. LG Aachen v. 11.3.1987 – 4 O 38/86, CR 1987, 857.
[13] Vgl. *Mehl*, VW 1996, 522; Seitz, VW 1990, 1300.
[14] Vgl. *Tita*, VW 2001, 1696.

rungsschutz, weil es an der Grundvoraussetzung einer nachteiligen Datenveränderung bzw. eines Datenverlustes fehlte.

2.2 Phase 2000 bis 2010

2.2.1 Daten-/-träger- und Softwareversicherung

Die Datenträger- und Datenversicherung und die Softwareversicherung fristeten bis zum Jahr 2000 sowohl in der Rechtsprechung als auch im Schrifttum ein Schattendasein.[15] Das änderte sich erst mit der Diskussion um den „Millenium Bug" (Jahr-2000-Fehler). Zur Vorsorgeplanung der Managements eines Unternehmens gehörte nämlich auch, die bestehenden Versicherungspolicen im Detail daraufhin zu untersuchen, ob mögliche Jahr-2000-Schäden abgedeckt waren.

Zunächst sollte es bei der Softwareversicherung jedoch zu einer Einschränkung des Versicherungsschutzes kommen. Auf Druck der Rückversicherer wurde die Deckung für vorsätzliche Programm- oder Datenänderungen durch Dritte z. B. durch Viren wegen des Kumulrisikos aus der Softwareversicherung wieder herausgenommen.[16] Deckung wurde nur noch für gezielte Angriffe gegen den Versicherungsnehmer gewährt. Eine darauf aufbauende Versicherung von Mehrkosten oder Ertragsausfall infolge einer Betriebsunterbrechung wurde nur ganz vereinzelt von ausländischen Versicherungsgesellschaften angeboten.

Die aktuellen Zusatzbausteine zur Elektronikversicherung (TK A 1928 ABE 2020 Datenversicherung und TK A 1929 ABE 2020 Erweiterte Datenversicherung) verlangen keinen Schaden am Datenträger und machen die nachteilige Datenveränderung nicht mehr zur Voraussetzung für die Deckung. Die Erweiterte Datenversicherung – wie die Softwareversicherung nunmehr heißt – umfasst auch Hackerangriffe, DoS-Attacken sowie Angriffe mittels Schadsoftware. Der Versicherer leistet Entschädigung bis zur Höhe der hierfür vereinbarten Versicherungssumme auf erstes Risiko für die Feststellung der Ursachen und Auswirkungen des Versicherungsfalls; für die Wiederbeschaffung, Wiederherstellung oder Wiedereingabe von verschlüsselten, beschädigten, verlorengegangenen oder gelöschten Daten und für die Beseitigung von Schadsoftware.

---

[15] Vgl. *Tita*, VW 2001, 1696; *Heussen/Damm*, BB 1999, 481, 484; Mehl, VW 1996, 522.

[16] S. TV-Rundschreiben (580) des GDV vom 16.10.2000 (Klausel 028 zu den ABE i. d. F. Oktober 2000) und TV-Rundschreiben (602) des GDV vom 20.6.2002 (Klausel 028 zu den ABE i. d. F. Mai 2002).

2.2.2 Haftpflichtversicherung

Im Fremdschadensbereich tat sich auf der Produktentwicklungsseite vor der Jahrtausendwende nichts. Erst im Jahr 2001 veröffentlichte der GDV Besondere Bedingungen und Risikobeschreibungen für die Haftpflichtversicherung von Software-Häusern (BBR Software), die auf AHB-Basis eine „offene" (Allgefahren-)Vermögensschadendeckung anboten. Die BBR Software waren allerdings ausschließlich auf das reine Software-Haus mit seinen typischen Annextätigkeiten zugeschnitten (Software-Erstellung, -Handel, -Implementierung, -Pflege; IT-Analyse, -Organisation, -Einweisung, -Schulung; Netzwerkplanung, -installation, -integration, -pflege).

Der Bereich des Internet-Providing blieb ausgeklammert. In einem zweiten Schritt erweiterte der GDV im Jahr 2002 die BBR Software zu einem umfassenden IT-Versicherungsmodell, das die Bezeichnung Besondere Bedingungen und Risikobeschreibungen für die Haftpflichtversicherung von IT-Dienstleistern (BBR IT-Dienstleister) trägt. Diese beziehen insbesondere auch die Internet-Provider sowie die Risiken aus Herstellung und Handel von Hardware in den Deckungsumfang mit ein. Die BBR IT-Dienstleister basieren auf den AHB und sind seit April 2007 nicht überarbeitet worden.

Mit der Neufassung der AHB wurden Schäden aus dem Austausch, der Übermittlung und der Bereitstellung elektronischer Daten z. B. im Internet, per E-Mail oder mittels Datenträger ausgeschlossen (Ziff. 7.15 AHB). Zugleich wurden diese Schäden in der Privathaftpflichtversicherung wiedereingeschlossen (Ziff. 4.16 BBR PHV). In der Betriebshaftpflichtversicherung auf Basis der BBR BHV blieb es dagegen bei der durch den IT-Risiko-Ausschluss in Ziff. 7.15 AHB bewirkten Nullstellung von Schäden, die aus IT-nutzungsspezifischen Risiken resultieren. Um diese Deckungslücke zu schließen, bestand die Möglichkeit der Vereinbarung des Zusatzbausteins Betriebshaftpflichtversicherung für die Nutzer von Internet-Technologien (BetrH IT). In den durchgeschriebenen Muster-Bedingungswerken des GDV sind diese Risiken nunmehr standardmäßig in der Betriebshaftpflichtversicherung ohne inhaltliche Änderungen versichert (vgl. A1-6.13.2 AVB BHV).

2.2.3 Vertrauensschadensversicherung

Die Vertrauensschadenversicherer weiteten ihre Deckung Mitte der 2010er Jahre auf unmittelbare und rechtswidrige Eingriffe in die elektronische Datenverarbeitung des Versicherungsnehmers unter Verzicht auf das Erfordernis einer Bereicherung des Dritten aus. Die Deckung blieb jedoch beschränkt auf den Ersatz von Wiederherstellungskosten, Wiederbeschaffungskosten der beschädigten Software, Daten und Dateien und Mehrkosten als Folge eines

zielgerichteten Angriffs gegen den Versicherungsnehmer.[17] Keine Deckung wurde gewährt, wenn sich der Eingriff gegen eine unbestimmte Anzahl von EDV-Nutzern richtete. Zudem wurde auch Versicherungsschutz für Fremdschäden geboten, die aus unerlaubten Handlungen der Vertrauenspersonen resultierten. Ausgenommen vom Versicherungsschutz waren mittelbare Schäden. Für Betrugsschäden durch falsche Identität wie z. B. beim „Fake President Fraud" bestand sublimitiert Versicherungsschutz, soweit die Vertrauensperson den Schaden nicht grob fahrlässig mitverursacht hatte.[18]

In ihrer aktuellen Erscheinungsform weist die Vertrauensschadensversicherung diese Einschränkung nicht mehr auf. Weiterhin sind im Grundsatz nur unmittelbare Schäden versichert. Für bestimmte mittelbare Schäden wird mittlerweile jedoch standardmäßig Versicherungsschutz gewährt, so z. B. für Überweisungen nach Ausspähen z. B. durch Phishing, Pharming, Spyware, Keylogger und durch Missbrauch von Benutzerzugangsdaten.[19] Ebenso werden an Dritte zur Minderung eines eingetretenen Reputationsschadens geleistete Zahlungen erstattet.[20] Durch Zusatzdeckungen kann der Versicherungsschutz etwa auf den unbefugten Zugriff auf Geschäftsgeheimnisse, den Ausfall von automatisierten Lagersystemen oder die Störung von Online-Vertriebssystemen erweitert werden.[21] Für Löse- und Erpressungsgeld wird jedoch keine Deckung gewährt.[22]

2.3 Phase ab 2010

Erst Anfang der 2010er Jahre wurden in Deutschland Deckungskonzepte angeboten, die ohne Beschränkung auf den Ersatz des unmittelbaren Schadens sowohl IT-Eigen- als auch IT-Fremdschadensrisiken – vielfach bereits unter der Bezeichnung Cyberversicherung – versicherten. Die Zahl der Versicherer, die ein solches Produkt anboten, war anfangs überschaubar. Die Vertragsabschlüsse erfolgten zaghaft. Spätestens mit der Veröffentlichung der AVB Cyber im Jahr 2017, in denen der GDV den spartenübergreifenden Ansatz (Multi Lines of Business) aufgriff, nahm der Wettlauf um Marktanteile zu, der dadurch gekennzeichnet war, dass die Cyberversicherer ihr Leistungsspektrum kontinuierlich ausweiteten, ohne die Versicherungsprämien anzupassen.

---

[17] *R. Koch*, Vertrauensschadensversicherung, 2006, S. 69 ff.

[18] *R. Koch*, Vertrauensschadensversicherung, 2006, S. 119.

[19] § 15 Nr. 2 Allianz Trade Allgemeine Bedingungen für die Vertrauensschadenversicherung PremiumPlus (AVB VSV PremiumPlus), https://www.allianz-trade.de/content/dam/onemarketing/aztrade/allianz-trade_de/dokumente/allgemeine-bedingungen-vertrauensschadenversicherung-premiumplus.pdf (zuletzt abgerufen am: 21.4.2023).

[20] §§ 19 f. AVB VSV PremiumPlus.

[21] Zusatzbedingungen zu den AVB VSV PremiumPlus – mittelbare Schäden.

[22] § 49 Nr. 1 AVB VSV PremiumPlus.

Nachdem die BaFin im September 2017 verlautbarte, „die Bündelung von Lösegeldversicherungen mit Cyberversicherungen […] in einem Vertrag zu akzeptieren“[23], dehnten viele Cyberversicherer den Versicherungsschutz auf Cyber-Erpressungsfälle aus. Diese Entwicklung ging bis 2020 gut. Danach stiegen die Schäden stark an. Nach Angaben des GDV zählten die Cyberversicherer im Jahr 2021 knapp 3.700 Schäden durch Hackerangriffe (+56 % gegenüber 2020) und leisteten Zahlungen über rund 137 Millionen Euro (fast dreimal so viel wie 2020). Die Schaden-Kostenquote 2021 betrug knapp 124 %. Für 2022 gibt es noch keine Zahlen.[24]

Die Cyberversicherer reagierten auf diese Entwicklung vornehmlich durch Prämienerhöhungen bei gleichzeitiger Kapazitätsverringerung, weniger durch Einschränkung des Leistungsspektrums. Bei Neuverträgen beläuft sich die Versicherungssumme eines einzelnen Versicherers im gewerblichen/industriellen Bereich in der Regel nur noch auf höchstens 10 Mio. EUR. Die Deckung für Lösegeld ist sublimitiert und beläuft sich zum Teil auf nicht mehr als 5 % der Versicherungssumme. Zudem wurden die Obliegenheiten zur Gewährleistung der IT-Sicherheit verschärft und Regelungen zur Gefahrerhöhung in den Bedingungswerken aufgenommen.

3. Umfang des Versicherungsschutzes der Cyberversicherung (Überblick)

3.1 Gegenstand der Cyberversicherung

Gemeinsames Merkmal sowohl der AVB Cyber als auch der Bedingungswerke der einzelnen Versicherer ist, dass sie keine Allgefahrendeckung bieten. Versichert sind vielmehr im Einzelnen beschriebene Eigen- und Fremdschäden infolge der Beeinträchtigung der Verfügbarkeit, Integrität und Vertraulichkeit (selten auch bei Beeinträchtigung der Zurechenbarkeit und Verbindlichkeit) von Daten und informationsverarbeitenden Systemen, die auf einer benannten Ursache (= Gefahr) beruht (Enumerationsprinzip). Mittlerweile hat sich der Begriff der Informationssicherheitsverletzung als Umschreibung für die Beeinträchtigung der Verfügbarkeit, Integrität und Vertraulichkeit weitgehend etabliert. Die Cyberversicherer bedienen sich somit einer Versicherungstechnik, die Ähnlichkeiten mit der Produkthaftpflichtversicherung aufweist, bei der nur im

[23] https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Meldung/2017/meldung_170915_loesegeldversicherung.html (zuletzt abgerufen am: 21.4.2023).

[24] https://www.gdv.de/gdv/medien/medieninformationen/cyber-ver-si-che-rermachen-erst-mals-ver-luste-markt-legt-wei-ter-zu-89766 (zuletzt abgerufen am: 21.4.2023).

Einzelnen bezeichnete Vermögensschäden aus im Einzelnen beschriebenen Produktionsvorgängen versichert sind.[25]

In struktureller Hinsicht sind die Bedingungswerke aller Cyberversicherer aufgeteilt in Versicherungsschutz für Eigenschäden und Fremdschäden, die regelmäßig als Haftpflichtschäden bezeichnet werden. Der Versicherungsschutz für Assistance-Leistungen wird oftmals in einem gesonderten Abschnitt aufgeführt, obgleich die Kosten für diese Leistungen zu den Eigenschäden zählen. Teilweise wird ein Allgemeiner Teil voran- oder nachgestellt, der für alle versicherten Schäden gilt.

3.2 Versicherte Gefahren

In den Musterbedingungen des GDV (AVB Cyber) werden die benannten Gefahren, die als Ereignisse bezeichnet werden, abschließend für die versicherten Eigen- und Fremdschäden sowie Assistance-Leistungen festgelegt.

Vgl. A1-2.4 AVB Cyber:

„Die Informationssicherheitsverletzung muss durch folgende Ereignisse ausgelöst werden:

- Angriffe auf elektronische Daten oder informationsverarbeitende Systeme des Versicherungsnehmers;
- unberechtigte Zugriffe auf elektronische Daten des Versicherungsnehmers;
- Eingriffe in informationsverarbeitende Systeme des Versicherungsnehmers;
- eine Handlung oder Unterlassung, die zu einer Verletzung von datenschutzrechtlichen Vorschriften durch den Versicherungsnehmer führt;
- Schadprogramme, die auf elektronische Daten oder informationsverarbeitende Systeme des Versicherungsnehmers wirken."

In der Marktpraxis wird der Begriff der Informationssicherheitsverletzung zum Teil unterteilt in Datenschutzverletzung, Datenvertraulichkeitsverletzung und Netzwerksicherheitsverletzung und die versicherten Gefahren werden gesondert für jede Unterform der Informationssicherheitsverletzung abschließend bestimmt.

Vgl. Ziff. 6.27 HDI Cyber+

„Als Netzwerksicherheitsverletzung gelten folgende Ereignisse:

- eine Infektion der IT-Systeme mit jeder Art von Schadsoftware;
- ein Denial-of-Service-Angriff auf oder durch IT-Systeme;

[25] *Koch*, in: Bruck/Möller, VVG, Bd. 5 (Haftpflichtversicherung), 10. Aufl. 2023, Vorbemerkung AVB Cyber Rn. 7.

- eine Verhinderung des autorisierten Zugangs zu IT-Systemen oder zu den darin gespeicherten Daten;
- eine unberechtigte Aneignung von Zugangscodes oder elektronischen Zugangsschlüsseln versicherter Unternehmen oder mitversicherter Personen (z. B. durch Phishing);
- eine unberechtigte Einwirkung auf IT-Systeme im Sinne von §§ 202a, 202b StGB (Ausspähen oder Abfangen von Daten);
- eine unberechtigte Löschung, Unterdrückung, Unbrauchbarmachung oder Veränderung von in IT-Systemen gespeicherten Daten im Sinne von § 303a StGB (Datenveränderung);
- eine Computersabotage von IT-Systemen im Sinne von § 303b StGB;
- ein Diebstahl oder Abhandenkommen von Hardware versicherter Unternehmen zur Informationsverarbeitung (einschließlich Laptops, Tablets und Smartphones). Nicht als Diebstahl oder Abhandenkommen gelten eine Beschlagnahme, Konfiszierung, Enteignung, Verstaatlichung oder eine Zerstörung von Hardware auf Anordnung staatlicher Behörden."

Zum Teil werden die versicherten Gefahren nur abstrakt und nicht abschließende durch Beispiele konkretisiert:

Vgl. Hiscox CyberClear Bedingungen 06/2022

„I. Was ist versichert?

[…]

1. Netzwerksicherheitsverletzung

Eine Netzwerksicherheitsverletzung ist jeder unzulässige Zugriff auf das IT-System oder jede unzulässige Nutzung des IT-Systems […] Eine Netzwerksicherheitsverletzung liegt insbesondere vor bei:

- (Hacker-)Angriffen – gezielt und ungezielt – auf das IT-System eines Versicherten, sofern die Angriffe die Veränderung, Beschädigung, Zerstörung, Löschung, Verschlüsselung, Kopie oder das Abhandenkommen von Daten zur Folge haben;
- Eingriffen in das IT-System des Versicherten zum Beispiel mit durch Täuschung (Phishing) erhaltenen Zugangsdaten von Mitarbeitern;
- Schadprogrammen, wie Viren, Würmern oder Trojanern, die sich im IT-System eines Versicherten ausbreiten;
- Denial-of-Service-Angriffen, durch die der Betrieb des IT-Systems eines Versicherten unterbrochen wird;
- jeder Weitergabe von Schadprogrammen an oder Denial-of-Service-Angriffen gegen das IT-System eines Dritten ausgehend vom IT-System eines Versicherten."

Viele Cyberversicherer erweitern den Kreis der versicherten Gefahren in Bezug auf Eigenschäden infolge von Betriebsunterbrechung und Datenwiederherstellung auf Bedienungsfehler und auf unvorhersehbare Fehlfunktionen (technische Probleme der IT-Systeme).

Vgl. Allianz Cyber Protect Premium (V200422)

„Ziff. VII.26 Technisches Problem

Technisches Problem ist eine Fehlfunktion des Computer Systems einer versicherten Gesellschaft, die weder durch fehlerhafte Bedienung noch durch eine Netzwerksicherheitsverletzung verursacht wird.

Als solche Fehlfunktion gelten Fehlfunktionen infolge

a) des Ausfalls der bzw. Über- oder Unterspannung in der Stromversorgung, wenn die Stromversorgung der unmittelbaren Kontrolle eines Versicherten unterliegt;

b) der elektrostatischen Aufladung der Hardware oder statischer Elektrizität in der Hardware;

c) der Überhitzung der Hardware;

d) eines Softwarefehlers;

e) eines Fehlers im internen Netzwerk, oder

f) eines Fehlers der Hardware."

3.3 Definition des Versicherungsfalles

In der Marktpraxis hat sich hinsichtlich der Bestimmung des Versicherungsfalles noch kein einheitlicher Standard herausgebildet. Es lassen sich im Groben drei Konzepte feststellen.[26]

3.3.1 Einheitliche Definition des Versicherungsfalles

Der GDV bedient sich in den Musterbedingungen einer Definition, die einheitlich für alle Eigen- und Fremdschäden sowie Assistance-Leistungen gilt. Abgestellt wird – wie in der Umwelthaftpflicht- und Umweltschadensversicherung – auf den „erstmals nachprüfbar festgestellten" Schaden (Manifestationsprinzip).[27] Mit dem Abstellen auf den erstmals nachprüfbar festgestellten Schaden will der GDV offenbar der Besorgnis Rechnung tragen, dass sich der Zeitpunkt des Eintritts des relevanten Cybervorfalls nicht rekonstruieren lässt. Andere Versicherer haben diese Befürchtungen nicht und stellen einheitlich auf den tatsächlichen Eintritt eines Ereignisses ab, welches die Schädigung eines

[26] *Malek/Schütz*, RuS 2019, 421, 425 f.

[27] LG Düsseldorf RuS 2019, 91, 92 (zur Umweltschadensversicherung):
„Die Wendung ‚nachprüfbare erste Feststellung' ist nach den maßgeblichen Erkenntnismöglichkeiten des durchschnittlichen VN dahin zu verstehen, dass auf der Grundlage von Tatsachen die Verursachung eines Schadens durch den VN feststellbar ist. Die Bedingungen verlangen keine zeitlich unbefristete Nachprüfbarkeit im Sinne einer Dokumentation oder Archivierung von Beweismitteln. Vielmehr reicht die Überprüfbarkeit eines gegebenen Zustands zu einem bestimmten Zeitpunkt aus […]".

Dritten oder den Eigenschaden eines Versicherten unmittelbar herbeiführt (Schadensereignisprinzip).

3.3.2 Differenzierung zwischen Eigenschäden und Fremdschäden

Ganz überwiegend differenzieren die Cyberversicherer zwischen Eigen- und Fremdschäden und legen bei Fremdschäden das Claims-Made-Prinzip zugrunde (mit den aus der D&O-Versicherung bekannten Regeln zur Rückwärtsdeckung, Umstandsmeldung und Nachmeldefrist). Bei Eigenschäden wird zumeist auf die „erste Feststellung" eines Schadens abgestellt. Soweit es um den Versicherungsschutz für Kommunikations- und Public-Relations-Maßnahmen geht, wird auf die erstmalige Berichterstattung in den Medien abgestellt.[28]

3.3.3 Gesonderte Versicherungsfalldefinition bei Eigenschäden und Assistance-Leistungen

Bezüglich Eigenschäden und Assistance-Leistungen finden sich auch Deckungskonzepte, die für jede versicherte Eigenschadensposition und Assistance-Leistung den Versicherungsfall gesondert definieren. Zum Teil wird an die Feststellung der zur Betriebsunterbrechung oder zum Datenverlust führenden Störung und bei Erpressung an den Zugang der Drohung angeknüpft.[29]

3.4 Versicherte Interessen

Nach A1-7 AVB Cyber ist nicht nur das Interesse des Versicherungsnehmers, sondern auch dasjenige sämtlicher aufgrund eines Arbeits- oder Dienstvertrages beschäftigter Arbeitnehmer und Zeitarbeitskräfte sowie ordnungsgemäß bestellter Organmitglieder versichert (mitversicherte Personen). Dies gilt nicht nur für versicherte Fremdschäden (Haftpflichtversicherung), sondern auch für versicherte Eigenschäden. Hinsichtlich der Eigenschäden ist das Sacherhaltungsinteresse des Versicherungsnehmers und zugleich auch das Sachersatzinteresse der versicherten Personen versichert.[30] Ist das (Fehl-)Verhalten einer mitversicherten Person z. B. mitursächlich für die Betriebsunterbrechung, weil sie den unberechtigten Zugriff auf elektronische Daten ihres Unternehmens fahrlässig ermöglicht hat, und nimmt der Versicherungsnehmer den Cyberversicherer daraufhin auf Ersatz des Unterbrechungsschadens gem. A4-1.3.1 AVB Cyber in

[28] Z. B. I.5.10 lit. a) Allianz Cyber Protect Premium (V200422).

[29] Z. B. Ziff. I.4.2 Allianz Cyber Protect Premium (V200422).

[30] *Koch*, in: Bruck/Möller, VVG, Bd. 5 (Haftpflichtversicherung), 10. Aufl. 2023, A1-7 AVB Cyber Rn. 4.

Anspruch, kann dieser deshalb keinen Regress bei der mitversicherten Person nehmen, da diese nicht Dritte im Sinne von § 86 Abs. 1 S. 1 VVG ist.

Soweit jüngst in der Literatur unter Hinweis auf A3-7.2 AVB-Cyber Gegenteiliges vertreten wird,[31] überzeugt dies vor dem Hintergrund, dass A1-7 AVB Cyber als Bestandteil des Basis-Bausteins auch für die Eigenschaden-Bausteine (A2 und A4 AVB Cyber) gilt, nicht.

Es ist zudem mit den für die Auslegung von AVB geltenden Grundsätzen (Grundsatz der anwenderfeindlichen Auslegung, Restriktionsprinzip)[32] nicht vereinbar, einen Ausschluss, dessen Regelungsgehalt sich nach seinem Wortlaut auf Versicherungsleistungen für Fremdschäden beschränkt, zur Auslegung, wessen Interesse bei Eigenschäden der Versicherungsnehmerin mitversichert ist, heranzuziehen.

Schließlich ist auch der Sinn und Zweck von Ziff. A3-7.2 AVB Cyber, der inhaltlich Ziff. 7.4 AHB 2016 entspricht, zu beachten. Ebenso wie Ziff. 7.4 AHB 2016 dient Ziff. A3-7.2 AVB Cyber dem Zweck, Interessenkonflikte zwischen dem VN und einer ihm persönlich oder wirtschaftlich nahestehenden Person zu vermeiden[33] und vom VR solche Schadensersatzansprüche fernzuhalten, bei denen eine besonders hohe Kollusionsgefahr besteht.[34] Außerdem sollen solche Schäden ausgeschlossen werden, bei denen eine gewisse tatsächliche Vermutung dafür besteht, dass die Ansprüche ohne Bestehen einer Haftpflichtversicherung aus privater und/oder beruflicher Rücksichtnahme nicht geltend gemacht würden.[35] Alle diese Zwecke greifen jedoch bei der Geltendmachung von Schäden infolge von Cyberattacken nicht ein. Dies gilt auch für den weiteren Zweck dieses Ausschlusses, Schäden von der Deckung auszunehmen, die den VN treffen können und deshalb wirtschaftlich betrachtet als Eigenschäden zu qualifizieren sind.[36] Dieser Zweck ist nur beachtlich, wenn eine Versicherung ausschließlich

---

[31] *Schilbach/Becker*, RuS 2023, 289, 292 ff. (nur stillschweigender Regressverzicht).

[32] Vgl. *Koch*, VersR 2015, 133, 136 m. w. N.

[33] *Koch*, in: Bruck/Möller, VVG, Bd. 5 (Haftpflichtversicherung), 10. Aufl. 2023, Ziff. 7 Rn. 164; Littbarski, AHB, 1999, § 4 Rn. 395.

[34] OLG Hamm v. 7.11.2018 – 20 U 107/17, VersR 2019, 533, 536; OLG Frankfurt a. M. v. 7.4.1999 – 7 U 136/98, NVersZ 2000, 242; Ziff. 7 Rn. 164; *Harsdorf-Gebhardt*, in: Späte/Schimikowski, Haftpflichtversicherung, 2. Aufl. 2015, AHB § 7 Rn. 60; *Lücke*, in: Prölss/Martin, VVG, 31. Aufl. 2021, AHB Abs. 7 Ziff. 7 Rn. 26; *Büsken*, in: Langheid/Wandt, VVG, 2. Aufl. 2017, Kap. 300 Rn. 165.

[35] Vgl. OLG Hamm v. 1.3.1995 – 20 U 313/94, NJW-RR 1995, 1309; *Koch*, in: Bruck/Möller, VVG, Bd. 5 (Haftpflichtversicherung), 10. Aufl. 2023, Ziff. 7 Rn. 164; *Späte*, AHB, 1. Aufl. 1993, § 4 Rn. 219.

[36] Vgl. auch OLG Hamm v. 1.3.1995 – 20 U 313/94, NJW-RR 1995, 1309; *Koch*, in: Bruck/Möller, VVG, Bd. 5 (Haftpflichtversicherung), 10. Aufl. 2023, Ziff. 7 Rn. 164; *Harsdorf-Gebhardt*, in: Späte/Schimikowski, Haftpflichtversicherung, 2. Aufl. 2015, AHB § 7 Rn. 60.

Fremdschäden versichert, nicht hingegen, wenn sie auch Eigenschäden versichert, wie das bei der Cyberversicherung gerade der Fall ist.

Will der Cyberversicherer bei Eigenschäden ausschließlich das Interesse des Versicherungsnehmers und nicht auch das Haftpflichtinteresse etwaiger mitversicherter Personen versichern, muss er eine ausdrückliche Regelung in den Vertrag aufnehmen. So verfahren einige Cyberversicherer.[37] Andere sehen einen ausdrücklichen Regressverzicht für mitversicherte Personen unterhalb der Repräsentantenebene vor, die einen Versicherungsfall grob fahrlässig herbeigeführt haben.[38]

3.5 Versicherungsleistungen

Die nachstehende Übersicht gibt einen Überblick über die am Markt angebotenen Versicherungsleistungen. Sie ist nicht der Police eines einzelnen Versicherers entnommen, sondern das Ergebnis eines Abgleichs der aktuellen (Premium-)Versicherungsbedingungen verschiedener Versicherer. Ob eine Police alle Leistungen standardmäßig enthält oder ihr Einschluss gesondert vereinbart werden muss, bedarf stets sorgfältiger Prüfung.

Fremdschäden (Haftpflichtversicherung)
Rückwärtsdeckung (Zeit begrenzt/unbegrenzt)
Nachmeldefrist (feste Fristen/Ansparmodell)
Rechtsschutz
Freistellung
Freistellung externer Dienstleister
Geldmittel, zu deren Hinterlegung der Versicherte verpflichtet ist, z. B. in einen Consumer-Redress-Fund (Konsumentenschutzfonds)
Versicherungsschutz für behördliche Verfahren wegen Datenrechtsverletzungen
Einstweiliger Rechtsschutz, Unterlassungs- oder Widerrufsklagen
Ausgegliederte Datenverarbeitung
Medienhaftpflicht
PCI-DSS-Vertragsstrafen durch einen E-Payment Service Provider
Vertragsstrafen wegen der Verletzung von Geheimhaltungspflichten
Vertragsstrafen wegen Leistungsverzugs
Geldbußen nach EU-DSGVO
Bring-your-own-device

[37] Z. B. I.2.6 Allianz Cyber Protect Premium (V200422).

[38] Z. B. IV.13 Hiscox CyberClear Bedingungen 06/2022.

Eigenschäden
Betriebsunterbrechung
Mehrkosten bei Betriebsunterbrechung
Betriebsunterbrechung durch Cloud-Ausfall
Wiederherstellung von Daten und der Funktionsfähigkeit der IT-Infrastruktur
Systemverbesserung (zur Verhinderung zukünftiger Informationssicherheitsverletzungen)
Eigenschäden durch mitversicherte Personen
Cyber-Erpressung
Cyber-Diebstahl (Abhandenkommen von Geld, auch Kryptowährungen, Waren oder Wertpapiere)
Cyber-Betrug (in Form von Fake-President- bzw. CEO-Fraud- und Lieferantenbetrugs-Fällen)
Bußgelder und Entschädigungen mit Strafcharakter im Ausland
Strafrechtsschutz
E-Discovery
Bedienfehler
Sachschäden am Computersystem
Unter- und Überspannung, elektromagnetische Störung
Sachschäden an Fertigungserzeugnissen
Aufwendungen für Schadensminderung
Bring-your-own-device
Assistance-Leistungen
Krisenmanagement
Cyber-Erpressungsmanagement
Soforthilfe bei Verdacht einer Informationssicherheitsverletzung
Forensische Dienstleistungen
Rechtsberatung
Kosten für Public-Relations-Maßnahmen (zur Erhaltung/Wiederherstellung der öffentlichen Reputation)
Kosten für Benachrichtigung/Information (inkl. Einrichtung eines Call-Centers)
Kosten einer freiwilligen Anzeige
E-Discovery
Kreditüberwachung
Sicherheitsanalyse/Systemverbesserungen/Präventationsmaßnahmen/Training
Hotline 24 Stunden/7 Tage

3.6 Aufwendungen vor Eintritt des Versicherungsfalles

Von besonderer Bedeutung sind Regelungen, die dem VN im Fall eines durch tatsächliche Anhaltspunkte begründeten Verdachts Anspruch auf Ersatz von Aufwendungen für alle Maßnahmen geben, die darauf abzielen, festzustellen, ob eine Informationssicherheitsverletzung eingetreten ist, wodurch diese verursacht wurde und welche die geeigneten Maßnahmen zur Reaktion auf die Informationssicherheitsverletzung sind.

Vgl. AVB Cyber

„A.2-3 Aufwendungen vor Eintritt des Versicherungsfalls

A2-3.1 Versichert sind darüber hinaus Aufwendungen für erforderliche Maßnahmen, die der VN zur Vermeidung eines unmittelbar bevorstehenden Schadens getätigt hat. Ein unmittelbar bevorstehender Schaden liegt vor, wenn aufgrund festgestellter oder objektiver Tatsachen, insbesondere der glaubhaften Androhung oder Kenntnisnahme, von einer Informationssicherheitsverletzung auszugehen ist. Nicht ersatzfähig sind allgemeine Aufwendungen zur Erhaltung, Nachrüstung, Sicherung oder Sanierung von informationsverarbeitenden Systemen des VN. Die Leistungspflicht des VR ist auf die im Versicherungsschein genannte Summe (Sublimit) begrenzt, welche auf die Versicherungssumme angerechnet wird.

A2-3.2 1 Der VN hat dem VR einen unmittelbar bevorstehenden Schaden unverzüglich anzuzeigen, soweit Aufwendungen gemäß A2-3.1 getätigt werden. Verstößt der VN gegen die Anzeigepflicht gilt Teil B3-4.“

Vgl. Allianz Cyber Protect Premium (V200422)

„I.6. Versicherungsschutz für die Sofortreaktion

I.6.1. Sofortreaktion

Im Falle eines durch tatsächliche Anhaltspunkte begründeten Verdachts einer Informationssicherheitsverletzung bietet der Versicherer der betroffenen versicherten Gesellschaft Versicherungsschutz für die notwendigen und angemessenen Honorare, Auslagen und Aufwendungen

a) eines externen Cyber-Krisenmanagers gemäß Ziffer I.5.1. (Cyber-Krisenmanagement),

b) eines externen IT-Spezialisten gemäß Ziffer I.5.3. (Forensische Dienstleitungen),

c) eines externen Rechtsanwaltes gemäß Ziffer I.5.4. (Rechtsberatung),

d) eines externen Krisenkommunikationsberaters gemäß Ziffer I.5.5. (Krisenkommunikation).

Der Versicherer übernimmt in diesem Fall für den im Versicherungsschein benannten Zeitraum ab erstmaliger Kontaktaufnahme über die im Versicherungsschein genannte Notrufnummer die notwendigen und angemessenen Honorare, Auslagen und Aufwendungen der über die Notrufnummer bereitgestellten Dienstleister, um festzustellen, ob eine Informationssicherheitsverletzung eingetreten ist, wodurch dieses verur-

sacht wurde und welches die geeigneten Maßnahmen zur Reaktion auf die Informationssicherheitsverletzung sind.

Ein Selbstbehalt kommt nicht zur Anwendung."

Ähnliche Regelungen finden sich in der Umwelthaftpflicht- (Ziff. 5 UmweltHM) und in der Umweltschadensversicherung (Ziff. 9 USV), bei der ebenfalls die erste nachprüfbare Feststellung des Schadens den Versicherungsfall markiert. Dort substituieren sie § 90 VVG, der für die Sachversicherung bestimmt, dass Aufwendungen, um einen unmittelbar bevorstehenden Versicherungsfall abzuwenden oder in seinen Auswirkungen zu mindern, nach Maßgabe von § 83 Abs. 1 Satz 1, Abs. 2 und 3 VVG ersatzfähig sind. Diese Regelung ist auf die Haftpflichtversicherung nicht anwendbar.[39]

Ob die Vorschriften zur Sachversicherung und somit auch § 90 VVG auf die Cyberversicherung Anwendung finden, hängt, soweit es um die Wiederherstellung der von der Informationssicherheitsverletzung betroffenen Daten sowie um die Entfernung der Schadsoftware und der die daraus resultierende Betriebsunterbrechung geht, davon ab, ob Daten Sachen im Sinne von § 90 BGB sind. Dies ist bis heute nicht eindeutig höchstrichterlich geklärt.[40] Um die daraus resultierenden Unsicherheiten zu beseitigen, bestimmt z. B. A1-3 Satz 2 AVB Cyber, dass Daten keine Sachen sind. Grundsätzlich bestehen gegen eine solche Festlegung keine Bedenken. Wenn es zulässig ist, dass ein Versicherer den Umfang des Versicherungsschutzes für Vermögens- und Sachschäden unterschiedlich ausgestaltet, dann muss es auch zulässig sein, Schäden an Daten nicht wie Sach-, sondern wie Vermögensschäden zu behandeln.

Durch eine solche eigenständige Definition des Sachbegriffs können jedoch die Vorgaben des Aufsichtsrechts und des Versicherungsvertragsrechts, soweit es (halb-) zwingend ausgestaltet ist, nicht umgangen werden.[41] Mit dem Aufsichtsrecht dürfte eine Klausel, die Daten vom Sachbegriff ausnimmt, nicht kollidieren. Im Versicherungsvertragsrecht ist diese Einordnung insoweit problematisch, als die für die Sachversicherung geltenden Vorschriften der §§ 88 ff. VVG Anwendung finden, soweit sie halbzwingend oder zumindest formularvertraglich nicht abdingbar sind. Bedeutsam ist die Einordnung insbesondere für den Anspruch auf Aufwendungsersatz gem. § 90 VVG, der nach wohl herrschender Meinung individualvertraglich, nicht jedoch formularvertraglich ab-

[39] *Klimke*, in: BeckOK, VVG, 18. Ed. 1.2.2023, § 90 Rn. 3; *Armbrüster*, in: Prölss/Martin, VVG, 31. Aufl. 2021, § 90 Rn. 2; *Koch*, in: Bruck/Möller, VVG, Bd. 3 (§§ 74–99), 9. Aufl. 2010, § 90 Rn. 6; *Halbach*, in: Rüffer/Halbach/Schimikowski, VVG, 4. Aufl. 2020, § 90 Rn. 2.

[40] Vgl. zum Streitstand *Bertsch/Fortmann*, RuS 2021, 485, 486.

[41] *Koch*, in: Bruck/Möller, VVG, Bd. 5 (Haftpflichtversicherung), 10. Aufl. 2023, Vorbemerkung AVB Cyber Rn. 22 und 24; *Klimke*, in: Prölss/Martin, VVG, 31. Aufl. 2021, Vorbem. A1-1 AVB Cyber Rn. 6.

dingbar ist.[42] Sollte § 90 VVG zur Anwendung kommen, stellt sich die Frage, in welchem Verhältnis der Anspruch auf Rettungskostenersatz zum dem als Hauptleistung geschuldeten Anspruch auf Aufwendungsersatz steht und ob der Versicherungsnehmer, falls die Versicherungssumme für den als Hauptleistung geschuldeten Aufwendungsersatz nicht ausreicht, den darüber hinausgehenden Betrag als Rettungskosten ersetzt verlangen kann. Diese Frage stellt sich im Übrigen auch dann, wenn Erpressungs-/Lösegeld als Hauptleistung versichert ist (sub 4.).

3.7 Cyberspezifische Ausschlüsse

Die Musterbedingungen des GDV enthalten einen relativ umfangreichen Katalog an Ausschlüssen, von denen nur der Ausschluss von Versicherungsfällen oder Schäden aufgrund des Ausfalls der Infrastruktur (auf den ersten Blick) cyberspezifisch ist.

Vgl. AVB Cyber

„A1-17.5 Ausfall Infrastruktur

Versicherungsfälle oder Schäden aufgrund des Ausfalls von Infrastruktur.

Ein Ausfall der Infrastruktur liegt vor, wenn

a) Gebietskörperschaften oder wesentliche Teile hiervon, wie Stadtteile, Gemeinden, Städte oder Kreise oder

b) Netzstrukturen, die der überregionalen Informationsvermittlung, insbesondere Telefon-, Internet- oder Funknetze dienen, oder

c) die nachfolgenden Einrichtungen der Daseinsvorsorge:
   - Abfallbeseitigung,
   - Trinkwasserversorgung,
   - Abwasserentsorgung,
   - Versorgung mit Gas und Strom sowie
   - Betrieb des öffentlichen Personennah- und Fernverkehrs

d) oder sonstige Infrastrukturbetriebe

vom Ausfall betroffen sind."

[42] *Klimke*, in: BeckOK, VVG, 18. Ed. 1.2.2023, § 90 Rn. 13; *Armbrüster*, in: Prölss/Martin, VVG, 31. Aufl. 2021, § 90 Rn. 5; *Koch*, in: Bruck/Möller, VVG, Bd. 3 (§§ 74–99), 9. Aufl. 2010, § 90 Rn. 23; *Halbach*, in: Rüffer/Halbach/Schimikowski, VVG, 4. Aufl. 2020, § 90 Rn. 8.

Dieser Ausschluss, der für alle Versicherungsleistungen gilt, soll offenbar dazu dienen, Kumulrisiken zu begegnen.[43] Indessen stellt sich die Frage, inwieweit sich auf Basis der AVB Cyber bei dem Ausfall von Infrastruktur infolge einer von A1-1 AVB Cyber geforderten Informationssicherheitsverletzung überhaupt ein Kumulrisiko verwirklichen kann. Führt ein Angriff auf elektronische Daten des Betreibers der Infrastruktureinrichtung zu einem Ausfall der Stromversorgung, besteht für die daraus resultierende Beeinträchtigung der Verfügbarkeit von Daten bei den Kunden des Betreibers – sofern diese selbst eine Cyberversicherung auf Basis der AVB Cyber abgeschlossen haben – keine Deckung, weil es bei den Kunden am Eintritt eines der in A1-2.4 AVB Cyber aufgeführten Ereignisse bzw. der versicherten Gefahr fehlt.[44] Ein Kumulrisiko besteht nur für den Betreiber der Infrastruktureinrichtung, wenn es bei ihm aufgrund einer Informationssicherheitsverletzung zum Ausfall seiner Einrichtung und daraus resultierend zu Schäden bei seinen Kunden kommt, für die er haftet.[45] Bezüglich dieser Drittschäden greift jedoch die Serienschadensregelung in A1-15 Satz 4 AVB Cyber, so dass dieser Ausschluss, soweit es sich bei dem Versicherungsnehmer um den Betreiber der Infrastruktureinrichtung handelt, nicht gerechtfertigt und deshalb nach § 307 Abs. 1 Satz 1 BGB unwirksam ist.[46] In der Literatur werden – aus anderen Gründen – Bedenken gegen die Wirksamkeit von A1-17.5 AVB Cyber geäußert, weil die Klausel teils intransparent sei (lit. a) und d)) und teils zu weit gehe (lit. b) und c)).[47]

Soweit Cyberversicherer weitergehend als die AVB Cyber Versicherungsschutz auch für Betriebsunterbrechungsschäden infolge technischer Störungen als Folge des Ausfalls der Stromversorgung bieten, sehen deren Bedingungen vor, dass die Fehlfunktion von dem Teil des IT-Systems und der Stromversorgung ausgehen muss, welcher der alleinigen Herrschaftsgewalt des Versicherungsnehmers unterliegt oder über den der Versicherungsnehmer die vollständige Kontrolle hat. Soweit die Stromversorgung nicht der Herrschaftsgewalt oder der Kontrolle des Versicherungsnehmers unterliegt, besteht für Schäden

[43] *Fortmann*, RuS 2019, 429, 434; vgl. auch *Müller/Topsch*, VW 2016, 54 zu den Grenzen der Versicherbarkeit.

[44] *Koch*, in: Bruck/Möller, VVG, Bd. 5 (Haftpflichtversicherung), 10. Aufl. 2023, A1-17 AVB Cyber Rn. 31; vgl. auch *Rudkowski*, VersR 2023, 416, 422 f.

[45] *Koch*, in: Bruck/Möller, VVG, Bd. 5 (Haftpflichtversicherung), 10. Aufl. 2023, A1-17 AVB Cyber Rn. 31; vgl. *Klimke*, in: Prölss/Martin, VVG, 31. Aufl. 2021, Vorbem. A1-1 AVB Cyber Rn. 6.

[46] Vgl. *Klimke*, in: Prölss/Martin, VVG, 31. Aufl. 2021, A1-17 AVB Cyber Rn. 18; *Fortmann*, RuS 2019, 429, 434.

[47] *Klimke*, in: Prölss/Martin, VVG, 31. Aufl. 2021, A1-17 AVB Cyber Rn. 16 ff.; vgl. auch *Rudkowski*, VersR 2023, 416, 423 f.; *Salm*, in: Rüffer/Halbach/Schimikowski, VVG, 4. Aufl. 2020, A.1-17 AVB Cyber Rn. 10, 13.

infolge des Ausfalls kein Versicherungsschutz. Eine solche Regelung ist geeignet, Kumulrisiken vorzubeugen.[48]

Vgl. HDI Cyber+

„4. Allgemeine Ausschlüsse

Die Allgemeinen Ausschlüsse gelten für den gesamten Vertrag.

Vom Versicherungsschutz ausgeschlossen sind ohne Rücksicht auf mitwirkende Ursachen

4.8 Unterbrechung oder Störung von Versorgungsinfrastrukturen

Versicherungsfälle oder Schäden aufgrund von oder im Zusammenhang mit jeder Art von Unterbrechung oder Störung

– der Versorgung mit Strom, Gas, Öl und/oder sonstigen Energieformen, oder
– von Internet-, Kabel-, Satelliten-, Telekommunikationsinfrastrukturen und/oder -verbindungen (Versorgungsinfrastrukturen),

sofern die Versorgungsinfrastruktur nicht im Kontrollbereich versicherter Unternehmen liegt".

3.8 Cyberspezifische Obliegenheiten

Die gefahrvorbeugenden cyberspezifischen Obliegenheiten zur Gewährleistung der IT-Sicherheit orientieren sich zum Teil an dem IT-Grundschutzkatalog des Bundesamts für Sicherheit in der Informationstechnik (BSI), der 2017 durch das IT-Grundschutz-Kompendium abgelöst wurde.

Vgl. AVB Cyber

„A1-16 Obliegenheiten vor Eintritt des Versicherungsfalls zur Gewährleistung der IT-Sicherheit

Der Versicherungsnehmer hat vor Eintritt des Versicherungsfalls alle vertraglichen Obliegenheiten einzuhalten.

A1-16.1 Dazu gehört insbesondere, dass die informationsverarbeitenden Systeme

a) einzelne Nutzer und Befugnisebenen unterscheiden. Hierzu sind individuelle Zugänge für alle Nutzer erforderlich, die mit ausreichend komplexen Passwörtern gesichert werden. Administrative Zugänge sind ausschließlich Administratoren und ausschließlich zur Erledigung administrativer Tätigkeiten vorbehalten;

b) mit einem zusätzlichen Schutz gegen unberechtigten Zugriff ausgerüstet sind, wenn diese einem erhöhten Risiko ausgesetzt sind. Ein erhöhtes Risiko besteht bei Geräten, die über das Internet erreichbar, oder im mobilen Einsatz sind. Zusätzliche Schutzmaßnahmen können z. B. sein: Firewall, 2-Faktor- Authentifizierung bei Servern, Ver-

[48] *Koch*, in: Bruck/Möller, VVG, Bd. 5 (Haftpflichtversicherung), 10. Aufl. 2023, A1-17 AVB Cyber Rn. 31.

schlüsselung von Datenträgern mobiler Geräte, Diebstahlsicherung oder ähnlich wirksame Maßnahmen;

c) über einen Schutz gegen Schadsoftware verfügen, der automatisch auf dem aktuellen Stand gehalten wird (z. B. Virenscanner, Code Signing, Application Firewall oder ähnlich wirksame Maßnahmen);

d) einem Patch-Management-Verfahren unterliegen, das eine unverzügliche Installation von relevanten Sicherheitspatches sicherstellt. Systeme und Anwendungen mit bekannten Sicherheitslücken dürfen nicht ohne zusätzliche geeignete Maßnahmen zur Absicherung eingesetzt werden;

e) einem mindestens wöchentlichen Sicherungsprozess unterliegen, wobei die Sicherungsdatenträger physisch getrennt aufbewahrt werden. Es ist sicher zu stellen, dass im Versicherungsfall auf Originale und Duplikate nicht gleichzeitig zugegriffen werden kann, oder diese manipuliert, oder zerstört werden können. Der Versicherungsnehmer hat eine ordnungsgemäße Funktion des Sicherungs- und Wiederherstellungsprozesses durch regelmäßige Prüfung nach einem festgelegten Turnus sicherzustellen."

Einige Bedingungswerke enthalten Regelungen zur Nutzung von Betriebssystemen, für die keine Sicherheitsupdates mehr bereitgestellt werden (Altsysteme).

Vgl. Hiscox CyberClear Bedingungen 06/2022

„Ziff. IV Allgemeine Regelungen

15. Obliegenheiten vor Eintritt des Versicherungsfalles

Der Versicherte hat vor Eintritt des Versicherungsfalles die folgenden Obliegenheiten zu beachten und zu erfüllen

[…]

15.3. Betrieb von Altsystemen

Sofern die Versicherten Betriebssysteme nutzen, für die ihnen keine Sicherheitsupdates mehr bereitgestellt werden (Altsysteme), hat der Betrieb dieser Altsysteme ausschließlich in einer isolierten Netzwerkumgebung ohne direkten Internetzugang und mit durchgehender Kontrolle des Datenverkehrs zu erfolgen."

3.9 Festlegung von Gefahrerhöhungstatbeständen

Bei den Regeln zur Gefahrerhöhung handelt es sich um eine gesetzliche Obliegenheit, so dass es an sich keines Hinweises auf diese Regelungen in den AVB bedarf. Da der Begriff der Gefahrerhöhung gesetzlich nicht definiert ist, findet sich in den AVB jedoch regelmäßig eine Definition dieses Begriffs, die mit derjenigen der Rechtsprechung des BGH übereinstimmt und insoweit nur informativen Wert hat.[49] Viele Cyberversicherer bedienen sich zudem der aus anderen Sparten bekannten Praxis und umschreiben Gefahrerhöhungstatbestände in ih-

[49] BGH v. 16.6.2010 – IV ZR 229/09, VersR 2010, 1032 Rn. 16; OLG Oldenburg 29.3.2012 – 5 U 11/11, NJOZ 2012, 1918, 1920; OLG Saarbrücken v. 22.6.2011 – 5 U

ren AVB. Diese knüpfen an Veränderungen hinsichtlich technischer und organisatorischer Maßnahmen zur Sicherstellung der IT-Sicherheit nach Abschluss des Versicherungsvertrages an.

Vgl. Allianz Cyber Protect Premium (V200422)

„Ziff. VI. Allgemeine Bestimmungen

VI.2 Gefahrerhöhung

Die Versicherungsnehmerin darf nach Abschluss des Vertrages ohne Einwilligung des Versicherers keine Gefahrerhöhung vornehmen oder deren Vornahme durch Versicherte oder einen Dritten gestatten.

Eine Gefahrerhöhung liegt vor, wenn nach Abgabe der Vertragserklärung der Versicherungsnehmerin die tatsächlich vorhandenen Umstände so verändert werden, dass der Eintritt des Versicherungsfalls oder eine Vergrößerung des Schadens oder die ungerechtfertigte Inanspruchnahme des Versicherers wahrscheinlicher wird. Eine Gefahrerhöhung *kann insbesondere dann vorliegen*, wenn

a) sich ein gefahrerheblicher Umstand ändert, nach dem der Versicherer vor Vertragsschluss gefragt hat;

b) technische oder organisatorische Maßnahmen zum Schutz der Funktionsfähigkeit des Computer Systems einer versicherten Gesellschaft, Komponenten oder Prozessen gegen Beeinträchtigungen der Verfügbarkeit, Integrität oder Vertraulichkeit des Computer Systems einer versicherten Gesellschaft oder der Daten der versicherten Gesellschaften verschlechtert werden;

c) eine Umstellung oder Migration von kritischen IT-Systemen (Produktions-, Kundendatenverwaltungs-, Warenwirtschafts-, Kontoführungssysteme oder dergleichen) vorgenommen wird;

d) eine Auslagerung von kritischen IT-Systemen (Produktions-, Kundendatenverwaltungs-, Warenwirtschafts-, Kontoführungssysteme oder dergleichen) zu Drittdienstleistern vorgenommen wird;

Die Versicherungsnehmerin hat jede Gefahrerhöhung, die ihr bekannt wird, dem Versicherer unverzüglich anzuzeigen, und zwar auch dann, wenn sie ohne ihren Willen eintritt.

Im Übrigen gelten die §§ 23 bis 27 VVG. Nach diesen Bestimmungen kann der Versicherer zur Kündigung berechtigt sein, eine Vertragsänderung vornehmen oder auch leistungsfrei sein. Hiervon abweichend gilt im Falle einer Verschmelzung auf die Versicherungsnehmerin Ziffer II. 9. Satz 2 (Verschmelzung auf die Versicherungsnehmerin) und im Falle des Erwerbs oder einer Gründung einer Tochtergesellschaft Ziffer II. 11. (Neue Tochtergesellschaft).“

(Hervorhebungen durch den Verfasser)

209/10-38, BeckRS 2012, 18770; OLG Karlsruhe v. 18.12.2003 – 12 U 97/03, NJW-RR 2004, 326, 327.

Diese Klausel begegnet insoweit keinen Wirksamkeitsbedenken, als die darin beispielhaft näher beschriebenen Umstände nur eine Gefahrerhöhung begründen können. Anders sieht das bei der nachstehenden Klausel aus.

Vgl. Hiscox CyberClear Bedingungen 06/2022

„14. Gefahrerhöhung

Eine Gefahrerhöhung liegt vor, wenn nach Abgabe der Vertragserklärung des Versicherungsnehmers die tatsächlich vorhandenen Umstände so verändert werden, dass der Eintritt eines Versicherungsfalles oder die Vergrößerung eines Schadens oder eine ungerechtfertigte Inanspruchnahme des Versicherers wahrscheinlicher wird. Eine Gefahrerhöhung *liegt insbesondere* bei folgenden Umständen vor:

- Änderung des Geschäftszwecks eines Versicherten;
- Aufnahme von Online-Handel;
- erhebliche technisch-organisatorische Änderungen in der Informationssicherheitsstruktur eines Versicherten wie zum Beispiel nachteilige Veränderungen im Informationssicherheitsmanagementsystem (ISMS), Veränderungen in der Datensicherungsstrategie oder Out- bzw. Insourcing von IT-Prozessen.

Der Versicherer fragt einmal jährlich typische gefahrerhöhende Umstände ab (Prämienregulierungsprozess). Unabhängig vom Prämienregulierungsprozess bleibt die gesetzliche Pflicht des Versicherungsnehmers, nach Vertragserklärung ohne die Einwilligung des Versicherers keine Gefahrerhöhungen vorzunehmen oder von einem Dritten vornehmen zu lassen, bestehen. Kommt es trotzdem zu einer Gefahrerhöhung, hat der Versicherungsnehmer sie abweichend von den gesetzlichen Regelungen innerhalb eines Monats nach Kenntniserlangung anzuzeigen."

(Hervorhebungen durch den Verfasser)

Hier ist beispielhaft („insbesondere") bestimmt, dass eine Gefahrerhöhung vorliegt, wenn die in der Klausel beschriebenen Umstände vorliegen. Da gem. § 32 S. 1 VVG von den §§ 23 ff. VVG nicht zum Nachteil des VN abgewichen werden darf und dieses Abweichungsverbot sich nicht nur auf das Rechtsfolgenregime, sondern auch auf die Definition der Gefahrerhöhung im Sinne von § 23 VVG bezieht, begegnet die Festlegung von Gefahrerhöhungstatbeständen nur dann keinen Wirksamkeitsbedenken, wenn sie eine Gefahrerhöhung im Sinne der Rechtsprechung des BGH darstellen. Ob das bezüglich der in der vorstehenden Klausel beschriebenen Umstände stets der Fall ist, scheint zumindest zweifelhaft. Ansonsten folgt aus dieser Klausel, dass der Versicherungsnehmer objektive bzw. ungewollte Gefahrerhöhungen dem Cyberversicherer abweichend von § 23 Abs. 1 VVG nicht unverzüglich nach Kenntniserlangung von der Gefahrerhöhung anzuzeigen hat, sondern erst auf Nachfrage des Cyberversicherers im Rahmen des Prämienregulierungsprozesses. Diese Abweichung ist wirksam, da sie den Versicherungsnehmer begünstigt.

Es gibt auch Cyberversicherer, die Gefahrerhöhungen grundsätzlich mitversichern und auf ihr Recht zur Kündigung verzichten. Zugleich wird dem Ver-

sicherungsnehmer die Obliegenheit auferlegt, dem Cyberversicherer bestimmte im Versicherungsvertrag als Gefahrerhöhung festgelegte Umstände unverzüglich nach Bekanntwerden mitzuteilen. Kommt es im Anschluss an einer solchen Mitteilung zu keiner Einigung zwischen dem Versicherer und dem Versicherungsnehmer über eine angemessene Prämienerhöhung oder Bedingungsanpassung innerhalb eines bestimmten Zeitraums, ist ein rückwirkender Wegfall des Versicherungsschutzes für den gefahrerhöhenden Umstand vorgesehen. Gegen eine solche Rechtsfolgenregelung bestehen grundsätzlich keine Bedenken, da sie im Ergebnis § 25 Abs. 1 VVG entspricht.

Vgl. Gothaer Cyber-Versicherung

„10. Gefahrerhöhungen

Abweichend zu §§ 23 bis 26 VVG gilt:

Gefahrerhöhungen und Gefahränderungen sind mitversichert und beeinträchtigen die Verpflichtung des Versicherers zur Leistung nicht. Dem Versicherer steht als Folge einer Gefahrerhöhung kein Kündigungsrecht zu. Der Versicherte verpflichtet sich, dem Versicherer gegenüber folgende Gefahrerhöhungen unverzüglich anzuzeigen, sobald sie ihm bekannt werden:

- Sitzverlegung des Versicherten ins Ausland;
- Änderung des Geschäftszweckes oder der Geschäftstätigkeit des Versicherten;
- Aufnahme oder Erweiterung des Online- oder Internethandels;
- wesentliche technisch-organisatorische Änderungen in der Informationssicherheitsstruktur des Versicherungsnehmers.

Der Versicherer wird im Rahmen einer regelmäßigen Abfrage erfolgte Veränderungen zu den für ihn erheblichen Gefahrumständen ermitteln. Der Versicherer hat zu diesen Gefahrerhöhungen, sofern sie erheblich sind, Anspruch auf eine angemessene Prämienerhöhung oder Bedingungsanpassung.

Kann eine Einigung über eine angemessene Prämienerhöhung oder Bedingungsanpassung innerhalb eines Monats, von dem Zeitpunkt an gerechnet, in welchem der Versicherer von der Gefahrerhöhung Kenntnis erlangt hat nicht erzielt werden, entfällt rückwirkend der Versicherungsschutz für den gefahrerhöhenden Umstand.

Im Übrigen gelten die §§ 23 bis 27 und 29 VVG."

4. Ausgewählte cyberversicherungsspezifische Fragestellungen

Der vorstehende Überblick über den Umfang des Versicherungsschutzes der Cyberversicherung hat vor allem deutlich gemacht, dass sich bislang kein einheitlicher Mindeststandard hinsichtlich der Ausgestaltung des Versicherungsschutzes in der Cyberversicherung herausgebildet hat. Die Cyberversicherung enthält darüber hinaus im Vergleich zu traditionellen Versicherungsarten Sonderregelungen, von denen nachstehend zwei näher in den Blick genommen werden sollen.

4.1 Prioritätsklausel

Zu den Besonderheiten der Cyberversicherung zählen sog. Prioritätsklauseln, denen zufolge die Cyberversicherung vorgeht, soweit Versicherungsschutz auch in einem anderen Versicherungsvertrag besteht. Solche Klauseln beziehen sich auf den Fall, dass der Versicherungsnehmer nicht nur eine Cyberversicherung abgeschlossen hat, sondern auch noch andere Versicherungen, die ausschnittsweise Schutz gegen Schäden aufgrund einer Beeinträchtigung der Integrität und/oder Verfügbarkeit von elektronischen Daten oder informationsverarbeitenden Systemen bieten. Die Prioritätsklauseln beziehen sich somit auf eine Situation, in der ein Interesse gegen dieselbe Gefahr in mehreren Versicherungsverträgen versichert ist. In diesen Fällen soll die Deckung aus der Cyberversicherung vorgehen. Ohne Bedeutung für die Anwendung der Klausel ist, ob der Versicherer, mit dem der Versicherungsnehmer die anderen Verträge abgeschlossen hat, identisch mit dem Cyberversicherer ist.[50]

4.1.1 Klauselbeispiele

Vgl. AVB Cyber

„1-12 Vorrangige Versicherung

Besteht Versicherungsschutz nach den Bedingungen dieses Vertrages auch in einem anderen Versicherungsvertrag, so geht die Cyberrisiko-Versicherung vor."

Vgl. Hiscox CyberClear Bedingungen 06/2022

Ziff. IV. Allgemeine Regelungen

„2. Vorrangige Versicherung

Ist ein Versicherungsfall oder ein Schaden auch unter einem anderen Versicherungsvertrag versichert, so geht der vorliegende Vertrag vor.

Dies gilt nicht, wenn es sich bei dem anderen Versicherungsvertrag um eine Cyber-Versicherung eines Versicherten handelt. In diesem Fall steht die vorliegende Versicherung erst im Anschluss an die Versicherungssumme der anderen Versicherung zur Verfügung. Versicherungsschutz besteht in Ergänzung zu der Leistung des anderen Versicherers, soweit der Versicherungsschutz unter dem vorliegenden Vertrag weiter ist als unter dem anderen einschlägigen Versicherungsvertrag (Konditionendifferenzdeckung) oder der anderweitige Versicherungsschutz durch Zahlung verbraucht ist (Summenausschöpfungsdeckung).

Erhält der Versicherte aus dem anderweitigen Versicherungsvertrag wegen dauerhafter Zahlungsunfähigkeit des anderen Versicherers keine Leistung, so leistet der Versicherer des vorliegenden Vertrags Zug um Zug gegen Abtretung der Leistungsansprüche des Versicherten.

---

[50] *Koch*, in: Bruck/Möller, VVG, Bd. 5 (Haftpflichtversicherung), 10. Aufl. 2023, A1-12 AVB Cyber Rn. 1.

Bestreitet der andere Versicherer seine Leistungspflicht ganz oder teilweise, so leistet der Versicherer des vorliegenden Vertrags unter Eintritt in die Rechte des Versicherten vor."

4.1.2 Sinn und Zweck von Prioritätsklauseln

Mithilfe von Prioritätsklauseln wollen die Cyberversicherer erreichen, dass der VN sie vorrangig in Anspruch nimmt. Dadurch soll sichergestellt werden, dass der VN im Schadensfall schnell professionelle Unterstützung erhält und hierdurch das Ausmaß des versicherten Eigen- oder Fremdschadens – z. B. Schadensermittlungskosten, Benachrichtigungskosten und Call-Center-Leistungen, Kosten für Krisenkommunikation und PR-Maßnahmen – begrenzt wird.[51] Die Klausel bezweckt nicht, den Versicherungsnehmer vor etwaig nachteiligen Folgen der Inanspruchnahme des anderen Versicherers (wie z. B. Schadensfallkündigung, Prämienerhöhung) zu schützen.[52]

Im Rahmen des Eigenschadenbausteins kommt eine Überschneidung nicht nur bei Allgefahrendeckungen (technische Versicherungen) und der Software-/Datenversicherung im Rahmen der Elektronikversicherung (TK A 1928 und A 1929 ABE 2020), sondern auch bei der Versicherung gegen benannte Gefahren (z. B. Feuerversicherung, Feuerbetriebsunterbrechungsversicherung) in Betracht, wenn sich eine benannte Gefahr verwirklicht (z. B. Cyberangriff löst einen Brand aus, infolge dessen der Betrieb unterbrochen und Daten verloren gehen). Im Bereich des Drittschadenbausteins kommen Überschneidungen mit der Betriebshaftpflichtversicherung in Betracht, insbesondere soweit es um die Deckung von Vermögensschäden geht (vgl. Ziff. 7.6.5.1 BBR BHV/Ziff. 1-6.12.3 AVB BHV, BBR IT-Dienstleister) oder die Zusatzbedingungen zur Betriebshaftpflichtversicherung für die Nutzer von Internet-Technologien (BetrH IT) vereinbart worden sind.

Prioritätsklauseln werfen eine Reihe von interessanten und schwierigen Rechtsfragen auf, die zum einen das (Deckungs-)Verhältnis zwischen dem Versicherungsnehmer und den beteiligten Versicherern und zum anderen das (Ge-

[51] *Koch*, in: Bruck/Möller, VVG, Bd. 5 (Haftpflichtversicherung), 10. Aufl. 2023, A1-12 AVB Cyber Rn. 2; *Schilbach*, SpV 2018, 2, 3; *Pache/Graß*, PHi 2017, 122, 126; *Malek/Schütz*, PHi 2018, 42, 53; *Fortmann*, RuS 2019, 429, 440; *Lesser*, Haftungsprobleme und Versicherungslösungen, 2021, S. 343 f., 348 f. (effizientes Schadensmanagement); nach Ansicht von *Klimke*, in: Prölss/Martin, VVG, 31. Aufl. 2021, A1-12 AVB Cyber Rn. 1 sollen auch Rechtsunsicherheiten vermieden werden, die sich aus einem Zusammentreffen mehrerer Subsidiaritätsabreden ergeben; ähnlich *Salm*, in: Rüffer/Halbach/Schimikowski, VVG, 4. Aufl. 2020, A.1-12 AVB Cyber Rn. 1 und *Achenbach*, VersR 2017, 1493, 1498.

[52] *Koch*, in: Bruck/Möller, VVG, Bd. 5 (Haftpflichtversicherung), 10. Aufl. 2023, A1-12 AVB Cyber Rn. 2.

samtschuld-)Verhältnis zwischen den Versicherern zueinander betreffen. Diesen Fragen soll anhand des nachstehenden Beispielsfalls nachgegangen werden.

4.1.3 Beispielsfall

Infolge einer Informationssicherheitsverletzung erbeuten unbekannte Täter Kreditkartennummern und Kartenablaufdaten von Gästen einer Restaurantkette, die sowohl eine Betriebshaftpflichtversicherung (BHV) als auch eine Cyberversicherung mit identischen Versicherungssummen auf Basis der Musterbedingungen des GDV abgeschlossen hat. Der VN informiert unverzüglich die betroffenen Gäste, die daraufhin ihre Karten sperren und sich Ersatzkarten ausstellen lassen. Der von dem Versicherungsnehmer in Abstimmung mit dem Cyberversicherer beauftragte Sachverständige stellt eine Sicherheitslücke fest, die daraus resultiert, dass der Versicherungsnehmer ein Betriebssystem verwendet, für das es keine Updates mehr gibt (Verstoß gegen A1-16.1 lit. d) AVB Cyber). Im Verhältnis zu den betroffenen Kunden liegt ein Verstoß gegen den Grundsatz der Integrität und Vertraulichkeit nach Art. 5 Abs. 1 lit. f) DSGVO vor. Die Sicherheitslücke hat eine unbefugte bzw. unrechtmäßige Verarbeitung durch die unbekannten Täter ermöglicht. Deshalb haben die betroffenen Gäste gegen den Versicherungsnehmer gemäß Art. 82 Abs. 1 und 2 DSGVO Anspruch auf Ersatz der Schäden, die ihnen durch die Kartensperrung und Ersatzausstellung entstanden sind und aus der missbräuchlichen Verwendung der Karten ggf. in der Zukunft noch entstehen werden.

4.1.3.1 Vorliegen einer Mehrfachversicherung

4.1.3.1.1 Rechtslage ohne Prioritätsklausel

Lässt man die Prioritätsklausel zunächst einmal unberücksichtigt, liegt eine Mehrfachversicherung im Sinne von § 78 Abs. 1 VVG vor. Der Anspruch auf Schadensersatz fällt sowohl in den Schutzbereich der Betriebshaftpflichtversicherung als auch in den Schutzbereich der Cyberversicherung. Nach Ziff. 7.6.5.1 BBR BHV (Ziff. 1-6.12.3 AVB BHV) sind Ansprüche wegen Vermögensschäden aus der Verletzung von Datenschutzgesetzen durch Verwendung personenbezogener Daten versichert. Unter Verwendung personenbezogener Daten versteht der durchschnittliche Versicherungsnehmer die Verarbeitung von Daten.[53] Diese muss gem. Art. 5 Abs. 1 lit. F.) DSGVO in einer Weise erfolgen, die die

[53] Vgl. *Schild* in BeckOK-DatenschutzR, 43. Ed. 1.2.2023, Art. 4 DS-GVO Rn. 48 (Verwendung umfasst jede Form der Datenverarbeitung); *Herbst*, in: Kühling/Buchner, DSGVO, 3. Aufl. 2020, Art. 4 Nr. 2 Rn. 28 (Verwendung bzw. das Nutzen personenbezogener Daten stellt Unterfall der Verarbeitung dar).

Integrität und Vertraulichkeit der Daten sicherstellt. A3-1 i. V. m. A1-2.1, A1-2.4 AVB Cyber bietet Schutz vor der Inanspruchnahme auf Ersatz von Vermögensschäden wegen der Beeinträchtigung der Vertraulichkeit elektronischer Daten infolge u. a. einer Verletzung datenschutzrechtlicher Vorschriften. Zwischen beiden Versicherungen besteht somit Vollidentität hinsichtlich des versicherten (Haftpflicht-)Interesses und im Hinblick auf das Erfordernis der Inanspruchnahme wegen Verletzung von Datenschutzgesetzen durch Verwendung personenbezogener Daten Teilidentität bezüglich der versicherten Gefahr. Die Voraussetzungen des § 78 Abs. 1 Alt. 2 VVG liegen somit vor.[54]

Die Mehrfachversicherung begründet gemäß § 78 Abs. 1 VVG eine Gesamtschuld, bei der die VR – abweichend von § 426 Abs. 1 Satz 1 BGB – nach § 78 Abs. 2 Satz 1 VVG im Verhältnis zueinander zu Anteilen nach Maßgabe der Beträge verpflichtet sind, die sie dem Versicherungsnehmer nach dem jeweiligen Vertrag zu zahlen haben. Der Innenausgleich zwischen den VR hat grundsätzlich Vorrang vor einem Regress nach § 86 Abs. 1 Satz 1 VVG.[55] Das bedeutet, dass jeder VR maximal für den Betrag haftet, der von ihm nach seinem Vertrag zu leisten ist. Darüber hinaus kann der Versicherungsnehmer nicht mehr als Ersatz seines Schadens verlangen.

Von diesen beiden Beschränkungen abgesehen, hat der Versicherungsnehmer nach § 421 BGB ein freies Wahlrecht bei der Inanspruchnahme der ihm zur Leistung verpflichteten VR. Er braucht deshalb grundsätzlich keine Rücksicht darauf zu nehmen, welcher von den jeweiligen VR im Innenverhältnis gegenüber den bzw. dem anderen ausgleichs- oder regresspflichtig ist. Das Wahlrecht des Versicherungsnehmers wird nur durch den allgemeinen Rechtsmissbrauchseinwand (§ 242 BGB) begrenzt.[56] In casu stünde es somit im Belieben des VN, ob er den Cyberversicherer oder den Betriebshaftpflichtversicherer in Anspruch nimmt. Vorliegend hat der Versicherungsnehmer seine Obliegenheit gem. A1-16.1 lit. d) AVB Cyber verletzt, so dass bei mutmaßlicher grober Fahrlässigkeit eine Leistungskürzung in Betracht kommt. Der Versicherungsnehmer wird

[54] Vgl. BGH v. 13.3.2018 – VI ZR 151/17, NJW 2018, 2120 Rn. 22; OLG Frankfurt a. M. v. 11.1.1995 – 10 U 36/94, OLG-Report 1995 113, 114; *Schnepp*, in: Bruck/Möller, VVG, 9. Aufl. 2010, § 77 Rn. 27 und § 78 VVG Rn. 18; *Armbrüster*, in: Prölss/Martin, VVG, 31. Aufl. 2021, § 78 Rn. 8 ff.

[55] Vgl. BGH v. 13.3.2018 – VI ZR 151/17, VersR 2018, 726 Rn. 22; s. a. BGH v. 13.9.2006 – IV ZR 273/05, BGHZ 169, 86, 96 f.; BGH v. 23.11.1988 – IV a ZR 143/87, VersR 1989, 250, 251; BGH v. 31.03.1976 – IV ZR 29/75, VersR 1976, 847, 848; OLG Frankfurt a. M. v. 11.1.1995 – 19 U 36/94, OLGR 1995, 113, 115; OLG München v. 13.1.2005 – 19 U 3792/0, RuS 2005, 107 (jeweils zu den Vorgängervorschriften § 59 und § 67 VVG a. F.).

[56] St. Rspr., vgl. nur BGH v. 18.6.2007 – II ZR 86/06, BGHZ 173, 1 = NJW-RR 2008, 51 Rn. 15; BGH v. 22.1.1991 – XI ZR 342/89, NJW 1991, 1289 m. w. N.

deshalb den Betriebshaftpflichtversicherer in Anspruch nehmen, der wegen § 78 Abs. 2 Satz 1 VVG nur anteilig Ausgleich beim Cyberversicherer nehmen kann.

4.1.3.1.2 Rechtslage mit Prioritätsklausel

Fraglich ist zunächst, ob eine im Cyberversicherungsvertrag vereinbarte Prioritätsklausel das Entstehen einer Gesamtschuld zwischen Cyber- und Betriebshaftpflichtversicherer und damit einer „echten" Mehrfachversicherung mangels Gleichstufigkeit der Haftung verhindert, wie die Rechtsprechung für Subsidiaritätsabreden gemeinhin annimmt.[57] Sollte dies der Fall sein, wäre der Tatbestand des § 421 BGB nicht erfüllt. Es wäre zu klären, ob der Anspruch des Versicherungsnehmers gegen den Betriebshaftpflichtversicherer nach § 86 Abs. 1 Satz 1 VVG auf den vorrangig haften wollenden Cyberversicherer übergeht, wenn letzterer die (gekürzte) Versicherungsleistung erbringt, oder die Prioritätsabrede als Regressverzicht zugunsten des Betriebshaftpflichtversicherer zu verstehen ist. Leistete der Betriebshaftpflichtversicherer, wäre zu klären, ob der gekürzte Anspruch gegen den Cyberversicherer gemäß § 86 Abs. 1 Satz 1 VVG auf ihn überginge. Bejahte man hingegen die Gleichstufigkeit trotz Prioritätsklausel, würde sich die Frage nach deren Bedeutung gleichwohl stellen, und zwar im Rahmen des Gesamtschuldnerausgleichs gemäß § 78 Abs. 2 Satz 1 VVG und § 426 Abs. 2 BGB.

Der Inhalt der Prioritätsklausel ist durch Auslegung zu ermitteln. Das Verständnis des Versicherungsnehmers wird maßgeblich durch den Umstand bestimmt, dass die Prämie, die an den Betriebshaftpflichtversicherer gezahlt wurde, auch das Risiko der Inanspruchnahme wegen Vermögensschäden aus der Verletzung von Datenschutzgesetzen abdeckt. Haben somit beide VR eine Prämie für die Übernahme desselben (Teil-)Risikos erhalten, muss es aus der Sicht des Versicherungsnehmers im Ausgangspunkt bei der im Gesetz vorgesehenen und für ihn vorteilhaften gesamtschuldnerischen Haftung der beiden VR bleiben. In dieser Hinsicht unterscheiden sich Prioritätsklauseln von Subsidiaritätsabreden.

Bei Subsidiaritätsabreden wird der Versicherungsnehmer davon ausgehen, dass der subsidiär haftende VR die Fälle nur subsidiärer Haftung (aufschiebende Bedingung) bei der Prämienkalkulation mitberücksichtigt hat. In solchen Fällen ist es deshalb aus seiner Sicht gerechtfertigt, dem Subsidiärversicherer,

[57] St. Rspr., vgl. BGH v. 4.7.2018 – IV ZR 121/17, NJW 2018, 2958 Rn. 12; BGH v. 18.11.2009 – IV ZR 58/06, RuS 2010, 69 Rn. 10; BGH v. 13.9.2006 – IV ZR 273/05, BGHZ 169, 86 Rn. 24; BGH v. 21.4.2004 – IV ZR 113/03, NJW-RR 2004 1100; a. A. *Armbrüster*, in: Prölss/Martin, VVG, 31. Aufl. 2021, § 78 VVG Rn. 30; kritisch gegenüber dem Erfordernis der Gleichstufigkeit *Looschelders*, in: Staudinger, BGB, Neub. 2022, § 421 Rn. 27 ff.

der irrtümlich die Versicherungsleistung erbringt, den Regress gegen den Primärversicherer in voller Höhe gem. § 86 Abs. 1 Satz 1 VVG zu gestatten und umgekehrt dem Primärversicherer, der zahlt, den Regress gegen den Subsidiärversicherer zu versagen.[58] Infolge der nur bedingten Haftung des Subsidiärversicherers fehlt es aus Sicht des Versicherungsnehmers im Verhältnis zum Primärversicherer an der Gleichstufigkeit. Dagegen lässt die Prioritätsklausel im Vertrag mit dem Cyberversicherer aus der Warte des Versicherungsnehmers die unbedingte Haftung des Betriebshaftpflichtversicherers unberührt. Die für eine Mehrfachversicherung mit Blick auf die gesamtschuldnerische Haftung erforderliche Gleichstufigkeit der Verpflichtung beider VR liegt in seinen Augen somit vor.[59] Festzuhalten ist somit, dass die Prioritätsklausel dem Entstehen eines Gesamtschuldverhältnisses zwischen den Versicherern und somit auch dem Vorliegen einer Mehrfachversicherung nicht entgegensteht.

4.1.3.2 Rechtsfolgen der Mehrfachversicherung

Bei der Betrachtung der Rechtsfolgen stellt sich die Frage, ob der Versicherungsnehmer zur vorrangigen Inanspruchnahme des Cyberversicherers verpflichtet ist und ob der Cyberversicherer im Verhältnis zum Betriebshaftpflichtversicherer den Schaden allein zu tragen hat.

4.1.3.2.1 Verpflichtung des Versicherungsnehmers zur vorrangigen Inanspruchnahme des Cyberversicherers?

Wie zuvor ausgeführt steht es grundsätzlich im Belieben des Versicherungsnehmers, ob er den Cyberversicherer oder den Betriebshaftpflichtversicherer in Anspruch nimmt. Fraglich ist, ob im Beispielsfall der durchschnittliche Versicherungsnehmer einer Cyberversicherung die Formulierung, dass die Cyber-Versicherung bzw. der Cyber-Versicherungsschutz vorgeht, als eine sein Wahlrecht beschränkende Abrede versteht. Da § 78 Abs. 1 und 2 VVG nicht zu den halbzwingenden Normen im Sinne von § 87 VVG zählen, wäre eine solche Abrede in den Grenzen der §§ 307 ff. BGB grundsätzlich wirksam. Jedoch lässt sich eine solche Einschränkung schon nicht aus der Formulierung – Cyberrisiko-Versicherung „geht vor" – entnehmen. Dies deshalb, weil die Klausel nicht den Versicherungsnehmer und dessen Verhalten adressiert, sondern lediglich objektiv auf den Versicherungsschutz unter dem Cyberversicherungsvertrag Bezug nimmt. Ein durchschnittlicher Versicherungsnehmer wird in der Prioritätsklau-

[58] BGH v. 23.1.1988 – IVa ZR 143/87, VersR 1989, 250, 251.

[59] *Koch*, in: Bruck/Möller, VVG, Bd. 5 (Haftpflichtversicherung), 10. Aufl. 2023, A1-12 AVB Cyber Rn. 10; vgl. auch *Fortmann*, RuS 2019 429, 439 f.

sel folglich keine ihn treffende Verhaltenspflicht oder -obliegenheit erkennen. Auch aus dem Zweck der Klausel, sicherzustellen, dass der Cyberversicherer im Schadensfall schnell professionelle Unterstützung leisten kann, wird der Versicherungsnehmer nicht folgern, dass ihn gegenüber dem Cyberversicherer eine Rechtspflicht im Sinne von § 241 Abs. 2 BGB oder auch nur eine Obliegenheit im Sinne von § 28 VVG zu dessen vorrangiger Inanspruchnahme trifft. Im Verhältnis zum Betriebshaftpflichtversicherer entfaltet die Prioritätsklausel keine Wirkung. Der Betriebshaftpflichtversicherer kann den Versicherungsnehmer deshalb nicht auf die vorrangige Inanspruchnahme des Cyberversicherers verweisen.

4.1.3.2.2 Verpflichtung des Cyberversicherers zum Verzicht auf anteiligen Ausgleich?

Nimmt der Versicherungsnehmer den Cyberversicherer in Anspruch (was im Beispielsfall wegen der Obliegenheitsverletzung gem. A1-16.1 lit. d) AVB Cyber fernliegend ist), stellt sich die Frage, ob dieser nach § 78 Abs. 2 Satz 1 VVG zum Regress beim Betriebshaftpflichtversicherer berechtigt ist. Diese Frage ist nicht nur bedeutsam im (Gesamtschuld-)Verhältnis zwischen dem Cyberversicherer und dem Betriebshaftpflichtversicherer, sondern auch im (Deckungs-)Verhältnis zwischen dem Versicherungsnehmer und dem Cyberversicherer. Es ist zu klären, ob der Versicherungsnehmer vom Cyberversicherer verlangen kann, es zu unterlassen, vom Betriebshaftpflichtversicherer anteilig Ausgleich zu verlangen, um den Betriebshaftpflichtversicherungsvertrag nicht zu belasten. Hierzu bedarf es wiederum der Auslegung der Prioritätsklausel. Gewährt diese Klausel dem Versicherungsnehmer ein solches Recht gegenüber dem Cyberversicherer, stellt sich im Verhältnis zwischen den beiden VR die Frage, ob sich der Betriebshaftpflichtversicherer im Rahmen des Gesamtschuldnerausgleichs auf die Prioritätsklausel berufen kann (Abrede zugunsten Dritter im Sinne von § 328 Abs. 1 BGB, die auf ein Unterlassen der Inanspruchnahme gerichtet ist).

Grundsätzlich können Gläubiger und Gesamtschuldner Regelungen für das Ausgleichsverhältnis wirksam treffen, soweit diese den anderen Gesamtschuldner nicht benachteiligen.[60] Die Verpflichtung des Cyberversicherers, den Betriebshaftpflichtversicherer nicht in Anspruch zu nehmen, benachteiligt letzteren nicht, sondern begünstigt ihn. Fraglich ist jedoch, ob die Prioritätsklausel eine solche Verpflichtung des Cyberversicherers gegenüber dem Versicherungsnehmer begründet bzw. als Abrede zugunsten des Betriebshaftpflichtversicherers verstanden werden kann. Da sich aus dem Wortlaut der Prioritätsklausel

[60] Vgl. BGH v. 14.7.1983 – IX ZR 40/82, BGHZ 88 185, 189=NJW 1983 2442; BGH v. 23.10.1986 – IX ZR 203/85, NJW 1987, 374, 375; *Staudinger/Looschelders* (2022), § 426 Rn. 55.

hierzu nichts entnehmen lässt, hängt die Antwort darauf vom erkennbaren Sinn und Zweck dieser Klausel ab.

Gegen eine Auslegung der Prioritätsklausel in dem Sinne, dass sie den Cyberversicherer verpflichtet, den Betriebshaftpflichtversicherer nicht anteilig auf Ausgleich in Anspruch zu nehmen, spricht zunächst der Grundsatz, dass Verzichtserklärungen stets eng auszulegen sind.[61] Nachdem die Prioritätsklausel ihren vorrangigen Zweck, die schnelle Leistung professioneller Unterstützung durch den Cyberversicherer, erfüllt hat, würde eine solche Auslegung aber zum kompensationslosen Verzicht des Cyberversicherers auf seinen Regressanspruch führen.

Gegen eine dahingehende Auslegung sprechen weiter die nachteiligen Folgen für den Cyberversicherer im Fall der Verletzung von Obliegenheiten, die nach Eintritt des Versicherungsfalles zu beachten sind. Der Cyberversicherer würde bei Annahme eines Verzichts auf den Regress im Innenverhältnis zum Betriebshaftpflichtversicherer nämlich nicht nur anteilig, sondern vollständig haften, selbst wenn der Versicherungsnehmer eine ihm gegenüber zu beachtende Obliegenheit verletzt hat und er deshalb gegenüber dem Versicherungsnehmer (teilweise) leistungsfrei ist. Dass ein solches Ergebnis nicht vom Cyberversicherer bezweckt ist, dürfte im Beispielsfall auf der Hand liegen. Schnelle und professionelle Unterstützung im Schadensfall kann der Cyberversicherer nur leisten, wenn der Versicherungsnehmer seine Anzeige-, Auskunfts- und Rettungsobliegenheiten beachtet. Verletzt der Versicherungsnehmer diese Obliegenheiten dem Cyberversicherer gegenüber, weil er – aus welchen Gründen auch immer – Deckung vom Betriebshaftpflichtversicherer begehrt, hätte dieser gegen den Cyberversicherer Anspruch nicht nur auf hälftigen, sondern auf vollen Ausgleich des Haftpflichtschadens, obgleich der Schaden möglicherweise geringer ausgefallen wäre, wenn der Versicherungsnehmer sich sofort an den Cyberversicherer gewendet und dessen Weisungen abgewartet hätte. Ein solches Ergebnis würde Sinn und Zweck der Prioritätsabrede in der Cyberversicherung konterkarieren.[62]

Eine Verpflichtung des Cyberversicherers gegenüber dem Versicherungsnehmer zum Verzicht auf den Regress wäre deshalb nur dann anzunehmen, wenn die Prioritätsklausel den Versicherungsnehmer vor den nachteiligen Folgen für den Vertrag mit dem Betriebshaftpflichtversicherer schützen will, die ihm ohne die Prioritätsklausel drohten. Als nachteilige Folge käme allenfalls die Schadensfallkündigung des Betriebshaftpflichtversicherers nach § 92 Abs. 1 VVG in Frage. Hiervor soll die Prioritätsklausel den Versicherungsnehmer jedoch nicht

[61] Vgl. RG v. 20.9.1927 – VII 155/27, RGZ 118, 63 ,66; BGH v. 18.4.1989 – X ZR 85/88, NJW-RR 1989, 1373, 1374; BGH v. 15.1.2002 – X ZR 91/00, NJW 2002, 1044, 1046.

[62] *Koch*, in: Bruck/Möller, VVG, Bd. 5 (Haftpflichtversicherung), 10. Aufl. 2023, A1-12 AVB Cyber Rn. 20.

schützen. Im Beispielsfall kann der Versicherungsnehmer deshalb nicht von dem Cyberversicherer verlangen, von der Geltendmachung des Ausgleichsanspruchs gegen den Betriebshaftpflichtversicherer gemäß § 78 Abs. 2 Satz 1 VVG und § 426 Abs. 2 BGB abzusehen. Ebenso wenig ist es deshalb dem Betriebshaftpflichtversicherer gestattet, sich gegenüber dem Cyberversicherer auf die Prioritätsklausel zu berufen.[63]

4.1.4 Zwischenergebnis

Weder verpflichten Prioritätsklauseln den Versicherungsnehmer oder legen ihm die Obliegenheit auf, den Cyberversicherer vorrangig vor anderen (Mehrfach-)Versicherern in Anspruch zu nehmen, noch verhindern sie das Zustandekommen einer Mehrfachversicherung oder den Regress des Cyberversicherers nach §§ 78 Abs. 2 S. 1 VVG oder § 426 Abs. 2 BGB. Es bleibt also festzuhalten, dass Prioritätsklauseln in der Cyberversicherung allein auf eine Verhaltenssteuerung des VN im Sinne eines „Nudging" abzielen, ihnen aber keine rechtlichen Wirkungen im eigentlichen Sinne zukommen.

4.2 Erstattung von Lösegeldzahlungen

4.2.1 Lösegeldzahlungen als Hauptversicherungsleistung

4.2.1.1 Aufsichtsrechtliche Zulässigkeit

Der Betrieb einer Lösegeldversicherung war in Deutschland lange Zeit unzulässig, da dieses Geschäftsmodell als unvereinbar mit wesentlichen Grundsätzen des deutschen Rechts erachtet wurde. 1998 gab das damalige Bundesaufsichtsamt für das Versicherungswesen, eine der Vorgängerbehörden der BaFin, diese strenge Sichtweise auf, so dass Versicherungen gegen Produkterpressung und Lösegeldforderungen seitdem unter bestimmten Voraussetzungen zulässig sind.[64] Die verbleibenden Einschränkungen sollen der Gefahr erpresserischer Entführungen entgegenwirken und eine Behinderung polizeilicher Ermittlungen sowie ein kollusives Zusammenwirken von Tätern, Opfern oder Mitarbeitern des Versicherers vermeiden.

---

[63] *Koch*, in: Bruck/Möller, VVG, Bd. 5 (Haftpflichtversicherung), 10. Aufl. 2023, A1-12 AVB Cyber Rn. 21; zu Konstellationen, in denen Prioritätsabreden von Bedeutung für das Verhältnis zwischen den VR sind s. *Koch*, Prioritätsklauseln in Versicherungsverträgen, 2020, S. 15.

[64] Rundschreiben 3/1998 (VA), https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/rs_9803_va_loesegeldversicherung.html (zuletzt abgerufen am: 22.4.2023).

Seit dem Erlass des Rundschreibens im Jahr 1998 hat die BaFin dieses bereits drei Mal angepasst. Nachdem im Jahr 2000 die Notwendigkeit einer gesonderten Erlaubnis entfiel,[65] gestattet die BaFin seit 2008 unter bestimmten Voraussetzungen automatische Vertragsverlängerungen[66] und billigte 2014, dass auf Seiten des Versicherungsnehmers im gewerblichen Bereich ausnahmsweise mehr als drei Personen Kenntnis vom Abschluss einer Lösegeldversicherung haben dürfen.[67]

In ihrer Mitteilung aus September 2017 wies die BaFin darauf hin, dass die übrigen im Rundschreiben aus 1998 geregelten Voraussetzungen für den Betrieb einer Lösegeldversicherung fortgelten.[68] So darf zwar die Cyberpolice als solche beworben werden, nicht jedoch der darin enthaltene Baustein Lösegeldversicherung. Zudem muss bei Einschluss einer Lösegeldversicherung in eine Cyberpolice weiterhin sichergestellt sein, dass die Ermittlungsarbeit der Polizei nicht beeinträchtigt wird. Außerdem muss ein kollusives Zusammenwirken zwischen Tätern, Opfern oder Mitarbeitern des Versicherers vermieden werden. Dazu ist im Einzelnen nach den Lockerungen noch erforderlich, dass

- die Versicherungssumme den wirtschaftlichen Verhältnissen des Versicherungsnehmers angemessen ist, damit das subjektive Risiko sich nicht erhöht;
- ein kompetentes Sicherheitsunternehmen eine präventive Beratung anhand eines Sicherheitskonzepts bei dem Versicherungsnehmer durchführt;
- dem Versicherungsnehmer die Obliegenheit zur Geheimhaltung des Versicherungsschutzes auferlegt wird;
- eine zentrale Stelle, die dem Vorstand direkt unterstellt ist, allein für die Verwaltung und Schadenbearbeitung zuständig ist. Die Vertragsdaten müssen verschlüsselt sein, sobald sie gespeichert oder übermittelt werden. In den Anstellungsverträgen der zuständigen Mitarbeiter sollte eine spezielle Verschwiegenheitsverpflichtung enthalten sein. Die Revisionen sollten vom Vorstand/ Sicherheitsunternehmen durchgeführt werden;
- der Versicherungsnehmer, seine Vertrauenspersonen und der Versicherer im Schadenfall verpflichtet sind, die Tat bei der Polizei unverzüglich anzuzeigen und das staatliche Strafverfolgungsinteresse zu unterstützen.[69]

---

[65] VerBAV 2000, 171.

[66] Siehe BaFin-Journal März 2008, S. 3.

[67] Siehe BaFin-Journal Juni 2014, S. 5.

[68] Mitteilung vom 15.9.2017, https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Meldung/2017/meldung_170915_loesegeldversicherung.html (zuletzt abgerufen am: 22.4.2023).

[69] Rundschreiben 3/1998 (VA)), https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/rs_9803_va_loesegeldversicherung.html (zuletzt abgerufen am: 22.4.2023).

Bei Einhaltung dieser Vorgaben verstößt das Angebot einer Lösegeldversicherung und der nachträglichen Erstattung von Lösegeldzahlungen nicht gegen den ordre public (§ 138 Abs. 1 BGB) und vermag auch keine Strafbarkeit von Verantwortlichen des Versicherers zu begründen.[70] Dem Versicherer ist deshalb auch verwehrt, gegenüber dem Leistungsverlangen des Versicherungsnehmers rechtliche Unmöglichkeit im Sinne von § 275 Abs. 1 BGB einzuwenden.

4.2.1.2 Marktpraxis

Seit der Mitteilung der BaFin im September 2017 zählt die Lösegeldversicherung zu den Standardbestandteilen von Cyberversicherungen einer Vielzahl von Anbietern.

Vgl. Allianz Cyber Protect Premium (V200422)

„I.4 Versicherungsschutz für Cyber Erpressung

I.4.1 Cyber Erpressung

Der Versicherer bietet Versicherungsschutz für Cyber Erpressungsschäden, die versicherte Gesellschaften aufgrund einer Cyber-Erpressung erleiden.

Cyber Erpressungsschäden sind notwendige und angemessene Geldbeträge, die eine versicherte Gesellschaft nach vorheriger Zustimmung des Versicherers in Textform zur Abwehr oder Beendigung einer Cyber Erpressung gezahlt hat (Lösegeld bzw. Erpressungsgeld). Als Zahlung eines Geldbetrages gilt auch die Zahlung mit einer Kryptowährung, wie zum Beispiel BitCoins. Es gilt insoweit das im Versicherungsschein festgelegte Sublimit.

Ziff. VII.9. Cyber Erpressung

Cyber Erpressung ist die widerrechtliche Drohung gegenüber einem Versicherten mit

a) einer Informationssicherheitsverletzung oder

b) der Fortsetzung einer bereits eingetretenen Informationssicherheitsverletzung

zu dem Zweck, ein Erpressungsgeld aus dem Vermögen eines Versicherten für die Nichtausführung der angedrohten Maßnahme nach Buchstabe a) oder b) dieser Ziffer zu erhalten. Soweit damit gedroht wird, Erzeugnisse, die eine versicherte Gesellschaft herstellt, be- oder verarbeitet oder vertreibt, zu ändern oder zu kontaminieren (Produkterpressung), gilt dies nicht als Cyber Erpressung."

Vgl. Gothaer Cyber Versicherung

„4.1 Gegenstand der Versicherung

Versicherungsschutz besteht im Rahmen der nachfolgenden Bedingungen für Aufwendungen und Kosten gemäß Ziffer 4.2 infolge einer Cyber-Erpressung. Als Cyber-Erpressung im Sinne dieser Bedingungen gilt eine angedrohte oder konkrete Handlung eines Dritten im unmittelbaren Zusammenhang mit – einer Datenrechtsverlet-

[70] *Sieg/Schilbach*, PHi 2023, 46, 49 ff.

zung (Teil I Ziffer 1.), – einer IT-Sicherheitsverletzung (Teil I Ziffer 2.) oder – einem Hacker-Angriff (Teil I Ziffer 3.).

4.2 Versichertes Risiko

Versichert ist der Ausgleich von Erpressungsgeldern, die aufgrund einer Cyber-Erpressung von dem Versicherten gezahlt werden. Als Erpressungsgelder gelten ebenfalls angemessene Belohnungen von Informanten zur Aufklärung der Erpressungshandlung und Täteridentifikation."

4.2.1.3 Ausschluss von Versicherungsfällen oder Schäden aus der Zahlung von Löse-/Erpressungsgeldern

Die Musterbedingungen des GDV sehen keinen Versicherungsschutz für die Zahlung von Löse-/Erpressungsgeldern vor. Vielmehr schließen die AVB Cyber die Zahlung von Löse-/Erpressungsgeldern oder die Erfüllung von Erpressungsforderungen aus.

Vgl. AVB Cyber

„A1-17 Allgemeine Ausschlüsse

Vom Versicherungsschutz ausgeschlossen sind ohne Rücksicht auf mitwirkende Ursachen

A1-17.7 Löse-/Erpressungsgeld

Versicherungsfälle oder Schäden aus der Zahlung von Löse-/Erpressungsgeldern oder der Erfüllung von Erpressungsforderungen."

Von dem Ausschluss betroffen sind Löse-/Erpressungsgeldzahlungen, die der Versicherungsnehmer vor Eintritt des Versicherungsfalls zur Vermeidung eines unmittelbar bevorstehenden Schadens leistet. Für sie besteht kein Anspruch auf Ersatz gem. A.2-3 AVB Cyber (III. 6.).

4.2.2 Lösegeldzahlungen als Rettungskosten gemäß § 83 Abs. 1 VVG

Im Hinblick auf die eingangs angesprochene Sublimitierung der Erstattung von Lösegeldzahlungen (II. 3.) und den Ausschluss in A1-17 AVB Cyber stellt sich nicht nur für Cyberversicherer, die keine Deckung für Löse-/Erpressungsgelder versprechen, sondern auch für Cyberversicherer, die Löse-/Erpressungsgelder versichern, die Frage, inwieweit solche Gelder (auch) als Schadensminderungskosten nach § 83 VVG ersetzt werden müssen und auf Verlangen des Versicherungsnehmers vorzuschießen sind. Dieser Frage soll anhand eines Beispiels nachgegangen werden, in dem die Cyberpolice keinen Versicherungsschutz für die Zahlung von Löse-/Erpressungsgeldern vorsieht.

4.2.2.1 Keine Versicherung von Lösegeldzahlungen als Hauptleistung vereinbart

Nach § 83 Abs. 1 S. 1 VVG hat der Versicherer Aufwendungen des Versicherungsnehmers nach § 82 Abs. 1 und 2 VVG, auch wenn sie erfolglos bleiben, insoweit zu erstatten, als der Versicherungsnehmer sie den Umständen nach für geboten halten durfte. Die Anknüpfung an § 82 Abs. 1 und 2 VVG gibt zunächst Anlass dazu, sich mit der Frage zu befassen, ob den Versicherungsnehmer eine Pflicht trifft, zum Zwecke der Abwendung oder Minderung des versicherten Schadens Lösegeld zu zahlen.

4.2.2.1.1 Obliegenheit zur Lösegeldzahlung gem. § 82 Abs. 1 und 2 VVG?

Ausgangsfall:

Die A-GmbH (VN), ein großes Paketzustellunternehmen, schließt mit dem Versicherer V (VR) eine Cyberversicherung ab. Die Versicherungssumme für Betriebsunterbrechung/Ertragsausfall und die Wiederherstellung beträgt 10 Mio. EUR. Die Haftzeit für die Betriebsunterbrechung beträgt 50 Tage, der Tagessatz beträgt 200.000 EUR. Gut ein Jahr nach Abschluss des Versicherungsvertrages wird die VN am späten Freitagnachmittag Opfer eines Cyber-Angriffs. Die Täter hatten Werbung auf verschiedenen Internetseiten geschaltet. Beim Anklicken dieser Seite installiert sich eine Schadsoftware selbstständig auf den Rechnern der Opfer. Mit Hilfe dieser Software wird ein Sperrbildschirm angezeigt, der in der jeweiligen Landessprache der Opfer zur Zahlung einer Summe von 100.000 EUR auffordert, damit das System wieder entsperrt wird. Die VN erreicht telefonisch niemanden mehr bei ihrem VR und hinterlässt eine entsprechende Nachricht per E-Mail. Anrufe unter der im Versicherungsvertrag angegebenen Notfallrufnummer sowohl am Freitag als auch am Wochenende bleiben ebenfalls erfolglos, da die Nummer stets besetzt ist. Erst am späten Montagnachmittag nach Betriebsschluss meldet sich der VR bei der VN und beauftragt einen Experten, dem es am Mittwochabend gelingt, den durch den Cyberangriff unterbrochenen Betrieb zum Laufen zu bringen. Die VN fordert vom VR Ersatz von 600.000 EUR für die Betriebsunterbrechung von Montag bis Mittwoch. Der VR ist lediglich zur Zahlung von 100.000 EUR bereit, da die VN ihre Schadensminderungsobliegenheit verletzt habe. Sie hätte spätestens am frühen Montagmorgen das Lösegeld zahlen müssen, um die Betriebsunterbrechung abzuwenden.

Da die Versicherungsnehmerin nur ihr zumutbare Maßnahmen zur Schadensminderung im Sinne von § 82 Abs. 1 VVG zu erbringen hat, liegt kein Verstoß vor, da ihr Lösegeldzahlungen nicht zumutbar sind. So hat der öOGH es für den Versicherungsnehmer einer Kaskoversicherung als nicht zumutbar angesehen, mit Kriminellen oder deren Mittelsmännern zu paktieren, um das ge-

stohlene Fahrzeug wieder herbeizuschaffen.[71] Dieser Maßstab zur Beurteilung der Zumutbarkeit von Schadensminderungsmaßnahmen dürfte auch dem deutschen Recht zugrunde zu legen sein.[72] In diesem Fall scheidet mangels Zumutbarkeit auch ein Verstoß gegen § 82 Abs. 2 VVG aus, weil die Versicherungsnehmerin eine Weisung des Versicherers zur Zahlung nicht hätte befolgen müssen. Folglich ist der Versicherer zum Ersatz der 600.000 EUR verpflichtet.

4.2.2.1.2 Anspruch auf Ersatz für Kosten überobligatorischer Rettungsmaßnahmen?

Abwandlung 1:

Bereits am frühen Montagmorgen leistet die VN die geforderte Geldzahlung in Höhe von 100.000 EUR über das von den Tätern bezeichnete Zahlungssystem, um ihren Betrieb nicht unterbrechen zu müssen. Erst am späten Montagnachmittag nach Betriebsschluss meldet sich der VR bei der VN. Die VN fordert vom VR Ersatz für die Lösegeldzahlung. Der VR weigert sich zu leisten, weil für Lösegeldzahlungen kein Versicherungsschutz bestehe.

Grundsätzlich besteht ein Anspruch auf Aufwendungsersatz gemäß § 83 Abs. 1 S. 1 VVG nur für Aufwendungen des Versicherungsnehmers nach § 82 Abs. 1 und 2 VVG, so dass man nach dem zuvor gefundenen Ergebnis zunächst geneigt sein könnte, einen Aufwendungsersatzanspruch abzulehnen. Dies wäre jedoch vorschnell. Die Zubilligung eines Ersatzanspruchs für die Kosten überobligatorischer Rettungsmaßnahmen ist gerechtfertigt, weil das Erfordernis der Zumutbarkeit allein dem Schutz des Versicherungsnehmers dient, auf den er verzichten kann, und weil die Maßnahme dem Versicherer im Erfolgsfall zugutekommt.[73] Für den Anspruch aus § 83 Abs. 1 VVG spielt die Zumutbarkeit der Rettungsmaßnahme somit keine Rolle. Zu Recht hat deshalb das OLG Saarbrücken den Ersatz von Lösegeld für die Rückbeschaffung des gestohlenen Kfz in der Kaskoversicherung bejaht.[74]

---

[71] ÖOGH v. 5.4.1995 – 7 Ob 14/95, ECLI:AT:OGH0002:1995:0070OB00014.95.0405.000.

[72] *Voit*, in: Prölss/Martin, VVG, 31. Aufl. 2021, § 82 Rn. 15; *Schmidt-Kessel*, in: Looschelders/Pohlmann, VVG, 3. Aufl. 2016, § 82 Rn. 13; *Looschelders*, in: Langheid/Wandt, VVG, 3. Aufl. 2022, § 82 Rn. 33; *Langheid*, in: Langheid/Rixecker, VVG, 7. Aufl. 2022, § 82 Rn. 10.

[73] Vgl. OLG Karlsruhe v. 16.9.1993 – 4 U 324/92 VersR 1994 468; *Looschelders*, in: Langheid/Wandt, VVG, 3. Aufl. 2022, § 83 Rn. 19; *Klimke*, in: BeckOK VVG, 18. Ed. 1.2.2023, § 83 Rn. 23; vgl. auch *Martin*, Sachversicherungsrecht, 3. Aufl. 1992, W II 30: „Die Schadensabwendungs- und -minderungspflicht bedeutet daher praktisch vor allem ein Recht des VN (‚Rettungsrecht'), nämlich das Recht, Maßnahmen gegen den Schaden auf Kosten des Versicherers zu ergreifen."

[74] OLG Saarbrücken v. 5.11.1997 – 5 U 501/97 – 50, NJW-RR 1998, 463 ff.; vgl. auch LG Freiburg v. 18.1.2001, zfs 2001, 174.

4.2.2.1.3 Objektive Gebotenheit der Lösegeldzahlung?

Der Versicherer hat nach § 83 Abs. 1 S. 1 letzter Halbs. VVG Aufwendungen des Versicherungsnehmers, „auch wenn sie erfolglos bleiben, insoweit zu erstatten, als der Versicherungsnehmer sie den Umständen nach für geboten halten durfte". Hieraus folgt im Umkehrschluss, dass dem Versicherungsnehmer objektiv gebotene Aufwendungen stets zu ersetzen sind, ohne dass es auf die Vorstellungen des Versicherungsnehmers ankommt.[75] Ansonsten stellt § 83 Abs. 1 S. 1 letzter Halbs. VVG klar, dass ein Anspruch auf Aufwendungsersatz nicht zwingend zur Voraussetzung hat, dass die Aufwendungen objektiv geboten waren. Es genügt vielmehr, dass der Versicherungsnehmer die Aufwendungen nach seinen Vorstellungen und den Umständen des Einzelfalls für geboten halten durfte.

Objektiv geboten sind alle Maßnahmen, die objektiv geeignet sind, den (Folge-)Schaden abzuwenden oder zu mindern. Sie müssen darüber hinaus auch objektiv erforderlich sein. Letzteres ist nur dann der Fall, wenn die mit den Rettungsmaßnahmen verbundenen Aufwendungen in einem vernünftigen Verhältnis zum angestrebten Erfolg der Schadensabwendung stehen, nicht aber, wenn sie unverhältnismäßige Kosten verursachen.[76] Die Rettungsmaßnahme darf nicht dazu führen, dass der Gesamtschaden für den VR (Entschädigung plus Rettungskosten) größer ausfällt als der ohne die Rettungshandlung drohende Versicherungsschaden i. e. S. (Entschädigung). Im Übrigen ist unter mehreren verfügbaren und gleich geeigneten Maßnahmen nur die kostengünstigste objektiv erforderlich.[77]

Diese Voraussetzungen liegen in der Abwandlung 1 vor. Durch die Zahlung von 100.000 EUR gelingt es der Versicherungsnehmerin den montäglichen Betriebsunterbrechungsschaden abzuwenden, der sich auf 200.000 EUR belaufen hätte. Die Zahlung war somit zur Abwendung des versicherten Schadens geeignet und erforderlich und stand in einem vernünftigen Verhältnis zum angestrebten Erfolg. Eine kostengünstigere Maßnahme stand der Versicherungsnehmerin nicht zur Verfügung. Die Zahlung war somit objektiv geboten.

---

[75] *Beckmann*, in: Beckmann/Matusche-Beckmann, Versicherungsrechts-Handbuch, 3. Aufl. 2015, § 15 Rn. 89; *Schimikowski*, in: Rüffer/Halbach/Schimikowski, VVG, 4. Aufl. 2020, § 83 Rn. 15; *Looschelders*, in: Langheid/Wandt, VVG, 3. Aufl. 2022, § 83 Rn. 21; vgl. auch BGH v. 25.6.2003 – IV ZR 276/02, VersR 2003, 1250; BGH v. 18.12.1996 – IV ZR 321/95, RuS 1997, 98, 99; a. A. *Langheid*, in: Langheid/Rixecker, VVG, 7. Aufl. 2022, § 83 Rn. 8; *Sieg/Schilbach*, Phi 2023, 46, 53.

[76] BGH v. 25.6.2003 – IV ZR 276/02, RuS 2003, 406, 407; OLG Karlsruhe v. 17.12.2015 – 12 U 101/15, NJW-RR 2016, 668; OLG Karlsruhe v. 7.5.2015 – 12 U 146/14, NJW-RR 2015, 1379; *Voit*, in: Prölss/Martin, VVG, 31. Aufl. 2021, § 83 Rn. 7; *Klimke*, in: BeckOK VVG, 18. Ed. 1.2.2023, § 83 Rn. 33.

[77] OLG Karlsruhe v. 7.5.2015 – 12 U 146/14, NJW-RR 2015, 1379, 1381 f.; *Klimke*, in: BeckOK VVG, 18. Ed. 1.2.2023, § 83 Rn. 33.2.

Nach § 83 Abs. 2 VVG muss der Versicherungsnehmer ggf. eine Kürzung des Anspruchs hinnehmen, wenn er seine Obliegenheit zur Weisungseinholung und -befolgung und/oder seine Aufwendungsminderungsobliegenheit grob fahrlässig verletzt hat. Hier käme allenfalls eine Verletzung der Obliegenheit zur Weisungseinholung in Betracht, weil die Versicherungsnehmerin die Weisungserteilung des Versicherers nicht abgewartet hat. Selbst wenn man dies bejahte, ist dem Versicherer durch die Zahlung jedoch kein Nachteil entstanden, weil er für einen Tag Betriebsunterbrechung mindestens einen um 100.000 EUR höheren Schaden zu tragen gehabt hätte, wenn die Versicherungsnehmerin abgewartet hätte. Der Versicherungsnehmerin gelingt damit der Kausalitätsgegenbeweis.

Die Konstellation, die der Abwandlung 1 zugrunde liegt, birgt im Übrigen als sogenanntes Silent-Cyber-Risiko „Sprengstoff" für traditionelle Betriebsunterbrechungsversicherungen wie zum Beispiel die Maschinenbetriebsunterbrechungsversicherung und die Elektronikbetriebsunterbrechungsversicherung. Diese sind nach herrschender Ansicht als Sachversicherung zu qualifizieren.[78] Hat der Erpresser die Schadensoftware bereits in die Systeme der Versicherungsnehmerin integriert und droht mit Beschädigung der Maschine, maschinellen Einrichtungen oder sonstigen (elektro-)technischen Anlagen oder Geräten, liegt zwar – soweit man Daten keine Sachqualität zunächst – noch kein Versicherungsfall vor, weil es am Eintritt eines Sachschadens fehlt. Es stellt sich jedoch die Frage, ob der Versicherungsfall nicht unmittelbar im Sinne von § 90 VVG bevorsteht. Lässt man es für die Unmittelbarkeit genügen, dass der Versicherungsfall in kurzer Zeit und mit hoher Wahrscheinlichkeit ohne die Rettungsmaßnahme eintreten werde, dürfte die Frage bei einem Ultimatum von sehr kurzer Dauer wohl zu bejahen sein.[79]

[78] *Wandt*, Versicherungsrecht, 6. Aufl. 2016, Rn. 968; *Looschelders*, in: Langheid/Wandt, VVG, 3. Aufl. 2022, § 82 Rn. 17; *Beckmann*, in: Beckmann/Matusche-Beckmann, Versicherungsrechts-Handbuch, 3. Aufl. 2015, § 15 Rn. 27; *Marx*, Rettungsobliegenheit und Rettungskostenersatz im Versicherungsvertragsrecht, 2008, S. 247 ff.; *Grünwald/Dallmayr*, Versicherungsteuergesetz, Feuerschutzsteuergesetz, 1. Aufl. (2016), FeuerschStG § 1 Rn. 11; vgl. BFH 30.8.1995 – II R 58/94, BeckRS 1995, 22011564 (zu FeuerschStG a. F.).

[79] BGH 13.7.1994 – IV ZR 250/93, NJW-RR 1994, 1366, 1367; BGH 20.2.1991 – IV ZR 202/90, BGHZ 113, 359, 360 f. = NJW 1991, 1609; OLG Saarbrücken 21.11.2007 – 5 W 257/07, BeckRS 2008, 19982; AG Köpenick 9.10.2003 – 6 C 129/02, NJW-RR 2003, 168, 169; vgl. *König*, in: Schwintowski/Brömmelmeyer/Ebers, VVG, 4. Aufl. 2021, § 90 Rn. 14; *Halbach*, in: Rüffer/Halbach/Schimikowski, VVG, 4. Aufl. 2020, § 90 Rn. 3.

4.2.2.1.4 Kein Ersatz von Lösegeldzahlungen als Rettungskosten wegen des Ausschlusses von Versicherungsfällen oder Schäden aus der Zahlung von Löse-/Erpressungsgeldern?

Fraglich ist, ob ein Anspruch auf Ersatz von Lösegeldzahlungen gem. § 83 Abs. 1 VVG auch dann besteht, wenn – wie in A1-17.7 AVB Cyber vorgesehen – Versicherungsfälle oder Schäden aus der Zahlung von Löse-/Erpressungsgeldern oder der Erfüllung von Erpressungsforderungen ausgeschlossen sind.

Da Rettungskosten in den AVB Cyber keine Erwähnung finden, wird man unter Zugrundelegung der für die Auslegung von AVB geltenden Regelungen – Restriktionsprinzip und Unklarheitenregel (§ 305c Abs. 2 BGB) – von diesem Ausschluss nur Versicherungsleistungen als umfasst ansehen, die der Cyberversicherer als Hauptleistung schuldet. Wollte man das anders sehen und auch Rettungskosten im Sinne von § 83 Abs. 1 VVG vom Versicherungsschutz ausnehmen, wäre A1-17.7 AVB Cyber gem. § 87 VVG unwirksam. Für Lösegeldzahlungen, die objektiv geboten sind, hat der Versicherungsnehmer somit stets Anspruch auf Ersatz als Rettungskosten.

Dieser Befund gibt Anlass zu der Folgefrage, ob etwas Anderes gilt, wenn der Versicherer die Lösegeldzahlung von vornherein durch eine (formularmäßige) Weisung untersagt oder die Zahlung von seiner Zustimmung abhängig macht. Grundsätzlich gilt, dass der Versicherungsnehmer auch bei überobligatorischen Rettungsmaßnahmen die Obliegenheit zur Weisungseinholung und -befolgung zu beachten hat und die Weisung für ihn grundsätzlich bindend ist. Den unter der Überschrift „Allgemeine Ausschlüsse" befindlichen Ausschluss des Löse-/Erpressungsgelds wird der Versicherungsnehmer allerdings nicht ohne weiteres als Weisung im Sinne von § 82 Abs. 2 VVG verstehen, weil in der Formulierung kein Unterlassungsgebot zum Ausdruck kommt. Unabhängig davon gilt jedoch auch hier, dass das Zuwiderhandeln gegen eine Weisung oder einen Zustimmungsvorbehalt folgenlos bleibt, wenn die Zahlung objektiv geboten war, weil es dann an einem Nachteil für den Cyberversicherer fehlt.

Im Übrigen brauchen Weisungen nicht befolgt zu werden, die dem Versicherungsnehmer Unbilliges zumuten bzw. zu einer Gefährdung wichtiger unversicherter eigener Vermögensinteressen des Versicherungsnehmers führen.[80] Deshalb kann der Cyberversicherer dem Versicherungsnehmer in einer Situation, in der der durch die Betriebsunterbrechung drohende Schaden potenziell über die Versicherungssumme hinausgeht, die Lösegeldzahlung weder untersa-

[80] Hans. OLG Hamburg v. 17.11.1983 – 6 U 43/83, VersR 1984, 258, 259; *Looschelders*, in: Langheid/Wandt, VVG, 3. Aufl. 2022, § 82 Rn. 50; *Voit*, in: Prölss/Martin, VVG, 31. Aufl. 2021, § 82 Rn. 24 f.

gen noch von seiner Zustimmung abhängig machen.[81] Insoweit ist der Hinweis geboten, dass der Versicherungsnehmer Weisungen des Versicherers nur dann befolgen muss, wenn sichergestellt ist, dass ihm die Aufwendungen, die über die Versicherungssumme hinausgehen, erstattet werden. Dies folgt aus § 83 Abs. 3 VVG. Die Untersagung der Lösegeldzahlung oder der Zustimmungsvorbehalt zu einer Zahlung haben jedoch keine Aufwendungen des Versicherungsnehmers zur Folge, sondern dienen im Gegenteil dazu, Aufwendungen in Form der Lösegeldzahlung zu vermeiden.

4.2.2.2 Lösegeldzahlung als Hauptleistung geschuldet

Abwandlung 2:

Wie Abwandlung 1, jedoch ist die Lösegeldzahlung als Hauptleistung geschuldet. Die Versicherungssumme für Lösegeldzahlungen beläuft sich auf 100.000 EUR. Der Erpresser fordert 150.000 EUR.

Hier stellt sich die Frage, ob die Versicherungsnehmerin Anspruch auf Erstattung des über die Versicherungssumme für Lösegeldzahlung hinausgehenden Betrags von 50.000 EUR nach § 83 Abs. 1 VVG hat. Da es der Versicherungsnehmerin durch die Zahlung von 150.000 EUR gelang, den montäglichen Betriebsunterbrechungsschaden abzuwenden, der sich auf 200.000 EUR belaufen hätte, war die Zahlung objektiv geboten, so dass man ihr diesen Anspruch nicht mit dem Argument verwehren kann, sie hätte die Zahlung subjektiv nicht für geboten halten dürfen. Die Rechtslage weicht insoweit nicht von der zuvor dargestellten Situation ab, in der die Lösegeldzahlung nicht als Hauptleistung geschuldet wird.

5. Fazit

Die Cyberversicherung markiert in ihrer aktuellen Erscheinungsform das Ende einer Entwicklung, die zu Beginn der 1970er Jahre ihren Anfang genommen hat. Neu und insoweit innovativ ist die Aufnahme zahlreicher Assistance-Leistungen in das Leistungsangebot, die insbesondere die Bedürfnisse von KMUs befriedigt.

Der Umfang der Deckung hat sich seit der Einführung der Cyberversicherung zu Beginn der 2010er Jahre kontinuierlich erweitert. Diese Entwicklung dürfte mittlerweile ihren Höhepunkt erreicht haben. Der nächste Schritt – die Deckung von Sach- und/oder Personenschäden – ist nicht zu erwarten, da es zu

[81] A. A. *Sieg/Schilbach*, PHi 2023, 46, 54.

erheblichen Überschneidungen mit der Sach- und Haftpflichtversicherung käme.

Die Zukunft der Lösegeldversicherung als Hauptleistungsbestandteil der Cyberversicherung, die nach der Herbstkonferenz der Innenminister am 02.12.2021 auf dem Spiel zu stehen schien,[82] ist wohl gesichert. So ist dem Bericht des BehördenSpiegel vom September 2022 zu entnehmen, dass sich die Bundesregierung gegen ein Verbot von Lösegeldversicherungen stellt, weil es einen Grundrechtseingriff darstelle und möglicherweise nicht in Proportion zum zu verhindernden Schaden stehe. Zudem sei es nicht zweckmäßig: „Ein solches Verbot würde im Übrigen gar nicht verhindern, dass Unternehmen Lösegeld selbst zahlen."[83] Im Übrigen könnte ein solches Verbot nur dann seinen angedachten Zweck erfüllen, wenn die Ersatzfähigkeit von Lösegeldzahlungen als Rettungskosten ebenfalls untersagt wird.

Die Verbreitung der Cyberversicherung wird zunehmen, so viel scheint sicher. Ob sich die in Aussicht genommenen Wachstumsraten realisieren lassen, bleibt abzuwarten. Als Haupthindernis erweist sich der fehlende einheitliche Standard in der Cyberversicherung, der nicht nur die Vergleichbarkeit der Deckungen, sondern auch Umdeckungen und den Aufbau eines Exzedentenprogramms erschwert. Dies gilt vor allem im Hinblick auf die unterschiedlichen Definitionen des Begriffs des Versicherungsfalls. Jeder Wechsel des Versicherungsvertrages vom Manifestations- oder Schadensereignisprinzip auf das Claims-made-Prinzip und umgekehrt birgt das Risiko von Deckungslücken, das letztlich die Makler zu tragen haben.

---

[82] Beschlüsse der Herbstkonferenz der Innenminister, 02.12.2021, https://stm.baden-wuerttemberg.de/de/service/presse/pressemitteilung/pid/beschluesse-der-herbstkonferenz-der-innenminister/ (zuletzt abgerufen am 22.4.2023): „‚[…] Und deshalb ist es auch in höchstem Maße problematisch, wenn Versicherungen Lösegeldzahlungen im Versicherungsschutz mit abdecken', so [Baden-Württembergs] Innenminister Thomas Strobl. Die Innenministerkonferenz hält deshalb fest, dass der Gewinn von Cyberkriminellen gesenkt werden muss. In diesem Sinne soll geprüft werden, ob man Lösegeldzahlungen vom Versicherungsschutz ausnehmen sollte und welche Maßnahmen darüber hinaus wirkungsvoll sein könnten."

[83] BehördenSpiegel/September 2022, S. 37, https://issuu.com/behoerden_spiegel/docs/2022_september?e=24296875/93510765 (zuletzt abgerufen am 22.4.2023).