Abhandlungen zum Deutschen und Europäischen
Gesellschafts- und Kapitalmarktrecht

Band 246

Cyberrisiken und Unternehmensorganisation

Von

Jonas David Schuck

Duncker & Humblot · Berlin

JONAS DAVID SCHUCK

Cyberrisiken und Unternehmensorganisation

Abhandlungen zum Deutschen und Europäischen Gesellschafts- und Kapitalmarktrecht

Herausgegeben von

Professor Dr. Holger Fleischer, LL.M., Hamburg
Professor Dr. Jens Koch, Köln
Professor Dr. Hanno Merkt, LL.M., Freiburg
Professor Dr. Gerald Spindler †

Band 246

Cyberrisiken und Unternehmensorganisation

Von

Jonas David Schuck

Duncker & Humblot · Berlin

Die Rechtswissenschaftliche Fakultät der Albert-Ludwigs-Universität Freiburg
hat diese Arbeit im Jahr 2024 als Dissertation angenommen.

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in
der Deutschen Nationalbibliografie; detaillierte bibliografische Daten
sind im Internet über http://dnb.d-nb.de abrufbar.

Satz: 3w+p GmbH, Rimpar
Druck: CPI books GmbH, Leck
Printed in Germany

ISSN 1614-7626
ISBN 978-3-428-19292-2 (Print)
ISBN 978-3-428-59292-0 (E-Book)

Gedruckt auf alterungsbeständigem (säurefreiem) Papier
entsprechend ISO 9706 ♾

Internet: http://www.duncker-humblot.de

Meinen Eltern
Cordula und Friedhelm

Vorwort

Die vorliegende Arbeit wurde von der Rechtswissenschaftlichen Fakultät der Albert-Ludwigs-Universität Freiburg im Sommersemester 2024 als Dissertation angenommen. Für die Verlagsveröffentlichung konnten relevante Literatur, Rechtsprechung und Gesetzgebung bis zum Januar 2024 berücksichtigt werden.

Mein herzlicher Dank gilt meinem Doktorvater, Herrn Prof. Dr. Jan Lieder, LL.M. (Harvard), für die engagierte Betreuung meiner Arbeit sowie den persönlichen Austausch. Er gewährte mir bei der Bearbeitung alle Freiheiten und stand stets mit Rat und Tat zur Seite. Ebenfalls danke ich Herrn Prof. Dr. Moritz Hennemann, M. Jur. (Oxon.), für die zügige Erstellung des Zweitgutachtens. Bei den Herausgebern der Schriftenreihe „Abhandlungen zum Deutschen und Europäischen Gesellschafts- und Kapitalmarktrecht“, den Herren Prof. Dr. Holger Fleischer, LL.M. (Michigan), Prof. Dr. Jens Koch und Prof. Dr. Hanno Merkt, LL.M. (Chicago), möchte ich mich für die Aufnahme meiner Arbeit bedanken.

Die Arbeit ist in wesentlichen Teilen während meiner Tätigkeit bei der Sozietät Allen Overy Shearman Sterling LLP entstanden. Für die Unterstützung und die Ermutigungen bin ich insbesondere dem Private Equity Team am Hamburger Standort zu Dank verpflichtet.

Mein größter Dank gilt schließlich meinen Eltern. Ihr Rückhalt, ihre bedingungslose Unterstützung und ihr Zuspruch haben mein Studium und diese Arbeit überhaupt erst ermöglicht.

Ihnen ist diese Arbeit gewidmet.

Hamburg, im Sommer 2024 *Jonas David Schuck*

Inhaltsübersicht

Kapitel 7

Kapitel 8

Inhaltsverzeichnis

Kapitel 5

Relevanz von Spezialgesetzen und Soft Law 97

Kapitel 6

Abkürzungsverzeichnis

AAO	Allgemeine Aufbauorganisation
AG	Aktiengesellschaft
AktG	Aktiengesetz
AtG	Atomgesetz
BAG	Bundesarbeitsgericht
BAIT	Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), Rundschreiben 10/2017 (BA) in der Fassung vom 16. 08. 2021: Bankaufsichtliche Anforderungen an die IT (BAIT)
BAO	Besondere Aufbauorganisation
BC-Beauftragter	Business-Continuity-Beauftragter
BC-Gremium	Business-Continuity-Gremium
BCM	Business-Continuity-Management
BCMS	Business-Continuity-Management-System
BC-Strategien	Business-Continuity-Strategien
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BilMoG	Gesetz zur Modernisierung des Bilanzrechts
BJR	Business Judgement Rule
BörsG	Börsengesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
BSIG-E	geändertes BSI-Gesetz auf Basis des Referentenentwurfs für das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CMS	Compliance-Management-System
d. h.	das heißt
DCGK	Deutscher Corporate Governance Kodex
DoS	Denial of Service
DSGVO	Datenschutz-Grundverordnung
EnWG	Energiewirtschaftsgesetz
FISG	Gesetz zur Stärkung der Finanzmarktintegrität
HinSchG	Gesetz für einen besseren Schutz hinweisgebender Personen
HinSchG-RegE	Entwurf eines Gesetzes für einen besseren Schutz hinweisgebender Personen sowie zur Umsetzung der Richtlinie zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden, 13. April 2022
IKS	internes Kontrollsystem
IRS	internes Revisionssystem
ISB	Informationssicherheitsbeauftragter
ISMS	Informationssicherheitsmanagementsystem
IT	Informationstechnologie/Informationstechnik

IT-SB	IT-Sicherheitsbeauftragter
KAGB	Kapitalanlagegesetzbuch
KMU	kleine und mittlere Unternehmen
KonTraG	Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
KRITIS-Betreiber	Betreiber kritischer Infrastrukturen im Sinne des § 2 Abs. 10 BSIG
KWG	Kreditwesengesetz
LG	Landgericht
LkSG	Lieferkettensorgfaltspflichtengesetz
m. w. N.	mit weiteren/weiterführenden Nachweisen
MaGo	Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), Rundschreiben 2/2017 (VA) – Mindestanforderungen an die Geschäftsorganisation von Versicherungsunternehmen (MaGo)
MAR	Market Abuse Regulation, Verordnung (EU) Nr. 596/2014 des Europäischen Parlaments und des Rates vom 16. April 2014 über Marktmissbrauch (Marktmissbrauchsverordnung) und zur Aufhebung der Richtlinie 2003/6/EG des Europäischen Parlaments und des Rates und der Richtlinien 2003/124/EG, 2003/125/EG und 2004/72/EG der Kommission (Text von Bedeutung für den EWR)
MaRisk	Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), Rundschreiben 05/2023 (BA) in der Fassung vom 29. 06. 2023: Mindestanforderungen an das Risikomanagement (MaRisk)
MTA	maximal tolerierbare Ausfallzeit
NIS-2-Richtlinie	Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148
NIS2UmsuCG	NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz, aktuell vorliegend als Referentenentwurf
OLG	Oberlandesgericht
PDCA	Plan-Do-Check-Act
RFS	Risikofrüherkennungs- und Überwachungssystem des § 91 Abs. 2 AktG, auch Risikofrüherkennungssystem
RMS	Risikomanagementsystem
TKG	Telekommunikationsgesetz
VAG	Versicherungsaufsichtsgesetz
VAIT	Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), Rundschreiben 10/2018 (BA) in der Fassung vom 03. 03. 2022: Versicherungsaufsichtliche Anforderungen an die IT (VAIT)
WAZ	Wiederanlaufzeit
WpHG	Wertpapierhandelsgesetz
z. B.	zum Beispiel

Kapitel 1

Einleitung

Das grundlegende Ziel einer jeden Aktiengesellschaft (AG) und damit die Leitungsaufgabe des Vorstands ist es, den Fortbestand des Unternehmens zu sichern und für eine dauerhafte Rentabilität zu sorgen. Als oberste Maxime hat sich jede Handlung des Vorstands daran zu orientieren.[1] Eine Gefahr für diese Zielerreichung sind die jeweiligen Risiken, die einem Unternehmen drohen. Während es sich dabei traditionell nur um analoge Risiken wie die physische Zerstörung der Unternehmenswerte oder wirtschaftliche Risiken durch Veränderungen des Marktes oder Finanzierungsprobleme handelte, drohen den Unternehmen zunehmend auch digitale Risiken.[2]

A. Relevanz von Cybersecurity in der AG

Digitale Risiken sind dabei ebenso vielseitig wie analoge. Allgemein bekannt dürfte die Gefahr durch unternehmensexterne Cyberangriffe sein. So waren vor Kurzem hunderte deutsche Unternehmen von einer Welle von Ransomwareangriffen betroffen.[3] Daneben existieren aber auch unternehmensinterne Gefahrenquellen, insbesondere verursacht durch die eigenen Mitarbeiter.[4] Insofern stellen auch diese ein Risiko für die digitalen Unternehmenswerte dar. Schließlich können sich physische Gefahren in digitalen Risiken verwirklichen. Beispielsweise führte die Durchtrennung eines Glasfaserkabels im Zuge von Bauarbeiten zu einem IT-Ausfall der Lufthansa und damit zu einer massiven Störung des Flugbetriebs.[5] In der Summe stellen solche Cyberrisiken sowie daraus folgende Betriebsunterbrechungen nach

---

[1] *Spindler*, in: MünchKomm AktG, § 76 Rn. 86, 87; *Cahn*, in: KölnKomm AktG, § 76 Rn. 21 ff.; *Koch*, in: Koch, AktG, § 76 Rn. 34; *Kort*, in: Großkomm AktG, § 76 Rn. 53; *Fleischer*, in: Spindler/Stilz, AktG, § 76 Rn. 27; *Weber*, in: Hölters/Weber, AktG, § 76 Rn. 19; *Bürgers*, in: Bürgers/Körber/Lieder, AktG, § 76 Rn. 11; *Fleischer*, AG 2022, 377, 382; *von dem Bussche/Schelinski*, in: Leupold/Wiebe/Glossner, IT-Recht, Teil 7.1 Rn. 87; *Voigt*, IT-Sicherheitsrecht, Kap. A Rn. 34.

[2] *Podebrad/Gabel*, in: Gabel/Kiefner/Heinrich, Rechtshandbuch Cyber-Security, Kap. 1 Rn. 1.

[3] BSI, Pressemitteilung 6. Februar 2023.

[4] Siehe hierzu Kapitel 2: B. II.

[5] Handelsblatt, IT-Chaos bringt Lufthansa in Erklärungsnot, 15. Februar 2023.

einschlägigen Umfragen mittlerweile die größte Gefahr für Unternehmen dar.[6] Regelmäßig wird diesen sogar existenzgefährdendes Potential zugesprochen.[7] Dabei ist die Bedrohung für Unternehmen insgesamt im Cyberraum „so hoch wie nie".[8] Gleichzeitig ist eine digitale Abstinenz für Unternehmen heutzutage nicht mehr möglich.[9] Vielmehr „durchdringt" die Nutzung von IT und des Internets die Wirtschaft „in immer größerem Maße".[10] Konsequenterweise bedürfen Unternehmen zunehmend einer angemessenen Sicherheitsstruktur, um die diesbezüglichen Risiken adäquat zu adressieren.

Entgegen landläufiger Meinung kann ein entsprechender Schutz nur etwa hälftig durch technische Maßnahmen erreicht werden, wie beispielsweise durch den Einsatz von Sicherheitsgateways und Paketfiltern (*Firewalls*) oder kryptographischen Verfahren, wie der Verschlüsselung von Kommunikationsverbindungen.[11] Im Übrigen sind organisatorische Sicherheitsmaßnahmen einzurichten. Dies liegt vor allem daran, dass der Mensch, für Unternehmen meist die eigenen Mitarbeiter, der größte Risikofaktor für die IT ist.[12] Da Mitarbeiter zur Erfüllung ihrer Tätigkeit weitreichende Zugriffsrechte auf die IT-Infrastruktur eines Unternehmens haben, können sie, ob vorsätzlich oder fahrlässig, leichter technische Schutzmechanismen umgehen und so einfacher größeren Schaden anrichten als Externe. Entsprechend werden Mitarbeiter von Cyberangreifern auch häufig als Werkzeug benutzt.

Risikominimierung in Bezug auf den Faktor Mensch funktioniert größtenteils nur durch organisatorische Maßnahmen. Folglich sind diese gleichbedeutend mit den technischen Vorkehrungen. Für Unternehmen sind solche Maßnahmen im Zuge der Unternehmensorganisation einzurichten. Dazu gehören etwa die Schaffung einer Risikokultur im Unternehmen, eine klare Zuordnung von Aufgaben und Verantwortungsbereichen sowie die Qualifikation und Weiterbildung von Mitarbeitern. Darüber hinaus ist es unerlässlich, sich regelmäßig über aktuelle Bedrohungen der Cybersicherheit zu informieren und geeignete Maßnahmen zu ergreifen.[13]

---

[6] Statista, „Umfrage zu den größten Geschäftsrisiken für Unternehmen weltweit in 2022"; Allianz Risk Barometer 2023, 4; *Grieger*, WM 2022, 1865, 1865; *Podebrad/Gabel*, in: Gabel/Kiefner/Heinrich, Rechtshandbuch Cyber-Security, Kap. 1 Rn. 2 f.; *Baranowski/von Halen/Kornmeier*, BB 2019, 2690, 2690; *Troßbach*, CCZ 2021, 121, 121.

[7] Siehe hierzu Kapitel 3: E. I.

[8] BSI, Lagebericht des Bundesamts für Sicherheit in der Informationstechnik 2022, 11.

[9] *Noack*, ZHR 183 (2019), 105, 113; *Spindler*, in: Bittner/Guntermann/Müller/Rostam, Cybersecurity als Unternehmensleitungsaufgabe, 9; *Voigt*, IT-Sicherheitsrecht, Kap. A Rn. 10; *Rath/Kuß*, in: Umnuß, Corporate Compliance Checklisten, § 10 Rn. 1.

[10] RegBegr. IT-Sicherheitsgesetz, BT-Drs. 18/4096, 1.

[11] BSI-Standard 200–1, 1.2; *Sohr/Kemmerich*, in: Kipker, Cybersecurity, 1. Auflage, Kap. 2 Rn. 197, 200; vgl. *Kiefner*, in: Gabel/Kiefner/Heinrich, Rechtshandbuch Cyber-Security, Kap. 2 Rn. 2; *Podebrad/Gabel*, in: Gabel/Kiefner/Heinrich, Rechtshandbuch Cyber-Security, Kap. 1 Rn. 18.

[12] Siehe hierzu unter Kapitel 2: B. II.

[13] *Sohr/Kemmerich*, in: Kipker, Cybersecurity, 1. Auflage, Kap. 2 Rn. 197, 200.

B. Problemaufriss

Entsprechend der Relevanz der Unternehmensorganisation für die IT-Sicherheit rückt das Thema auch stärker in die Aufmerksamkeit der gesellschaftsrechtlichen Diskussion.[14] Kern dieser Debatte ist hinsichtlich der hier gegenständlichen AG die Frage nach den rechtlichen Rahmenbedingungen der Cybersecurity, insbesondere im Hinblick auf die Unternehmensorganisation. Eng verknüpft damit ist die Frage nach dem Pflichtenkanon des Vorstands und bestehenden, aus anderen Regelungsbereichen bekannten Regelungen, die in diesem Kontext Relevanz entwickeln.

I. Rechtsgrundlagen

Dabei ist zunächst festzustellen, dass kein allgemeingültiges, umfassendes Regelwerk für die Unternehmensorganisation im Hinblick auf Cybersecurity existiert.[15] Allerdings gibt es einen Fundus an gesetzlichen Vorgaben, die in diesem Bereich relevant sein können. Hier lassen sich grundsätzlich zwei Regelungsquellen unterscheiden.[16] Auf der einen Seite stehen die allgemeinen Vorgaben des AktG[17]. Hier wird Cybersecurity als spezifische Materie nicht ausdrücklich angesprochen. Rechtliche Vorgaben ergeben sich aus den allgemeinen Organisations- und Sorgfaltspflichten des Vorstands im Regelungsbereich Corporate Governance.[18] Auf der anderen Seite gibt es branchenspezifische Rechtsgrundlagen, die nur bei bestimmten AGs, die auf regulierten Märkten agieren, Anwendung finden, sogenannte Spezialgesetze. Dabei handelt es sich größtenteils um Präzisierungen der allgemeinen aktienrechtlichen Vorschriften im Hinblick auf einen bestimmten Anwendungsbe-

---

[14] Vgl. beispielhaft nur: *Gabel/Kiefner/Heinrich*, Rechtshandbuch Cyber-Security; *Bittner/Guntermann/Müller/Rostam*, Cybersecurity als Unternehmensleitungsaufgabe; *Kipker*, Cybersecurity; *Voigt*, IT-Sicherheitsrecht.

[15] *Kiefner*, in: Gabel/Kiefner/Heinrich, Rechtshandbuch Cyber-Security, Kap. 2 Rn. 7, 8; *Schmidt-Versteyl*, in: Bittner/Guntermann/Müller/Rostam, Cybersecurity als Unternehmensleitungsaufgabe, 47; *Spindler*, in: Bittner/Guntermann/Müller/Rostam, Cybersecurity als Unternehmensleitungsaufgabe, 43.

[16] Zur grundsätzlichen Gegenüberstellung siehe *von dem Bussche*, in: Kipker, Cybersecurity, Kap. 6 Rn. 35; *Rath/Kuß*, in: Umnuß, Corporate Compliance Checklisten, Kap. 8, B, I. Rn. 7 f.; *Voigt*, IT-Sicherheitsrecht, Kap. A Rn. 32 f.; *Kipker*, in: Kipker, Cybersecurity, Kap. 1 Rn. 21.

[17] Aktiengesetz, 6. September 1965, BGBl. 1965 I S. 1089.

[18] *Kiefner*, in: Gabel/Kiefner/Heinrich, Rechtshandbuch Cyber-Security, Kap. 2 Rn. 7, 8; *Schmidt-Versteyl*, in: Bittner/Guntermann/Müller/Rostam, Cybersecurity als Unternehmensleitungsaufgabe, 47; *Spindler*, in: Bittner/Guntermann/Müller/Rostam, Cybersecurity als Unternehmensleitungsaufgabe, 43; *Kipker*, in: Kipker, Cybersecurity, Kap. 1 Rn. 20; *Kipker*, in: Möslein/Omlor, FinTech-Handbuch, § 17 Rn. 8 f.; *von dem Bussche*, in: Kipker, Cybersecurity, Kap. 6 Rn. 25, 27; *von dem Bussche/Schelinski*, in: Leupold/Wiebe/Glossner, Teil 7.1 Rn. 1; *Bensinger*, in: Schulz, Compliance Management im Unternehmen, Kap. 13 Rn. 83; *Voigt*, IT-Sicherheitsrecht, Kap. A Rn. 24.