

Inhaltsverzeichnis

Abkürzungen	8
1. Kapitel: Einleitung	15
2. Kapitel: Tatsächliche und rechtliche Ausgangslage bei Cyber-Angriffen	19
A. Formen von Cyber-Angriffen	20
I. Systembasierte Angriffe („Hacking“)	20
1. Schadsoftware („Malware“)	21
a) Übertragungsmechanismus	21
b) Schadwirkung	22
c) Insbesondere: Ransomware-Angriff	23
2. Netzwerkvermittelte Angriffe	24
3. Anwendungsvermittelte Angriffe	25
II. Nutzerbasierte Angriffe („Social Engineering“)	26
1. „Fake President“-Betrugsmasche	26
2. „Phishing“	27
III. Cyber-Angriffe im weiteren Sinne	28
B. Schäden durch Cyber-Angriffe	29
I. Eigenschäden	29
II. Zivilrechtliche Haftungsschäden	30
1. Vertragliche Haftung	31
2. Deliktische Haftung	32
III. Öffentlich-rechtliche Sanktionen	33
C. Anspruchsgegner und Anspruchsverfolgung	34
I. Arbeitnehmer	34
II. IT-Dienstleister	37
III. Verkäufer und Hersteller von Software	38
IV. Zahlungsdienstleister	40
V. Versicherungen	42
VI. Organhaftung als letzter Ausweg	43

3. Kapitel: Pflicht des Geschäftsführers zum Risikomanagement	45
A. Bestandteile eines Risikomanagementsystems im betriebswirtschaftlichem Sinne	47
B. Rechtsquellen zur Einrichtung von Risikomanagementsystemen in der GmbH	48
I. Gesellschaftsrecht	49
1. § 91 Abs. 2 AktG	49
a) Reichweite des § 91 Abs. 2 AktG	50
aa) Früherkennungssystem	50
bb) Überwachungssystem	52
b) Anwendbarkeit auf die GmbH	55
aa) Zielsetzungen des KonTraG	56
bb) Strukturelle Unterschiede zwischen GmbH und Aktiengesellschaft	57
cc) Ausnahme nach Hommelhoff	58
(1) Kapitalmarktorientierte GmbH	59
(2) GmbH mit paritätisch besetztem Aufsichtsrat	59
(3) Zwischenergebnis	61
2. § 91 Abs. 3 AktG	61
3. § 43 Abs. 1 GmbHG	63
II. Restrukturierungsrecht (§ 1 Abs. 1 StaRUG)	67
III. Aufsichtsrecht	69
IV. Anderweitige Risikomanagementansätze (z. B. LkSG, GwG)	70
C. Zwischenergebnis	70
4. Kapitel: Pflicht des Geschäftsführers zum Cyber-Risikomanagement	73
A. Cyber-Risiken als Gegenstand der Risikovorsorge	73
B. Verantwortlichkeiten für das Cyber-Risikomanagement	75
I. Rechtsquellen der Pflicht zum Cyber-Risikomanagement	76
1. Allgemeine Sorgfaltspflichten	77
2. § 91 Abs. 2 AktG analog	77
3. Branchenspezifische Vorgaben	78

II. Mitverantwortlichkeit der Gesellschafter im Rahmen der Risikobewertung	80
1. Primäre Zuständigkeit der Gesellschafter	81
2. Subsidiäre Zuständigkeit des Geschäftsführers	84
III. Zwischenergebnis	87
C. Bestandteile des Cyber-Risikomanagements	88
I. Risikoerkennung	90
1. Risikoidentifizierung	91
2. Risikoanalyse	93
a) Eintrittswahrscheinlichkeit	93
b) Auswirkungen des Eintritts	94
3. Risikobewertung	95
II. Risikosteuerung	96
1. Organisatorische Maßnahmen	97
a) Koordinierung von Zuständigkeiten	97
b) Notfallplan/CIRP	99
c) Personalmanagement	100
aa) IT-Richtlinie	100
(1) Private IT-Nutzung durch Arbeitnehmer	101
(2) BYOD-Konzepte	102
(3) IT-Schutz im Homeoffice	103
(4) Weitere Regelungsgegenstände	104
bb) Schulungen	105
cc) Überwachung	106
(1) Privatnutzung von Internet und E-Mail	107
(2) „Social Engineering“-Tests	110
dd) Arbeitsrechtliche Sanktionen	111
ee) Zwischenergebnis	112
2. Technische Maßnahmen	112
a) Sicherheitssoftware	112
b) IT-Personal	115
c) Datensicherheit	115
aa) Verfügbarkeits- und Integritätskontrolle	116
bb) Vertraulichkeitskontrolle	118
3. Krisenmanagement im Ernstfall	119
a) Wiederherstellung des Geschäftsbetriebs	120
b) Beweissicherung	120
c) Einhaltung gesetzlicher Meldepflichten	121

d) Kommunikationsstrategie	121
e) Umgang mit Lösegeldforderungen	122
4. Risikotransfer: Cyber-Versicherung	123
a) Umfang des Versicherungsschutzes	124
aa) Versichertes Risiko	124
bb) Versicherungsfall	126
cc) Risikoausschlüsse	127
(1) Krieg und kriegsähnliche Handlungen	127
(2) Geldstrafen und Bußgelder	128
(3) Erpressungs- und Lösegelder	129
b) Vorteile einer Cyber-Versicherung	130
III. Überwachung	131
D. Zwischenergebnis	132
5. Kapitel: Haftung des Geschäftsführers für Verstöße gegen die Pflicht zum Risikomanagement	133
A. Innenhaftung gegenüber der GmbH	133
I. Geltendmachung von Ersatzansprüchen	134
II. Pflichtverletzungen des Geschäftsführers im Zusammenhang mit dem Cyber-Risikomanagement	135
1. Risikoerkennung	137
a) Risikoidentifizierung	138
aa) Eingeschränkter Schutz durch die Business Judgment Rule	138
bb) Mittelbare Bedeutung für die Risikosteuerung	139
cc) Inhaltliche Mindestanforderungen an die Risikoidentifizierung	139
b) Risikoanalyse	141
c) Risikobewertung	141
2. Risikosteuerung	143
a) Mindestanforderungen an den IT-Schutz	144
b) Haftungsrechtliche Besonderheiten bei Cyber- Versicherungspolicen	146
aa) Verpflichtung zum Abschluss einer Cyber- Versicherung?	146

bb) Auswirkungen bestehenden Versicherungsschutzes auf die Haftung des Geschäftsführers	147
3. Überwachung	149
4. Ergebnis	150
III. Enthaftende Tatbestände	150
1. Weisung oder Billigung durch die Gesellschafterversammlung	150
2. Entlastung, Verzicht und Vergleich	152
3. Delegation	152
4. D&O-Versicherung	155
IV. Verschuldensmaßstab: Haftungserleichterung nach den arbeitsrechtlichen Grundsätzen des innerbetrieblichen Schadensausgleichs	157
1. Historische Entwicklung der Rechtsprechung zum innerbetrieblichen Schadensausgleich	157
2. Heutige Rechtslage	160
3. Begründungsansätze für eine Übertragbarkeit des arbeitsrechtlichen Haftungsprivilegs auf Geschäftsführer	162
a) Direkte Anwendung: Geschäftsführer als Arbeitnehmer?	162
aa) § 611a BGB	162
bb) Europarechtlicher Arbeitnehmerbegriff	163
b) Analoge Anwendung	164
aa) Keine abschließende Regelung der Organhaftung im GmbH-Recht	166
bb) Entgegenstehende Wertungen des Gesellschaftsrechts	167
(1) Gläubigerschutz	168
(2) Gesellschafterschutz	170
(3) Zwischenergebnis	174
cc) Vergleichbarkeit von Geschäftsführer und Arbeitnehmer	175
(1) Beherrschen des Betriebsrisikos	175
(aa) Rechtliche Einflussnahmemöglichkeiten	176
(bb) Vorrang der tatsächlichen Weisungsgebundenheit	178

Inhaltsverzeichnis

(cc) Zwischenergebnis	180
(2) Vertrauens- bzw. Fürsorgeerwägungen	181
(3) Fremdnützigkeit	185
(4) Verfassungsrechtliche Begründung	187
(5) Ergebnis	188
B. Zivilrechtliche Außenhaftung des Geschäftsführers	189
I. Deliktsrecht	190
II. Datenschutzrecht?	193
C. Exkurs: Strafrechtliche Verantwortlichkeit des Geschäftsführers	194
I. Strafbewehrte Offenbarung von Geheimnissen	194
II. Datenschutzstrafrecht	195
III. Verletzung der Aufsichtspflicht (§§ 130, 9 Abs. 1 Nr. 1 OWiG)	196
IV. Untreue (§ 266 StGB)	197
6. Kapitel: Zusammenfassung	201
Literaturverzeichnis	203