

Abhandlungen zum Deutschen und Europäischen  
Gesellschafts- und Kapitalmarktrecht

---

Band 246

# Cyberisiken und Unternehmensorganisation

Von

Jonas David Schuck



Duncker & Humblot · Berlin

JONAS DAVID SCHUCK

## Cyberisiken 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

# Cyberisiken 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.

Alle Rechte vorbehalten  
© 2025 Duncker & Humblot GmbH, Berlin  
Satz: 3w+p GmbH, Rimpf  
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 1*

### **Einleitung** 31

A. Relevanz von Cybersecurity in der AG	31
B. Problemaufriss	33
I. Rechtsgrundlagen	33
II. Anknüpfungspunkte im AktG	34
III. Gang der Untersuchung	36

## *Kapitel 2*

### **Grundlagen Cybersecurity** 38

A. Definitionen im Bereich der Cybersecurity	38
B. Arten von Cyberrisiken	41
I. Externe Risiken	42
II. Interne Risiken	46
III. Mitarbeiter als größter Risikofaktor	47

## *Kapitel 3*

### **Cybersecurity im Kontext von Leitungsaufgaben und Corporate Governance** 48

A. Cybersecurity als Leitungsaufgabe	48
I. Allgemeine Anforderungen	49
II. Cybersecurity als Leitungsaufgabe	50
III. Rechtliche Rahmenbedingungen einer Leitungsaufgabe	53
B. Corporate-Governance-Systeme	54
C. Risikomanagement	56
I. Rechtsgrundlage Risikomanagement	57
II. Differenzierung innerhalb des Risikomanagements	58
III. Risikomanagementpflicht	59

D. Compliance .....	62
I. Rechtsgrundlage Compliance .....	63
II. Ausgestaltung der Compliance .....	64
E. Cybersecurity als Spezialgebiet .....	68
I. Cyberrisiken als Unternehmensrisiken .....	69
II. Cyberrisiken als Compliance-Risiken .....	71
F. Zwischenergebnis .....	71

### *Kapitel 4*

<b>Aktienrechtliche Grundlagen der Cybersecurity</b> .....	<b>73</b>
A. § 91 Abs. 3 AktG .....	73
I. Risikomanagementsystem in Bezug auf Cyberrisiken .....	74
II. Funktionen eines Risikomanagementsystems .....	75
III. Angemessenheit und Wirksamkeit im Rahmen des § 91 Abs. 3 AktG .....	78
B. § 91 Abs. 2 AktG .....	80
I. Risikofrüherkennungssystem hinsichtlich Cyberrisiken .....	81
II. Ausgestaltung des Risikofrüherkennungssystems .....	82
C. §§ 76 Abs. 1, 93 Abs. 1 S. 1 AktG .....	83
I. § 76 Abs. 1 AktG .....	83
II. § 93 Abs. 1 AktG .....	84
III. IT-Risikomanagement .....	87
IV. IT-Compliance .....	89
D. § 93 Abs. 1 S. 2 AktG .....	90
I. Allgemein .....	91
II. Tatbestandsvoraussetzungen .....	92
III. Rechtlich gebundene Entscheidungen und unbestimmte Rechtsbegriffe .....	93
E. Zwischenergebnis .....	95

### *Kapitel 5*

<b>Relevanz von Spezialgesetzen und Soft Law</b> .....	<b>97</b>
A. Ausstrahlungswirkung von Spezialgesetzen .....	98
I. Methodische Grundlagen der Ausstrahlungswirkung .....	99
II. Arten der Ausstrahlungswirkung .....	102
III. Spezialgesetze als Lex specialis .....	103
IV. Bedenken gegen Ausstrahlungswirkung .....	104

V. Zwischenergebnis .....	108
B. Ausstrahlungswirkung von Soft Law .....	108
I. Relevanz von Soft Law .....	109
II. Übertragbarkeit der Vorgaben .....	109
C. Bedeutung von Spezialgesetzen und Soft Law bei Cybersecurity .....	110
I. Risikomanagement und Compliance .....	111
II. Cybersecurity .....	115
III. Business Judgement Rule .....	122
IV. Stand der Technik .....	125
V. Vertragliche Übertragungen .....	126
D. Zwischenergebnis .....	127

### *Kapitel 6*

<b>Relevanz von Cybersecurity für Vorstand und Aufsichtsrat</b> .....	<b>129</b>
A. Anforderungen an die Qualifikation des Vorstands .....	129
I. Aktienrechtliche Qualifikationsanforderungen .....	130
II. Ermessen des Aufsichtsrats bei der Bestellung des Vorstands .....	133
III. Einfluss des KWG und des VAG auf die Qualifikationsanforderungen .....	133
IV. Zwischenergebnis .....	136
B. Delegation durch den Gesamtvorstand .....	136
I. Leitungsaufgaben in der Delegation .....	137
II. Delegation von Cybersecurity .....	138
III. Nicht delegierbare Kernbereiche von Cybersecurity .....	154
IV. Kontroll- und Überwachungspflichten bei Delegation von Cybersecurity .....	155
V. Zwischenergebnis .....	158
C. Aufsichtsrat .....	158
I. Überwachung .....	158
II. Beratung .....	162
III. Information des Aufsichtsrats .....	164
IV. Anforderungen an die Qualifikation .....	169
V. Interne Organisation .....	175
VI. Zwischenergebnis .....	182

*Kapitel 7***Unternehmensorganisation durch ein ISMS** 183

A. Informationssicherheitsmanagementsystem	184
I. Grundlagen	185
II. Verpflichtende Einrichtung	186
B. Rechtliche Anforderungen an ein ISMS	189
I. Aktienrechtliche Anforderungen	189
II. Spezialgesetzliche Anforderungen	190
C. Ausgestaltung nach Soft-Law-Vorgaben	198
I. BSI-IT-Grundschutz	198
II. BAIT und VAIT	200
III. Ausgestaltung nach BSI-Standard 200–1	203
IV. Vergleichbarkeit der Systeme	209
D. Zwischenergebnis	209

*Kapitel 8***Preparedness: Funktionen eines ISMS** 211

A. IT-Sicherheitsziele und Rahmenbedingungen	212
I. Sicherheitsziele	212
II. Sicherheitskultur	213
III. Gesetzliche Rahmenbedingungen und Compliance	214
B. Sicherheitsstrategie	215
I. Allgemein	215
II. Informationsverbund	216
III. Risikotragfähigkeit, Risikoappetit und Risikotoleranz	216
C. Sicherheitsorganisation	218
I. Allgemeines	218
II. Leitlinie zur Informationssicherheit	223
III. IT-Richtlinie des Unternehmens	224
IV. Informationssicherheitsbeauftragter	231
V. Interne Kommunikation	247
VI. Zwischenergebnis	259
D. Cybersecurity-Konzept als Risikomanagementprozess	260
I. Analyse der Risiken	261
II. Steuerung der Risiken	271
III. Auswahl der Maßnahmen	276

IV. Umsetzung der Maßnahmen .....	293
V. Zwischenergebnis .....	293
E. Rechtliche Beschränkungen von IT-Sicherheitsmaßnahmen .....	294
I. Arbeitsrechtliche Problemfelder .....	295
II. Datenschutzrechtliche Problemfelder .....	297
III. Strafrechtliche Problemfelder .....	298
F. Überprüfung und Überwachung .....	298
I. Anleihen des allgemeinen Aktienrechts .....	299
II. Konkrete Anforderungen an die Überwachung .....	300
G. Anpassungen .....	304
H. Dokumentation .....	306

## *Kapitel 9*

### **Response: Business-Continuity**

308

A. Business-Continuity-Management-System .....	309
I. Spezialgesetzliche Grundlagen .....	310
II. Verpflichtende Einrichtung eines BCMS .....	311
III. Ausgestaltung .....	313
IV. Leitlinie des BCMS .....	314
V. Verhältnis zu anderen Managementsystemen .....	315
B. Organisation .....	316
I. BC-Aufbauorganisation .....	317
II. Besondere Aufbauorganisation und das Notfallteam .....	318
III. Externe Berater .....	322
C. Notfallkonzept .....	324
I. BCM-Analysen .....	324
II. BC-Strategien .....	326
III. Umsetzung der Strategien .....	327
D. Bewältigung .....	329
I. Chronologischer Ablauf der Bewältigung .....	330
II. Ausgewählte Maßnahmen .....	332
III. Rechtliche Maßnahmen .....	335
IV. Nachgelagerte Maßnahmen .....	336
E. Interne Kommunikation .....	337
I. Initialmeldung und Informationskette bei Cyberincidents .....	337
II. Kommunikation von Entscheidungen .....	341
III. Offenlegung gegenüber Beratern und Ermittlungsbehörden .....	341

F. Meldepflichten .....	341
I. DSGVO .....	342
II. BSIG .....	345
III. Vertragliche Meldepflichten .....	347
G. Insiderrecht und Ad-hoc-Publizität .....	348
I. Adressat der Ad-hoc-Publizitätspflicht .....	348
II. Cyberincident als Insiderinformation .....	350
III. Veröffentlichungspflicht .....	356
IV. Aufschieben der Veröffentlichung .....	363
V. Verfahren und Inhalt .....	382
VI. Zwischenergebnis .....	383
H. Externe Kommunikation .....	384
I. Aufgaben .....	385
II. Konsequenzen für die Unternehmensorganisation .....	386
III. Relevante Gruppen .....	386
I. Rechtliche Rahmenbedingungen von Lösegeldzahlungen .....	389
I. Allgemeines .....	390
II. Strafrechtliche Relevanz .....	391
III. Anderweitige gesetzliche Verstöße .....	393
IV. Aktienrechtliche Implikationen .....	394
V. Zwischenergebnis .....	397
J. Kontrolle und Verbesserung .....	398
K. Dokumentation .....	399

### *Kapitel 10*

<b>Gesetzlicher Regelungsbedarf für Cybersecurity</b>	<b>401</b>
A. Möglichkeit der Formulierung abstrakter Vorgaben .....	401
I. Regelungsbedarf .....	402
II. Gründe gegen eine Regelung .....	406
III. Schutzgut einer Regelung .....	407
IV. Regelungsqualität .....	408
V. Zwischenergebnis .....	412
B. Regelungsbedarf nach NIS2UmsuCG .....	412
I. Regelungsinhalt .....	413
II. Übertragbarkeit auf die allgemeine AG .....	416
III. Zwischenergebnis .....	417

C. Ansatzpunkte und Inhalte einer möglichen Regelung .....	418
I. Anwendungsbereich .....	418
II. Regelungskonzepte .....	419
III. Konkrete Regelungsvorschläge .....	422
IV. Mehrwert einer prinzipienbasierten Regelung .....	425
V. Regelung auf Ebene des Aufsichtsrats .....	426
VI. Zwischenergebnis .....	427

*Kapitel 11*

**Thesen**

429

<b>Literaturverzeichnis</b> .....	432
<b>Stichwortverzeichnis</b> .....	452





# Inhaltsverzeichnis

## *Kapitel 1*

### **Einleitung** 31

A. Relevanz von Cybersecurity in der AG	31
B. Problemaufriss	33
I. Rechtsgrundlagen	33
II. Anknüpfungspunkte im AktG	34
III. Gang der Untersuchung	36

## *Kapitel 2*

### **Grundlagen Cybersecurity** 38

A. Definitionen im Bereich der Cybersecurity	38
B. Arten von Cyberrisiken	41
I. Externe Risiken	42
1. Ransomware	42
2. Advanced Persistent Thread	43
3. Weitere Malware	44
4. DoS-Attacken	44
5. Phishing und Social Engineering	45
II. Interne Risiken	46
III. Mitarbeiter als größter Risikofaktor	47

## *Kapitel 3*

### **Cybersecurity im Kontext von Leitungsaufgaben und Corporate Governance** 48

A. Cybersecurity als Leitungsaufgabe	48
I. Allgemeine Anforderungen	49
II. Cybersecurity als Leitungsaufgabe	50
1. Leitungsaufgabe im Aktienrecht	51
2. Leitungsaufgabe in Spezialgesetzen und Soft Law	52
III. Rechtliche Rahmenbedingungen einer Leitungsaufgabe	53

B. Corporate-Governance-Systeme .....	54
C. Risikomanagement .....	56
I. Rechtsgrundlage Risikomanagement .....	57
II. Differenzierung innerhalb des Risikomanagements .....	58
III. Risikomanagementpflicht .....	59
1. <i>Ob</i> der Risikomanagementpflicht .....	60
2. <i>Wie</i> der Risikomanagementpflicht .....	61
D. Compliance .....	62
I. Rechtsgrundlage Compliance .....	63
II. Ausgestaltung der Compliance .....	64
1. Börsennotierte AG .....	65
2. Nichtbörsennotierte AG .....	66
3. CMS .....	67
4. Ausgestaltung im Übrigen .....	67
E. Cybersecurity als Spezialgebiet .....	68
I. Cyberrisiken als Unternehmensrisiken .....	69
II. Cyberrisiken als Compliance-Risiken .....	71
F. Zwischenergebnis .....	71

#### *Kapitel 4*

<b>Aktienrechtliche Grundlagen der Cybersecurity</b>	<b>73</b>
A. § 91 Abs. 3 AktG .....	73
I. Risikomanagementsystem in Bezug auf Cyberrisiken .....	74
II. Funktionen eines Risikomanagementsystems .....	75
III. Angemessenheit und Wirksamkeit im Rahmen des § 91 Abs. 3 AktG .....	78
B. § 91 Abs. 2 AktG .....	80
I. Risikofrüherkennungssystem hinsichtlich Cyberrisiken .....	81
II. Ausgestaltung des Risikofrüherkennungssystems .....	82
C. §§ 76 Abs. 1, 93 Abs. 1 S. 1 AktG .....	83
I. § 76 Abs. 1 AktG .....	83
II. § 93 Abs. 1 AktG .....	84
1. Legalitätspflicht .....	85
2. Legalitätskontrollpflicht .....	86
III. IT-Risikomanagement .....	87
IV. IT-Compliance .....	89
D. § 93 Abs. 1 S. 2 AktG .....	90
I. Allgemein .....	91

II. Tatbestandsvoraussetzungen .....	92
III. Rechtlich gebundene Entscheidungen und unbestimmte Rechtsbegriffe .....	93
E. Zwischenergebnis .....	95

### *Kapitel 5*

<b>Relevanz von Spezialgesetzen und Soft Law</b> .....	<b>97</b>
A. Ausstrahlungswirkung von Spezialgesetzen .....	98
I. Methodische Grundlagen der Ausstrahlungswirkung .....	99
1. Rechtsfortbildung .....	100
2. Auslegung .....	101
II. Arten der Ausstrahlungswirkung .....	102
III. Spezialgesetze als Lex specialis .....	103
IV. Bedenken gegen Ausstrahlungswirkung .....	104
V. Zwischenergebnis .....	108
B. Ausstrahlungswirkung von Soft Law .....	108
I. Relevanz von Soft Law .....	109
II. Übertragbarkeit der Vorgaben .....	109
C. Bedeutung von Spezialgesetzen und Soft Law bei Cybersecurity .....	110
I. Risikomanagement und Compliance .....	111
1. Spezialgesetze .....	111
2. Soft Law .....	113
II. Cybersecurity .....	115
1. Spezialgesetzliche Vorgaben .....	115
2. Soft Law .....	118
a) Relevanz im Rahmen des Aktienrechts .....	118
b) Einzelne Standards .....	122
III. Business Judgement Rule .....	122
1. Gesetzliche Vorgaben .....	123
2. Soft Law .....	123
IV. Stand der Technik .....	125
V. Vertragliche Übertragungen .....	126
D. Zwischenergebnis .....	127

*Kapitel 6*

<b>Relevanz von Cybersecurity für Vorstand und Aufsichtsrat</b>	<b>129</b>
A. Anforderungen an die Qualifikation des Vorstands	129
I. Aktienrechtliche Qualifikationsanforderungen	130
II. Ermessen des Aufsichtsrats bei der Bestellung des Vorstands	133
III. Einfluss des KWG und des VAG auf die Qualifikationsanforderungen	133
IV. Zwischenergebnis	136
B. Delegation durch den Gesamtvorstand	136
I. Leitungsaufgaben in der Delegation	137
II. Delegation von Cybersecurity	138
1. Horizontale Delegation	138
a) Allgemein	138
b) Überwachungspflicht	141
2. Vertikale Delegation	143
a) Allgemein	144
b) Überwachungsaufgabe	146
3. Delegation an Dritte	147
a) Im Aktienrecht	147
b) Besonderheiten bei Cybersecurity	149
aa) Outsourcing digitaler Funktionen	149
bb) Outsourcing von Cybersecurity-Maßnahmen	150
c) Ausgestaltung des Outsourcings	151
aa) Generelles zur Ausgestaltung und Relevanz von Spezialgesetzen	151
bb) Kettenauslagerung	152
cc) Finanzielles Risiko	152
dd) Schutzrechte im Vertrag	153
III. Nicht delegierbare Kernbereiche von Cybersecurity	154
IV. Kontroll- und Überwachungspflichten bei Delegation von Cybersecurity	155
1. Auswahl des Delegationsempfängers	156
2. Kontrolle des Delegationsempfängers	157
V. Zwischenergebnis	158
C. Aufsichtsrat	158
I. Überwachung	158
1. Unternehmensorganisation und Cybersecurity als Überwachungsgegenstand	159
2. Überwachung des ISB	162
II. Beratung	162
III. Information des Aufsichtsrats	164
1. Durch den Vorstand	164

2. Eigene Informationspflicht und -möglichkeit .....	165
a) Allgemein .....	165
b) Informationsordnung .....	166
c) Auskunftsverlangen gegenüber Mitarbeitern .....	166
d) Auskunftsrecht des Prüfungsausschusses .....	168
IV. Anforderungen an die Qualifikation .....	169
1. Aktienrechtliche Anforderungen .....	169
a) Allgemeine persönliche Qualifikation .....	169
b) Anforderung in Abhängigkeit vom jeweiligen Unternehmen .....	171
2. DCGK .....	172
3. Digitalisierungs- und Cybersecurity-Expertise .....	172
a) Cybersecurity-Know-how des Aufsichtsrats .....	173
b) Technologische Unterstützung .....	174
c) Steigerung der IT-Sicherheitskenntnisse .....	175
V. Interne Organisation .....	175
1. Zustimmungspflichtiges Geschäft .....	176
2. Expertenmitglied .....	177
3. Aufsichtsratsausschuss .....	179
a) Cybersecurity-Ausschuss .....	180
b) Cybersecurity im Rahmen bestehender Ausschüsse .....	181
VI. Zwischenergebnis .....	182

## *Kapitel 7*

### **Unternehmensorganisation durch ein ISMS** 183

A. Informationssicherheitsmanagementsystem .....	184
I. Grundlagen .....	185
II. Verpflichtende Einrichtung .....	186
1. ISMS nach § 91 Abs. 3 AktG .....	186
2. ISMS nach § 91 Abs. 2 AktG .....	187
3. ISMS nach §§ 76 Abs. 1, 93 Abs. 1 AktG .....	187
4. Spezialgesetze .....	189
B. Rechtliche Anforderungen an ein ISMS .....	189
I. Aktienrechtliche Anforderungen .....	189
II. Spezialgesetzliche Anforderungen .....	190
1. DSGVO .....	190
2. BSIG .....	192
a) Allgemein .....	192
b) Gesetzliche Anforderungen .....	193

3. KWG .....	195
4. VAG .....	196
5. GeschGehG .....	197
C. Ausgestaltung nach Soft-Law-Vorgaben .....	198
I. BSI-IT-Grundschatz .....	198
II. BAIT und VAIT .....	200
III. Ausgestaltung nach BSI-Standard 200–1 .....	203
1. Sicherheitsprozess als PDCA-Zyklus .....	203
a) <i>Plan</i> .....	204
b) <i>Do</i> .....	204
c) <i>Check</i> .....	205
d) <i>Act</i> .....	205
2. Managementprinzipien .....	205
a) Aufgaben und Pflichten des Managements .....	206
b) Weitere Managementprinzipien .....	207
3. Ressourcen .....	207
4. Einbindung der Mitarbeiter .....	208
IV. Vergleichbarkeit der Systeme .....	209
D. Zwischenergebnis .....	209

## *Kapitel 8*

### **Preparedness: Funktionen eines ISMS** 211

A. IT-Sicherheitsziele und Rahmenbedingungen .....	212
I. Sicherheitsziele .....	212
II. Sicherheitskultur .....	213
III. Gesetzliche Rahmenbedingungen und Compliance .....	214
B. Sicherheitsstrategie .....	215
I. Allgemein .....	215
II. Informationsverbund .....	216
III. Risikotragfähigkeit, Risikoappetit und Risikotoleranz .....	216
C. Sicherheitsorganisation .....	218
I. Allgemeines .....	218
1. Organisationsstrukturen .....	219
2. Prozesse .....	220
3. Rollen und Aufgaben .....	220
4. Three-Lines-Modell .....	221
II. Leitlinie zur Informationssicherheit .....	223

III. IT-Richtlinie des Unternehmens .....	224
1. Inhalt und Ziele .....	224
2. Verpflichtende Einrichtung durch den Vorstand .....	225
3. Verbindliche Einhaltung durch die Mitarbeiter .....	226
4. Inhaltliche Ausgestaltung .....	228
5. Meldepflichten und Verhalten bei Verdachtsfällen .....	230
IV. Informationssicherheitsbeauftragter .....	231
1. Verpflichtende Bestellung .....	232
2. Aufgaben und Verantwortung .....	234
3. Qualifikation des ISB .....	237
4. Strukturelle Anbindung an das Unternehmen .....	238
a) Interner ISB .....	239
aa) Organisatorische Anbindung .....	240
bb) Weisungsunabhängigkeit .....	241
cc) Angemessene Ressourcen .....	242
b) Externer ISB .....	243
5. Verhältnis zu übrigen Unternehmensbeauftragten .....	243
6. Haftung .....	245
V. Interne Kommunikation .....	247
1. Informationssystem und -organisation ( <i>bottom-up</i> ) .....	248
a) Pflicht zur Einrichtung eines Informationssystems .....	248
aa) Aktienrechtliche Sorgfaltspflicht .....	249
bb) Meldepflichten als Grundlage der Informationsverantwortung .....	250
cc) BJR als Grundlage der Informationsverantwortung .....	251
b) Ausgestaltung des Informationssystems .....	251
c) Information weiterer interner Stakeholder .....	253
2. Hinweisgebersystem (Whistleblower) .....	254
a) Rechtliche Rahmenbedingungen .....	254
b) Konzept und Nutzen .....	255
c) Inhaltliche Reichweite .....	258
3. Kommunikation von Entscheidungen ( <i>top-down</i> ) .....	259
VI. Zwischenergebnis .....	259
D. Cybersecurity-Konzept als Risikomanagementprozess .....	260
I. Analyse der Risiken .....	261
1. Verpflichtende Risikoanalyse .....	263
2. Ausgestaltung .....	265
a) Risikoidentifikation .....	266
aa) Lokalisierung der Schutzgüter .....	266
bb) Mögliche Risiken .....	267
cc) Relevante IT-Risikquellen .....	269



b) Risikobewertung .....	269
c) Compliance-Risikoanalyse .....	271
II. Steuerung der Risiken .....	271
1. Rechtliche Grundlagen .....	272
2. Steuerungsmöglichkeiten .....	272
a) Risikoakzeptanz .....	273
b) Risikovermeidung .....	275
c) Risikotransfer .....	276
d) Risikoreduzierung .....	276
III. Auswahl der Maßnahmen .....	276
1. Rechtliche Rahmenbedingungen .....	277
2. Technische Maßnahmen .....	278
a) Allgemeine Maßnahmen .....	278
b) Wahrung des Stands der Technik .....	281
3. Organisatorische Maßnahmen .....	283
4. Physische Maßnahmen .....	283
5. Personelle Maßnahmen .....	284
6. Cyberversicherungen .....	284
a) Aufbau einer Cyberversicherung .....	285
aa) Basis-Baustein .....	286
bb) Service- und Kostenbaustein .....	287
cc) Drittschaden-Baustein .....	288
dd) Eigenschaden-Baustein .....	288
ee) Lösegeld-Baustein .....	288
b) Vorgaben zum Sicherheitsniveau .....	289
c) Pflicht zum Abschluss einer Cyberversicherung .....	291
IV. Umsetzung der Maßnahmen .....	293
V. Zwischenergebnis .....	293
E. Rechtliche Beschränkungen von IT-Sicherheitsmaßnahmen .....	294
I. Arbeitsrechtliche Problemfelder .....	295
1. Mitbestimmung des Betriebsrats .....	295
2. Arbeitnehmerhaftung .....	296
II. Datenschutzrechtliche Problemfelder .....	297
III. Strafrechtliche Problemfelder .....	298
F. Überprüfung und Überwachung .....	298
I. Anleihen des allgemeinen Aktienrechts .....	299
II. Konkrete Anforderungen an die Überwachung .....	300
1. Prozessintegrierte Überwachung .....	301
2. Prozessunabhängige Überwachung .....	303

G. Anpassungen .....	304
H. Dokumentation .....	306

## *Kapitel 9*

<b>Response: Business-Continuity</b>	<b>308</b>
A. Business-Continuity-Management-System .....	309
I. Spezialgesetzliche Grundlagen .....	310
II. Verpflichtende Einrichtung eines BCMS .....	311
III. Ausgestaltung .....	313
IV. Leitlinie des BCMS .....	314
V. Verhältnis zu anderen Managementsystemen .....	315
B. Organisation .....	316
I. BC-Aufbauorganisation .....	317
II. Besondere Aufbauorganisation und das Notfallteam .....	318
1. Aufgaben des Notfallteams .....	318
2. Zusammensetzung des Notfallteams .....	319
3. Involvierung des Vorstands .....	321
III. Externe Berater .....	322
C. Notfallkonzept .....	324
I. BCM-Analysen .....	324
II. BC-Strategien .....	326
III. Umsetzung der Strategien .....	327
1. IT-Notfallpläne .....	328
2. IT-Notfallhandbuch .....	328
D. Bewältigung .....	329
I. Chronologischer Ablauf der Bewältigung .....	330
II. Ausgewählte Maßnahmen .....	332
1. Systeme zur Angriffserkennung .....	332
2. Datenrettung .....	332
3. Alternative Prozesse und Ressourcen .....	333
4. IT-Forensik zur Angriffsanalyse .....	334
III. Rechtliche Maßnahmen .....	335
IV. Nachgelagerte Maßnahmen .....	336
E. Interne Kommunikation .....	337
I. Initialmeldung und Informationskette bei Cyberincidents .....	337
1. Initialmeldung .....	337
2. Informationskette .....	338

3. Informationssystem während der Bewältigung .....	340
II. Kommunikation von Entscheidungen .....	341
III. Offenlegung gegenüber Beratern und Ermittlungsbehörden .....	341
F. Meldepflichten .....	341
I. DSGVO .....	342
1. Art. 33 Abs. 1 DSGVO .....	343
2. Art. 34 Abs. 1 DSGVO .....	345
II. BSIG .....	345
III. Vertragliche Meldepflichten .....	347
G. Insiderrecht und Ad-hoc-Publizität .....	348
I. Adressat der Ad-hoc-Publizitätspflicht .....	348
II. Cyberincident als Insiderinformation .....	350
1. Präzise Information .....	351
2. Unmittelbare Betroffenheit .....	352
3. Nicht öffentlich bekannt .....	352
4. Kursbeeinflussungspotential .....	353
III. Veröffentlichungspflicht .....	356
1. Kenntnis des Emittenten .....	357
2. Informationssystem des Unternehmens .....	359
a) Informationserkennung .....	360
b) Informationsweiterleitung .....	360
c) Informationsbewertung .....	361
d) Informationsveröffentlichung .....	361
3. Überprüfungszeit .....	362
IV. Aufschieben der Veröffentlichung .....	363
1. Berechtigte Interessen .....	363
a) Allgemein .....	364
b) Berechtigtes Interesse im Rahmen eines Cyberincidents .....	366
2. Keine Irreführung der Öffentlichkeit .....	368
3. Sicherstellung der Geheimhaltung .....	370
a) Weitergabe der Insiderinformation .....	371
b) Cyberspezifische Probleme der Geheimhaltung .....	373
c) Fehlende Geheimhaltung wegen Kenntnis des Cyberangreifers .....	375
d) Meldepflichten eines Cyberincidents im Rahmen der Geheimhaltung .....	377
4. Aufschiebungsentscheidung .....	378
a) Zuständiges Organ .....	379
b) Beurteilungsspielraum .....	380
5. Veröffentlichung von Zwischenschritten .....	381
6. Rechtsfolge und Meldepflicht .....	382
V. Verfahren und Inhalt .....	382

VI. Zwischenergebnis .....	383
H. Externe Kommunikation .....	384
I. Aufgaben .....	385
II. Konsequenzen für die Unternehmensorganisation .....	386
III. Relevante Gruppen .....	386
1. Mitarbeiter des Unternehmens .....	387
2. Aktionäre .....	387
3. Geschäfts- und Vertragspartner .....	388
4. Breite Öffentlichkeit .....	389
I. Rechtliche Rahmenbedingungen von Lösegeldzahlungen .....	389
I. Allgemeines .....	390
II. Strafrechtliche Relevanz .....	391
III. Anderweitige gesetzliche Verstöße .....	393
IV. Aktienrechtliche Implikationen .....	394
1. Annahme der Strafbarkeit/Rechtswidrigkeit .....	394
2. Unklare Rechtslage .....	396
3. Unternehmensinteresse .....	396
V. Zwischenergebnis .....	397
J. Kontrolle und Verbesserung .....	398
K. Dokumentation .....	399

## *Kapitel 10*

<b>Gesetzlicher Regelungsbedarf für Cybersecurity</b>	401
A. Möglichkeit der Formulierung abstrakter Vorgaben .....	401
I. Regelungsbedarf .....	402
1. Cybersecurity-Vorgaben als Flickenteppich .....	402
2. Gefahr der Organhaftung .....	403
a) Tatbestandliche Voraussetzungen .....	403
b) Enthaftung .....	404
c) Folgen .....	405
3. Positive Effekte einer Regelung .....	405
II. Gründe gegen eine Regelung .....	406
III. Schutzgut einer Regelung .....	407
IV. Regelungsqualität .....	408
1. Lagebericht .....	409
2. DCGK .....	409
V. Zwischenergebnis .....	412

B. Regelungsbedarf nach NIS2UmsuCG .....	412
I. Regelungsinhalt .....	413
1. Anwendungsbereich .....	413
2. IT-Risikomanagement .....	414
3. Katalog technischer und organisatorischer Maßnahmen .....	414
4. Geschäftsleiterpflichten .....	415
II. Übertragbarkeit auf die allgemeine AG .....	416
III. Zwischenergebnis .....	417
C. Ansatzpunkte und Inhalte einer möglichen Regelung .....	418
I. Anwendungsbereich .....	418
II. Regelungskonzepte .....	419
1. Prinzipienbasierte Regelung .....	419
2. Regelungskonzepte in Zusammenarbeit mit staatlichen Stellen .....	420
III. Konkrete Regelungsvorschläge .....	422
1. Angemessenheit und Wirksamkeit .....	422
2. Technische und organisatorische Maßnahmen .....	423
3. Stand der Technik .....	424
4. Informationssicherheitsbeauftragter .....	424
IV. Mehrwert einer prinzipienbasierten Regelung .....	425
V. Regelung auf Ebene des Aufsichtsrats .....	426
VI. Zwischenergebnis .....	427

## *Kapitel 11*

<b>Thesen</b>	429
---------------	-----

<b>Literaturverzeichnis</b> .....	432
-----------------------------------	-----

<b>Stichwortverzeichnis</b> .....	452
-----------------------------------	-----

## 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.<sup>1</sup> 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.<sup>2</sup>

## **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.<sup>3</sup> Daneben existieren aber auch unternehmensinterne Gefahrenquellen, insbesondere verursacht durch die eigenen Mitarbeiter.<sup>4</sup> 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.<sup>5</sup> In der Summe stellen solche Cyberrisiken sowie daraus folgende Betriebsunterbrechungen nach

---

<sup>1</sup> *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.

<sup>2</sup> *Podebrad/Gabel*, in: Gabel/Kiefner/Heinrich, Rechtshandbuch Cyber-Security, Kap. 1 Rn. 1.

<sup>3</sup> BSI, Pressemitteilung 6. Februar 2023.

<sup>4</sup> Siehe hierzu Kapitel 2: B. II.

<sup>5</sup> Handelsblatt, IT-Chaos bringt Lufthansa in Erklärungsnot, 15. Februar 2023.



einschlägigen Umfragen mittlerweile die größte Gefahr für Unternehmen dar.<sup>6</sup> Regelmäßig wird diesen sogar existenzgefährdendes Potential zugesprochen.<sup>7</sup> Dabei ist die Bedrohung für Unternehmen insgesamt im Cyberraum „so hoch wie nie“.<sup>8</sup> Gleichzeitig ist eine digitale Abstinenz für Unternehmen heutzutage nicht mehr möglich.<sup>9</sup> Vielmehr „durchdringt“ die Nutzung von IT und des Internets die Wirtschaft „in immer größerem Maße“.<sup>10</sup> 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.<sup>11</sup> 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.<sup>12</sup> 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.<sup>13</sup>

---

<sup>6</sup> 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.

<sup>7</sup> Siehe hierzu Kapitel 3: E. I.

<sup>8</sup> BSI, Lagebericht des Bundesamts für Sicherheit in der Informationstechnik 2022, 11.

<sup>9</sup> 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.

<sup>10</sup> RegBegr. IT-Sicherheitsgesetz, BT-Drs. 18/4096, 1.

<sup>11</sup> 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.

<sup>12</sup> Siehe hierzu unter Kapitel 2: B. II.

<sup>13</sup> 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.<sup>14</sup> 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.<sup>15</sup> Allerdings gibt es einen Fundus an gesetzlichen Vorgaben, die in diesem Bereich relevant sein können. Hier lassen sich grundsätzlich zwei Regelungsquellen unterscheiden.<sup>16</sup> Auf der einen Seite stehen die allgemeinen Vorgaben des AktG<sup>17</sup>. 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.<sup>18</sup> 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-

---

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

<sup>15</sup> *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.

<sup>16</sup> 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.

<sup>17</sup> Aktiengesetz, 6. September 1965, BGBl. 1965 I S. 1089.

<sup>18</sup> *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.