Daniel Adolph

Die Cyberversicherung

Die Musterbedingungen des Gesamtverbands der Deutschen Versicherungswirtschaft für die Cyberrisiko-Versicherung (AVB-Cyber 2017 und AVB-Cyber 2024) auf dem Prüfstand

Schriften zum Versicherungs- und Haftungsrecht

Band 6

herausgegeben von

Prof. Dr. Roland Michael Beckmann

Prof. Dr. Annemarie Matusche-Beckmann

Prof. Dr. Roland Rixecker

Die Cyberversicherung

Die Musterbedingungen des Gesamtverbands der Deutschen Versicherungswirtschaft für die Cyberrisiko-Versicherung (AVB-Cyber 2017 und AVB-Cyber 2024) auf dem Prüfstand

von

Daniel Adolph

Verlag Alma Mater

Die Deutsche Bibliothek verzeichnet diese Veröffentlichung in der Deutschen Nationalbibliographie. Die bibliographischen Daten im Detail finden Sie im Internet unter http:/ /dnb.de

ISBN 978-3-946851-83-7

www.Verlag-Alma-Mater.de
Druck: Conte, St. Ingbert

Meinen Eltern
Christine und Thomas
&
meiner Großmutter
Angelika

Vorwort und Danksagung

Die vorliegende Arbeit entstand im Zeitraum von März 2021 bis Juni 2024 während meiner Tätigkeit als wissenschaftlicher Mitarbeiter am Lehrstuhl für Bürgerliches Recht, deutsches und europäisches Handels- und Wirtschaftsrecht sowie Privatversicherungsrecht von Frau Univ.-Prof. Dr. Annemarie Matusche-Beckmann an der Universität des Saarlandes. Sie wurde vom Promotionsausschuss der Rechtswissenschaftlichen Fakultät der Universität des Saarlandes im Dezember 2024 als Dissertation angenommen.

Per aspera ad astra (dt.: „Durch Mühsal gelangt man zu den Sternen") – Unter diesem althergebrachten römischen Leitspruch möchte ich meine zurückliegende Promotionszeit zusammenfassen. Als ich zu Beginn des Jahres 2021 mitten in den Wirren der Covid-19-Pandemie auf der Suche nach einem passenden Promotionsthema beim Stöbern in den Regalen des Deutsch-Europäischen Juridicums auf ein neuartiges Versicherungsprodukt namens Cyberversicherung stieß, konnte ich den mir bevorstehenden „Weg zu den Sternen" nur in Ansätzen erahnen. Cyberversicherungen wurden zu dieser Zeit erst seit wenigen Jahren auf dem deutschen Versicherungsmarkt vertrieben. Die Musterbedingungen des GDV zur Cyberrisikoversicherung (AVB-Cyber 2017), die den späteren Hauptuntersuchungsgegenstand der Arbeit bilden sollten, waren damals noch keine vier Jahre alt. Dementsprechend war auch die bestehende Literatur zu dem Thema rar gesät; einschlägige Rechtsprechung zum damaligen Zeitpunkt noch keine vorhanden. Trotz oder besser gesagt gerade wegen dieser spärlichen Arbeitsgrundlage war mein Pionier- und Forschergeist geweckt. Mein Ziel war schnell gefasst: Ich wollte die AVB-Cyber 2017 in möglichst umfassender Weise auf den juristischen Prüfstand stellen und mit anderen Cyberversicherungsbedingungen vergleichen, um ihre rechtliche und praktische Tauglichkeit en détail beurteilen zu können.

Zwischen Lockdowns und Ausgangsperren entstanden in der Folge die ersten Zeilen dieser Arbeit. Die unerforschten Gebiete der Cyberversicherung erwiesen sich dabei prompt als Herausforderung und Chance zugleich. Ungelöste oder kaum im Schrifttum behandelte Rechtsfragen waren fortan an der Tagesordnung. Grundkenntnisse in den Bereichen IT- und Cybersicherheit sowie rechtliches Wissen zu anderen Versicherungssparten erwiesen sich rasch als unerlässlich, um zu fundierten Analysen und Ergebnissen zu gelangen. Augenscheinlich randständige Fragen offenbarten sich im Zuge

der Bearbeitung oftmals als relevanter und problemträchtiger als zunächst gedacht. Außerdem musste eine Vielzahl an Cyberversicherern zunächst zur wissenschaftlichen Freigabe ihrer Bedingungen bewegt werden, um anschließend das vorgefundene Bedingungsgestrüpp systematisieren und bewerten zu können.

All dies war gewiss nicht immer trivial und mit manchen Rückschlägen und Frustrationen verbunden. Dennoch war diese Zeit nicht nur in fachlicher, sondern auch in persönlicher Hinsicht überaus lehrreich und ich würde sie keinesfalls missen wollen. Als besonders motivierend empfand ich es dabei, stets „am Puls der Zeit" zu arbeiten. Mit erschreckender Verlässlichkeit fanden sich in den monatlich erscheinenden Fachzeitschriften regelmäßig neue (Praxis-)Beiträge und erste Urteile zur Cyberversicherung. Auch die Monographie- und Kommentarliteratur wagte sich zunehmend auf das neue Terrain, wodurch sich viele bereichernde Denkanstöße für die weitere Arbeit ergaben. Besonders interessant war zudem die Teilnahme am 5. Berliner Cyberversicherungstag an der Freien Universität Berlin im Oktober 2023, bei dem mir wertvolle Eindrücke und Informationen aus der Praxis zuteil wurden.

Als im Februar 2024 die überarbeiteten AVB-Cyber 2024 erschienen, war ich von deren Erscheinen zwar nicht überrascht, da die anstehende Revision der Bedingungen in informierten Kreisen bereits seit längerem bekannt war. Indes war meine Anspannung bei der Lektüre der neuen Bedingungen greifbar. Schließlich war das Manuskript zu den AVB-Cyber 2017 so gut wie fertiggestellt. Eine umfassende Novelle der Bedingungen hätte – in Anlehnung an das berühmte Zitat von Julius von Kirchmann – die gesamte Arbeit mit einem Federstrich des GDV zur Makulatur machen können. Glücklicherweise bewahrheiteten sich diese Befürchtungen nicht, so dass sich mir in der Folge die Chance bot, die inhaltlichen Neuerungen der Musterbedingungen in einem gesonderten Addendum abzuhandeln. Dass sich hierdurch die abschließende Fertigstellung des Manuskripts noch eine Weile verzögerte, bleibt ein kleiner Wermutstropfen, der mit Blick auf den erzielten Zugewinn für die Arbeit jedoch verschmerzbar war.

In der Rückschau war die Anfertigung dieses Werkes somit eine mühsame Freude, bei der ich viel über das Versicherungsrecht, eigenständiges wissenschaftliches Arbeiten und eine Menge anderer Themen gelernt habe. Auch wenn die Arbeit an manchen Stelle etwas kleinteilig daherkommt, habe ich stets versucht, nie den Blick für das große Ganze zu verlieren. Selbstverständlich bleibt es dem geneigten Leser selbst überlassen, ob er diese Beurteilung teilt. Ich hoffe jedenfalls, dass ich mit dieser Arbeit einen Beitrag zum wissenschaftlichen Diskurs leiste, der ein wenig mehr Licht in die noch dunklen Ecken der Cyberversicherung bringt und zugleich zum kritischen Nachdenken anregt.

Rechtsprechung und Literatur befinden sich auf dem Stand vom 01. Juni 2024. Der Vollständigkeit und guten Form halber möchte ich jedoch an dieser Stelle auf vier für die Cyberversicherung besonders bedeutsame, gerichtliche Entscheidungen hinweisen, die in der Zwischenzeit veröffentlicht wurden und keine Berücksichtigung mehr in der Arbeit finden konnten. Zunächst möchte ich das Urteil des BGH vom 25.9.2024 – IV ZR 350/22 anführen, das sich mit der AGB-rechtlichen Wirksamkeit einer Obliegenheit zur Einhaltung aller vertraglichen behördlichen und gesetzlichen Sicherheitsvorschriften in der Wohngebäudeversicherung auseinandersetzt. Zu den (überraschenden) Implikationen dieses Urteils auf die gleichlautende Obliegenheit in den AVB-Cyber habe ich bereits in Ansätzen im Rahmen meiner Disputation referiert und beabsichtigte an anderer Stelle hierzu noch näher Stellung zu beziehen. Weiter möchte ich auf die (Hinweis-)Beschlüsse des OLG Schleswig vom 14.10.2024 – 16 U 63/24 sowie vom 9.1.2025 – 16 U 63/24 hinweisen, die sich mit den praxisrelevanten Problemfeldern betreffend die Beantwortung von vorvertraglichen Risikofragen durch den Versicherungsnehmer sowie der Arglistanfechtung eines Cyberversicherungsvertrages durch den Versicherer befassen. Zuletzt möchte ich das Urteil des LG Hagen vom 15.10.2024 – 9 O 258/23 benennen, das sich mit der Auslegung des in vielen Cyberversicherungsverträgen anzutreffenden Begriffs der Netzwerksicherheitsverletzung beschäftigt.

Abschließend möchte ich noch einige Worte des Dankes ausrichten.

Mein besonderer Dank gilt zunächst meiner Doktormutter, Frau Professorin Dr. Annemarie Matusche-Beckmann, für ihre hervorragende Unterstützung und ihr persönliches Engagement bei der Betreuung dieser Arbeit. Durch ihre konstruktiven Anmerkungen und Hinweise hat sie entscheidend zum Gelingen meiner Arbeit beigetragen. Ebenfalls herzlich bedanken möchte ich mich bei dem Präsidenten des Verfassungsgerichtshofs des Saarlandes Herrn Professor Dr. Roland Rixecker für die freundliche Übernahme und überaus zeitnahe Erstellung des Zweitgutachtens. Über seine positiven wie kritischen, indes jederzeit wohlwollenden Gedanken und Anmerkungen in seinem Votum habe ich mich sehr gefreut.

Ein herzlicher Dank gebührt weiter meinen (ehemaligen) Kollegen und Studienfreunden an der Universität des Saarlandes. Jeder hat meine Studien- und Promotionszeit auf seine Art und Weise geprägt. Besonders möchte ich mich jedoch bei meinen langjährigen Lehrstuhls- und Bürokollegen Frau Dr. Mona Fasching, Frau Ass.-iur. Ida Scharhag, Herrn Dipl.-Jur. Matthias Michael Thielen, Herrn Dipl.-Jur. Christian Breiden sowie unserer Lehrstuhlsekretärin Frau Dagmar Schug-Kruchten, dem Mensatrio bestehend aus Herrn Dipl.-Jur. Hendrik Mayer, Herrn Ass.-iur. Alexander Kratz und Herrn Dipl.-Jur. David Gölz sowie nicht zuletzt bei Frau Dipl.-Jur. Lea-Marie Berzl

bedanken, durch deren allzeitige Kollegialität, Hilfsbereitschaft und Freundschaft ich meine Promotionszeit in schöner Erinnerung behalten werde.

Einen besonderen Dank möchte ich zum Schluss an meine Partnerin Lara Bauer richten, die mich in dieser fordernden Phase meines Lebens allumfassend unterstützt und mir gerade in schwierigen Zeiten immer wieder Mut und Optimismus zugesprochen hat. Mein größter Dank gilt jedoch meinen Eltern, Christine und Dr. Thomas Adolph, sowie meiner Großmutter Angelika Müller, die mir diese Ausbildung erst ermöglicht und mich auf meinem bisherigen Lebensweg vorbehaltlos unterstützt, gefördert und gefordert haben und dadurch die Basis für meine persönliche und berufliche Entwicklung gelegt haben. Durch ihren steten Rückhalt, ihren Zuspruch und ihre Liebe haben sie im wesentlichen Maße zum Gelingen der Arbeit beigetragen. Ihnen widme ich daher diese Arbeit.

Lebach, im Januar 2025

Daniel Adolph

Inhaltsverzeichnis

Vorwort VII
Abkürzungsverzeichnis XXIX

Kapitel 1: Einführung 1

Kapitel 2: Leistungsumfang der AVB-Cyber 37

Kapitel 3: Allgemeine Risikoausschlüsse 163

Kapitel 4: Obliegenheiten des Versicherungsnehmers 235

Kapitel 5: Schlussbetrachtung 315

Kapitel 6: Addendum – Die neuen „AVB-Cyber 2024“ 319

Literaturverzeichnis 335

Inhaltsverzeichnis

Vorwort VII
Abkürzungsverzeichnis XXIX

Kapitel 1: Einführung 1

A) Problemaufriss und Gegenstand der Arbeit 1

B) Gang der Untersuchung 5

C) Überblick zur Cyberrisikolage für Unternehmen 6

I) Begriffsdefinition 6

II) Kategorien von Cyberrisiken 7

1) Cyberangriffe 7
a) Einschleusen von Schadsoftware 7
(1) Ransomware 8
(2) Spyware und Advanced-Persistent-Threads 10
b) (Distributed-)Denial-of-Service-Attacken 11
c) Sonstige Cyberangriffsarten 12

2) Social-Engineering 13
a) Phishing 13
b) Fake-President-Masche 13

3) Sonstige Informationstechnologie- und Informationssicherheitsrisiken 14

III) Verstärkende Faktoren 14

IV) Schadenspositionen 16

1) Eigenschäden 16

2) Drittschäden 18
a) Vertragliche Haftungsszenarien 18
b) Außervertragliche Haftungsszenarien 19
(1) Ansprüche gemäß § 823 Abs. 1 BGB 19
(2) Ansprüche gemäß § 823 Abs. 2 BGB i.V.m. der Verletzung eines Schutzgesetzes 21

(3) Ansprüche gemäß Art. 82 Abs. 1 DS-GVO 22

D) Grundlagen zur Cyberversicherung 24

I) Begriffserläuterung 24

II) Ursprung und aktueller Stand der Entwicklung in Deutschland 24

III) Ökonomische Versicherbarkeit von Cyberrisiken 26

IV) Überblick zu Konzeption und Inhalt von Cyberversicherungen 28

1) Die Cyberrisiko-Versicherung des GDV (AVB-Cyber) 29

2) Gegenwärtige Bedingungswerke auf dem Cyberversicherungsmarkt 30

V) Auslegungsmaßstab bei Cyberversicherungen 31

1) Grundlagen 31

2) Verständnishorizont eines durchschnittlichen Versicherungsnehmers in der gewerblichen Cyberversicherung 32

3) Restriktionsprinzip und Unklarheitenregel gemäß § 305c Abs. 2 BGB 34

Kapitel 2: Leistungsumfang der AVB-Cyber 37

A) Gegenstand der Versicherung (Ziff. A1-1 AVB-Cyber) 37

I) Informationssicherheitsverletzung (Ziff. A1-2.1 AVB-Cyber) 37

1) Schutzziele der Informationssicherheit 37
a) Verfügbarkeit 38
b) Integrität 38
c) Vertraulichkeit 39
d) Beeinträchtigung eines Schutzziels 39

2) Elektronische Daten des Versicherungsnehmers 40
a) Datenbegriff der AVB-Cyber 40
b) Zuordnung der Daten 42

3) Informationsverarbeitende Systeme 43

4) Betriebliche oder berufliche Zwecksetzung 45

5) Aufenthaltsort der versicherten Daten und informationsverarbeitenden Systeme (Satz 1 Ziff. A1-2.2 AVB-Cyber) 45

6) Risikoausschluss bei Inanspruchnahme externer Dienstleister (Satz 2 Ziff. A1-2.2 AVB-Cyber) 46
a) Externe Dienstleister 47
(1) Dienstleistungen innerhalb der Betriebsstätte 47
(2) Dienstleistungen von Tochterunternehmen 48
b) Ausfall, Unterbrechung oder Störung der Dienstleistung 49
(1) Art der Beeinträchtigung 49
(2) Ort der Beeinträchtigung 50
c) AGB-rechtliche Zulässigkeit des Risikoausschlusses 51
(1) Vereinbarkeit mit § 305c Abs. 1 BGB 51
(2) Vereinbarkeit mit § 307 Abs. 1 S. 1 BGB 52
aa) Verstoß gegen das Transparenzgebot gemäß § 307 Abs. 1 S. 2 BGB 53
bb) Leitbildverstoß und Vertragszweckgefährdung gemäß § 307 Abs. 2 Nr. 1 und 2 BGB 53
7) Versicherte Ereignisse (Ziff. A1-2.4 AVB-Cyber) 55
a) Angriffe auf elektronische Daten oder informationsverarbeitende Systeme 55
(1) Vorsätzlichkeit der Handlung 55
(2) Zielgerichtetheit der Handlung 56
b) Unberechtigte Zugriffe auf elektronische Daten 57
(1) Vorsätzlichkeit der Handlung 58
(2) Möglichkeit der Kenntnisnahme 58
(3) Fehlende Berechtigung 59
c) Eingriffe in informationsverarbeitende Systeme 59
(1) Begrenzung auf informationstechnische Einwirkungen 60
(2) Unmittelbarkeitserfordernis 60
(3) Vorsätzlichkeit der Handlung 61
(4) Beschränkung auf unberechtigte Handlungen 62
d) Verletzung datenschutzrechtlicher Vorschriften 63
(1) Datenschutzrechtlicher Normverstoß aufgrund einer Handlung oder Unterlassung 63
(2) Art und Weise der Handlung oder Unterlassung 64
e) Einwirkung von Schadprogrammen 64
8) Marktvergleich 65
9) Stellungnahme zur Schadensereignisdefinition im Basis-Baustein und Änderungsvorschlag 67
II) Versicherte Schäden 70
1) Vermögensschaden (Ziff. A1-3 AVB-Cyber) 70
a) Einschluss von Vermögensfolgeschäden 70
b) Sachqualität von elektronischen Daten 72
c) Verlust von elektronischen Daten infolge des Abhandenkommens von Sachen 73
2) Zusatz: „im Umfang der nachfolgenden Bestimmungen“ 74

B) Service und Kosten-Baustein (Ziff. A2 AVB-Cyber) 75

I) Forensik/Schadenfeststellungskosten (Ziff. A2-1 AVB-Cyber) 75

1) Ersatzfähige Kosten 76
a) Kosten für externe Sachverständige zur Ermittlung der Ursache und zur Feststellung des versicherten Schadens.....76
b) Ersatzfähigkeit von Rechtsanwalts- und Rechtsberatungskosten .76
c) Ersatzfähigkeit von innerbetrieblichen Sachverständigenkosten ..77
d) Ersatzfähigkeit von Sachverständigenkosten bei Übersteigen der Versicherungssumme 78
e) Angemessenheit und Erforderlichkeit der Sachverständigenkosten 79

2) Vorherige Abstimmung mit dem Versicherer 79
a) Direktionsrecht des Versicherers 80
b) Verzicht auf Abstimmung in Eilfällen.....80
c) Auswirkungen einer unterbliebenen Abstimmung 81

3) Kostenübernahme bei Nicht-Vorliegen eines Versicherungsfalls 81

II) Versicherte Kosten im Versicherungsfall (Ziff. A2-2 AVB-Cyber) 83

1) Benachrichtigungskosten und Call-Center-Leistungen (Ziff. A2-2.1 AVB-Cyber).....83
a) Ersatzfähigkeit von Rechtsanwaltskosten 84
b) Ersatzfähigkeit von innerbetrieblichen Prüf- und Erfüllungskosten 85
c) Auswirkungen von Irrtümern bei der Prüfung 85
(1) Ersatzfähigkeit von irrtümlichen Prüfungskosten 85
(2) Ersatzfähigkeit von irrtümlichen Erfüllungskosten.....86

2) Krisenkommunikation und PR-Maßnahmen (Ziff. A2-2.2 AVB-Cyber) 87
a) Kosten zur Wiederherstellung der öffentlichen Reputation 87
b) Kosten für Krisenmanagement- und PR-Berater 88
(1) Begriffserläuterungen 88
(2) Vorherige Zustimmung des Versicherers.....88

III) Aufwendungen vor Eintritt des Versicherungsfalls (Ziff. A2-3 AVB-Cyber) 89

1) Unmittelbar bevorstehender Schaden 89

2) Ersatzfähige Aufwendungen 90
a) Erforderlichkeit der Maßnahmen zur Schadenabwehr 90
b) Allgemeine Aufwendungen für Systemverbesserungen 91

3) Anzeigeobliegenheit des Versicherungsnehmers (Ziff. A2-3.2 AVB-Cyber).....92

a) Reichweite der Anzeigeobliegenheit 92
b) Rechtsfolgen eines Obliegenheitsverstoßes 93
IV) Marktvergleich 93
V) Stellungnahme zum Service und Kosten-Baustein 94
C) Drittschaden-Baustein (Ziff. A3 AVB-Cyber) 95
I) Gegenstand der Versicherung (Ziff. A3-1 AVB-Cyber) 95
1) Eintritt eines Vermögensschadens infolge einer Informationssicherheitsverletzung 96
2) Inanspruchnahme auf Schadensersatz durch einen Dritten 96
a) Begriff: „Dritter" 97
b) Inanspruchnahme auf Schadensersatz 97
3) Gesetzliche Haftpflichtbestimmungen privatrechtlichen Inhalts 98
II) Risikoausschlüsse im Drittschaden-Baustein 99
1) Besondere Ausschlüsse (Ziff. A3-7 AVB-Cyber) 100
a) Rückruf 100
b) Ansprüche der Versicherten untereinander 101
c) Verbundene Unternehmen 101
d) Schadenfälle von Angehörigen des Versicherungsnehmers, gesetzlichen Vertretern, Gesellschaftern und anderen Personen 102
III) Deckungserweiterungen (Ziff. A3-4 AVB-Cyber) 102
1) Rechtswidrige elektronische Kommunikation (Ziff. A3-4.1 AVB-Cyber) 103
a) Versicherte Ansprüche 103
b) Veröffentlichung elektronischer Medieninhalte 104
2) E-Payment (Ziff. A3-4.2 AVB-Cyber) 105
3) Vertragliche Schadensersatzansprüche (Ziff. A3-4.3 AVB-Cyber) 106
IV) Inhalt und Umfang der Versicherungsleistung 106
1) Leistung der Versicherung/Vollmacht des Versicherers (Ziff. A3-5 AVB-Cyber) 106
2) Begrenzung der Leistung (Ziff. A3-6 AVB-Cyber) 107
V) Marktvergleich 108
VI) Stellungnahme zum Drittschaden-Baustein und Änderungsvorschlag 109
D) Eigenschaden-Baustein (Ziff. A4 AVB-Cyber) 110

I) Betriebsunterbrechung/Ertragsausfall (Ziff. A4-1 AVB-Cyber) 110

1) Gegenstand der Versicherung (Ziff. A4-1.1 AVB-Cyber)....110
a) Betriebsunterbrechung 111
(1) Verfügbarkeits- bzw. Leistungsbeeinträchtigung 111
(2) Kausalzusammenhang....112
(3) Rückwirkungsschäden....113
b) Unterbrechungsschaden 113
(1) Betriebsgewinn und die fortlaufenden Kosten 113
(2) Nicht-Erwirtschaftbarkeit....114
(3) Zeitliche Beschränkungen 114
aa) Zeitraum der Betriebsunterbrechung....114
bb) Haftzeit 115

2) Besondere Ausschlüsse (Ziff. A4-1.2 AVB-Cyber) 115
a) Geplante Abschaltung informationsverarbeitender Systeme 115
b) Geplante Löschung oder Veränderung elektronischer Daten 117
c) Einführung neuer informationsverarbeitender Systeme oder Verfahren sowie Software 118
d) Einsatz ungetesteter oder für den Einsatzzweck nicht freigegebener informationsverarbeitender Systeme oder Verfahren sowie Software 119
e) Unberechtigte Verwendung informationsverarbeitender Systeme, Verfahren sowie Software 120
f) Softwarefehler, die keine Sicherheitslücke darstellen 120

3) Umfang der Entschädigung (Ziff. A4-1.3 AVB-Cyber) 122
a) Entschädigungsberechnung/Tagessatzregelung 122
(1) Anspruchskürzung nach § 76 S. 2 Hs. 2 VVG 122
(2) Lösungsansätze und Stellungnahme....123
b) Risikoausschluss für Verlängerungen des Unterbrechungsschadens 124
(1) Außergewöhnliche Ereignisse 124
(2) Behördliche Wiederherstellungs- oder Betriebsbeschränkungen 125
(3) Fehlende finanzielle Mittel 125
(4) Veränderungen oder Verbesserungen 126
(5) Sach- oder Personenschaden 126
c) Grenze der Entschädigung/Zeitliche Selbstbeteiligung 126

II) Wiederherstellung von Daten (Ziff. A4-2 AVB-Cyber) 127

1) Gegenstand der Versicherung (Ziff. A4-2.1 AVB-Cyber)....127
a) Datenwiederherstellung 127
b) Schadsoftwareentfernung 128
c) Notwendigkeit der Aufwendungen 128

2) Versicherte Daten (Ziff. A4-2.2 AVB-Cyber)....129

3) Besondere Ausschlüsse (Ziff. A4-2.3 AVB-Cyber) 130
4) Versicherungssumme und Umfang der Entschädigung (Ziff. A4-2.4 AVB-Cyber)....130
III) Marktvergleich 131
1) Betriebsunterbrechungsschäden....131
2) Kosten zur Daten- bzw. Systemwiederherstellung....133
3) Weitere Schadenspositionen....133
IV) Stellungnahme zum Eigenschaden-Baustein und Änderungsvorschlag 134
E) Eintritt des Versicherungsfalls im versicherten Zeitraum 136
I) Versicherungsfall/Versicherter Zeitraum (Ziff. A1-4 AVB-Cyber) 136
1) AGB-rechtliche Zulässigkeit des Feststellungsprinzips 137
2) Maßgeblicher Zeitpunkt: „Erstmals nachprüfbar festgestellter Schaden“ 138
a) Reichweite des Feststellungserfordernisses 139
b) Anforderungen an die Nachprüfbarkeit der Schadensfeststellung 139
II) Nachhaftung (Ziff. A1-5 AVB-Cyber) 141
III) Rückwärtsdeckung (Ziff. A1-6 AVB-Cyber) 142
1) Keine Feststellung im Zeitpunkt des Vertragsschlusses 143
2) Eintritt nach dem im Versicherungsschein bestimmten Zeitpunkt....143
3) Wechselwirkungen zwischen Nachhaftung und Rückwärtsdeckung 144
IV) Marktvergleich 145
V) Stellungnahme zur Versicherungsfalldefinition in den AVB-Cyber 146
F) Persönlicher und räumlicher Geltungsbereich der Versicherung....148
I) Persönlicher Geltungsbereich der Versicherung (Ziff. A1-7 AVB-Cyber; Ziff. A1-8 AVB-Cyber)....148
II) Räumlicher Geltungsbereich der Versicherung (Ziff. A1-10 AVB-Cyber; Ziff. A1-11 AVB-Cyber)....150

G) Zurechnung und Organisationsverschulden 151

I) Zurechnung nach den Grundsätzen der Repräsentantenhaftung und Repräsentantenbegriff (Ziff. A1-9 AVB-Cyber) 151

II) Eigenes Organisationsverschulden 152

H) Selbstbeteiligungen, Serienschaden (Ziff. A1-15 AVB-Cyber) 154

I) Ursachenklausel 155

II) Erweiterte Ursachenklausel 155

1) Inhaltliche Voraussetzungen 156
a) Gleichheit der Ursachen 156
b) Innerer Zusammenhang 157
(1) Sachlicher Zusammenhang 157
(2) Zeitlicher Zusammenhang 157

2) AGB-rechtliche Zulässigkeit der erweiterten Ursachenklausel 158
a) Leitbildverstoß und Vertragszweckgefährdung gemäß § 307 Abs. 2 Nr. 1 und 2 BGB 158
b) Verstoß gegen das Transparenzgebot gemäß § 307 Abs. 1 S. 2 BGB 160

3) Lösungsvorschlag 161

Kapitel 3: Allgemeine Risikoausschlüsse 163

A) Vorvertragliche Informationssicherheitsverletzung (Ziff. A1-17.1 AVB-Cyber) 163

I) Maßgeblicher Zeitpunkt: „Beginn des Versicherungsvertrages“ 163

II) (AGB-rechtliche) Zulässigkeit des Risikoausschlusses 164

1) Vereinbarkeit mit den §§ 19 ff. VVG, § 32 VVG 164

2) Vereinbarkeit mit § 307 Abs. 1 S. 1 BGB 165
a) Verstoß gegen das Transparenzgebot gemäß § 307 Abs. 1 S. 2 BGB 165
b) Leitbildverstoß und Vertragszweckgefährdung gemäß § 307 Abs. 2 Nr. 1 und 2 BGB 166

B) Krieg, Politische Gefahren und Terrorakte (Ziff. A1-17.2 AVB-Cyber bis Ziff. A1-17.4 AVB-Cyber) 167

I) Praktische und wirtschaftliche Bedeutung der Risikoausschlüsse 167
II) Krieg (Ziff. A1-17.2 AVB-Cyber) 169
1) Kriegsdefinition der AVB-Cyber 170
2) Politisch-motivierte Cyberangriffe als „Krieg" im Sinne der AVB-Cyber 171
a) Kriegsparteifähigkeit 171
b) Bewaffnete, gewaltsame Auseinandersetzung 173
(1) Allgemeinsprachliche Erwägungen 173
(2) Teleologische und folgenbezogene Erwägungen 175
(3) Systematische und historische Erwägungen 176
(4) Unklarheitenregel und Restriktionsprinzip 177
(5) (Zwischen-)Ergebnis 178
3) Krieg als kausale Ursache für Versicherungsfälle und Schäden infolge politisch-motivierter Cyberangriffe 178
III) Politische Gefahren (Ziff. A1-17.3 AVB-Cyber) 181
IV) Terrorakte (Ziff. A1-17.4 AVB-Cyber) 183
V) Marktvergleich 185
VI) Stellungnahme und Lösungsvorschlag 187
C) Ausfall Infrastruktur (Ziff. A1-17.5 AVB-Cyber) 189
I) Praktische und wirtschaftliche Bedeutung des Risikoausschlusses 190
II) Ausfall von Infrastruktur 191
1) Betroffenheit vom Ausfall 191
2) Gebietskörperschaften oder wesentliche Teile hiervon 192
3) Netzstrukturen und Einrichtungen der Daseinsvorsorge 193
4) Sonstige Infrastrukturbetriebe 194
III) Rechtsfolge und (Zwischen-)Ergebnis 196
D) Löse-/Erpressungsgeld (Ziff. A1-17.7 AVB-Cyber) 196
I) Hintergrund des Risikoausschlusses 196
II) Praktische und wirtschaftliche Bedeutung des Risikoausschlusses 197
III) Gesetzliche Ersatzfähigkeit von Lösegeldzahlungen nach § 83 Abs. 1 S. 1 VVG 199

1) Maßgeblicher Zeitpunkt: „Eintritt des Versicherungsfalls“ 199
2) Gebotenheit der Lösegeldzahlung.....200
3) Einwand des rechtsmissbräuchlichen Verhaltens.....200
IV) Vertragliche Deckungsoptionen 201
1) Marktvergleich.....202
2) Notwendigkeit einer vertraglichen Versicherungslösung.....203
3) Lösungsvorschlag 203
E) Vorsatz und wissentliche Pflichtverletzung (Ziff. A1-17.10 AVB-Cyber) 206
I) Inhalt und AGB-rechtliche Zulässigkeit des Risikoausschlusses 206
1) Vorsätzliche Schadensherbeiführung 206
2) Schadensherbeiführung infolge wissentlicher Pflichtverletzung 207
II) Verhältnis des Risikoausschlusses zu § 81 Abs. 2 VVG 209
F) Behördliche Maßnahmen, Strafen/Bußgelder (Ziff. A1-17.11 AVB-Cyber) 212
I) Praktische und wirtschaftliche Bedeutung des Risikoausschlusses 213
II) Marktvergleich 215
III) Versicherungsverbot für (Datenschutz-)Bußgelder 216
1) Nichtigkeit nach § 134 BGB 217
a) Straftatbestand der Straf(verfolgungs-)vereitelung (§ 258 Abs. 1 StGB) als Verbotsgesetz.....217
b) Straftatbestand der Straf(vollstreckungs-)vereitelung (§ 258 Abs. 2 StGB) als Verbotsgesetz.....218
c) Straftatbestand der Untreue (§ 266 Abs. 1 StGB) als Verbotsgesetz 220
d) Straftatbestand der Begünstigung (§ 257 Abs. 1 StGB) als Verbotsgesetz 221
e) Beteiligung an einer Straftat (§ 27 StGB) bzw. an einer Ordnungswidrigkeit (§ 14 OWiG) als Verbotsgesetz.....221
f) Gewohnheitsrecht als Verbotsgesetz.....222
2) Nichtigkeit nach § 138 Abs. 1 BGB 222
a) Herrschende Ansicht 223
b) Gegenansicht.....224
c) Differenzierende Ansichten 225

(1) Ausnahme bei fahrlässiger Aufsichtspflichtverletzung nach § 130 OWiG 225
(2) Ausnahme bei einfachem Mitarbeiterfehlverhalten....225
d) Stellungnahme und Schlussfolgerungen 226
3) (Zwischen-)Ergebnis 229

G) Sonstige Risikoausschlüsse 230

I) Fahrzeuge (Ziff. A1-17.6 AVB-Cyber)....230

II) Finanzmarkttransaktionen (Ziff. A1-17.8 AVB-Cyber) 230

III) Abfluss von Vermögenswerten (Ziff. A1-17.9 AVB-Cyber) 231

IV) Verletzung von Immaterialgüterrechten (Ziff. A1-17.12 AVB-Cyber) 232

V) Kernenergie (Ziff. A1-17.13 AVB-Cyber) 233

VI) Diskriminierung (Ziff. A1-17.14 AVB-Cyber)....233

Kapitel 4: Obliegenheiten des Versicherungsnehmers....235

A) Obliegenheiten des Versicherungsnehmers bei und nach Abgabe der Vertragserklärung 235

I) Vorvertragliche Anzeigeobliegenheit (§§ 19 ff. VVG; Ziff. B3-1 AVB-Cyber)....235

1) Risikoerfassung durch Fragebögen 236
2) Erneute Risikoprüfung nach Vertragsverlängerung 237
3) Rechtsfolgen von Obliegenheitsverletzungen 238

II) Gefahrerhöhung (§§ 23 ff. VVG; Ziff. B3-2 AVB-Cyber) 240

1) Begriff der Gefahrerhöhung 241
2) Problemfelder von Gefahrerhöhungen bei Cyberversicherungen .242
a) Unterschreiten von IT-Sicherheitsvorkehrungen 242
b) Installation neuer Software 243
c) Zunahme von Remote-Arbeit....244
d) Sonstige Fallgestaltungen....245
3) Begrenzung der Gefahrerhöhungsregelungen durch vorvertragliche Risikofragen 245
4) Rechtsfolgen von Obliegenheitsverletzungen 247

B) Obliegenheiten des Versicherungsnehmers vor Eintritt des Versicherungsfalls (Ziff. A1-16 AVB-Cyber) 247

I) Besondere Obliegenheiten zur Gewährleistung der IT-Sicherheit (Ziff. A1-16.1 AVB-Cyber) 248

1) „Nutzer- und Passwort"-Klausel (Buchst. a Ziff. A1-16.1 AVB-Cyber) 249
a) Individuelle Nutzerzugänge 249
b) Unterscheidung von Befugnisebenen 250
c) Anforderungen an die Passwortkomplexität 251
(1) (Mindest-)Komplexitätsanforderungen 251
(2) Kompensationsmöglichkeit bei unterkomplexen Passwörtern 253
(3) Verstoß gegen das Transparenzgebot gemäß § 307 Abs. 1 S. 2 BGB 254

2) „Erhöhtes Risiko"-Klausel (Buchst. b Ziff. A1-16.1 AVB-Cyber) 255
a) Erreichbarkeit über das Internet 256
b) Geräte im mobilen Einsatz 256
c) Zusätzliche Schutzmaßnahmen gegen unberechtigten Zugriff 257
(1) Schutzmaßnahmen bei Erreichbarkeit über das Internet 258
aa) Firewall 258
bb) 2-Faktor-Authentifizierung bei Servern 259
(2) Schutzmaßnahmen bei Geräten im mobilen Einsatz 260
aa) Verschlüsselung von Datenträgern 260
bb) Diebstahlsicherung 261
(3) Ähnlich wirksame Maßnahmen 261
(4) Qualitative Anforderungen an die Schutzmaßnahmen 262

3) „Sicherheitssoftware"-Klausel (Buchst. c Ziff. A1-16.1 AVB-Cyber) 263
a) Schutz gegen Schadsoftware 263
(1) Code Signing 263
(2) Virenscanner 264
(3) Application Firewall 265
(4) Ähnlich wirksame Maßnahmen 266
b) Automatisch auf dem aktuellen Stand 267
(1) Einbeziehung von nicht-sicherheitsrelevanten Funktionsupdates 268
(2) Automatische Aktualisierung 268
c) Stellungnahme und Änderungsvorschlag 269

4) „Patch-Management"-Klausel (Buchst. d Ziff. A1-16.1 AVB-Cyber) 270
a) Patch-Management-Verfahren 270
(1) Inhalt und Umfang der Obliegenheit 271
(2) Unverzüglichkeit der Installation 271

(3) Relevante Sicherheitspatches 272
b) Zusätzliche Absicherung bei bekannten Sicherheitslücken 273
(1) Bekanntheit der Sicherheitslücke 273
(2) Zusätzliche geeignete Maßnahmen zur Absicherung....274
c) Verhältnis zur Aktualisierungsobliegenheit in Buchst. c Ziff. A1-16.1 AVB-Cyber....275
5) „Backup"-Klausel (Buchst. e Ziff. A1-16.1 AVB-Cyber)....275
a) Inhalt und Umfang der Sicherung....276
b) Art und Weise der Sicherung 277
c) Turnus der Datensicherung 278
d) Kontrolle des Sicherungs- und Wiederherstellungsprozesses 279
II) Allgemeine Obliegenheiten zur Gewährleistung der IT-Sicherheit (Ziff. A1-16.2 AVB-Cyber)....280
1) „Sicherheitsvorschriften"-Klausel (Buchst. a Ziff. A1-16.2 AVB-Cyber)....280
a) Gesetzliche, behördliche und vertraglich vereinbarte Sicherheitsvorschriften 280
(1) Vorschriften zur Gewährleistung der IT-Sicherheit von Unternehmen....281
aa) Gesetzliche Bestimmungen zur IT-Sicherheit von Unternehmen....282
bb) Behördliche und private Bestimmungen zur IT-Sicherheit von Unternehmen....284
(2) Datenschutzrechtliche Vorschriften 285
b) AGB-rechtliche Zulässigkeit von Buchst. a Ziff. A1-16.2 AVB-Cyber 288
(1) Leitbildverstoß gemäß § 307 Abs. 2 Nr. 1 BGB 288
(2) Vertragszweckgefährdung gemäß § 307 Abs. 2 Nr. 2 BGB 289
(3) Verstoß gegen das Transparenzgebot gemäß § 307 Abs. 1 S. 2 BGB 290
(4) (Zwischen-)Ergebnis 292
2) Beseitigung von gefahrdrohenden Umständen (Buchst. b A1-16.2 AVB-Cyber)....292
a) Besonders gefahrdrohende Umstände....293
b) Beseitigungsverlangen....294
c) Angemessene Frist 294
d) Zumutbarkeit der Beseitigung 295
III) Stellungnahme zu dem Obliegenheitskonzept von Ziff. A1-16 AVB-Cyber 295
IV) Marktvergleich und -analyse....298
1) Vor- und Nachteile von generalklauselartigen Obliegenheiten zur Gewährleistung der IT-Sicherheit 299

2) AGB-rechtliche Zulässigkeit von generalklauselartigen Obliegenheiten zur Gewährleistung der IT-Sicherheit 300
a) Vertragszweckgefährdung gemäß § 307 Abs. 2 Nr. 2 BGB 300
b) Verstoß gegen das Transparenzgebot gemäß § 307 Abs. 1 S. 2 BGB 301
(1) Unbestimmter Rechtsbegriff: „Stand der Technik" 302
(2) Unbestimmter Rechtsbegriff: „Angemessenheit" 303
3) (Zwischen-)Ergebnis 304
V) Lösungsvorschlag 304
1) Zertifikatsmodell 304
2) Inhaltliche Ausgestaltung des Zertifikatsmodells 305
a) Anforderungen an das Zertifikat 305
b) Anforderungen an den referenzierten IT-Sicherheitsstandard 306
3) Vertragliche Umsetzung 307
C) Obliegenheiten des Versicherungsnehmers bei und nach Eintritt des Versicherungsfalls (Ziff. B3-3 AVB-Cyber) 307
I) Schadenabwehr bzw. Schadenminderungsobliegenheit (Ziff. B3-3.1 AVB-Cyber) 308
1) Inhalt der Obliegenheit 308
2) Aufwendungsersatz für Rettungskosten (§ 83 Abs. 1 S. 1 VVG, § 90 VVG) 309
II) Sonstige Obliegenheiten (Ziff. B3-2 AVB-Cyber bis Ziff. B3-6 AVB-Cyber) 311
1) Obliegenheit zur Schadenanzeige 311
2) Obliegenheit zur Anzeige von haftpflichtrelevanten Tatsachen 311
3) Obliegenheit zur Auskunftserstattung 312
4) Obliegenheit zur Unveränderbarkeit bzw. Dokumentation des Schadenbildes 312
5) Obliegenheit zur Erstattung von Schadenberichten sowie zur Unterstützung bei der Schadenregulierung 312
6) Obliegenheit zur Einlegung von Rechtsbehelfen 313

Kapitel 5: Schlussbetrachtung 315

Kapitel 6: Addendum – Die neuen „AVB-Cyber 2024" 319

A) Revision der Musterbedingungen 319

B) Überblick zu den wichtigsten Änderungen 319

I) Änderungen im Bereich der primären Risiko- und Leistungsbeschreibung.....319

1) Änderungen am Begriff der Informationssicherheitsverletzung.....319

2) Änderungen hinsichtlich der Mitversicherung von Immaterialgüterrechten im Drittschaden-Baustein 320

3) Änderungen hinsichtlich der Mitversicherung des Haftpflichtrisikos des Versicherungsnehmers bei der Verletzung von Datenschutzgesetzen 321

II) Änderungen im Bereich der Risikoausschlüsse 322

1) Risikoausschluss bei Inanspruchnahme von externen Dienstleistern 322

2) Risikoausschluss für Krieg und staatliche Cyberangriffe 323

3) Risikoausschluss für Vorsatz und wissentliche Pflichtverletzung .326

4) Besondere Ausschlüsse im Drittschaden-Baustein 326

5) Besondere Ausschlüsse im Eigenschaden-Baustein 327

III) Änderungen im Bereich der Obliegenheiten des Versicherungsnehmers vor Eintritt des Versicherungsfalls 328

1) „Nutzer- und Passwort"-Klausel 329

2) „Erhöhtes Risiko"-Klausel 329

3) „Sicherheitssoftware"-Klausel 330

4) „Patch-Management"-Klausel 331

5) „Backup"-Klausel.....331

C) Zusammenfassende Bewertung der AVB-Cyber 2024.....332

Literaturverzeichnis.....335

A) Literatur 335

B) Versicherungsbedingungen.....354

C) Sonstiges.....356

Abkürzungsverzeichnis

a.A.	andere Ansicht
a.F.	alte Fassung
ABl.	Amtsblatt
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AG	Aktiengesellschaft
AGB	Allgemeine Geschäftsbedingungen
AktG	Aktiengesetz
Anm.	Anmerkung
APT	Advanced-Persistent-Thread
Art.	Artikel
ähnl.	ähnlich
BaFin	Bundeanstalt für Finanzdienstleistungsaufsicht
BAG	Bundesarbeitsgericht
BAV	Bundesaufsichtsamt für Versicherungswesen
BB	Betriebs-Berater (Zeitschrift)
BDSG	Bundesdatenschutzgesetz
Begr.	Begründer
Beschl. v.	Beschluss vom
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BKA	Bundeskriminalamt
BMI	Bundesministerium des Innern und für Heimat
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
bspw.	beispielsweise
BT-Drucks.	Bundestagsdrucksache
Buchst.	Buchstabe
BVerfG	Bundesverfassungsgericht
bzgl.	bezüglich
bzw.	beziehungsweise
CCZ	Corporate Compliance Zeitschrift (Zeitschrift)

CR	Computer und Recht (Zeitschrift)
D&O	Directors-and-Officers
d.h.	das heißt
DB	Der Betrieb (Zeitschrift)
DDoS	Distributed-Denial-of-Service
DoS	Denial-of-Service
DÖV	Die Öffentliche Verwaltung (Zeitschrift)
DS-GVO	Datenschutz-Grundverordnung
DSRITB	Deutsche Stiftung für Recht und Informatik (Zeitschrift)
DuD	Datenschutz und Datensicherheit (Zeitschrift)
e. V.	eingetragener Verein
EDV	Elektronische Datenverarbeitung
EnWG	Gesetz über die Elektrizitäts- und Gasversorgung
etc.	et cetera
EU	Europäische Union
EuGH	Gerichtshof der Europäischen Union
EUR	Euro
EuR	Europarecht (Zeitschrift)
EuZW	Europäische Zeitschrift für Wirtschaftsrecht (Zeitschrift)
EWR	Europäischer Wirtschaftsraum
f.	folgend
ff.	fortfolgend
Fn.	Fußnote
FS	Festschrift
GDV	Gesamtverband der Deutschen Versicherungswirtschaft
GeschGehG	Gesetz zum Schutz von Geschäftsgeheimnissen
GG	Grundgesetz
GmBHG	Gesetz betreffend die Gesellschaften mit beschränkter Haftung
GP	The Geneva Papers on Risk and Insurance – Issues and Practice (Zeitschrift)
GRCh	Charta der Grundrechte der Europäischen Union
GRUR	Gewerblicher Rechtsschutz und Urheberrecht (Zeitschrift)
GRUR-Prax	Gewerblicher Rechtsschutz und Urheberrecht in der Praxis (Zeitschrift)
GSZ	Zeitschrift für das Gesamte Sicherheitsrecht (Zeitschrift)

HMD	Praxis der Wirtschaftsinformatik (Zeitschrift)
Hrsg.	Herausgeber
ICO	Information Commissioner's Office
i.E.	im Ergebnis
i.H.v.	in Höhe von
i.V.m.	in Verbindung mit
IP	Internet Protocol
IT	Informationstechnik / informationstechnisch/e
JA	Juristische Arbeitsblätter (Zeitschrift)
Jura	Juristische Ausbildung (Zeitschrift)
JuS	Juristische Schulung (Zeitschrift)
JZ	Juristenzeitung (Zeitschrift)
Kap.	Kapitel
KMU	Kleine und mittlere Unternehmen
krit.	kritisch
KRITIS	Kritische Infrastrukturen
KWG	Kreditwesengesetz
LG	Landgericht
m.w.Nw.	mit weiteren Nachweisen
Mio.	Millionen
MMR	Multimedia und Recht (Zeitschrift)
Mrd.	Milliarden
NJOZ	Neue Juristische Online Zeitschrift (Zeitschrift)
NJW	Neue Juristische Wochenschrift (Zeitschrift)
NJW-RR	Neure Juristische Wochenschrift Rechtsprechungs-Report (Zeitschrift)
NStZ	Neue Zeitschrift für Strafrecht (Zeitschrift)
NVersZ	Neue Zeitschrift für Versicherung und Recht (Zeitschrift)
NVwZ	Neue Zeitschrift für Verwaltungsrecht (Zeitschrift)
NZA	Neue Zeitschrift für Arbeitsrecht (Zeitschrift)
NZG	Neue Zeitschrift für Gesellschaftsrecht (Zeit schrift)
NZKart	Neue Zeitschrift für Kartellrecht (Zeitschrift)
NZWiSt	Neue Zeitschrift für Wirtschaft-, Steuer- und Unternehmensstrafrecht (Zeitschrift)
OLG	Oberlandesgericht
OWiG	Gesetz über Ordnungswidrigkeiten
PC	Personal Computer
PCI	Payment Card Industry
PCI-DSS	Payment Card Industry Data Security Standard

PHi	Haftpflicht international, Recht und Versicherung (Zeitschrift)
PR	Public Relations
r+s	Recht und Schaden (Zeitschrift)
RG	Reichsgericht
Rn.	Randnummer
Rspr.	Rechtsprechung
S. A.	Société Anonyme
S. E.	Societas Europaea
S.	Seite/Satz
sh.	siehe
sog.	sogenannte/r
SpV	Spektrum für Versicherungsrecht (Zeitschrift)
StGB	Strafgesetzbuch
StV	Strafverteidiger (Zeitschrift)
TKG	Telekommunikationsgesetz
TTDSG	Telekommunikation-Telemedien-Datenschutz-Gesetz
u.a.	und andere
Urt. v.	Urteil vom
US	United States
USA	United States of America / Vereinigte Staaten von Amerika
USD	US-Dollar
v.	von / versus
VAG	Gesetz über die Beaufsichtigung der Versicherungsunternehmen
VersPrax	Die Versicherungspraxis (Zeitschrift)
VersR	Versicherungsrecht (Zeitschrift)
vgl.	vergleiche
VN	Versicherungsnehmer
Vorbem.	Vorbemerkung
VPN	Virtual Private Network
VR	Versicherer
VuR	Verbraucher und Recht (Zeitschrift)
VVG	Versicherungsvertragsgesetz
VVO	Versicherungsverband Österreich
VW	Versicherungswirtschaft (Zeitschrift)
WpHG	Wertpapierhandelsgesetz
z.B.	zum Beispiel
ZaöRV	Zeitschrift für ausländisches öffentliches Recht und Völkerrecht (Zeitschrift)
ZD	Zeitschrift für Datenschutz (Zeitschrift)

ZEuP	Zeitschrift für europäisches Privatrecht (Zeitschrift)
ZHR	Zeitschrift für das gesamte Handelsrecht und Wirtschaftsrecht (Zeitschrift)
Ziff.	Ziffer
ZIP	Zeitschrift für Wirtschaftsrecht (Zeitschrift)
ZJS	Zeitschrift für das Juristische Studium (Zeitschrift)
ZRP	Zeitschrift für Rechtspolitik (Zeitschrift)
zust.	zustimmend/er
ZVersWiss	Zeitschrift für die gesamte Versicherungswissenschaft (Zeitschrift)

Im Übrigen wird verwiesen auf das Abkürzungsverzeichnis bei Kirchner (Begr.), Abkürzungsverzeichnis der Rechtssprache, 10. Auflage, Berlin 2021.

Kapitel 1: Einführung

A) Problemaufriss und Gegenstand der Arbeit

„Die Bedrohung im Cyberraum ist so hoch wie nie zuvor" – mit diesen alarmierenden Worten resümiert das Bundesamt für Sicherheit in der Informationstechnik (BSI) in seinem Bericht zur Lage der IT-Sicherheit in Deutschland 2023 die aktuelle Cyberrisikolage für deutsche Unternehmen.[1] Ähnliches lässt das Allianz Risk-Barometer aus dem Jahr 2024 verlautbaren, das sog. „cyber incidents" als das weltweit bedeutsamste Geschäftsrisiko für Unternehmen identifiziert.[2] Belegt und unterstrichen werden diese Befunde unter anderem durch den jährlichen Wirtschaftsschutzbericht des Branchenverbandes der deutschen Informations- und Telekommunikationsbranche (Bitkom e.V.). Dieser beziffert die gesamtwirtschaftlichen Schäden, die der deutschen Wirtschaft allein im Jahr 2023 durch cyberkriminelle Aktivitäten entstanden sind, auf knapp 206 Mrd. EUR.[3] Zugleich gaben in einer für den Wirtschaftsschutzbericht durchgeführten repräsentativen Umfrage unter 1000 deutschen Unternehmen mit mindestens zehn Beschäftigten und einem Jahresumsatz von 1 Mio. EUR über 80 % der befragten Unternehmen an, dass sie eine weitere Zunahme von Cyberangriffen auf ihr Unternehmen erwarten; 52 % sehen sich durch derartige Attacken sogar in ihrer Existenz bedroht.[4] In diesem Zusammenhang ist außerdem der Cyber-Readiness-Report des Spezialversicherers *Hiscox S. A.* aus dem Jahr 2023 von Signifikanz, der anhand statistischer Erhebungen darlegt, dass jedes Jahr mehr als die Hälfte der Unternehmen in Deutschland mindestens einmal das Ziel einer Cyberattacke werden.[5]

Trotz all dieser Warnzeichen sind insbesondere kleine und mittlere Unternehmen (KMU) sowie Kleinstunternehmen oftmals weder ausreichend über die allgemeine Bedrohungslage noch ihr individuelles Risikoprofil informiert.[6] Sofern dennoch ein entsprechendes Problembewusstsein besteht, scheitert ein adäquater Schutz vor der Verwirklichung von Cyberrisiken nicht selten daran, dass diese Unternehmen entweder kostspielige Investitionen in

1 BSI, Die Lage der IT-Sicherheit in Deutschland (2023), S. 11.
2 Allianz, Risk Barometer (2024), S. 4, 11 ff.
3 Bitkom, Wirtschaftsschutz (2023), S. 4.
4 Bitkom, Wirtschaftsschutz (2023), S. 12, 14.
5 Hiscox, Cyber Readiness Report (2023), S. 16.
6 BSI, Die Lage der IT-Sicherheit in Deutschland (2023).

ihre IT-Sicherheit scheuen oder nicht das notwendige dedizierte IT-Personal zur Implementierung und Umsetzung der erforderlichen technischen bzw. organisatorischen IT-Sicherheitsvorkehrungen zur Verfügung steht.[7] Es verwundert daher kaum, dass gerade diese Unternehmensgruppe zunehmend in das Visier von cyberkriminellen Akteuren gerät.[8] Diese Entwicklung ist umso problematischer, je deutlicher man sich vor Augen führt, dass gerade kleinere Unternehmen häufig mit der Bewältigung der Folgen eines erfolgreichen Cyberangriffs überfordert sind. So wissen Betroffene im Ereignisfall häufig nicht einmal, an wen sie sich wenden können, um fachlich versierte Hilfe zu erhalten.[9]

Regelmäßig sind es jedoch die wirtschaftlichen Einbußen bzw. Kosten nach einer Cyberattacke, welche die Unternehmen vor erhebliche Herausforderungen stellen. Wird etwa infolge eines Cyberangriffs die Verfügbarkeit von IT-Systemen oder Daten des Unternehmens beeinträchtigt, kann dies langwierige Betriebsstörungen bzw. Betriebsunterbrechungen zur Folge haben. Häufig fallen nach einem Cyberangriff auch Kosten zur Behebung bzw. im Umgang mit einer angriffsbedingten Störung der IT-Systeme und Daten an, insbesondere wenn externe IT-Spezialisten oder sonstige Krisendienstleister hinzugezogen werden müssen. Sofern es sich um einen erpresserischen Cyberangriff handelt, kann zudem die Zahlung von Lösegeldern bzw. Erpressungsforderungen als Kostenposition im Raum stehen. Nicht zu unterschätzen sind außerdem die mittelbaren Umsatzeinbußen nach einer Cyberattacke, die durch den Reputationsverlust des Unternehmens bei Kunden und Geschäftspartnern sowie durch Datendiebstahl entstehen können. Im Falle von Datenschutzverletzungen können Kosten für die Ermittlung und Benachrichtigung von Betroffenen und Behörden sowie für die Zahlung von Datenschutzbußgelder anfallen. Sofern Dritte geschädigt werden, kann sich das Unternehmen auch Kosten zur Anspruchsabwehr bzw. zur Begleichung von berechtigten Schadensersatzansprüchen ausgesetzt sehen.

Das zunehmende Gefahr- und Schadenpotential von Cyberrisken für Unternehmen hat die Versicherungsbranche auf den Plan gerufen. Immer mehr Versicherer bieten in ihren Produktportfolios spezielle Versicherungsprodukte an, die der Absicherung von Schaden- bzw. Kostenszenarien bei der Verwirklichung von unternehmerischen Cyberrisiken dienen. Diese spezifischen Versicherungsprodukte, die im Allgemeinen unter dem Etikett „Cyber(risiko)versicherung“[10] vertrieben und plakativ als die „Feu-

7 BSI, Die Lage der IT-Sicherheit in Deutschland (2023), S. 64 f.
8 BSI, Die Lage der IT-Sicherheit in Deutschland (2023), S. 11, 64; sh. zu dieser Entwicklung auch *Griese*, VW 9/2023, 28 (29); *Lohmann/Breitenstein*, VW 11/2021, 68 (70).
9 BSI, Die Lage der IT-Sicherheit in Deutschland (2023), S. 65.
10 Sh. zum Begriff S. 30.

erversicherungen des 21. Jahrhunderts“ [11] betitelt werden, haben in den letzten Jahren an erheblicher Signifikanz für Unternehmen im Rahmen des versicherungstechnischen Risikotransfers gewonnen. Besonders deutlich wird dieser Bedeutungszuwachs anhand der in den letzten Jahren erwirtschafteten Prämienvolumina. Während die Beitragseinahmen der deutschen Versicherungswirtschaft aus dem Vertrieb von Cyberversicherungen im Jahr 2020 noch ca. 106 Mio. EUR betrugen, waren es im Jahr 2022 bereits knapp 250 Mio. EUR.[12] Auch für die Zukunft wird dem deutschen Cyberversicherungsmarkt ein immenses Wachstumspotential prognostiziert, zumal sich bislang erst ein geringer Teil der deutschen Unternehmen mit adäquatem Cyberversicherungsschutz eingedeckt hat (sh. dazu unten S. 25 f.).

Im diametralen Gegensatz zu dieser rasanten Markterschließung durch die Versicherungswirtschaft steht die noch geringe Praxiserprobung sowie rechtswissenschaftliche Befassung mit diesem neuartigen Versicherungsprodukt. So sind in Deutschland – soweit ersichtlich – erst zwei gerichtliche Entscheidungen in Zusammenhang mit einer Cyberversicherung veröffentlicht worden.[13] Auch die wissenschaftliche Beschäftigung mit dem Thema steht noch am Anfang und hat erst mit Veröffentlichung der Musterbedingungen zur Cyberrisikoversicherung (AVB-Cyber)[14] durch den Gesamtverband der deutschen Versicherungswirtschaft e.V. (GDV) im Jahr 2017 erkennbar zugenommen.

Trotz erster rechtswissenschaftlicher Beiträge und Abhandlungen, die sich mit Rechtsproblemen der AVB-Cyber und Cyberversicherungen im Allgemeinen befassen, sind viele der grundlegenden Fragestellungen und versicherungsrechtlichen Fallstricke noch nicht abschließend geklärt. So besteht etwa mit Blick auf die Bestimmungen zur primären und sekundären Leistungsbeschreibung von Cyberversicherungen noch erhebliches Analysepotential, insbesondere hinsichtlich der Auslegung von cyberspezifischen oder aus anderen Versicherungssparten herrührenden Begrifflichkeiten.

11 Vgl. zu dieser Bezeichnung statt vieler nur *Dammalacks*, VersPrax 3/2023, 9 (10); *Rüskamp/Altschäffel*, VW 12/2021, 64 (64); *Lohmann*, VersPrax 4/2016, 8 (10); *Beckmann/Köhler*, in: FS Herberger (2016), S. 44; *Erichsen*, CCZ 2015, 247 (249); *Flicke*, in: Handelsblatt v. 20.10.2015, „Cyberpolicen sind die Feuerversicherung des 21. Jahrhunderts“, online abrufbar unter https://www.handelsblatt.com/unternehmen/der-feind-in-meiner-firma-cyberpolicen-sind-die-feuerversicherung-des-21-jahrhunderts/12440686.html (zuletzt eingesehen am 1.6.2024); Assekuranz Maklerhaus, Cyberversicherung – die Feuerversicherung des 21. Jahrhunderts, online abrufbar unter https://www.asse.de/news/cyberversicherung-die-feuerversicherung-des-21-jahrhunderts (zuletzt eingesehen am 1.6.2024).

12 GDV, Cyberversicherer kehren in die Gewinnzone zurück – Markt wächst weiter, online abrufbar unter https://www.gdv.de/gdv/medien/medieninformationen/cyberversicherer-kehren-in-die-gewinnzone-zurueck-markt-waechst-weiter--147652 (zuletzt eingesehen am 1.6.2024); sh. näher zur Prämienentwicklung unten S. 29 f.

13 LG Kiel, Urt. v. 23.5.2024 – 5 O 128/21, BeckRS 2024, 11432; LG Tübingen, Urt. v. 26.5.2023 – 4 O 193/21, NJW-RR 2023, 1194.

14 GDV, GDV stellt Musterbedingungen für Cyberversicherung vor, online abrufbar unter https://www.gdv.de/gdv/medien/medieninformationen/gdv-stellt-musterbedingungen-fuer-cyberversicherung-vor-8270 (zuletzt eingesehen am 1.6.2024).

Auch erscheint bis dato nicht hinreichend untersucht, ob einzelne Bestimmungen einer AGB-rechtlichen Kontrolle standhalten oder wie verschiedene, aus unterschiedlichen Versicherungssparten übernommene Bestimmungen im Rahmen der Cyberversicherung zusammenwirken. Darüber hinaus haben auch die gesetzlichen und vertraglich fixierten Obliegenheiten des Versicherungsnehmers trotz ihrer enormen praktischen Bedeutung für den Versicherungsschutz bislang kaum ausreichende wissenschaftliche Beachtung erfahren.

Angesichts des bestehenden Analysestandes will die vorliegende Arbeit mehr Klarheit in das nur fragmentarisch erforschte Themengebiet der Cyberversicherung bringen. Um dies zu bewerkstelligen, werden im Rahmen der nachfolgenden Untersuchung die Musterbedingungen des GDV zur Cyberrisikoversicherung (AVB-Cyber) aus dem Jahr 2017 aus rechtlicher und praktischer Sicht eingehend analysiert. Die Anknüpfung der Untersuchung an die unverbindlichen Musterbedingungen des GDV ist insbesondere deshalb sinnvoll und zielführend, weil sich das Deckungsangebot der AVB-Cyber an die besonders gefährdete Zielgruppe der KMU richtet (sh. dazu unten S. 29) und das Musterbedingungswerk zugleich eine potentielle Vorlage für die Bedingungswerke anderer Versicherungsunternehmen bildet. Um das Analysebild zu vervollständigen, werden zudem divergierende Bedingungswerke von deutschen Cyberversicherern in die Betrachtung mit einbezogen (sh. dazu unten S. 30). In inhaltlicher Hinsicht fokussiert sich die Untersuchung auf eine tiefgehende rechtliche und praktische Analyse der unmittelbar deckungsrelevanten Bestimmungen, namentlich auf die Regelungen zur primären und sekundären Leistungsbeschreibung sowie zu den Obliegenheiten. Sofern die Untersuchung ergeben sollte, dass die AVB-Cyber defizitäre Bestimmungen enthalten oder systemische Konflikte innerhalb des Musterbedingungswerks bestehen, werden außerdem alternative Gestaltungsvorschläge unter Berücksichtigung marktüblicher Standards unterbreitet.

Lediglich mittelbar deckungsrelevante Bestimmungen und Fragestellungen, wie etwa die Anwendung von Vorrangigkeits- bzw. Subsidiaritätsklauseln bei Deckungsüberschneidungen zu anderen Versicherungen (Stichwort: „Silent Cyber")[15] oder die Regelungen zum Übergang von

15 Zu Deckungsüberschneidungen zu anderen Versicherungen sh. *Bertsch/Fortmann*, r+s 2021, 549 (549 ff.); *Bertsch/Fortmann*, r+s 2021, 485 (485 ff.); *Bertsch*, S. 37 ff.; *Erichsen*, CCZ 2015, 247 (249 f.); *Thull*, S. 225 ff.; *Lesser*, S. 299 ff.; *Armbrüster*, in: Promok (Hrsg.) Cyberversicherung, S. 40 ff.; *Hirs*, VW 6/2019, 38 (38 f.); *Lehmann*, in: Veith/Gräfe/Lange/Rogler[5] § 24 Rn. 4 ff.; *Haas*, S. 159 ff.; ausf. zu den Rechtsfolgen von Deckungsüberschneidungen und der Bedeutung von Vorrangigkeitsklauseln in der Cyberversicherung *Thull*, S. 288 ff.; *Lesser*, S. 331 ff.; *Schilbach*, VW 8/2020, 90 (90 ff.); *Malek/Schütz*, PHi 2018, 174 (184 f.); *Wirth*, BB 2018, 200 (205 ff.); *Achenbach*, VersR 2017, 1493 (1494 ff.); *Drave*, VersPrax 3/2017, 30 (30 ff.); *Beckmann/Köhler*, in: FS Herberger (2016), S. 47 ff.; spezifisch zu Deckungsüberschneidungen im Bereich der Haftpflichtkomponente *Scheuba*, in: Promok (Hrsg.) Cyberversicherung, S. 99 ff.; sh. näher zum Verhältnis zwischen Kumulregelungen und Vorrangigkeitsklauseln *Torbohm*, VersPrax 3/2023, 3 (5 ff.); *Heidemann/Flagmeier*, S. 102 ff.

Ersatzansprüchen und die damit einhergehende Frage nach Regressansprüchen des Unternehmens gegen Dritte,[16] werden aus der Untersuchung ausgeklammert, weil zu diesen spezifischen Themen bereits umfangreiche rechtswissenschaftliche Abhandlungen existieren.

B) Gang der Untersuchung

Bevor die AVB-Cyber inhaltlich untersucht werden, wird im ersten Kapitel (beginnend ab S. 6) zunächst ein kursorischer Überblick über die aktuelle Cyberrisikolage für Unternehmen gegeben und anschließend die wichtigsten Grundlagen zur Cyberversicherung erläutert.

Das zweite Kapitel (beginnend ab S. 37) ist Ausgangspunkt der inhaltlichen Analyse der Musterbedingungen und befasst sich mit dem Deckungsumfang der AVB-Cyber nach der primären Leistungsbeschreibung. Im Vordergrund steht dabei der Gegenstand der Versicherung im Basis-Baustein sowie die Leistungsbeschreibung der einzelnen Deckungsbausteine. Unter anderem wird an dieser Stelle untersucht, wie der für die AVB-Cyber zentrale Begriff der „Informationssicherheitsverletzung" zu verstehen ist und welche Auswirkungen der Risikoausschluss bei Inanspruchnahme externer Dienstleister auf den Versicherungsschutz des Versicherungsnehmers nimmt. Zudem werden in diesem Kapitel die Bestimmungen zum Eintritt des Versicherungsfalls, die Regelungen zum zeitlichen, räumlichen und personellen Umfang der Deckung, zur Verhaltenszurechnung sowie zur Handhabung von Serienschäden behandelt.

Im dritten Kapitel (beginnend ab S. 163) werden die allgemeinen Risikoausschlüsse der AVB-Cyber analysiert, die den maßgeblichen Teil der sekundären Leistungsbeschreibung darstellen. Konkret wird bspw. die Frage untersucht, wie sich die Ausschlüsse für vorvertragliche Informationssicherheitsverletzungen und Infrastrukturausfälle praktisch und rechtlich auswirken. Zudem wird geprüft, ob politisch-motivierte Cyberangriffe unter einen der Ausschlussgründe für politische Risiken fallen und inwiefern Datenschutzbußgelder sowie die Zahlung von Lösegeldern infolge einer Cybererpressung versichert bzw. versicherbar sind. Abschließend wird untersucht, welche (gesetzlichen) Regelungen zur Begrenzung des subjektiven Risikos bestehen und inwieweit diese im Rahmen der AVB-Cyber anwendbar sind.

Das vierte Kapitel (beginnend ab S. 235) befasst sich mit den gesetzlichen und vertraglichen Obliegenheiten des Versicherungsnehmers. Zunächst

16 Allgemein zu den Regressmöglichkeiten von betroffenen Unternehmen *Mehrbrey/Schreibauer*, MMR 2016, 75; zur Geschäftsführerhaftung sh. *Schilbach/Becker*, r+s 2023, 289 (289 ff.); *Schilbach*, VersPrax 2/2023, 10 (12 f.) – mit Blick auf das Spannungsfeld zur D&O-Versicherung; *Lesser*, S. 142 ff.; *Kiefner/Happ*, BB 2020, 2051 (2057); *Schmidt-Versteyl*, NJW 2019, 1637 (1638 ff.); vgl. ferner zu der Frage, ob eine Pflicht der Geschäftsleitung zum Abschluss einer Cyberversicherung besteht *Beckmann/Köhler*, in: FS Herberger (2016), S. 55 ff.

werden die rechtlichen Fragestellungen im Zusammenhang mit der vorvertraglichen Anzeigepflicht des Versicherungsnehmers sowie den Regelungen zur Gefahrerhöhung betrachtet. Der Schwerpunkt der Analyse liegt auf den vertraglichen Obliegenheiten des Versicherungsnehmers, die dieser vor Eintritt des Versicherungsfalls zu erfüllen hat. Sowohl die entsprechenden Obliegenheiten der Musterbedingungen als auch die Obliegenheitskonzepte der Cyberversicherer werden auf ihren Regelungsgehalt hin untersucht, um die jeweiligen Vor- und Nachteile der unterschiedlichen Obliegenheitskonzepte zu eruieren. Zuletzt wird ein Blick auf die Obliegenheiten des Versicherungsnehmers geworfen, die dieser bei und nach Eintritt des Versicherungsfalls zu erfüllen hat, wobei die Obliegenheit zur Schadenabwehr bzw. Schadenminderung sowie der Aufwendungsersatzanspruch des Versicherungsnehmers für Rettungskosten gegen den Versicherer im Fokus stehen.

Im fünften Kapitel (beginnend ab S. 315) werden die erarbeiteten Ergebnisse in einer konzisen Schlussbetrachtung zusammenfassend gewürdigt.

C) Überblick zur Cyberrisikolage für Unternehmen

I) Begriffsdefinition

Für den Terminus der „Cyberrisiken" hat sich bislang keine einheitliche Begriffsdefinition herausgebildet.[17] In Teilen des Schrifttums werden Cyberrisiken in einem engen Sinne als die Risiken definiert, die sich aufgrund von (un-)beabsichtigten Bedrohungen im oder aus dem Cyberraum heraus ergeben.[18] Unter dem Ausdruck „Cyberraum" wird der virtuelle Raum aller weltweit auf Datenebene vernetzten bzw. vernetzbaren informationstechnischen Systeme (IT-Systeme) [19] einschließlich darauf basierender Kommunikation, Anwendungen, Prozesse und verarbeiteter Informationen verstanden.[20] Nach diesem Verständnis sind Cyberrisiken daher nur solche Risiken, die einen Bezug zu diesem virtuellem Raum aufweisen, wie z.B. digitale Angriffe auf IT-Systeme bzw. elektronische Daten[21] (Cyberangriffe) oder betrügerische Aktivitäten im Internet (Social-Engineering).[22]

17 Sh. zu den unterschiedlichen Definitionen *Zängerle/Schiereck*, HMD 2023, 214 (215 ff.); *Haas*, S. 24 ff.; *Königs*, S. 407 f.

18 *Königs*, S. 407 f.; *Zängerle/Schiereck*, HMD 2023, 214 (215) – m.w.Nw.

19 Nach der Definition des BSI sind IT-Systeme *technische Anlagen, die der Informationsverarbeitung dienen und eine abgeschlossene Funktionseinheit bilden. Typische IT-Systeme sind Server, Clients, Mobiltelefone, Smartphones, Tablets, IoT-Komponenten, Router, Switches und Firewalls*, BSI, IT-Grundschutzkompendium (2023), Kap. Glossar, S. 4.

20 BSI, IT-Grundschutzkompendium (2023), Kap. Glossar, S. 2; BMI, Cyber-Sicherheitsstrategie für Deutschland (2021), S. 133.

21 Sh. zum Begriff unten S. 40 f.

22 Vgl. dazu *Zängerle/Schiereck*, HMD 2023, 214 (215 ff.).

Andere Stimmen im Schrifttum definieren Cyberrisiken hingegen in einem weiten Sinne als die Gesamtheit der operationellen Risiken für Informations- und Technologieressourcen, die sich auf die Vertraulichkeit, Verfügbarkeit oder die Integrität von Daten oder IT-Systemen auswirken können.[23] Nach dieser Definition sind somit nicht nur Bedrohungen aus dem Cyberraum als Cyberrisiken zu klassifizieren, sondern darüber hinaus z.B. auch technische Störungen der IT-Systeme sowie Mitarbeiterfehlverhalten im Umgang mit Daten. Insofern überschneidet sich dieses Begriffsverständnis mit den Informationstechnologie- und Informationssicherheitsrisiken.[24]

Da Cyberversicherungen – wie noch zu zeigen sein wird (sh. dazu unten S. 65 f.) – nicht immer trennscharf zwischen den jeweiligen Risikobereichen differenzieren, legt diese Arbeit das zweitgenannte Begriffsverständnis von Cyberrisiken zu Grunde legt, weil nur so das Leistungsspektrum von Cyberversicherungsverträgen adäquat beurteilt werden kann.

II) Kategorien von Cyberrisiken

1) Cyberangriffe

Wie die angeführten statistischen Erhebungen und repräsentative Umfragen belegen (sh. dazu oben S. 1 f.), sind Cyberangriffe das mit Abstand bedeutsamste Cyberrisiko für Unternehmen.

a) Einschleusen von Schadsoftware

Besonders häufig erfolgen Cyberangriffe durch das Einschleusen von Schadsoftware (sog. Malware) in IT-Systeme von Unternehmen.[25] Unter Schadsoftware sind speziell entwickelte Computerprogramme (z.B. Computerviren, -würmer und -trojaner)[26] zu verstehen, die darauf ausgelegt sind, unerwünschte und ggf. schädliche Funktionen in dem betroffenen IT-System auszuführen.[27] Ein Beispiel für Malware ist etwa der Computerwurm „Stuxnet", der zur Sabotage von industriellen Steuerungsanlagen

23 Vgl. dazu *Biener/Eling/Wirfs*, GP 40/2015, 131 (133); ähnl. auch *Haas*, S. 37 ff.
24 Zu den Begriffen sowie zu Abgrenzungsfragen sh. *Zängerle/Schiereck*, HMD 2023, 214 (224 f.).
25 Sh. dazu *Sohr/Kemmerich*, in: Kipker² Kap. 3 Rn. 170 ff.; Bitkom, Wirtschaftsschutz (2023), S. 13.
26 Begriffserläuterungen bei *Sohr/Kemmerich*, in: Kipker² Kap. 3 Rn. 172 ff.; *Schmid/Pruß*, in: Auer-Reinsdorff/Conrad³ § 3 Rn. 267 ff.
27 *Schmidl*, S. 168; ähnl. auch *Sohr/Kemmerich*, in: Kipker² Kap. 3 Rn. 171; BSI, Die Lage der IT-Sicherheit in Deutschland (2023), S. 12.

entwickelt wurde.[28] Der wichtigste Angriffsvektor, um Malware in das anvisierte IT-System einzuschleusen, sind Sicherheitslücken in Programmen oder Webanwendungen,[29] wobei sog. Zero-Day-Exploits[30] ein besonderes Gefahrpotential innewohnt.[31] So wurde bspw. die sog. Zero-Day-Schwachstelle „CVE-2021-30116" in der Remote Monitoring & Management-Software VSA des US-amerikanischen Softwareherstellers *Kaseya Ltd.* ausgenutzt, um massenhaft Schadsoftware auf die mittels VSA verwalteten Computer zu verteilen.[32] Weitere beliebte Angriffsvektoren von Cyberkriminellen sind das sog. Cross-Site-Scripting[33], die sog. SQL-Injection-Methode[34] oder sog. Drive-by-Exploits[35]. Daneben kann Schadsoftware auch durch böswilliges bzw. unvorsichtiges Mitarbeiterverhalten im Umgang mit Hard- und Software (z.B. unberechtigtes Anschließen eines privaten USB-Sticks, Download eines nicht-vertrauenswürdigen E-Mail-Anhangs) in die IT-Systeme von Unternehmen gelangen.

(1) Ransomware

Die praktisch bedeutsamste Form von Malware ist Verschlüsselungs- und Erpressungssoftware (sog. Ransomware).[36] Mittels dieser können die Daten infizierter IT-Systeme verschlüsselt oder der Zugriff auf das gesamte IT-System gesperrt werden.[37] Für die Wiederfreigabe bzw. Entschlüsselung der Daten verlangen die Angreifer in der Regel die Zahlung eines Lösegeldes, meist in Form von Kryptowährung (bspw. Bitcoin).[38] Allein im Jahr 2022 wurden weltweit knapp 500 Mio. Ransomware-Attacken gemeldet, was einem Anteil von ca. 70 % der weltweit aufgedeckten Cyberangriffe in diesem

28 Süddeutsche Zeitung v. 2.10.2023, Computer-Virus Stuxnet trifft deutsche Industrie, online abrufbar unter https://www.sueddeutsche.de/digital/gefaehrliches-schadprogramm-computer-virus-stuxnet-trifft-deutsche-industrie-1.1007379 (zuletzt eingesehen am 1.6.2024); *Beuth*, in: Spiegel v. 17.6.2020, Die erste Cyberwaffe und ihre Folgen, online abrufbar unter https://www.spiegel.de/netzwelt/web/die-erste-cyberwaffe-und-ihre-folgen-a-a0ed08c9-5080-4ac2-8518-ed69347dc147 (zuletzt eingesehen am 1.6.2024).

29 Vgl. dazu BSI, Die Lage der IT-Sicherheit in Deutschland (2023), S. 12 f.; *Sohr/Kemmerich*, in: Kipker² Kap. 3 Rn. 155.

30 Sh. zum Begriff ENISA, Glossar „Zero Day", online abrufbar unter https://www.enisa.europa.eu/topics/incident-response/glossary/zero-day (zuletzt eingesehen am 1.6.2024).

31 Vgl. hierzu *Brodowski/Schmid/Scholzen/Zoller*, NStZ 2023, 385 (386).

32 Sh. dazu näher BSI, Die Lage der IT-Sicherheit in Deutschland (2022), S. 36.

33 Sh. zum Begriff *Sohr/Kemmerich*, in: Kipker² Kap. 3 Rn. 161 ff.

34 Sh. zum Begriff *Sohr/Kemmerich*, in: Kipker² Kap. 3 Rn. 161 ff.

35 Sh. zum Begriff BSI, Die Lage der IT-Sicherheit in Deutschland (2023), S. 89.

36 Vgl. zur (zunehmenden) Bedeutung von Ransomware-Attacken Sophos, The State of Ransomware (2023), S. 4 ff.; BSI, Die Lage der IT-Sicherheit in Deutschland (2023), S. 14 ff.; BKA, Bundeslagebild Cybercrime (2022), S. 14; BMI, Cybersicherheitsstrategie für Deutschland (2021), S. 14; *Pain*, S. 9 f.; vgl. ferner auch *Sohr/Kemmerich*, in: Kipker² Kap. 3 Rn. 177; *Malek/Zürn*, VersPrax 2/2021, 3 (3 ff.).

37 Vgl. dazu BSI, Die Lage der IT-Sicherheit in Deutschland (2023), S. 14 f.; BSI, Ransomware Bedrohungslage (2022), S. 5 ff.; *Podebrad/Gabel*, in: Gabel/Heinrich/Kiefer Kap. 1 Rn. 9; *Sohr/Kemmerich*, in: Kipker² Kap. 3 Rn. 177.

38 Vgl. BSI, Die Lage der IT-Sicherheit in Deutschland (2023), S. 14; *Podebrad/Gabel*, in: Gabel/Heinrich/Kiefer Kap. 1 Rn. 9; *Sohr/Kemmerich*, in: Kipker² Kap. 3 Rn. 177.

Jahr entspricht.[39] Mediale Aufmerksamkeit haben insbesondere die beiden Ransomware-Attacken „NotPetya" und „WannaCry" aus dem Jahr 2017 erregt, weil durch diese eine Vielzahl von namhaften Unternehmen geschädigt wurden.[40] Statistische Erhebungen in Deutschland belegen jedoch, dass jedes dritte deutsche Unternehmen in der Vergangenheit mindestens einmal einer Ransomware-Attacke zum Opfer fiel.[41] Dieser Befund deckt sich mit den Aussagen des BKA, wonach immer häufiger KMU in den Fokus von Ransomware-Akteuren geraten, obwohl immer seltener – immerhin aber noch in ca. 40 % der Fälle –[42] die geforderten Lösegelder gezahlt werden.[43]

Die praktische Bedeutung von Ransomware-Attacken wird zudem durch die organisatorische Professionalisierung der Täter sowie durch die Entwicklung neuer Geschäftsmodelle (z.B. „Ransomware-as-a-Service"[44]) befördert.[45] Auch scheint das Gefahrpotential von Ransomware-Angriffen in qualitativer Hinsicht zuzunehmen. So erfreut sich unter den Ransomware-Akteuren die sog. Double-Extortion-Methode immer größerer Beliebtheit, bei der die Daten des betroffenen Unternehmens nicht bloß verschlüsselt, sondern zugleich auch exfiltriert werden, um zusätzlichen Druck durch die

39 Statista, Annual number of ransomware attempts worldwide from 2017 to 2022, online abrufbar unter https://www.statista.com/statistics/494947/ransomware-attempts-per-year-worldwide/ (zuletzt eingesehen am 1.6.2024); Statista, Distribution of detected cyberattacks worldwide in 2022, by type, online abrufbar unter https://www.statista.com/statistics/1382266/cyber-attacks-worldwide-by-type/ (zuletzt eingesehen am 1.6.2024).

40 *Hern*, in: The Guardian v. 30.12.2017, WannaCry, Petya, NotPetya: how ransomware hit the big time in 2017, online abrufbar unter https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware (zuletzt eingesehen am 1.6.2024); Spiegel v. 13.5.2017, „WannaCry"-Attacke - Fakten zum globalen Cyberangriff, online abrufbar unter https://www.spiegel.de/netzwelt/web/wannacry-attacke-fakten-zum-globalen-cyberangriff-a-1147523.html (zuletzt eingesehen am 1.6.2024); *Brühl*, in: Süddeutsche Zeitung v. 11.7.2020, Das waren die spektakulärsten Hackerangriffe, online abrufbar unter https://www.sueddeutsche.de/digital/it-sicherheit-das-waren-die-spektakulaersten-hackerangriffe-1.4960052 (zuletzt eingesehen am 1.6.2024).

41 Statista, War Ihr Unternehmen schon einmal von einem Ransomware-Angriff betroffen?, online abrufbar unter https://de.statista.com/statistik/daten/studie/1038985/umfrage/betroffenheit-durch-ransomware-nach-umsatzgroessenklasse-der-unternehmen-in-deutschland/ (zuletzt eingesehen am 1.6.2024).

42 Vgl. dazu die Studie von GetApp, 56 % der betroffenen KMU wurden seit Pandemiebeginn Opfer von Angriffen, online abrufbar unter https://www.getapp.de/blog/2695/umfrage-ransomware-zunahme-von-angriffen (zuletzt eingesehen am 1.6.2024).

43 BKA, Bundeslagebild Cybercrime (2022), S. 15.

44 Sh. zum Begriff BKA, Bundeslagebild Cybercrime (2022), S. 16 – Bei „Ransomware-as-a-Service" vermieten Ransomware-Entwickler den Einsatz ihrer Schadsoftware an sogenannte „Affiliates", die Ransomware-Angriffe durchführen und Anteile des erpressten Lösegelds erhalten; vgl. ferner zur Funktionsweise sowie zu den Gefahren dieses Geschäftsmodells Sophos, The State of Ransomware (2023), S. 4.

45 BSI, Ransomware Bedrohungslage (2022), S. 9 f.; vgl. zur zunehmenden technischen und organisatorischen Professionalisierung von Cyberkriminellen *Wimmer*, VersPrax 2/2021, 11 (11 f.); *Caiazza*, To Maze and Beyond: How the Ransomware Double Extortion Space Has Evolved, online abrufbar unter https://www.rapid7.com/blog/post/2022/07/27/to-maze-and-beyond-how-the-ransomware-double-extortion-space-has-evolved/ (zuletzt eingesehen am 1.6.2024).

Androhung der Veröffentlichung bzw. des Weiterverkaufs der Daten auf die Betroffenen aufzubauen.[46]

(2) Spyware und Advanced-Persistent-Threads

Neben dem Einsatz von Ransomware zur Lösegelderpressung verwenden Cyberkriminelle auch Spionagesoftware (sog. Spyware) zum Zwecke der Wirtschaftsspionage.[47] Cyberwirtschaftsspionage soll angeblich wegen der geringen Entdeckungs- und Nachverfolgungsgefahr vermehrt auch von staatlichen Akteuren in Auftrag gegeben bzw. durchgeführt werden.[48] Im Jahr 2020 wurde bspw. von der Hackergruppe Lazarus, die nach Meinung von IT-Experten vom nordkoreanischen Staat unterstützt wird,[49] der Versuch unternommen, in die IT-Systeme der deutschen Rüstungsunternehmen *Rheinmetall AG* und *Renk Group AG* einzudringen und diese auszuspionieren. Staatliche Cyberwirtschaftsspionage wird zudem in aller Regel professioneller und über einen längeren Zeitraum durchgeführt.[50] Im Fachjargon werden solche Angriffe als sog. Advanced-Persistent-Threads (APT) bezeichnet.[51] Neben großen Organisationen bzw. Unternehmen sind zunehmend auch KMU durch (staatliche) Cyberwirtschaftsspionage bedroht, insbesondere wenn sie in ihrem Marktsegment (z.B. wegen Technologievorsprüngen) eine herausragende Position einnehmen oder geschäftliche Verbindungen zu größeren Unternehmen unterhalten, die ein Sprungbrett für Cyberkriminelle bzgl. weitergehender Angriffsmöglichkeiten bieten.[52]

46 Sh. dazu BSI, Die Lage der IT-Sicherheit in Deutschland (2023), S. 19 ff.; vgl. dazu aus strafrechtlicher Sicht *Brodowski/Schmid/Scholzen/Zoller*, NStZ 2023, 385 (386); *König*, NZWiSt 2023, 167 (167).

47 *Sohr/Kemmerich*, in: Kipker² Kap. 3 Rn. 176; *Podebrad/Gabel*, in: Gabel/Heinrich/Kiefer Kap. 1 Rn 12.

48 Vgl. dazu BfV, Verfassungsschutzbericht (2022), S. 284 ff., 293 ff. – besondere Gefahren gehen für deutsche Unternehmen von der Volksrepublik China und der russischen Föderation aus; vgl. auch BMI, Mehr Angriffe auf Politik, Behörden und Wirtschaft durch Cyber-Spionage, online abrufbar unter https:// www.bmi.bund.de/DE/themen/sicherheit/spionageabwehr-wirtschafts-und-geheimschutz/cyberspionage/cyberspionage-node.html (zuletzt eingesehen am 1.6.2024).

49 Vgl. dazu *Schlitt/Biermann*, in: Zeit online v. 2.2.2023, Nordkorea spioniert offenbar gezielt Forschungsinstitute aus, online abrufbar unter https:// www.zeit.de/digital/2023-02/cyberangriff-nordkorea-forschungseinrichtung-lazarus-group (zuletzt eingesehen am 1.6.2024); *Muth*, in: Süddeutsche Zeitung v. 18.2.2021, USA klagen „beste Bankräuber der Welt" an, online abrufbar unter https://www.sueddeutsche.de/digital/hacker-nordkorea-lazarus-us-justiz-1.5210297 (zuletzt eingesehen am 1.6.2024).

50 Vgl. dazu BfV, Verfassungsschutzbericht (2022), S. 285.

51 Vgl. dazu BSI, Die Lage der IT-Sicherheit in Deutschland (2023), S. 25; vgl. ferner den Überblick zu bekannten APT-Angriffen BfV, Verfassungsschutzbericht (2022), S. 285 ff.

52 BSI, Advanced Persistent Threat, online abrufbar unter https:// www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Gefaehrdungen/APT/aptnode.html (zuletzt eingesehen am 1.6.2024); vgl. auch *Herrmann*, VersPrax 3/2020, 10 (10).

b) (Distributed-)Denial-of-Service-Attacken

Eine andere praxisrelevante Form von Cyberangriffen auf Unternehmen bilden die sog. Denial-of-Service-Attacken (kurz: DoS-Attacken).[53] Bei einer DoS-Attacke wird ein IT-System – in der Regel ein Server – mit so vielen Kontaktanfragen eines anderen IT-Systems überhäuft, dass es wegen der damit einhergehenden Überlastung der Rechenkapazitäten seine eigentliche Aufgabe nicht mehr bewältigen kann und schlimmstenfalls zusammenbricht.[54] DoS-Attacken bei denen, wie praktisch üblich, das Bombardement an Kontaktanfragen nicht von einem einzelnen IT-System ausgeht, sondern zahlreiche IT-Systeme bzw. Bot-Netze[55] an der Attacke beteiligt sind, werden als Distributed-Denial-of-Service-Attacken (kurz: DDoS-Attacken) bezeichnet.[56] Besonders gefährdet von DDoS-Attacken sind Unternehmen, die auf die dauerhafte Verfügbarkeit ihrer IT-Systeme bzw. Online-Dienstleistungen angewiesen sind.[57]

Verdeutlicht wird das Gefährdungspotential dieser Angriffe am Beispiel der DDoS-Attacke auf den US-amerikanischen DNS-Dienstleister *Dyn, Inc.* aus dem Jahr 2016, der einen weitreichenden Ausfall der Online-Präsenz namhafter Unternehmen (z.B. *Amazon.com, Inc.*; *Netflix*, *Inc.* und *Spotify AB*) zur Folge hatte.[58] Statistisch gesehen ist die Frequenz von DDoS-Attacken auf deutsche Unternehmen seit dem Ende der Covid-19-Pandemie im Jahr 2023 zwar leicht zurückgegangen.[59] Dennoch wird die Gefährdungslage für deutsche Unternehmen von den deutschen Sicherheitsbehörden weiterhin

53 Sh. zu technischen Einzelheiten *Sohr/Kemmerich*, in: Kipker[2] Kap. 3 Rn. 181 ff.; *Schmid/Pruß*, in: Auer-Reinsdorff/Conrad[3] § 3 Rn. 271 ff.; sh. zur praktischen Bedeutung dieser Angriffsform BSI, Die Lage der IT-Sicherheit in Deutschland (2023), S. 28 ff.; BKA, Bundeslagebild Cybercrime (2022), S. 19 ff.; Bitkom, Wirtschaftsschutz (2023), S. 13.

54 BSI, DoS- und DDoS-Attacken, online abrufbar unter https:// www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/DoS-Denial-of-Service/dos-denial-of-service_node.html (zuletzt eingesehen am 1.6.2024); vgl. auch *Sohr/Kemmerich*, in: Kipker[2] Kap. 3 Rn. 181; *Schmid/Pruß*, in: Auer-Reinsdorff/Conrad[3] § 3 Rn. 271.

55 Sh. zum Begriff *Schmid/Pruß*, in: Auer-Reinsdorff/Conrad[3] § 3 Rn. 270 ff.; *Sohr/Kemmerich*, in: Kipker[2] Kap. 3 Rn. 183; BSI, Botnetze – Auswirkungen und Schutzmaßnahmen, online abrufbar unter https://www.bsi.bund.de/DE/ Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Botnetze/botnetze_node.html (zuletzt eingesehen am 1.6.2024).

56 BSI, DoS- und DDoS-Attacken, online abrufbar unter https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/DoS-Denial-of-Service/dos-denial-of-service_node.html (zuletzt eingesehen am 1.6.2024); vgl. auch *Sohr/Kemmerich*, in: Kipker[2] Kap. 3 Rn. 181; *Schmid/Pruß*, in: Auer-Reinsdorff/Conrad[3] § 3 Rn. 271.

57 Vgl. hierzu *Podebrad/Gabel*, in: Gabel/Heinrich/Kiefer Kap. 1 Rn. 11– sehen insbesondere Online-Shops und andere Kundenportale als gefährdet an; vgl. auch *Sohr/Kemmerich*, in: Kipker[2] Kap. 3 Rn. 181 ff.

58 *Kühl/Breitegger*, in: Zeit online v. 24.10.2016, Der Angriff, der aus dem Kühlschrank kam, online abrufbar unter https://www.zeit.de/digital/internet/2016-10/ddos-attacke-dyn-internet-der-dinge-us-wahl (zuletzt eingesehen am 1.6.2024).

59 Vgl. Bitkom, Wirtschaftsschutz (2023), S. 13; BKA, Bundeslagebild Cybercrime (2022), S. 19 f.

als bedrohlich eingeschätzt.[60] Denn DDoS-Akteure haben in den letzten Jahren nicht nur noch schlagkräftigere Angriffsstrategien entwickelt, sondern neben bloßen Sabotageakten auch die DDoS-Schutzgelderpressung als neues „Geschäftsmodell" für sich entdeckt.[61] Mit Beginn des Russland-Ukraine-Kriegs[62] ist zudem die Gefahr gestiegen, in das Visier von sog. hacktivistischen[63] DDoS-Akteuren, wie etwa der pro-russischen Gruppierung Killnet, zu geraten.[64]

c) Sonstige Cyberangriffsarten

Neben der Einschleusung von Malware in IT-Systeme und der Durchführung von DDoS-Attacken existieren eine Reihe weiterer Angriffsarten, die von cyberkriminellen Akteuren genutzt werden, um sich Zugang zu IT-Systemen oder Unternehmensdaten zu verschaffen. Ein praxisrelevantes Beispiel stellen sog. Man-in-the-Middle-Angriffe dar, bei denen sich der Angreifer durch technische Hilfsmittel heimlich in die Kommunikation zwischen zwei Kommunikationspartnern einschleust, um sensible Daten abzufangen oder zu manipulieren.[65] Nennenswerte Arten von Cyberangriffen sind außerdem das sog. Spoofing[66] von (IP-)Adressdaten oder das (versuchte) Entschlüsseln von passwortgesicherten Nutzerzugängen mittels sog. Brut-Force-Attacken[67] oder durch den Einsatz von sog. Key-Loggern[68].

60 Vgl. BKA, Bundeslagebild Cybercrime (2022), S. 19 ff.; BSI, Die Lage der IT-Sicherheit in Deutschland (2023), S. 28 ff.

61 Sh. dazu näher BSI, Die Lage der IT-Sicherheit in Deutschland (2023), S. 28.

62 Die Bezeichnung „Russland-Ukraine-Krieg" bezieht sich auf die Kriegssituation zwischen der russischen Föderation und der Ukraine seit dem 24. Februar 2022.

63 „Hacktivismus" vereint die Konzepte des Hackings und des Aktivismus und beschreibt ideologisch, sozial und/oder politisch motivierte Aktionen unter Nutzung von Hackingtools, sh. zu dieser Definition BKA, Bundeslagebild Cybercrime (2022), S. 20.

64 Vgl. dazu BKA, Bundeslagebild Cybercrime (2022), S. 19; BSI, Cybersicherheitslage im Zusammenhang mit dem russischen Angriff auf die Ukraine, online abrufbar unter https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Ukraine-Krise/ukraine-krise_node.html (zuletzt eingesehen am 1.6.2024); vgl. auch *Lehmann*, in: Spiegel v. 4.4.2023, Prorussische Hackergruppe greift Ukraine-Plattform der Bundesregierung an, online abrufbar unter https://www.spiegel.de/politik/deutschland/attacke-auf-entwicklungsministerium-prorussische-hackergruppe-greift-ukraine-plattform-an-a-64b0e4de-183b-47c7-bd95-05b31202c18f (zuletzt eingesehen am 1.6.2024).

65 Vgl. zur praktischen Bedeutung dieser Angriffsart Bitkom, Wirtschaftsschutz (2023), S. 13; sh. näher zum Begriff sowie zur Funktionsweise *Ernst*, NJW 2003, 3233 (3234); *Pohlmann*, S. 46; *Graf*, in: MüKo-StGB[4] Bd. IV § 202a StGB Rn. 94 – nennt als Beispiel für ein solches technisches Hilfsmittel den sog. ISMI-Catcher, mithilfe dessen Telefongespräche von Mobiltelefonen abgehört werden können.

66 Sh. dazu näher *Deusch/Eggendorfer*, in: Taeger/Pohle (Stand: 38. El. 2023) Ziff. 50.1 Rn. 37 ff.

67 Sh. zum Begriff und zur Funktionsweise BSI, Die Lage der IT-Sicherheit in Deutschland (2023), S. 88.

68 Sh. zum Begriff und zur Funktionsweise *Ernst*, NJW 2003, 3233 (3234).

2) Social-Engineering

Neben Cyberangriffen stellt die soziale Beeinflussung und Manipulation von Unternehmensmitarbeitern (sog. Social-Engineering[69]) ein weiteres bedeutendes Cyberrisiko für Unternehmen dar.[70]

a) Phishing

Die mit Abstand wichtigste Form des Social-Engineerings ist das sog. Phishing.[71] Bei diesem versuchen die Angreifer sich mittels gefälschter E-Mails, Kurznachrichten oder Webseiten, die den Eindruck der Echtheit vermitteln sollen, als vertrauenswürdige Kommunikationspartner auszugeben um das betroffene Gegenüber zur Preisgabe von vertraulichen Daten oder Informationen (z.B. Passwörter oder Unternehmensinterna) zu bewegen.[72] Wie bedrohlich Phishing-Angriffe für Unternehmen sind, wird anhand einer Bitkom-Studie aus dem Jahr 2023 deutlich: Über 30 % der 1000 befragten Unternehmen gaben an, dass 25 % der IT-Angriffe der letzten zwölf Monate, die zu einem Schaden geführt haben, auf Phishing zurückzuführen waren.[73] Neben den unmittelbaren Schäden, die dem betroffenen Unternehmen durch erfolgreiche Phishing-Angriffe entstehen können (z.B. Datenverlust oder -veröffentlichung, kompromittierte Nutzerkonten etc.), stellt Phishing auch einen äußerst beliebten Angriffsvektor zur Vornahme weiterführender Cyberangriffe (z.B. Einschleusung von Schadsoftware, Vorbereitung einer DDoS-Attacke) dar.[74]

b) Fake-President-Masche

Eine andere beliebte Methode des Social Engineerings ist die sog. Fake-President-Masche, die teilweise auch als „CEO-Fraud" bezeichnet wird.[75] Bei dieser Variante gibt sich der Täter gegenüber einem Mitarbeiter der Finanzabteilung als Geschäftsführer bzw. Mitglied der Unternehmensführung aus und fordert diesen dazu auf, eine Geldüberweisung des Unternehmens

69 Sh. zum Begriff BSI, IT-Grundschutzkompendium (2023), Kap. G – Elementare Gefährdungen, S. 42 – „Social-Engineering" umfasst alle Vorgehensweisen und Methoden, die menschliche bzw. soziale Eigenschaften wie Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autoritäten ausnutzen, um unberechtigten Zugang zu Informationen oder IT-Systemen zu erlangen.

70 Vgl. dazu *Sohr/Kemmerich*, in: Kipker[2] Kap. 3 Rn. 178 ff.; BSI, Die Lage der IT-Sicherheit in Deutschland (2023), S. 13, 42 ff.

71 Vgl. zur praktischen Bedeutung BSI, Die Lage der IT-Sicherheit in Deutschland (2023), S. 30 ff.; BKA, Bundeslagebild Cybercrime (2022), S. 10 ff.; Bitkom, Wirtschaftsschutz (2023), S. 13; vgl. ferner auch *Sohr/Kemmerich*, in: Kipker[2] Kap. 3 Rn. 178; *Schmid/Pruß*, in: Auer-Reinsdorff/Conrad[3] § 3 Rn. 274.

72 Sh. dazu näher *Schmid/Pruß*, in: Auer-Reinsdorff/Conrad[3] § 3 Rn. 274; *Grimm/Weidner*, in: Hornung/Schallbruch § 2 Rn. 71.

73 Bitkom, Wirtschaftsschutz (2023), S. 13.

74 Sh. dazu BSI, Die Lage der IT-Sicherheit in Deutschland (2023), S. 30 ff.; BKA, Bundeslagebild Cybercrime (2022), S. 10.

75 Vgl. dazu *Podebrad/Gabel*, in: Gabel/Heinrich/Kiefer Kap. 1 Rn. 13.

auf ein (ausländisches) Bankkonto zu veranlassen.[76] Die Kontaktaufnahme zu dem Mitarbeiter erfolgt in der Regel über gehackte E-Mail-Accounts der Geschäftsführung oder über täuschend echt aussehende Fake-E-Mail-Adressen. Zwar führen entsprechende Betrugsversuche, was die geringe Zahl an bekannt gewordenen Schadensfällen nahelegt,[77] anscheinend nur selten zum Erfolg. Gelingt die Täuschung, sind die wirtschaftlichen Schäden für die betroffenen Unternehmen jedoch meist enorm. Im Jahr 2016 hatte bspw. der deutsche Automobilzulieferer *Leoni AG* infolge einer derartigen Betrugsmasche einen Vermögensabfluss in Höhe von 40 Mio. EUR zu verzeichnen,[78] das österreichische Luftfahrttechnikunternehmen *FACC AG* im Jahr zuvor einen Schaden von mehr als 50 Mio. EUR.[79]

3) Sonstige Informationstechnologie- und Informationssicherheitsrisiken

Ferner sind Unternehmen durch sonstige Informationstechnologie- und Informationssicherheitsrisiken bedroht. So können bspw. hohe Schäden dadurch entstehen, dass betriebsnotwendige IT-Systeme infolge höherer Gewalt (z.B. Naturkatastrophen, Unterbrechung der Strom- oder Internetversorgung) ausfallen oder aufgrund technischer Störungen oder der Falschbedienung durch einen Mitarbeiter nicht einsatzfähig sind. Denkbar sind außerdem Schadenszenarien, die aus physischen Angriffen auf IT-Systeme oder Daten (z.B. Zerstörung von Servern, Diebstahl von Datenträgern) resultieren.[80] Auch schuldhafte Verstöße gegen datenschutzrechtliche Bestimmungen (z.B. versehentliche Veröffentlichung von personenbezogenen Daten durch Unternehmensmitarbeiter) können beträchtliche Kosten und Schäden für das Unternehmen zur Folge haben.

III) Verstärkende Faktoren

Die Gefährdungslage für Unternehmen im Bereich der Cyberrisiken wird durch eine Reihe weiterer Faktoren, Erscheinungen und Entwicklungen nachteilhaft beeinflusst. Ein besonders wichtiger Risikomultiplikator ist die stetig anwachsende Nutzung von moderner Kommunikations- und Infor-

76 Sh. zum Begriff und zur Funktionsweise BSI, Die Lage der IT-Sicherheit in Deutschland (2023), S. 88.
77 Vgl. dazu Bitkom, Wirtschaftsschutz (2023), S. 13.
78 Vgl. dazu Spiegel v. 16.8.2016, Betrüger prellen Leoni um 40 Millionen Euro, online abrufbar unter https://www.spiegel.de/wirtschaft/unternehmen/leoni-betrueger-bringen-autozulieferer-um-40-millionen-euro-a-1107981.html (zuletzt eingesehen am 1.6.2024).
79 Vgl. dazu Salzburger Nachrichten v. 25.5.2016, FACC schreibt millionenschwere Verluste, CEO muss gehen, online abrufbar unter https:// www.sn.at/wirtschaft/oesterreich/facc-schreibt-millionenschwere-verluste-ceo-muss-gehen-1426753 (zuletzt eingesehen am 1.6.2024).
80 Vgl. dazu Bitkom, Wirtschaftsschutz (2023), S. 8.

mationstechnologie.[81] Denn die fortschreitende Digitalisierung von Betriebsabläufen und Geschäftsprozessen, die in Deutschland unter anderem unter den Schlagworten „Industrie 4.0"[82] und „Big Data"[83] vorangetrieben wird, vergrößert nicht nur die Angriffsfläche für fast alle Formen von Cyberrisiken, sondern zieht auch immer weitreichendere Abhängigkeiten bei Unternehmen hinsichtlich der Verfügbarkeit von Daten sowie des reibungslosen Funktionierens von IT-Systemen nach sich.[84] Risikoverschärfend wirkt sich insoweit auch der Einsatz von gleichartigen Betriebssystemen oder Programmen sowie die zunehmende Vernetzung von IT-Systemen, insbesondere mit Blick auf Interdependenzen sowie die kaskadenartige Verbreitung von Malware aus.[85]

Des Weiteren haben technologische bzw. organisatorische Entwicklungen der letzten Jahre zu einem Aufwuchs von neuen Angriffsvektoren geführt. Ein Beispiel hierfür ist der vermehrte Einsatz internetfähiger Geräte, wie z.B. mobile Endgeräte,[86] Netzwerkdrucker[87] oder sonstige Geräte im „Internet-der-Dinge"[88]. Weitere Beispiele sind die zunehmende Inanspruchnahme von Web-Applikationen,[89] die Nutzung von IT-Dienstleistungen im Rahmen des sog. Cloud Computing[90] sowie die Veränderungen in der internen Arbeits-

81 Vgl. dazu Statistisches Bundesamt, IKT-Nutzung in Unternehmen (2022) – Computernutzung, Internetzugang und weiteren Kennzahlen im Zeitvergleich, online abrufbar unter https://www.destatis.de/DE/Themen/Branchen-Unternehmen/Unternehmen/IKT-in-Unternehmen-IKT-Branche/Tabellen/iktu-01-computernutzung-internetzugang.html (zuletzt eingesehen am 1.6.2024).

82 „Industrie 4.0" bezeichnet die intelligente Vernetzung von Maschinen und Abläufen in der Industrie mit Hilfe von Informations- und Kommunikationstechnologie; sh. zu dieser Definition Plattform Industrie 4.0, Was ist Industrie 4.0?, online abrufbar unter https://www.plattform-i40.de/IP/Navigation/DE/Industrie40/WasIndustrie40/was-ist-industrie-40.html (zuletzt eingesehen am 1.6.2024).

83 „Big Data" ist ein Schlagwort, das einerseits große Mengen von Daten bezeichnet (sog. „Massendaten"), andererseits aber auch moderne, digitale Verfahren und Technologien, mit deren Hilfe Massendaten nutzbringend ausgewertet werden können, sh. zu dieser Definition *Sarre/Pruß*, in: Auer-Reinsdorff/Conrad[3] § 2 Rn. 186.

84 Vgl. dazu *Stanczyk*, VW 9/2018, 20.

85 Vgl. dazu *Haas*, S. 31 f.

86 Zu potentiellen Bedrohungen gegen mobile Endgeräte sh. *Sohr/Kemmerich*, in: Kipker[2] Kap. 3 Rn. 184 ff.

87 Zu potentiellen Bedrohungen gegen Netzwerkdrucker sh. *Dickmann*, r+s 2020, 131.

88 Unter „Internet der Dinge"/„Internet of Things" versteht man informations- und sensortechnisch aufgerüstete Gegenstände, die aus der physischen und virtuellen Welt Daten erfassen, verarbeiten und speichern und miteinander vernetzt sind, sh. zu dieser Definition BSI, Die Lage der IT-Sicherheit in Deutschland (2022), S. 90; vgl. zu Beispielen, Gefahrpotentialen und technischen Einzelheiten *Sohr/Kemmerich*, in: Kipker[2] Kap. 3 Rn. 232 ff.; *Schmid/Pruß*, in: Auer-Reinsdorff/Conrad[3] § 3 Rn. 431 ff.; *Haas*, S. 117 ff.

89 Sh. zu dieser Gefahrenquelle *Herrmann*, VersPrax 3/2020, 10 (11).

90 „Cloud Computing" bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Die Spannbreite der im Rahmen von Cloud Computing angebotenen Dienstleistungen umfasst das komplette Spektrum der Informationstechnik und beinhaltet unter anderem Infrastruktur (z. B. Rechenleistung, Speicherplatz), Plattformen und Software, sh. zu dieser Definition BSI, Die Lage der IT-Sicherheit in Deutschland (2023), S. 89; vgl. zu Beispielen, Gefahrpotentialen und technischen Einzelheiten *Pruß*, in: Auer-Reinsdorff/Conrad[3] § 3 Rn. 322 ff.; *Völker/Schnatz/Breyer*, MMR 2022, 427; *Haas*, S. 75 ff.

organisation von Unternehmen, wie z.B. die vermehrte Wahrnehmung von Remote-Arbeitsmöglichkeiten aus dem „Home-Office" oder die Nutzung privater Geräte zu beruflichen Zwecken (sog. bring-your-own-device)[91].

Die Gefahrenlage für Unternehmen spitzt sich außerdem durch den Umstand zu, dass Cyberangriffe immer häufiger aus dem Bereich der organisierten Kriminalität herrühren,[92] was sich in professionelleren Angriffsmustern und der Entwicklung neuer Geschäftsmodelle (z.B. „Cybercrime-as-a-Service"[93]) niederschlägt.[94] Darüber hinaus wird die Bedrohungslage für Unternehmen im Moment zusätzlich durch den Russland-Ukraine-Krieg befördert, in dessen Rahmen die Sicherheitsbehörden in Deutschland eine vermehrte Zahl von cyberkriminellen Aktivitäten von sog. Hacktivisten[95] verzeichnen.[96]

IV) Schadenspositionen

Um das Bild zur Cyberrisikolage für Unternehmen zu vervollständigen, sind die wichtigsten Schadenspositionen für Unternehmen bei der Verwirklichung eines Cyberrisikos in den Blick zu nehmen.

1) Eigenschäden

Ein praktisch wie wirtschaftlich äußerst bedeutsames Schadensrisiko für Unternehmen stellen Ertragsausfälle infolge von Betriebsunterbrechungen dar, die auf den Ausfall bzw. die Störung von IT-Systemen oder die (vorübergehende) Nichtverfügbarkeit von Daten zurückzuführen sind.[97] Neben dem reinen Unterbrechungsschaden fallen in Fällen dieser Art regelmäßig

91 Vgl. zu Beispielen, Gefahrpotentialen und technischen Einzelheiten *Grieger*, MMR 2023, 168 (168 ff.); *Von dem Busche*, in: Kipker² Kap. 6 Rn. 105 ff.; *Blunk/Reimers*, in: Kipker² Kap. 23 Rn. 20 ff.

92 Vgl. dazu Bitkom, Wirtschaftsschutz (2023), S. 7.

93 „Cybercrime-as-a-Service" beschreibt einen Phänomenbereich des Cybercrime, bei dem Straftaten von Cyber-Kriminellen auftragsorientiert begangen bzw. dienstleistungsorientiert ermöglicht werden; sh. zu dieser Definition BSI, Die Lage der IT-Sicherheit in Deutschland (2023), S. 89; sh. zur spezifischen Variante „Ransomware-as-a-Service" oben S. 8 ff.

94 Vgl. dazu BKA, Bundeslagebild Cybercrime (2022), S. 7 ff.

95 „Hacktivismus" vereint die Konzepte des Hackings und des Aktivismus und beschreibt ideologisch, sozial und/oder politisch motivierte Aktionen unter Nutzung von Hackingtools, sh. zu dieser Definition BKA, Bundeslagebild Cybercrime (2022), S. 20.

96 Vgl. dazu BSI, Cybersicherheitslage im Zusammenhang mit dem russischen Angriff auf die Ukraine, online abrufbar unter https://www.bsi.bund.de/DE/ Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Ukraine-Krise/ukraine-krise_node.html (zuletzt eingesehen am 1.6.2024); BKA, Bundeslagebild Cybercrime (2022), S. 20 ff.

97 Vgl. dazu Bitkom, Wirtschaftsschutz (2023), S. 4 – in Bezug auf Cyberkriminalität; vgl. ferner auch *Mühlmann-Burger*, Betriebsunterbrechungen durch Cybereereignisse, online abrufbar unter https://www.munichre.com/de/insights/cyber/business-interruptions-due-to-cyber-events.html (zuletzt eingesehen am 1.6.2024); *Hessel/Callewaert/Klose*, MMR 2023, 471 (472); für ein praktisches Beispiel sh. LG Tübingen, Urt. v. 26.5.2023 – 4 O 193/21, NJW-RR 2023, 1194 – im konkreten Fall ist dem betroffenen Unternehmen durch einen Cyberangriff ein Betriebsunterbrechungsschaden i.H.v. 2.507.809 EUR entstanden.

noch weitere Kosten für die (forensische) Ermittlung und Behebung der Schadensursache (z.B. Wiederherstellung bzw. Austausch von IT-Systemen und Daten, Schließen von Sicherheitslücken und Vornahme von Systemverbesserungen) sowie ggf. für die Beauftragung von spezialisierten Krisen- bzw. IT-Dienstleistern an.[98]

Wenn sensible Unternehmensdaten, wie z.B. Kundendaten, geistiges Eigentum oder sonstige Geschäftsgeheimnisse durch Cyberkriminelle ausgespäht oder entwendet werden, kann dies zudem gravierende Umsatzeinbußen für das betroffene Unternehmen zur Folge haben; die Ursache hierfür kann der Verlust von Wettbewerbsvorteilen, die Konkurrenz durch nachgeahmte Produkte (Produktpiraterie) oder der Image- und Reputationsverlust bei Kunden oder Geschäftspartnern sein.[99] Um einen drohenden Reputationsverlust abzuwenden bzw. zu minimieren oder um eine verloren gegangene Reputation nachträglich wiederherzustellen, ist es aus Unternehmenssicht oftmals opportun, einen spezialisierten PR-Berater für die Krisenkommunikation zu engagieren oder kostspielige PR-Maßnahmen, wie z.B. das Versenden von Kulanz-Gutscheinen an Kunden, in die Wege zu leiten.[100]

Sofern eine Verletzung datenschutzrechtlicher Bestimmungen im Raum steht, ist das Unternehmen zudem mit Prüf- bzw. Erfüllungskosten hinsichtlich datenschutzrechtlicher Melde- und Informationspflichten konfrontiert (z.B. Art. 33, 34 DS-GVO bzw. §§ 65, 66 BDSG).[101] Zusätzlich können Verstöße gegen datenschutzrechtliche Vorschriften auch mit Geldbußen gegen das Unternehmen geahndet werden (z.B. nach Art. 83 Abs. 4 und 5 DS-GVO bzw. § 43 Abs. 1 und 2 BDSG, sh. dazu unten S. 216 ff.).[102]

Im Falle einer Datenverschlüsselung nach einer Ransomware-Attacke können unter Umständen zudem beträchtliche Aufwendungen zur Zahlung von Löse- und Erpressungsgeldern in Frage kommen.[103] Darüber hinaus können dem Unternehmen durch nicht-autorisierte Vermögens- bzw. Zahlungsabflüsse infolge von cyberbetrügerischen Aktivitäten erhebliche Schäden entstehen.[104] Nicht zu vernachlässigen sind zuletzt die Kosten, die

98 Vgl. dazu Bitkom, Wirtschaftsschutz (2023), S. 4; zu Schadensbeispielen sh. *Erichsen*, CCZ 2015, 247 (248).

99 Vgl. dazu Bitkom, Wirtschaftsschutz (2023), S. 4; zu Schadensbeispielen sh. *Erichsen*, CCZ 2015, 247 (248).

100 Vgl. hierzu *Erichsen*, in: Halbach/Rüffer/Schimikowski[4] AVB-Cyber A.2-2 Rn. 13; *Klimke*, in: Prölss/Martin[31] AVB-Cyber A2_2 Rn. 1; *Armbrüster*, S. 624; *Erichsen*, CCZ 2015, 247 (248).

101 Vgl. hierzu *Brams*, ZD 2023, 484 (485 f.); *Schröder/Lantwin*, ZD 2021, 614 (618 f.) – unter Berücksichtigung US-amerikanischer Melde- und Informationspflichten; *Wybitul*, NJW 2020, 2577 (2577).

102 Vgl. dazu *Brams*, ZD 2023, 484 (486 f.); *Wybitul*, NJW 2020, 2577 (2577).

103 Vgl. dazu Sophos, The State of Ransomware (2023), S. 12 ff.; Bitkom, Presseinformation v. 25.10.2023 – Jedes neunte Ransomware-Opfer bezahlt Lösegeld, online abrufbar unter https://www.bitkom.org/Presse/Presseinformation/Ransomware-Opfer-Loesegeld (zuletzt eingesehen am 1.6.2024).

104 Vgl. dazu Bitkom, Wirtschaftsschutz (2023), S. 4; sh. zu weiteren Schadensbeispielen oben S. 13.

im Rahmen anschließender Behörden- und Rechtsstreitigkeiten anfallen können.[105]

2) Drittschäden

Die Verwirklichung eines Cyberrisiko kann bei dem betroffenen Unternehmen auch zu Schäden bei Dritten führen, was zivilrechtliche (Schadensersatz-) Ansprüche nach sich ziehen kann.[106]

a) Vertragliche Haftungsszenarien

Im Rahmen einer vertraglichen Verbindung können schuldrechtliche Erfüllungs(folge)ansprüche nach den §§ 280 ff. BGB gegen das betroffene Unternehmen entstehen, etwa wenn infolge eines Ausfalls der IT-Systeme vertragliche Lieferpflichten gegenüber Vertragspartnern nicht eingehalten werden oder eine Dienstleistung nicht ordnungsgemäß erbracht wird.[107] Hat eine Störung der IT-gesteuerten Produktion zu Fehlern bei den hergestellten Produkten geführt, können betroffene Unternehmen Mängelansprüchen nach den §§ 437 ff. BGB bzw. § 635 ff. BGB ausgesetzt sein.[108]

Neben hauptleistungsbezogenen Erfüllungs(folge)ansprüchen können im Falle einer Risikoverwirklichung auch schuldrechtliche Schadensersatzansprüche wegen Nebenpflichtverletzungen gemäß § 280 Abs. 1 BGB i.V.m. § 241 Abs. 2 BGB in Betracht kommen. Führt etwa ein Cyberangriff zu einem Verlust von vertraulichen Daten eines Geschäftspartners, kann dies als schuldhafte Schutzpflichtverletzung des angegriffenen Unternehmens zu bewerten sein, wenn vorab keine hinreichenden IT-Sicherheitsvorkehrungen zum Schutz der Daten getroffen wurden.[109] Gleiches gilt, wenn ein Dritter durch eine virenversuchte E-Mail geschädigt wird, die durch einen Unternehmensmitarbeiter versendet wurde.[110]

105 Vgl. dazu Bitkom, Wirtschaftsschutz (2023), S. 4.

106 Sh. dazu näher *Voigt*, in: IT-Sicherheitsrecht² Teil H Rn. 544 ff.; *Langen/Stier*, in: Gabel/Heinrich/Kiefer Kap. 10 Rn. 21 ff.; *Bertsch/Fortmann*, r+s 2021, 549 (549 f.); *Mehrbrey/Schreibauer*, MMR 2016, 75 (80 ff.); *Seitz/Thiel*, PHi 2013, 42 (42 ff.); *Thull*, S. 186 ff.; *Lesser*, S. 21 ff.

107 Vgl. dazu *Bertsch/Fortmann*, r+s 2021, 549 (550); *Schmidt-Versteyl*, NJW 2019, 1637 (1638); *Mehrbrey/Schreibauer*, MMR 2016, 75 (80); *Langen/Stier*, in: Gabel/Heinrich/Kiefer Kap. 10 Rn. 22; *Thull*, S. 188; zu Ansprüchen wegen Verzugsschäden vgl. *Lapp*, in: Kipker² Kap. 10 Rn. 35 ff.

108 Vgl. dazu *Bertsch/Fortmann*, r+s 2021, 549 (550); *Mehrbrey/Schreibauer*, MMR 2016, 75 (80); *Langen/Stier*, in: Gabel/Heinrich/Kiefer Kap. 10 Rn. 22; *Thull*, S. 188 f.; vgl. ferner zur Mängelhaftung von Softwareherstellern bei Sicherheitslücken in entwickelter Software *Klett/Gehrmann*, MMR 2022, 435.

109 Vgl. dazu *Bertsch/Fortmann*, r+s 2021, 549 (550); *Strauß/Schweers*, DSRITB 2019, 111 (119 f.); *Langen/Stier*, in: Gabel/Heinrich/Kiefer Kap. 10 Rn. 23; *Thull*, S. 189 f.; zur dogmatischen Herleitung von IT-bezogenen vertraglichen Schutzpflichten sh. *Voigt*, in: IT-Sicherheitsrecht² Teil B Rn. 134 ff.; *Libertus*, MMR 2005, 507 (511); *Koch*, NJW 2004, 801 (806); *Rafsendjani/Bomhard*, in: Hornung/Schallbruch § 9 Rn. 77 ff.; ferner auch *Mehrbrey/Schreibauer*, MMR 2016, 75 (80); *Beucher/Utzerath*, MMR 2013, 362 (367); zur Haftung bei vertraglich vereinbarten IT-Sicherheitspflichten sh. *Kahl*, VersPrax 7/2019, 19 (20).

110 Vgl. hierzu *Libertus*, MMR 2005, 507 (511); *Koch*, NJW 2004, 801 (806).

Ferner drohen Unternehmen empfindliche Vertragsstrafen bzw. Schadensersatzansprüche nach § 10 GeschGehG, wenn gegen vertragliche Datenschutz- bzw. Geheimhaltungsvereinbarungen verstoßen wird.[111] Besonders relevant sind in diesem Zusammenhang sog. PCI-Strafzahlungen, die von Kreditkartenunternehmen gegenüber ihren Vertragspartnern geltend gemacht werden können, wenn diese bei Kreditkartentransaktionen nicht den vereinbarten Payment Card Industry Data Security Standard (PCI-DSS) einhalten.[112]

b) Außervertragliche Haftungsszenarien

(1) Ansprüche gemäß § 823 Abs. 1 BGB

Im Rahmen der außervertraglichen Haftung sind zunächst deliktische Schadensersatzansprüche nach § 823 Abs. 1 BGB zu erwähnen, die in Frage kommen, wenn das betroffene Unternehmen seinen Verkehrssicherungspflichten im Hinblick auf die Gewährleistung von IT-Sicherheit seiner IT-Systeme nicht genügt.[113] Jedoch ist ihm Rahmen der deliktischen Haftung gemäß § 823 Abs. 1 BGB anerkannt, dass das Löschen, Verändern und Sperren von Daten – mangels selbstständiger Sachqualität von Daten (vgl. § 90 BGB) –[114] lediglich eine Eigentumsverletzung am physischen Datenträger darstellt.[115] Eine Inanspruchnahme nach § 823 Abs. 1 BGB unter dem Aspekt der Eigentumsverletzung ist in Fällen dieser Art folglich nur möglich, wenn der betreffende physische Datenträger nicht im Eigentum des schädigenden

111 Vgl. hierzu *Schmidt-Versteyl*, NJW 2019, 1637 (1638); *Thull*, S. 191; allgemein zum Geschäftsgeheimnisschutz bei Cyberangriffen *Dittrich*, NZWiSt 2023, 8; zur Angemessenheit von IT-Sicherheitsvorkehrungen beim Geheimnisschutz sh. OLG Schleswig, Urt. v. 28.4.2022 – 6 U 39/21, GRUR-RR 2022, 404.

112 Sh. dazu näher *Krüger/Peintinger*, in: Martinek/Semmler/Floh[4] § 36 Rn. 351 f.; *Kociok*, in: Auer-Reinsdorff/Conrad[3] § 27 Rn. 50 f.

113 Beispiele bei *Mehrbrey/Schreibauer*, MMR 2016, 75 (81); *Seitz/Thiel*, PHi 2013, 42 (43 ff.); zu Reichweite und Umfang deliktischer IT-Verkehrssicherungspflichten sh. *Andrees*, S. 57 ff.; *Voigt*, in: IT-Sicherheitsrecht[2] Teil H Rn. 578 ff.; *Seitz/Thiel*, PHi 2013, 42 (46 ff.); *Libertus*, MMR 2005, 507 (508 ff.); *Koch*, NJW 2004, 801 (802 ff.); ferner auch OLG München, Urt. v. 15.3.2002 – 21 U 1914/02, MMR 2002, 625 – bzgl. der „Internetverkehrssicherungspflicht" bei Setzen eines Hyperlinks.

114 Vgl. dazu OLG Dresden, Beschl. v. 5.9.2012 – 4 W 961/12, NJW-RR 2013, 27 (28); LG Konstanz, Urt. v. 10.5.1996 – 1 S 292/95, NJW 1996, 2662 – stellen jeweils auf die fehlende Körperlichkeit von magnetisch bzw. elektronisch gespeicherten Daten ab; im versicherungsrechtlichen Kontext *Buchner*, S. 229 ff.

115 *Wagner*, in: MüKo-BGB[9] Bd. VII § 823 BGB Rn. 285 f.; *Hager*, in: Staudinger (Stand: 2017) § 823 BGB Rn. B 60; *Spindler*, in: BeckOGK-BGB (Stand: 1.12.2023) § 823 BGB Rn. 139 ff.; *Voigt*, in: IT-Sicherheitsrecht[2] Teil H Rn. 573; *Langen/Stier*, in: Gabel/Heinrich/Kiefer Kap. 10 Rn. 37; *Zech*, S. 269, 343; *Andrees*, S. 122 ff.; *Riehm*, VersR 2019, 714 (717); *Seitz/Thiel*, PHi 2013, 42 (43 f.); *Bartsch*, CR 2010, 553 (554); *Faustmann*, VuR 2006, 260 (262 f.); *Koch*, NJW 2004, 801 (802 f.); *Meier/Wehlau*, NJW 1998, 1585 (1588).

Unternehmens steht.[116] Eine Verletzung des „Rechts am (Daten-)Besitz"[117] als sonstiges Recht im Sinne von § 823 Abs. 1 BGB scheidet dagegen aus, weil an Daten mangels Sachqualität kein sachenrechtlicher Besitz (vgl. § 854 BGB) bestehen kann.[118] Auch dürften Ansprüche wegen der Verletzung des „Rechts am eingerichteten und ausgeübten Gewerbebetrieb" nur selten in Frage kommen, weil in aller Regel kein betriebsbezogener Eingriff durch das schädigende Unternehmen gegeben sein wird.[119]

Nur am Rande ist in diesem Zusammenhang noch zu bemerken, dass sich die Aktivlegimitation an eigentumsbezogenen Schadensersatzansprüchen gemäß § 823 Abs. 1 BGB infolge der anwachsenden Nutzung von Cloud-Computing-Diensten zunehmend hin zu den jeweiligen Cloud-Computing-Dienstleistern verschiebt.[120] Im Sinne eines besseren (unmittelbaren) Schutzes des „Dateneigentümers" wird daher in Teilen des Schrifttum für die Anerkennung eines „Rechts am eigenen Datenbestand" als sonstiges Recht im Sinne von § 823 Abs. 1 BGB geworben.[121]

Zu haftungsauslösenden Rechtsgutsverletzungen kann es ferner dann kommen, wenn Daten ausgespäht oder kopiert werden. Zwar wird in diesen Fällen regelmäßig das Eigentumsrecht am physischen Datenträger nicht berührt, weil durch das bloße Ausspähen bzw. Kopieren von Daten die bestimmungsgemäße Verwendung des Datenträgers nicht beeinträchtigt wird.[122] Sofern allerdings personenbezogene Daten ausspioniert bzw. entwendet werden, kann das allgemeine Persönlichkeitsrecht des Betroffenen (Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG)[123] in Form seines „Rechts auf in-

116 Vgl. hierzu auch *Bertsch/Fortmann*, r+s 2021, 549 (549 f.); *Lesser*, S. 34 f.; *Thull*, S. 201 – nennt als Beispiel den Fall, dass über eine DDoS-Attacke die IT-Systeme des betroffenen Unternehmens missbraucht werden, um auf Geräte Dritter zuzugreifen und dort hinterlegte Daten zu manipulieren.

117 Allgemein zum Besitzrechtsschutz mittels § 823 Abs. 1 BGB *Spindler*, in: BeckOGK-BGB (Stand: 1.12.2023) § 823 BGB Rn. 173 ff.; *Wagner*, in: MüKo-BGB[9] Bd. VII § 823 BGB Rn. 370 ff.

118 A.A. *Hoeren*, MMR 2019, 5 (7 f.); vgl. ferner zur Untauglichkeit des Besitzschutzes bei fremden Datenträgern *Andrees*, S. 126 ff.; *Riehm*, VersR 2019, 714 (717 f.).

119 So auch *Lesser*, S. 39 ff.; *Voigt*, in: IT-Sicherheitsrecht[2] Teil H Rn. 572 ff.; vgl. ferner auch *Riehm*, VersR 2019, 714 (718); a.A. *Seitz/Thiel*, PHi 2013, 42 (44 f.).

120 Vgl. hierzu *Bertsch/Fortmann*, r+s 2021, 549 (549 f.).

121 Befürwortend *Zech*, S. 386 f.; *Wagner*, in: MüKo-BGB[9] Bd. VII § 823 BGB Rn. 378 ff.; *Spindler*, in: BeckOGK-BGB (Stand: 1.12.2023) § 823 BGB Rn. 141, 186 ff.; *Lapp*, in: Kipker[2] Kap. 10 Rn. 20; *Riehm*, VersR 2019, 714 (720 ff.); *Markendorf*, ZD 2018, 409 (410 ff.); *Hoeren*, MMR 2013, 486 (488 ff.); *Bartsch*, CR 2010, 553 (554 ff.); *Faustmann*, VuR 2006, 260 (262 f.); *Meier/Wehlau*, NJW 1998, 1585 (1588 f.); ein solches Recht ablehnend dagegen *Hager*, in: Staudinger (2017) § 823 BGB Rn. B 192; *Andrees*, S. 142 ff., 167 f.; *Eichberger*, VersR 2019, 709 (710); *Boehm*, ZEuP 2016, 358 (385 f.); *Grützmacher*, CR 2016, 485 (489 ff.); *Härting*, CR 2016, 646 (646 ff.); *Heymann*, CR 2016, 650 (652 ff.); mittelbar auch OLG Dresden, Beschl. v. 5.9.2012 – 4 W 961/12, NJW-RR 2013, 27 (28).

122 Vgl. dazu *Hager*, in: Staudinger (2017) § 823 BGB Rn. B 60; *Seitz/Thiel*, PHi 2013, 42 (44).

123 Vgl. dazu *Wagner*, in: MüKo-BGB[9] Bd. VII § 823 BGB Rn. 466 ff.; *Hager*, in: Staudinger (2017) § 823 BGB Rn. C 15 ff.; *Specht-Riemenschneider*, in: BeckOGK-BGB (Stand: 1.12.2023) § 823 BGB Rn. 1170 ff.

formationelle Selbstbestimmung“[124] oder seines „Rechts auf Vertraulichkeit und Integrität informationstechnischer Systeme“[125] als sonstiges Recht im Sinne von § 823 Abs. 1 BGB verletzt sein.[126]

Ein weiteres deliktisches Haftungsrisiko besteht für Unternehmen bei Schadensereignissen im Zusammenhang mit fehlerhaft hergestellten Produkten.[127] So sind bspw. Schadensersatzansprüche nach § 823 Abs. 1 BGB i.V.m. mit den Grundsätzen der Produzentenhaftung oder bei Sach- und Personenschäden nach § 1 ProdHaftG denkbar, wenn Dritte durch systembedingte Produktfehler geschädigt werden, die durch cyberangriffsbedingte Störungen der IT-gesteuerten Produktion hervorgerufen wurden.[128]

(2) Ansprüche gemäß § 823 Abs. 2 BGB i.V.m. der Verletzung eines Schutzgesetzes

Im Falle von Vermögensschäden können auch deliktische Ansprüche gemäß § 823 Abs. 2 BGB i.V.m. der Verletzung eines Schutzgesetzes bestehen.[129] Dies ist bspw. der Fall, wenn gegen drittschützende datenschutzrechtliche Bestimmungen (z.B. Art. 32 DS-GVO, § 165 TKG) verstoßen wird.[130] Theoretisch kommen auch Ansprüche aufgrund eines Verstoßes gegen die Strafvorschriften der §§ 202a StGB (Ausspähen von Daten), 202b StGB (Abfangen von Daten), 202c StGB (Vorbereiten des Ausspähens und Abfangens von Daten), 202d StGB (Datenhehlerei), 303a StGB (Datenveränderung) und 303b StGB (Computersabotage) in Betracht.[131] Praktisch dürfte deren Anwendung jedoch am regelmäßig fehlenden Schädigungsvorsatz des versicherten Unternehmens scheitern.[132] Bei gesetzlichen Anforderungen an die IT-Sicherheit ist im Einzelfall zu prüfen, ob die jeweiligen Normen über Schutzgesetzqualität verfügen.[133] Hinsichtlich der praxisrelevanten IT-Sicherheitsvorschriften der §§ 8a ff. BSIG (sh. dazu näher unten S. 281 ff.) ist deren Schutzgesetzcharakter

124 Grundlegend zu diesem Recht BVerfG, Urt. v. 1.12.1983 – 1 BvR 209/83, NJW 1984, 419 (421 ff.).

125 Grundlegend zu diesem Recht BVerfG, Urt. v. 27.2.2008 – 1 BvR 370/07, NJW 2008, 822 (824 ff.).

126 Sh. dazu näher *Strauß/Schweers*, DSRITB 2019, 111 (117 ff.); *Bartsch*, CR 2008, 613 (613 ff.).

127 Allgemein zu cyberspezifischen Produkthaftungsrisiken für Unternehmen *Drave*, VersPrax 4/2016, 3 (4 f.).

128 Vgl. hierzu *Voigt*, in: IT-Sicherheitsrecht[2] Teil H Rn. 584 ff.; *Langen/Stier*, in: Gabel/Heinrich/Kiefer Kap. 10 Rn. 37; *Beucher/Utzerath*, MMR 2013, 362 (367); *Thull*, S. 199 f.; zur Frage, ob Software als „bewegliche Sache“ im Sinne des ProdHaftG zu behandeln ist, sh. *Lapp*, in: Kipker[2] Kap. 10 Rn. 70; zur Frage, ob ein Produkt wegen unzureichender IT-Sicherheitsvorkehrungen fehlerhaft ist, sh. *Andrees*, S. 95 ff.

129 Sh. dazu näher *Voigt*, in: IT-Sicherheitsrecht[2] Teil H Rn. 583 ff.

130 *Strauß/Schweers*, DSRITB 2019, 111 (118); *Mehrbrey/Schreibauer*, MMR 2016, 75 (81); *Spindler*, in: BeckOGK-BGB (Stand: 1.12.2023) § 823 BGB Rn. 344 ff.; *Wagner*, in: MüKo-BGB[9] Bd. VII § 823 BGB Rn. 680.

131 Zum Schutzgesetzcharakter dieser Vorschriften sh. *Spindler*, in: BeckOGK-BGB (Stand: 1.12.2023) § 823 BGB Rn. 286 ff.; *Wagner*, in: MüKo-BGB[9] Bd. VII § 823 BGB Rn. 690; *Bertsch/Fortmann*, r+s 2021, 549 (550); *Mehrbrey/Schreibauer*, MMR 2016, 75 (76).

132 Vgl. hierzu *Riehm*, VersR 2019, 714 (718).

133 Sh. dazu näher *Andrees*, S. 73 ff.

zu verneinen, weil diese in erster Linie öffentliche Interessen verfolgen und allenfalls reflexhaft Drittschutz vermitteln.[134]

(3) Ansprüche gemäß Art. 82 Abs. 1 DS-GVO

Über die erörterten deliktischen Haftungstatbestände hinaus, hat – abseits einiger sektorspezifischer Haftungsnormen (z.B. § 32 Abs. 3 EnWG, § 69 Abs. 1 TKG) –[135] vor allem der datenschutzrechtliche Schadensersatzanspruch gemäß Art. 82 Abs. 1 DS-GVO herausragende praktische und wirtschaftliche Bedeutung.[136] Nach dieser Vorschrift hat jede Person, der wegen eines Verstoßes gegen die DS-GVO ein materieller oder immaterieller Schaden entstanden ist, Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.[137] Zu entsprechenden Schadensersatzforderungen von Geschädigten kann es bspw. kommen, wenn im Zuge einer Ransomware-Erpressung personenbezogene Daten exfiltriert und veröffentlicht werden und keine geeigneten technischen und organisatorischen Sicherheitsvorkehrungen zum Schutze personenbezogener Daten nach Art. 32 DS-GVO vorhanden waren oder die Betroffenen nicht (rechtzeitig) gemäß Art. 34 DS-GVO über den Datenschutzverstoß informiert wurden.[138]

Die praktische Haftungsrelevanz von Art. 82 Abs. 1 DS-GVO wird zudem durch gleich mehrere Umstände verschärft. Zum einen wurden die Hürden für die Geltendmachung eines Schadensersatzanspruchs nach Art. 82 Abs. 1 DS-GVO in den letzten Jahren durch die Rechtsprechung des EuGH stetig herabgesenkt, wobei drei Entscheidungen des Gerichtshofs herausstechen: Mit Urteil vom 4. Mai 2023 hat die dritte Kammer des EuGH in dem Vorabentscheidungsverfahren *UI/Österreichische Post AG* entschieden, dass für die Geltendmachung von immateriellen Schäden nach Art. 82 Abs. 1 DS-GVO keine Erheblichkeitsschwelle bestehe.[139] Hieran anschließend entschied dieselbe Kammer mit Urteil vom 14. Dezember 2023 im Vorabentscheidungsverfahren *VB/Natsionalna agentsia za prihodite*, dass im Falle einer durch einen Cyberangriff verursachten Datenpanne ein immaterieller Schadensersatzan-

134 So auch *Andrees*, S. 83; *Spindler*, CR 2016, 297 (306); *Roos*, MMR 2015, 636 (641); *Bussche/Schelinski*, in: Leupold/Wiebe/Glossner[4] Teil 7.1 Rn. 36 ff.

135 Vgl. hierzu *Mehrbrey/Schreibauer*, MMR 2016, 75 (81); *Voigt*, in: IT-Sicherheitsrecht[2] Teil H Rn. 572, Teil G Rn. 423 ff.; *Andrees*, S. 41 ff.

136 *Spittka*, GRUR-Prax 2023, 31 (31 f.); *Paal/Kritzer*, NJW 2022, 2433 (2434); *Wybitul*, NJW 2020, 2577 (2579 f.); *Schmidt-Versteyl*, NJW 2019, 1637 (1638); vgl. ferner die Übersicht zu nationalen gerichtlichen Entscheidungen zu Art. 82 DS-GVO im Zeitraum von 2019 bis 2021 bei *Leibold*, ZD 2022, 18 (19 ff.).

137 Überblick zu einzelnen Haftungsvoraussetzungen, offenen Auslegungsfragen, noch anhängigen Vorabentscheidungsverfahren beim EuGH sowie zur aktuellen Rechtsprechung bei *Spittka*, GRUR-Prax 2023, 31; *Malek/Spittka*, VersPrax 3/2023, 11; *Wybitul/Leibold*, ZD 2022, 207; *Paal*, NJW 2022, 3673; *Hellgardt*, ZEuP 2022, 7; *Strauß/Schweers*, DSRITB 2019, 111; *Geissler/Ströbel*, NJW 2019, 3414.

138 Weitere Beispiele bei *Schröder/Lantwin*, ZD 2021, 614 (614 ff.); *Wybitul*, NJW 2020, 2577 (2577 f.); *Strauß/Schweers*, DSRITB 2019, 111 (111 ff.); zur früheren Rechtslage beim datenschutzrechtlichen Schadensersatzanspruch nach § 7 BDSG a.F. sh. *Mehrbrey/Schreibauer*, MMR 2016, 75 (81).

139 EuGH, Urt. v. 4.5.2023 – C-300/21 (UI/Österreichische Post AG), NJW 2023, 1930 (1931 ff.).

spruch auch auf die (begründete) Angst vor zukünftigem Datenmissbrauch gestützt werden könne.[140] Am 11. April 2024 folgte zuletzt ein Entscheidung der dritten Kammer des EuGH in dem Vorabentscheidungsverfahren *GP/juris*, in dem das Gericht urteilte, dass ein schuldhaftes Mitarbeiterfehlverhalten dem Unternehmen im Rahmen von Art. 82 Abs. 1 DS-GVO selbst dann zuzurechnen sei, wenn der Mitarbeiter entgegen einer innerbetrieblichen Weisung der Unternehmensleitung gehandelt hat.[141]

Zum anderen betreffen haftungsauslösende Datenschutzverstöße oftmals eine Vielzahl von Personen, wodurch der Schadensumfang, auch wenn die individuelle Schadenshöhe bei jedem einzelnen Betroffenen gering ausfällt, in seiner Gesamtheit ein hohes Ausmaß erreichen kann.[142] In prozessualer Hinsicht wird dieses Streuschadenrisiko zudem durch den Trend von einer individuellen Rechtsdurchsetzung hin zu einer gebündelten Geltendmachung von Ansprüchen durch spezialisierte Legal-Tech-Unternehmen im Rahmen von Zessionsmodellen befördert.[143] Hinzu kommt, dass auch die kollektiven Rechtsdurchsetzungsmöglichkeiten für Betroffene fortwährend erweitert werden.[144] So ist in Deutschland zum 13. Oktober 2023 in Umsetzung der unionalen Verbandsklagen-Richtlinie[145] das Verbraucherrechtedurchsetzungsgesetz (VDuG)[146] in Kraft getreten, das neben der aus der ZPO überführten Musterfeststellungsklage (§§ 41 f. VDuG)[147] nunmehr auch eine neuartige Verbandsklage auf Leistung, die sog. Abhilfeklage, für

140 EuGH, Urt. v. 14.12.2023 – C-340/21 (VB/Natsionalna agentsia za prihodite), BeckRS 2023, 35786, Rn. 79 ff.; im konkreten Fall einen immateriellen Schaden aus diesem Grund ablehnend EuGH, Urt. v. 15.1.2024 – C-687/21 (BL/MediaMarktSaturn Hagen-Iserlohn GmbH, vormals Saturn Electro-Handelsgesellschaft mbH Hagen), NZA 2024, 320 (324).

141 EuGH, Urt. v. 11.4.2024 – C-741/21 (GP/juris), GRUR 2024, 784 (787).

142 *Spittka*, GRUR-Prax 2023, 31 (31); *Paal/Kritzer*, NJW 2022, 2433 (2434); *Wybitul*, NJW 2020, 2577 (2581).

143 Sh. dazu näher *Spittka*, GRUR-Prax 2023, 31 (32 f.); *Malek/Spittka*, VersPrax 3/2023, 11 (12 f.); *Paal/Kritzer*, NJW 2022, 2433 (2434); *Wybitul*, NJW 2020, 2577 (2577); zur Frage der Abtretbarkeit derartiger Schadensersatzansprüche sh. *Veeck/Stepanova*, ZD 2023, 317 (317 ff.); *Lühmann/Schumacher/Stegemann*, ZD 2023, 131 (135 f.).

144 Zur Entwicklung der kollektiven Rechtsdurchsetzung im Datenschutzrecht sh. *Lühmann/Schumacher/Stegemann*, ZD 2023, 131; *Paal/Kritzer*, NJW 2022, 2433 (2433 f.); *Ruschemeier*, MMR 2021, 942 (942 ff.).

145 Richtlinie (EU) 2020/1828 des Europäischen Parlaments und des Rates vom 25.11.2020 über Verbandsklagen zum Schutz der Kollektivinteressen der Verbraucher und zur Aufhebung der Richtlinie 2009/22/EG, ABl. L 409 v. 4.12.2020, S. 1 ff.; sh. dazu näher *Schuschnigg*, EuZW 2022, 1043; *Augenhofer*, NJW 2021, 113; *Hakenberg*, NJOZ 2021, 673; *Röthemeyer*, VuR 2021, 43; *Rentsch*, EuZW, 2021, 524.

146 Gesetz zur Umsetzung der Richtlinie (EU) 2020/1828 über Verbandsklagen zum Schutz der Kollektivinteressen der Verbraucher und zur Aufhebung der Richtlinie 2009/22/EG sowie zur Änderung des Kapitalanleger-Musterverfahrensgesetzes (Verbandsklagenrichtlinienumsetzungsgesetz - VRUG), BGBl. I 2023 Nr. 272; sh. dazu näher *Röthemeyer*, VuR 2023, 332; *Janal*, GRUR 2023, 985; *Lühmann/Schumacher/Stegemann*, ZD 2023, 131.

147 Allgemein zur Durchsetzung von datenschutzrechtlichen Schadensersatzansprüchen im Musterfeststellungsverfahren *Geissler/Ströbel*, NJW 2019, 3414 (3416 ff.); *Malek/Schütz*, r+s 2019, 421 (426 f.).

gleichartige Ansprüche von Verbrauchern vorsieht (§§ 14 ff. VDuG).[148] Zuvor hatte bereits die dritte Kammer des EuGH in ihrem Urteil vom 28. April 2022 in dem Vorabentscheidungsverfahren *Meta Platforms Ireland Limited/ Verbraucherzentrale Bundesverband e. V.* die Klagebefugnis von (deutschen) Verbraucherschutzverbänden nach Art. 80 Abs. 2 DS-GVO im Hinblick auf Ansprüche von Betroffenen nach Art. 82 Abs. 1 DS-GVO anerkannt.[149]

D) Grundlagen zur Cyberversicherung

I) Begriffserläuterung

Die BaFin definiert „Cyberversicherungen" als Versicherungen, die gegen die Folgen von Cyberrisiken absichern: 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.[150] Innerhalb dieses Versicherungsart wird zwischen Cyberversicherungsprodukten für Privat- und Gewerbekunden differenziert, weil diese unterschiedliche Risikofelder abdecken.[151] Da sich die vorliegende Arbeit auf gewerbliche Cyberversicherungen fokussiert, beziehen sich die nachfolgenden Ausführungen ausschließlich auf diese Produktkategorie.

II) Ursprung und aktueller Stand der Entwicklung in Deutschland

Cyberversicherungen haben ihren Ursprung in den USA und sind dort seit der Jahrtausendwende ein etabliertes Versicherungsprodukt.[152] In Deutschland wagte sich hingegen – soweit ersichtlich – erst im Jahr 2011 der international tätige Spezialversicherer Hiscox S. A. als erster Anbieter mit einer Cyberpolice auf den Versicherungsmarkt.[153] In den Folgejahren drängten immer mehr Anbieter mit unterschiedlichen und zum Teil neuartigen Po-

148 Sh. näher zu dieser neuen Klagemöglichkeit *Röthemeyer*, VuR 2023, 332 (332 ff.); *Janal*, GRUR 2023, 985 (990 ff.); zu Fragen der Zuständigkeit und Sperrwirkung sh. *Thönissen*, EuZW 2023, 637.

149 EuGH, Urt. v. 28.4.2022 – C-319/20 (Meta Platforms Ireland Limited/Verbraucherzentrale Bundesverband e. V.), NJW 2022, 1740 (1742 f.); zum Verhältnis zwischen der Klagebefugnis nach Art. 80 Abs. 2 DS-GVO und der unionalen Verbandsklage-Richtlinie sh. *Ruschemeier*, MMR 2021, 942 (943 ff.).

150 BaFin, Journal v. 9/2017, S. 5.

151 Sh. näher zur Cyberversicherung für Privatkunden *Fortmann*, S. 33 ff.; *Effler*, S. 10 ff.

152 *Choudry*, S. 1 f.; *Heidemann/Flagmeier*, S. 61; *Schaloske/Wagner*, in: Sassenberg/Faber[2] § 18 Rn. 48; *Dammalacks*, VersPrax 3/2023, 9 (9); sh. näher zur Entstehung und Entwicklung eines dedizierten Cyber-Versicherungsmarktes *Haas*, S. 168.

153 Vgl. hierzu *Behrends/Droberg/Krischer*, VW 2/2021, 40 (40); *Müller/Topsch*, VW 3/3016, 54 (54).

licen auf den deutschen Cyberversicherungsmarkt.[154] Im Laufe des Jahres 2013 hatten z.B. drei internationale (Industrie-)Versicherungsunternehmen, namentlich die Zurich Gruppe Deutschland AG, die Allianz Versicherungs-AG und die HDI Deutschland AG das in Entstehung befindliche Marktumfeld betreten, bevor im Juli 2014 die Württembergische Versicherung AG als erster nationaler Versicherer eine Cyberpolice speziell für KMU in ihr Portfolio aufnahm.[155]

Um der aufkeimenden Bedingungsvielfalt entgegenzuwirken und der Versicherungswirtschaft eine Orientierungshilfe zu bieten, setzte der GDV zu Beginn des Jahres 2016 eine Arbeitsgruppe „Cyber" ein, die mit der Entwicklung von Musterbedingungen betraut wurde.[156] Im April 2017 wurden die Allgemeinen Versicherungsbedingungen für die Cyberrisiko-Versicherung (AVB-Cyber) vom GDV veröffentlicht.[157] Zwar passten einige Versicherungsunternehmen ihre Bedingungswerke den Musterbedingungen an, jedoch blieb die erhoffte marktvereinheitlichende Wirkung der AVB-Cyber größtenteils aus.[158]

Seither wächst der Cyberversicherungsmarkt beständig weiter, was statistische Erhebungen des GDV belegen. Während im Umfragejahr 2020 lediglich 33 der befragten Versicherungsunternehmen über spezielle Cyberversicherungsprodukte verfügten, waren es zwei Jahre später bereits 41 Versicherungsunternehmen.[159] Im gleichen Zeitraum konnte zudem das Gesamtprämienvolumen von 106 Mio. EUR auf 249 Mio. EUR und die Anzahl der laufenden Verträge von knapp 115 Mio. auf fast 280 Mio. gesteigert werden.[160] Obwohl im Vergleichszeitraum die Leistungen der Versicherer von 37 Mio. EUR auf 121 Mio. EUR anstiegen und die Schaden-Kosten-Quote im Jahr 2021

154 Sh. dazu näher *Erichsen/Pawig-Sander/Salm*, VersPrax 3/2017, 3 (3 f.); zur früheren Einordung als Nischenprodukt sh. *Wirth*, BB 2018, 200 (201); zu vertrieblichen Schwierigkeiten in der Anfangsphase sh. *Dammalacks*, VersPrax 3/2023, 9 (9); zur Frühphase der Bedingungsentwicklung sh. *Beckers*, VersPrax 6/2015, 22 (22 f.); *Drave*, VersPrax 7/2014, 128 (128 ff.).

155 Vgl. dazu *Choudry*, S. 2 f.

156 *Erichsen*, in: Rüffer/Halbach/Schimikowski[4] Vorbem. AVB-Cyber Rn. 1.

157 Vgl. dazu GDV, GDV stellt Musterbedingungen für Cyberversicherung vor, online abrufbar unter https://www.gdv.de/gdv/medien/medieninformationen/gdv-stellt-musterbedingungen-fuer-cyberversicherung-vor-8270 (zuletzt eingesehen am 1.6.2024); zu den im Herbst 2018 veröffentlichen österreichischen Musterbedingungen des Verbandes der Versicherungsunternehmen Österreichs (VVO) zur Cyberrisiko-Versicherung (ACB 2018) sh. *Promok*, in: Promok (Hrsg.) Cyberversicherung, S. 54 ff.

158 Vgl. dazu *Heidemann/Flagmeier*, S. 60 ff.; *Erichsen*, in: Rüffer/Halbach/Schimikowski[4] Vorbem. AVB-Cyber Rn. 2; *Pawig-Sander*, VersPrax 1/2019, 3 (3 f.) – erklärt diesen Umstand mit dem erheblichen Anpassungsaufwand für die Versicherer.

159 Vgl. dazu GDV, Cyberversicherer kehren in die Gewinnzone zurück – Markt wächst weiter, online abrufbar unter https://www.gdv.de/gdv/medien/medieninformationen/cyberversicherer-kehren-in-die-gewinnzone-zurueck-markt-waechst-weiter--147652 (zuletzt eingesehen am 1.6.2024).

160 Vgl. zur Beitragssteigerung GDV, Cyberversicherer kehren in die Gewinnzone zurück – Markt wächst weiter, online abrufbar unter https://www.gdv.de/ gdv/medien/medieninformationen/cyberversicherer-kehren-in-die-gewinnzone-zurueck-markt-waechst-weiter--147652 (zuletzt eingesehen am 1.6.2024); vgl. zur Anzahl der laufenden Verträge Finlex, D&O & Cyber Market Report (2023), S. 8.

sogar bei über 123 % lag,[161] wird dem (deutschen) Cyberversicherungsmarkt in Fachkreisen – trotz der verschlechterten (Preis-)Konditionen sowie verringerter Kapazitäten –[162] aufgrund der gesteigerten Bedrohungslage sowie der vergleichsweise geringen Marktdurchdringung weiterhin ein enormes Wachstumspotential prognostiziert.[163] Plausibilisiert wird diese Prognose anhand einer repräsentativen Umfrage aus dem Jahr 2021 zum Bestand bzw. Interesse an Cyberversicherungen im deutschen Mittelstand, bei der über 40 % der befragten Unternehmen angaben, dass sie sich bisher nicht aktiv mit dem Abschluss einer Cyber-Versicherung auseinandergesetzt haben; knapp 20 % der befragten Unternehmen waren zum Umfragezeitpunkt auf der Suche nach einer passenden Versicherungslösung.[164]

III) Ökonomische Versicherbarkeit von Cyberrisiken

Trotz der geschilderten Markt- und Wachstumspotentiale bestehen in Teilen der Versicherungsbranche Vorbehalte hinsichtlich einer risikoadäquaten und zugleich ökonomisch tragfähigen Versicherbarkeit von Cyberrisiken.[165] Dies liegt unter anderem daran, dass die Vertragszeichner und Aktuare vor der Herausforderung stehen, Risiken bewerten bzw. kalkulieren zu müssen, für die es aufgrund der Neuartigkeit an einer ausreichenden Schadenhistorie

161 Vgl. dazu GDV, Cyberversicherer kehren in die Gewinnzone zurück – Markt wächst weiter, online abrufbar unter https://www.gdv.de/gdv/medien/medieninformationen/cyberversicherer-kehren-in-die-gewinnzone-zurueck-markt-waechst-weiter--147652 (zuletzt eingesehen am 1.6.2024); vgl. zum globalen Kontext *Pain*, S. 10 f.

162 Vgl. dazu *Dammalacks*, VersPrax 3/2023, 9 (9 f.); *Kammerer-Galahn/Vinck*, VersPrax 6/2022, 6 (6); *Dammalacks*, VersPrax 5/2022, 3 (3).

163 Vgl. dazu Finlex, D&O & Cyber Market Report (2023), S. 6 ff.; KPMG, Digitalisierung und Cyber (2017), S. 28 ff.; im globalen Kontext Munich Re, Cyber-Versicherung: Risiken und Trends (2023), online abrufbar unter https:// www.munichre.com/de/insights/cyber/cyber-insurance-risks-and-trends-2023.html (zuletzt eingesehen am 1.6.2024); *Gorr*, VW 3/2021, 44 (45); *Sanz*, Vier Säulen für nachhaltiges Wachstum im Bereich Cyber, online abrufbar unter https://axaxl.com/de/fast-fast-forward/articles/vier-saulen-fur-nachhaltiges-wachstum-im-bereich-cyber (zuletzt eingesehen am 1.6.2024); *Geiger*, Swiss Re: Cyber-Versicherungsmarkt hat enormes Wachstumspotenzial, online abrufbar unter https://www.handelszeitung.ch/insurance/swiss-re-der-cyber-versicherungsmarkt-hat-ein-enormes-wachstumspotenzial-545423 (zuletzt eingesehen am 1.6.2024); mit zurückhaltender Prognose dagegen *Dammalacks*, VersPrax 3/2023, 9 (9 f.); *Behrends/Droberg/Krischer*, VW 2/2021, 40 (41 f.); *Lohmann/Breitenstein*, VW 11/2021, 68 (70) – im Kontext der globalen Covid-19-Pandemie; *Erichsen/Pawig-Sander/Salm*, VersPrax 3/2017, 3 (7); *Müller/Topsch*, VW 3/3016, 54 (54).

164 CyberDirekt, Risikolage 2022: Studie zu Cyberrisiken im deutschen Mittelstand, S. 14.

165 Vgl. dazu Handelszeitung v. 4.1.2023, Zurich-CEO Mario Greco warnt: Cyber-Risiken werden «unversicherbar», online abrufbar unter https://www.handelszeitung.ch/insurance/lautzurich-ceo-werden-cyberangriffe-nicht-mehr-versicherbar-sein-560659 (zuletzt eingesehen am 1.6.2024); CFO Magazine v. 6.2.2015, Lloyd's Insurer Says Cyber Risks Too Big to Cover, online abrufbar unter https://www.cfo.com/news/lloyds-insurer-says-cyber-risks-too-big-to-cover/664487/ (zuletzt eingesehen am 1.6.2024); *Müller/Topsch*, VW 3/3016, 54 (54 f.); zur ökonomischen Versicherbarkeit von Erpressungsforderungen und Datenschutzbußgeldern sh. *Eggen*, S. 34 ff.

fehlt.[166] Hinzu kommt, dass selbst zurückliegende Schadensereignisse nur eine bedingt zuverlässige Aussagekraft über zukünftige Schadenspotentiale beinhalten, weil die versicherten Risiken hochdynamischer Natur sind.[167] Insbesondere der rasch fortschreitende technologische Wandel führt dazu, dass eine verlässliche und belastbare Risiko- und Prämienkalkulation zum Zeitpunkt der Risikoübernahme kaum möglich bzw. oftmals schnell überholt ist.[168]

Zusätzlich wird die Risiko- und Prämienkalkulation durch die unwägbaren Kumulgefahren bei der Verwirklichung von Cyberrisiken erschwert.[169] So besteht bspw. die Gefahr, dass über eine einzelne Sicherheitslücke in einer Softwareanwendung eine Vielzahl von versicherten Unternehmen gleichzeitig mit Schadsoftware infiziert und geschädigt wird oder ein DDoS-Angriff auf einen Cloud-Dienstleister eine große Zahl an Betriebsunterbrechungsschäden bei versicherten Unternehmen nach sich zieht.[170]

Darüber hinaus besteht im Rahmen der versicherungsökonomisch notwendigen Risikodiversifikation die Schwierigkeit, dass sich bislang kaum genügend homogene Risikokollektive herausgebildet haben.[171] Ein weiteres Problem bei der Versicherung von Cyberrisken sind die versicherungsökonomischen Gefahren einer negativen Risikoauslese (sog. adverse selection). Diese entstehen infolge einer asymmetrischen Informationsverteilung in Bezug auf die Risikosituation des zu versichernden Unternehmens sowie die moralischen Risiken (sog. moral hazard) von versicherten Unternehmen hinsichtlich eines hinreichenden Eigenschutzes ihrer Daten und IT-Systeme.[172]

Trotz dieser schwierigen Rahmenbedingungen scheint die Versicherung von Cyberrisiken aus versicherungsökonomischer Perspektive jedoch nicht per se unmöglich zu sein, weil verschiedene versicherungstechnische Instrumente existieren, um die Risiken beherrschbar(er) zu machen.[173] Den

166 Vgl. dazu *Pain*, S. 16; Deutsche Aktuarvereinigung, Cyberrisiken – Herausforderungen und Einfluss auf das Risikomanagement in Versicherungsunternehmen, S. 13; Deutsche Aktuarvereinigung, Cyberversicherungen: Neue Herausforderungen & neue Märkte, S. 6; *Haas*, S. 214; *Biener/Eling/Wirfs*, GP 40/2015, 131 (142); *Eling/Schnell*, S. 30; *Müller/Topsch*, VW 3/3016, 54 (54 f.); *Gebert/Klapper*, in: Veith/Gräfe/Gebert[4] § 24 Rn. 47.

167 Vgl. dazu *Pain*, S. 16; *Haas*, S. 214 f.; *Biener/Eling/Wirfs*, GP 40/2015, 131 (142); *Eling/Schnell*, S. 30.

168 Vgl. dazu *Haas*, S. 214 f.; *Biener/Eling/Wirfs*, GP 40/2015, 131 (142); *Eling/Schnell*, S. 30.

169 Sh. dazu näher *Pain*, S. 17, 20 ff.; *Cremer/Materne*, in: Arnold et. al. (Hrsg.) Risiko im Wandel, S. 241 ff.; Deutsche Aktuarvereinigung, Cyberrisiken – Herausforderungen und Einfluss auf das Risikomanagement in Versicherungsunternehmen, S. 11 ff.; *Torbohm*, VersPrax 3/2023, 3 (3 f.); *Müller/Topsch*, VW 3/2016, 54 (54 f.); *Biener/Eling/Wirfs*, GP 40/2015, 131 (141).

170 Vgl. dazu *Pain*, S. 22 ff.; *Torbohm*, VersPrax 3/2023, 3 (4); Deutsche Aktuarvereinigung, Cyber-Versicherungen: Neue Herausforderungen & neue Märkte, S. 6 f.

171 Vgl. dazu *Biener/Eling/Wirfs*, GP 40/2015, 131 (141 f.); *Eling/Schnell*, S. 30.

172 *Biener/Eling/Wirfs*, GP 40/2015, 131 (143 f.); *Eling/Schnell*, S. 31; *Haas*, S. 205 ff.

173 Für Versicherbarkeit auch *Eling/Schnell*, S. 31; *Biener/Eling/Wirfs*, GP 40/2015, 131 (147); *Pain*, S. 35 f.; Deutsche Aktuarvereinigung, Cyberrisiken – Herausforderungen und Einfluss auf das Risikomanagement in Versicherungsunternehmen, S. 21 f.; Deutsche Aktuarvereinigung, Cyber-Versicherungen: Neue Herausforderungen & neue Märkte, S. 7; krit. dagegen *Stanczyk*, VW 11/2023, 10 (14).

Unwägbarkeiten in der Risiko- und Prämienkalkulation kann etwa durch eine restriktive Vertragsgestaltung (z.B. Begrenzung der Deckungssummen,[174] Vereinbarung von Laufzeitbeschränkungen, Eingrenzung der versicherten Gefahren) oder durch Sicherheitszuschläge begegnet werden.[175] Den Gefahren im Zusammenhang mit einer negativen Risikoauslese sowie den moralischen Risiken kann durch eine sorgfältige vorvertragliche Risikoprüfung bzw. durch die Vereinbarung von Obliegenheiten zur Einhaltung von IT-Sicherheitsvorkehrungen vorgebeugt werden.[176] Ferner kann das wirtschaftliche Risiko des Versicherers auch über den Abschluss einer Rückversicherung minimiert werden.[177]

IV) Überblick zu Konzeption und Inhalt von Cyberversicherungen

Cyberversicherungen verfolgen zumeist einen ganzheitlichen Ansatz und bieten aus diesem Grund nicht nur Deckung für unterschiedliche Schäden (z.B. Ersatz von Ertragsausfällen infolge von Betriebsunterbrechungen, Freistellung von begründeten Haftpflichtansprüchen), sondern sehen regelmäßig auch Kostenübernahmeregelungen für verschiedenartige Service- und Assistance-Leistungen (z.B. Übernahme von Kosten für forensische Untersuchungen oder Aufwendungen für das Krisen- und Reputationsmanagement) vor.[178] In der Regel handelt es sich bei Cyberversicherungen daher um Mehrspartenprodukte (sog. Multi-Line-Policen).[179] Im Gegensatz zu herkömmlichen Sachversicherungen decken Cyberversicherungen hauptsächlich Vermögensschäden, die in aller Regel nach dem Prinzip der konkreten Bedarfsdeckung erstattet werden.[180]

174 Zu den marktüblichen Kapazitäten und Haftungslimits sh. *Haas*, S. 186 ff.

175 Vgl. dazu *Gebert/Klapper*, in: Veith/Gräfe/Gebert[4] § 24 Rn. 47; *Armbrüster*, S. 627; zu den vertrieblichen Folgeproblemen einer restriktiven Vertrags- bzw. Prämiengestaltung sh. *Griese*, VW 9/2023, 28 (31).

176 Vgl. dazu *Haas*, S. 206 f.; zu den vertrieblichen Umsetzungsproblemen bei ressourcenschwachen KMU sh. *Griese*, VW 9/2023, 28 (31).

177 Vgl. dazu Deutsche Aktuarvereinigung, Cyberrisiken – Herausforderungen und Einfluss auf das Risikomanagement in Versicherungsunternehmen, S. 19.

178 Vgl. dazu *Griese*, VW 9/2023, 28 (30); *Lohmann/Breitenstein*, VW 11/2021, 68 (70 f.); zu den Vorteilen einer solchen Mosaiklösung sh. *Beckmann/Köhler*, in: FS Herberger (2016), S. 54.; zum Bestehen und der Notwendigkeit optionaler Zusatzdeckungen sh. *Wirth*, BB 2018, 200 (202 ff.); *Armbrüster*, S. 628.

179 *Schilbach*, SpV 2018, 2 (3); *Malek/Schütz*, PHi 2018, 174 (179); *Pache/Graß*, VW 12/2017, 39; *Armbrüster*, in: Promok (Hrsg.) Cyberversicherung, S. 32 f.; *Haas*, S. 185 ff.; zu Fragen der versicherungsaufsichtsrechtlichen Einordnung von Cyberversicherungsprodukten sh. *Fortmann*, r+s 2019, 429 (430); *Lesser*, S. 200 ff.

180 Zur abweichenden Berechnung des Unterbrechungsschadens sh. unten S. 122.

1) Die Cyberrisiko-Versicherung des GDV (AVB-Cyber)

Die AVB-Cyber des GDV sind speziell auf KMU mit einem Umsatz bis 50 Mio. EUR und einer Größe bis 250 Mitarbeiter zugeschnitten.[181] Der modular aufgebaute Teil A der AVB-Cyber ist in vier Bausteine unterteilt, die jeweils spezifische Bestimmungen zur Ausgestaltung des Versicherungsschutzes enthalten.[182]

Der Basis-Baustein in Abschnitt A1 AVB-Cyber ist „vor die Klammer gezogen" und sieht bausteinübergreifend geltende Bestimmungen vor, wie z.B. Regelungen zum versicherten Risiko (sh. dazu unten S. 37 ff.), zum Versicherungsfall (sh. dazu unten S. 136 ff.), zum persönlichen und räumlichen Geltungsbereich der Versicherung (sh. dazu unten S. 148 ff.), zur Verhaltenszurechnung (sh. dazu unten S. 151 ff.), zur Behandlung von Serienschäden (sh. dazu unten S. 154 ff.) zu den allgemeinen Risikoausschlüssen (sh. dazu unten S. 163 ff.) und zu den Obliegenheiten des Versicherungsnehmers vor Eintritt des Versicherungsfalls (sh. dazu unten S. 235 ff.).

Der konkrete Umfang des Versicherungsschutzes wird durch die Leistungsbausteine in Abschnitt A2 AVB-Cyber bis Abschnitt A4 AVB-Cyber festgelegt. Der Service- und Kosten-Baustein in Abschnitt A2 AVB-Cyber beinhaltet mehrere Kostenübernahmeregelungen für unterschiedliche Service- und Assistance-Leistungen (sh. dazu unten S. 75 ff.). Im Drittschaden-Baustein in Abschnitt A3 AVB-Cyber ist die (Betriebs-)Haftpflichtkomponente der AVB-Cyber enthalten (sh. dazu unten S. 95 ff.). Über den Eigenschaden-Baustein in Abschnitt A4 AVB-Cyber besteht Deckung für Betriebsunterbrechungsschäden sowie Datenwiederherstellungskosten (sh. dazu unten S. 110 ff.).

In Teil B der AVB-Cyber, der ebenfalls in vier Abschnitte untergliedert ist, finden sich allgemeine Bestimmungen über die Rechte und Pflichten der Versicherungsvertragsparteien. Abschnitt B1 AVB-Cyber enthält Regelungen zum Beginn des Versicherungsschutzes und zur Beitragszahlung. In Abschnitt B2 AVB-Cyber ist Beginn, Dauer und Ende des Versicherungsschutzes geregelt. Hervorzuheben ist Abschnitt B3 AVB-Cyber, in dem mehrere (gesetzliche) Obliegenheiten des Versicherungsnehmers vertraglich festgelegt werden (sh. dazu unten 235 ff., 307 ff.). Abschnitt B4 AVB-Cyber beinhaltet versicherungsrechtliche Regelungen allgemeiner Art.

181 GDV, GDV stellt Musterbedingungen für Cyberversicherung vor, online abrufbar unter https://www.gdv.de/gdv/medien/medieninformationen/gdv-stellt-musterbedingungen-fuer-cyberversicherung-vor-8270 (zuletzt eingesehen am 1.6.2024).

182 Zu den Vorteilen eines modularen Ansatzes sh. *Schilbach*, SpV 2018, 2 (2); *Pache/Graß*, VW 12/2017, 39.

2) Gegenwärtige Bedingungswerke auf dem Cyberversicherungsmarkt

Die gegenwärtigen[183] Bedingungswerke auf dem Cyberversicherungsmarkt sind inhaltlich und konzeptionell unterschiedlich ausgestaltet, was die Vergleichbarkeit der Versicherungsprodukte erschwert.[184] Einige Cyberversicherer orientieren sich am Aufbau der AVB-Cyber.[185] Andere Bedingungswerke verzichten hingegen auf bausteinübergreifende Regelungen zur primären Risikobeschreibung und fixieren den Inhalt sowie den Umfang des Versicherungsschutzes gesondert für jeden einzelnen Deckungsbaustein.[186] Neben diesen aufbautechnischen Differenzen bestehen auch in inhaltlicher Hinsicht deutliche Unterschiede zwischen den Bedingungswerken, auf die noch im Detail eingegangen wird und daher an dieser Stelle nur kursorisch angesprochen werden. So haben sich bspw. auf dem Cyberversicherungsmarkt bislang keine einheitlichen Schadensereignis- und Versicherungsfalldefinitionen herausgebildet (sh. dazu unten S. 65 f., 145 f.). Auch hinsichtlich Art und Umfang der versicherten Schäden bzw. der Kostenübernahmeregelungen für Service- und Assistance-Leistungen besteht keine einheitliche Marktpraxis (sh. dazu unten S. 93 f., 108 f., 131 f.). Unterschiede bestehen darüber hinaus bei der Mitversicherung von Betriebsunterbrechungen aufgrund des Ausfalls von Cloud-Dienstleistern (sh. dazu unten S. 65 f., 131 f.), der Deckung von Ansprüchen wegen Datenschutzverletzungen (sh. dazu unten S. 108 f.), dem Ausschluss von Risiken im Zusammenhang mit politisch-motivierten Cyberangriffen (sh. dazu unten S. 185 f.) sowie der Mitversicherung von Datenschutzbußgeldern (sh. dazu unten S. 215) und Erpressungsforderungen (sh. dazu unten S. 202 f.). Uneinheitlich wird zudem die Vereinbarung von Obliegenheiten des Versicherungsnehmers vor Eintritt des Versicherungsfalls zur Gewährleistung der IT-Sicherheit gehandhabt (sh. dazu unten S. 298 f.).

183 Der Untersuchung liegen die Bedingungswerke von insgesamt 23 Versicherungsunternehmen zu Grunde, sh. zu den einzelnen Bedingungen unten S. 354. Die letzte Aktualitätsabfrage der Bedingungen erfolgte im Rahmen telefonischer Rücksprache mit den jeweiligen Anbietern am 13. März und 14. März 2024.

184 Vgl. zur heterogenen Marktlage *Wirth*, BB 2018, 200 (202 ff.); *Malek/Schütz*, PHi 2018, 174 (174 ff.); *Beckmann/Köhler*, in: FS Herberger (2016), S. 53 ff.; ein Überblick zu den verschiedenen Deckungskonzepten findet sich bei *Heidemann/Flagmeier*, S. 98 ff.

185 Vgl. dazu die Versicherungsbedingungen von Provinzial; ARAG; Hiscox; Baloise; Alte Leipziger; Dual; Nürnberger; Mannheimer; Continentale; VHV; Barmenia; R+V; HDI; Gothaer; Württembergische; Allianz.

186 Vgl. dazu die Versicherungsbedingungen von Ostangler; ERGO; AXA; Markel; Berkley; Zurich; AIG.

V) Auslegungsmaßstab bei Cyberversicherungen

1) Grundlagen

Bei der Auslegung von Cyberversicherungen sind grundsätzlich die allgemeinen Grundsätze zur Auslegung von AVB zu beachten.[187] Nach ständiger Rechtsprechung des BGH sind AVB so auszulegen, wie sie ein durchschnittlicher, um Verständnis bemühter Versicherungsnehmer bei verständiger Würdigung, aufmerksamer Durchsicht und unter Berücksichtigung des erkennbaren Sinnzusammenhangs versteht. Dabei kommt es auf die Verständnismöglichkeiten eines Versicherungsnehmers ohne versicherungsrechtliche Spezialkenntnisse und damit auch auf seine Interessen an. In erster Linie ist vom Bedingungswortlaut auszugehen. Der mit dem Bedingungswerk verfolgte Zweck und der Sinnzusammenhang der Klauseln sind zusätzlich zu berücksichtigen, soweit sie für den Versicherungsnehmer erkennbar sind.[188] Unbeachtlich für die am Bedingungswortlaut ausgerichtete Auslegung von AVB ist, welche Entstehungsgeschichte den Bedingungen zugrunde liegt oder wie vergleichbare Begrifflichkeiten in anderen Bedingungen interpretiert werden.[189] Aus diesem Grund kann z.B. das nicht-öffentliche Hinweisdokument des GDV zu den AVB-Cyber keine Berücksichtigung bei der Auslegung der Musterbedingungen finden.[190]

Ausnahmsweise kommt es nach ständiger Rechtsprechung des BGH nicht auf die Verständnismöglichkeiten des durchschnittlichen Versicherungsnehmer, sondern auf das juristische Begriffsverständnis an, wenn es sich bei dem Ausdruck um einen Begriff der Rechtssprache mit fest umrissenen Bedeutungsgehalt handelt.[191] Eine Rückausnahme gilt für Fälle, in denen das allgemeine Sprachverständnis von der Rechtssprache in einem Randbereich

187 So auch *Rudkowski*, VersR 2023, 416 (417); *Notthoff*, r+s 2022, 61 (63 f.); *Malek/Schütz*, r+s 2019, 421 (424); *Klimke*, in: Prölss/Martin[31] Vorbem. zu A1-1 AVB-Cyber Rn. 8 ff.

188 Vgl. zum Vorstehenden BGH, Urt. v. 18.1.2023 – IV ZR 465/21, NJW 2023, 684 (686); BGH, Urt. v. 26.1.2022 – IV ZR 144/21, NJW 2022, 872 (873); BGH, Urt. v. 14.7.2021 – IV ZR 153/20, NJW 2021, 2970 (2970 f.) – m.w.Nw. zur st. Rspr.; grundlegend zur Auslegung von AVB und dem Leitbild des durchschnittlichen Versicherungsnehmers *Pionetk*, r+s 2023, 337 (337 ff.); *Koch*, VersR 2015, 133 (133 ff.); zur diesbezüglichen Entwicklung der Rechtsprechung sh. *Armbrüster*, in: Prölss/Martin[31] Einl. Rn. 259 ff.

189 Vgl. hierzu *Rixecker*, in: Langheid/Rixecker[7] § 1 VVG Rn. 36; *Armbrüster*, in: Prölss/Martin[31] Einl. Rn. 285; zur Unbeachtlichkeit der Entstehungsgeschichte von AVB, selbst wenn die Berücksichtigung der historischen Entwicklung bei der Auslegung für den Versicherungsnehmer von Vorteil wäre, sh. BGH, Urt. v. 17.5.2000 – IV ZR 113/99, NJW-RR 2000, 1341 (1342); *Reiff*, in: Langheid/Wandt[2] Bd. III Ziff. 50 Rn. 85; a.A. *Armbrüster*, in: Prölss/Martin[31] Einl. Rn. 266 ff., 284 – m.w.Nw.

190 A.A. *Salm*, in: Rüffer/Halbach/Schimikowski[4] AVB-Cyber A.1-17 Rn. 2 – sofern zur Auslegung der AVB-Cyber nicht-öffentliche Hinweisdokumente des GDV herangezogen werden.

191 Vgl. dazu BGH, Urt. v. 10.4.2019 – IV ZR 59/18, r+s 2019, 326 (327); BGH, Urt. v. 8.5.2013 – IV ZR 84/12, r+s 2013, 601 (603) – m.w.Nw. zur st. Rspr.

deutlich abweicht, oder wenn der Sinnzusammenhang der Versicherungsbedingungen etwas anderes ergibt.[192]

2) Verständnishorizont eines durchschnittlichen Versicherungsnehmers in der gewerblichen Cyberversicherung

Der Verständnishorizont eines durchschnittlichen Versicherungsnehmer bemisst sich nach den Verständnismöglichkeiten und Interessen des typischerweise durch die Bedingungen adressierten Kundenkreises.[193] Grundsätzlich gilt, je geschäftserfahrener der durch die Bedingungen angesprochene Kundenkreis ist, desto höhere Anforderungen können an dessen Verständnismöglichkeiten gestellt werden.[194] Im Rahmen der gewerblichen Cyberversicherung wird deshalb diskutiert, ob und inwieweit von einem durchschnittlichen Versicherungsnehmer die Kenntnis sowie das fachsprachliche Verständnis von IT-Terminologie verlangt werden kann.[195]

Der mehrheitliche Teil des Schrifttums ist der Ansicht, dass ein durchschnittlicher Versicherungsnehmer zumindest allgemein bekannte und gebräuchliche IT-Begriffe, wie z.B. Server, Virus, Malware oder Firewall, in der fachsprachlichen Bedeutung kennen und verstehen muss, ohne dass es dazu einer gesonderten Definition im jeweilen Vertragswerk bedürfte.[196] Zur Begründung wird angeführt, dass sich gewerbliche Cyberversicherungen ausschließlich an geschäftserfahrene Unternehmen richten, denen eine Recherche der fachsprachlichen Bedeutung in einem Nachschlagewerk zumutbar sei.[197]

Dieser Sichtweise ist beizupflichten, weil bei allgemein bekannten und gebräuchlichen IT-Begriffen in aller Regel kein unüberbrückbarer Rechercheaufwand für den durchschnittlichen Versicherungsnehmer bestehen dürfte. Auch KMU, als die primäre Zielgruppe der AVB-Cyber, dürften mit diesen Anforderungen nicht überfordert sein.

Im Einzelfall kann allerdings die Frage auftreten, ob ein auslegungsbedürftiger IT-Fachbegriff über hinreichende Bekanntheit bzw. Gebräuchlichkeit in dem jeweils adressierten Kundenkreis verfügt. So wird bspw.

192 Vgl. dazu BGH, Urt. v. 10.4.2019 – IV ZR 59/18, r+s 2019, 326 (327); BGH, Urt. v. 14.6.2017 – IV ZR 161/16, r+s 2017, 421 (422) – m.w.Nw. zur st. Rspr.

193 Vgl. dazu BGH, Urt. v. 18.11.2020 – IV ZR 217/19, r+s 2021, 27 (28); BGH, Urt. v. 25.5.2011 – IV ZR 117/09, NJW-RR 2011, 1595 (1596) – m.w.Nw. zur st. Rspr.; *Armbrüster*, r+s 2023, 837 (839 f.); *Koch*, VersR 2015, 133 (137); *Rixecker*, in: Langheid/Rixecker[7] § 1 VVG Rn. 43.

194 Vgl. dazu BGH, Urt. v. 18.11.2020 – IV ZR 217/19, r+s 2021, 27 (28); BGH, Urt. v. 25.5.2011 – IV ZR 117/09, NJW-RR 2011, 1595 (1596).

195 Allgemein zur Auslegung von Fachbegriffen in AVB *Armbrüster*, r+s 2023, 837 (837 ff.).

196 *Malek/Schütz*, r+s 2019, 421 (424); *Notthoff*, r+s 2022, 61 (63 f.); *Klimke*, in: Prölss/Martin[31] Vorbem. zu A1-1 AVB-Cyber Rn. 9; *Thull*, S. 64; i.E. auch *Rudkowski*, VersR 2023, 416 (417); *Wojciechowski*, VersR 2022, 341 (342); *Malek/Schütz*, PHi 2018, 174 (178); a.A. *Koch*, in: Bruck/Möller[10] Bd. V AVB-Cyber Vorbem. AVB-Cyber Rn. 12.

197 *Malek/Schütz*, r+s 2019, 421 (424); *Notthoff*, r+s 2022, 61 (64); *Klimke*, in: Prölss/Martin[31] Vorbem. zu A1-1 AVB-Cyber Rn. 10 – jedoch mit abgeschwächten Anforderungen bei KMU; a.A. *Koch*, in: Bruck/Möller[10] Bd. V Vorbem. AVB-Cyber Rn. 12.

hinsichtlich der drei Schutzziele der IT-Sicherheit (Verfügbarkeit, Integrität und Vertraulichkeit)[198] im Schrifttum unterschiedlich beurteilt, ob es sich um allgemein bekannte bzw. gebräuchliche IT-Grundbegriffe oder um nicht-allgemein verbreitete Begriffsbildungen handelt.[199] Im Ergebnis ist Ersteres auch mit Blick auf KMU zu bejahen, weil die Begriffe seit längerer Zeit eine zentrale Rolle im IT-Grundschutzkompendium des BSI, das mitunter an KMU adressiert ist,[200] einnehmen und somit eine Art Indizwirkung für ihre Bekanntheit und Gebräuchlichkeit entfalten.[201]

Darüber hinaus stellt sich die Frage, welcher Maßstab bei nicht gebräuchlichen IT-Begriffen anzulegen bzw. wie mit IT-Begriffen zu verfahren ist, für die keine allgemeingültige fachspezifische Definition existiert. Nach einer Ansicht sind Fachtermini, die weder in einem Nachschlagewerk aufgeführt sind noch durch die Versicherungsbedingungen definiert werden und zu deren Verständnis es eines fachspezifischen Dritten bedarf, als zu unbestimmt und damit als intransparent gemäß § 307 Abs. 1 S. 2 BGB zu bewerten.[202] Nach anderer Ansicht kommt es in diesen Fällen – angelehnt an die im Schrifttum entwickelten Grundsätze zur Auslegung von Klauseln zur Überschussbeteiligung in der kapitalbildenden Lebensversicherung –[203] dagegen auf die Verständnismöglichkeiten eines neutralen Dritten an, der mit den Gegebenheiten der modernen Informations- und Kommunikationstechnik vertraut ist.[204]

Eine dritte Ansicht wendet gegen den zuletzt genannten Auslegungsmaßstab mehrere Bedenken ein. Unter anderem wird gegen die Verlagerung des Empfängerhorizonts von dem Versicherungsnehmer auf einen fachkundigen Vertreter vorgebracht, es sei einem Versicherungsnehmer ohne eigene IT-Abteilung nicht zumutbar, sich der Expertise eines externen Fachmanns zu bedienen.[205] Gegen eine Übertragung der aus der kapitalbildenden Lebensversicherung angestrengten Auslegungsgrundsätze spreche zudem, dass die inhaltliche Erfassung einer Cyberversicherung für einen durchschnittlichen

198 Sh. näher zu diesen Begrifflichkeiten unten S. 37 ff.

199 Für Einordung als IT-Grundbegriff *Malek/Schütz*, r+s 2019, 421 (424); i.E. auch *Notthoff*, r+s 2022, 61 (64) – sofern auf das Vorhandensein in einem Nachschlagewerk abgestellt wird; *Rudkowski*, VersR 2023, 416 (417); *Pawig-Sander*, in: Rüffer/Halbach/Schimikowski[4] AVB-Cyber A.1-2 Rn. 2; dagegen *Klimke*, in: Prölss/Martin[31] Vorbem. zu A1-1 AVB-Cyber Rn. 10.

200 Vgl. dazu BSI, IT-Grundschutzkompendium (2023), Kap. IT-Grundschutz – Basis für Informationssicherheit, S. 1.

201 Für eine solche Indizwirkung auch *Malek/Schütz*, r+s 2019, 421 (424); *Malek/Schütz*, PHi 2018, 176 (181); a.A. *Klimke*, in: Prölss/Martin[31] Vorbem. zu A1-1 AVB-Cyber Rn. 8, 10 – in Bezug auf die AVB-Cyber mit dem Argument, dass die Musterbedingungen keine Hinweise auf die Veröffentlichungen des BSI enthalten.

202 *Notthoff*, r+s 2022, 61 (64); tendenziell auch *Thull*, S. 64 f. – jedoch einschränkend für den kontrollfreien Teil der primären Leistungsbeschreibung; zur möglichen Unbestimmtheit von vertraglichen Nebenabreden in diesem Zusammenhang sh. *Malek/Schütz*, r+s 2019, 421 (424 f.).

203 Vgl. dazu *Rixecker*, in: Langheid/Rixecker[7] § 1 VVG Rn. 44; *Römer*, NVersZ 1999, 97 (104).

204 *Malek/Schütz*, r+s 2019, 421 (424 f.); i.E. auch *Wojciechowski*, VersR 2022, 341 (342).

205 *Notthoff*, r+s 2022, 61 (64).

Versicherungsnehmer auch ohne vergleichbares (technisches) Fachwissen wie in der kapitalbildenden Lebensversicherung möglich sei.[206] Vor allem überzeugt jedoch das vorgebrachte Argument, dass die vorgeschlagene Modifikation des maßgeblichen Verständnishorizontes („neutraler Dritter, der mit den Gegebenheiten der modernen Informations- und Kommunikationstechnik vertraut ist") zu einer gesetzesähnlichen Auslegung der Bedingungen führen und damit die Schutzfunktion des versicherungsrechtlichen Auslegungsmaßstabs („durchschnittlicher Versicherungsnehmer") untergraben würde.[207]

Angesichts der überzeugenden Argumentation der letztgenannten Ansicht ist eine Auslegung von gewerblichen Cyberversicherung am Verständnishorizont eines neutralen Dritten, der mit den Gegebenheiten der modernen Informations- und Kommunikationstechnik vertraut ist, somit abzulehnen. Für die Auslegung im Bedingungstext nicht definierter unbekannter bzw. ungebräuchlicher IT-Fachbegriffe ist daher – den allgemeinen Grundsätzen folgend – allein das allgemeine Sprachverständnis des durchschnittlichen Versicherungsnehmers ausschlaggebend.[208]

3) Restriktionsprinzip und Unklarheitenregel gemäß § 305c Abs. 2 BGB

Grundsätzlich werden auch Risikoausschlüsse und sonstige Deckungsbegrenzungen anhand der vorbezeichneten Kriterien ausgelegt.[209] Jedoch ist im Auslegungsprozess zusätzlich das sog. Restriktionsprinzip[210] zu beachten, das auf der ständigen Rechtsprechung des BGH fußt. Danach geht das Interesse des Versicherungsnehmers bei einer deckungsbeschränkenden Klausel in aller Regel dahin, dass der Versicherungsschutz nicht weiter verkürzt wird, als der erkennbare Zweck der Klausel dies gebietet. Auch braucht der durchschnittliche Versicherungsnehmer nicht mit Lücken im Versicherungsschutz zu rechnen, ohne dass die Klausel ihm dies hinreichend verdeutlicht. Deshalb sind Risikoausschlussklauseln eng und nicht weiter auszulegen, als es ihr Sinn unter Beachtung ihres wirtschaftlichen Zwecks und der gewählten Ausdrucksweise erfordert.[211]

Darüber hinaus ist für die Auslegung von Cyberversicherungsverträgen, die in aller Regel als Allgemeine Geschäftsbedingungen (AGB) im Sinne der §§ 305 ff. BGB zu klassifizieren sind, auch die sog. Unklarheitenregel gemäß

206 *Rudkowski*, VersR 2023, 416 (417).
207 *Klimke*, in: Prölss/Martin[31] Vorbem. zu A1-1 AVB-Cyber Rn. 10; *Thull*, S. 67.
208 So auch *Klimke*, in: Prölss/Martin[31] Vorbem. zu A1-1 AVB-Cyber Rn. 11; *Thull*, S. 67 f.
209 *Rixecker*, in: Langheid/Rixecker[7] § 1 VVG Rn. 53.
210 Vgl. zu dieser Bezeichnung *Koch*, VersR 2015, 133 (136).
211 Vgl. zum Vorstehenden BGH, Urt. v. 9.11.2022 – IV ZR 62/22, r+s 2023, 21 (23); BGH, Urt. v. 20.5.2021 – IV ZR 324/19, NJW 2021, 2584 (2586); BGH, Urt. v. 26.2.2020 – IV ZR 235/19, NJW 2020, 1743 (1744) – m.w.Nw. zur st. Rspr.; vgl. auch *Rixecker*, in: Langheid/Rixecker[7] § 1 VVG Rn. 53 ff.; *Reiff*, in: Langheid/Wandt[2] Bd. III Ziff. 50 Rn. 82.

§ 305c Abs. 2 BGB von Bedeutung. Danach gehen Zweifel bei der Auslegung von AGB zu Lasten des Verwenders, d.h. es ist jenes Auslegungsergebnis heranzuziehen, das für den Vertragspartner des Verwenders am günstigsten ist.[212] „Verwender" ist nach der Legaldefinition in § 305c Abs. 1 S. 1 BGB jene Vertragspartei, die der anderen Vertragspartei die AGB bei Abschluss des Vertrages stellt.[213] Bei Versicherungsbedingungen ist dies im Regelfall der Versicherer, so dass einzig der Versicherungsnehmer von dieser Auslegungsregel profitiert.[214] Zu berücksichtigen ist jedoch, dass der Anwendungsbereich von § 305c Abs. 2 BGB nach der Rechtsprechung des BGH nur eröffnet ist, wenn nach Ausschöpfung der in Betracht kommenden Auslegungsmethoden ein nicht behebbarer Zweifel an der Auslegung der Bestimmung verbleibt und mindestens zwei unterschiedliche Auslegungen vertretbar sind.[215]

212 Vgl. dazu BGH, Urt. v. 18.1.2023 – IV ZR 465/21, NJW 2023, 684 (687); BGH, Urt. v. 14.6.2017 – IV ZR 161/16, NJW-RR 2017, 992 (993) – m.w.Nw. zur st. Rspr.; zu den Tatbestandsvoraussetzungen der Unklarheitenregel sh. *Beckmann*, in: Beckmann/Matusche-Beckmann[3] § 10 Rn. 186; *Reiff*, in: Langheid/Wandt[2] Bd. III Ziff. 50 Rn. 96; *Armbrüster*, in: Prölss/Martin[31] Einl. Rn. 287.

213 Zum Tatbestandsmerkmal „stellen" sh. *Becker*, in: BeckOK-BGB[68] § 305 BGB Rn. 26 ff.; *Fornasier*, in: MüKo-BGB[9] Bd. II § 305 BGB Rn. 20 ff.

214 Vgl. dazu *Beckmann*, in: Beckmann/Matusche-Beckmann[3] § 10 Rn. 185; *Reiff*, in: Langheid/Wandt[2] Bd. III Ziff. 50 Rn. 95; *Armbrüster*, in: Prölss/Martin[31] Einl. Rn. 289.

215 BGH, Urt. v. 18.1.2023 – IV ZR 465/21, NJW 2023, 684 (687); BGH, Urt. v. 14.6.2017 – IV ZR 161/16, NJW-RR 2017, 992 (993).