Inhaltsverzeichnis

Teil 1: Cyberangriffe – Problemstellung und Grundlagen 19

A. Problemaufriss und Anlass der Untersuchung 19
I. Aktualität und Praxisrelevanz 19
II. Gefahrenpotential 25
III. Unzureichende Sensibilisierung und Vorbereitung auf Unternehmensebene 29
IV. Fehlende Rechtssicherheit 31
V. Vielfältige Anknüpfungspunkte für eine Vorstandshaftung 32

B. Gegenstand und Gang der Untersuchung 34

C. Hintergründe und Erscheinungsformen von Cyberangriffen 36
I. Begriff des Cyberangriffs 36
II. Schädigungsformen 39
1. Allgemeines 39
2. Konkrete Arten von Cyberangriffen 41
a. Malware 41
b. Ransomware 43
c. DoS-/DDoS-Angriffe 45
d. APT-Angriffe 46
e. Phishing 47
III. Person des Schädigers 49

Teil 2: Pflichtenprogramm des Vorstands im Zusammenhang mit Cyberangriffen 53

A. Pflichten zur Unterbindung von Cyberangriffen („*Cyber-Incident-Prevention*“) 53
I. Rechtliche Rahmenbedingungen 54
1. Aktienrechtliche Pflichten 54
a. Einrichtung eines Früherkennungs- und Überwachungssystems, § 91 Abs. 2 AktG 54
aa. Cyberangriffe als bestandsgefährdende Entwicklung 55
bb. Aussagegehalt von § 91 Abs. 2 AktG 57

b. Einrichtung eines internen Kontrollsystems und Risikomanagementsystems, § 91 Abs. 3 AktG 58
c. Allgemeiner Leitungsauftrag und Sorgfaltsmaßstab, §§ 76 Abs. 1, 93 Abs. 1 AktG 60
aa. Rechtsdogmatische Einordung 60
bb. Terminologie 62
cc. Abgeleitetes Pflichtenprogramm 65
(1). Legalitätspflicht 65
(2). Legalitätskontrollpflicht 66
(3). Allgemeine Schadensabwendungspflicht 68
dd. Allgemeine Kriterien bei der Ermessensausübung 71
2. Datenschutzrechtliche Pflichten 73
a. Adressat der Pflichten der DSGVO 74
b. Cybersicherheitsbezogene Anforderungen der DSGVO 75
c. Verhältnis zum aktienrechtlichen Pflichtenprogramm 77
d. Spannungsverhältnis zwischen Datenschutz und IT-Sicherheit 79
3. Kapitalmarktrechtliche Pflichten 80
a. Pflichten nach dem Kreditwesengesetz (KWG) 80
aa. Anwendungsbereich 80
bb. Regelungsgehalt und Auswirkungen auf Cybersicherheit 81
cc. Übertragbarkeit der Vorgaben der MaRisk und BAIT auf das allgemeine Aktienrecht 84
b. Pflichten nach dem Wertpapierhandelsgesetz (WpHG) 86
c. Pflichten nach dem Zahlungsdiensteaufsichtsgesetz (ZAG) 87
d. Pflichten nach dem Börsengesetz (BörsG) 88
4. Regelungen des Geschäftsgeheimnis-Schutzgesetzes (GeschGehG) 88
a. Allgemeines 89
b. Relevanz des GeschGehG bei Cyberangriffen 90
aa. Diebstahl/Kopie von Geschäftsgeheimnissen 91
bb. Vernichtung von Geschäftsgeheimnissen 92
cc. Veröffentlichung von Geschäftsgeheimnissen 92

dd. Folgerungen für das Geheimnismanagement bei Cyberangriffen 94
5. Sektorspezifische Regelungen 95
II. Konkretes Pflichtenprogramm des Vorstands zur Gewährleistung von Cybersicherheit 99
1. Schritt 1: Analyse des Risikopotentials 101
2. Schritt 2: Risikosteuerung durch geeignete Maßnahmen 103
a. Prävention 104
aa. Organisatorische Maßnahmen 104
(1). Festlegung klarer Zuständigkeiten 104
(2). Ausarbeitung und Dokumentation eines IT-Sicherheitskonzepts 105
(3). Berechtigungskonzept und Zugriffsbeschränkungen 108
(4). Physische Sicherheit 108
(5). Mitarbeitersensibilisierung und interne Guidelines 110
(6). Personelle Organisation 112
(a). Chief Information Officer (CIO) 112
(b). Chief Information Security Officer (CISO) 113
(c). Datenschutzbeauftragter 113
(d). IT-Sicherheitsbeauftragter 115
(7). Geheimnismanagement 117
bb. Technische Maßnahmen 120
(1). Technische Mindeststandards 120
(2). Mitarbeiterüberwachung 122
(3). Stand der Technik 125
(4). Informationstechnische Normen und Standards 130
(5). Externe Dienstleister und IT-Sicherheitsaudits 131
b. Vorbereitung des Ernstfalls 132
aa. Zuständigkeitsordnung 133
bb. Notfallkonzept 134
cc. Sicherstellung der Protokollierung des Cyberangriffs 135
dd. Abschluss einer Cyber-Versicherung 136

3. Schritt 3: Vornahme regelmäßiger Überprüfungen und Anpassungen 141

B. Pflichten bei Realisierung eines Cyberangriffs („*Cyber-Incident-Response-Management*") 143

I. Rechtliche Rahmenbedingungen 143

1. Aktienrechtliche Pflichten 143

2. Datenschutzrechtliche Pflichten 144

a. Meldung an die Datenschutz-Aufsichtsbehörde 144

aa. Voraussetzungen 144

bb. Zeitpunkt der Meldung 147

cc. Inhalt der Meldung 148

dd. Teilmeldepflicht, Art. 33 Abs. 4 DSGVO 149

b. Benachrichtigung der betroffenen Personen 149

aa. Voraussetzungen 149

bb. Zeitpunkt der Benachrichtigung 151

cc. Inhalt der Benachrichtigung 153

dd. Ausnahmetatbestand, Art. 34 Abs. 3 DSGVO 154

c. Meldung an den Verantwortlichen im Falle der Auftragsverarbeitung 154

3. Kapitalmarktrechtliche Pflichten 155

a. Vorliegen einer Insiderinformation 155

aa. Präzise Information 155

bb. Nicht öffentlich bekannt 157

cc. Emittent unmittelbar betroffen 158

dd. Erhebliches Kursbeeinflussungspotential 158

(1). Anzuwendender Maßstab 158

(2). Potentielle Kursrelevanz von Cyberangriffen 160

(3). Konkrete Beurteilungskriterien 160

(4). Bezugspunkt der Ad-hoc-Mitteilung 162

b. Pflicht zur unverzüglichen Veröffentlichung 163

c. Bisherige Praxis 164

d. Aufschub der Veröffentlichung, Art. 17 Abs. 4 MAR 166

aa. Zuständigkeit 166

bb. Berechtigtes Interesse am Aufschub 166

(1). Gefahr irrationaler Kursverluste 167

(2). Gefahr weiterer Cyberangriffe 169

cc. Keine Irreführung der Öffentlichkeit 170

dd. Gewährleistung der Vertraulichkeit 170
(1). Relevanz von Gerüchten 171
(2). Spannungsverhältnis zu bestehenden Meldepflichten 172
ee. Provisorische Selbstbefreiung 174
e. Besonderheiten bei Ransomware 174
aa. Vorliegen einer Insiderinformation 175
(1). Präzise Information 175
(2). Erhebliches Kursbeeinflussungspotential 175
(a). Empirische Daten 176
(b). Bezugspunkt der Ad-hoc-Mitteilung 178
(aa). Zeitpunkt vor Lösegeldzahlung bzw. vor Ablauf der Zahlungsfrist 179
(bb). Zeitpunkt nach Zahlung des Lösegeldes bzw. nach Ablauf der Zahlungsfrist 180
bb. Aufschub 181
f. Besonderheiten bei der Erlangung einer Insiderinformation durch den Angreifer 183
4. Sektorspezifische Regelungen 185
II. Konkretes Pflichtenprogramm 185
1. Klärung der Zuständigkeit 186
2. Analyse und Bewältigung des Angriffs 187
3. Entscheidung über die Zahlung eines Löse-/Erpressungsgeldes 189
a. Bestehen von Ermessensspielraum 190
aa. Strafbarkeit der Zahlung des Lösegeldes 190
bb. Relevanz von Empfehlungen öffentlicher Stellen 193
b. Entscheidung im Rahmen des unternehmerischen Ermessens 194
4. Melde- und Anzeigepflichten 198
5. Öffentlichkeitsarbeit 198
6. Aufklärung, Beweissicherung und Anspruchsverfolgung 199
7. Interne Konsequenzen 201
C. Zulässigkeit von Delegation und Outsourcing 202
I. Horizontale Delegation der IT-Sicherheitspflichten 203
1. IT-Sicherheit als delegationsfähiges Ressort 204
2. Anforderungen an die Delegation 205

3. Wiederaufleben der Gesamtzuständigkeit 206
II. Vertikale Delegation der IT-Sicherheitspflichten 207
1. Vertikale Delegation im Rahmen der Cyber-Incident-Prevention 208
2. Vertikale Delegation des Cyber-Incident-Response-Managements 210
III. Outsourcing der IT-Sicherheitspflichten 211
IV. Auslagerung der IT-Sicherheitspflichten bei Kredit- und Finanzdienstleistungsinstituten 213

Teil 3: Haftungsrisiken des Vorstands 219

A. Innenhaftung gegenüber der Gesellschaft 219
I. Haftungsvoraussetzungen des § 93 Abs. 2 S. 1 AktG 220
1. Anspruchsgegner 220
2. Pflichtverletzung 221
a. Prozessuale Ausgangslage 221
b. Pflichtverstöße im Einzelnen 225
aa. Keine oder unzureichende Auseinandersetzung mit Cyber-Risiken 225
bb. Verletzung der Legalitätspflicht 225
cc. Verletzung der Legalitätskontrollpflicht 226
dd. Unzureichend ausgestaltetes ISMS 227
ee. Unzureichende Dokumentation des ISMS 228
(1). Im Vorfeld des Cyberangriffs 228
(2). Bei Realisierung des Cyberangriffs 229
ff. Unvorteilhafte Vertragsgestaltung 230
gg. Fehler im Rahmen der Ad-hoc-Publizität 231
(1). Keine oder verspätete Veröffentlichung einer Insiderinformation 231
(2). Auswirkungen der Möglichkeit zur Selbstbefreiung 231
(a). Unterbliebene Prüfung einer Selbstbefreiung 231
(b). Entscheidung gegen eine Selbstbefreiung 233
(c). Entscheidung für eine Selbstbefreiung 233
c. Rechtsfolgen von Delegation und Outsourcing 234
aa. Rechtsfolgen unzulässiger Delegation 234

bb. Rechtsfolgen zulässiger Delegation 235
(1). Folgepflichten einer horizontalen Delegation 235
(2). Folgepflichten einer vertikalen Delegation 238
(a). Ordnungsgemäße Auswahl des IT-sicherheitsverantwortlichen Delegationsempfängers 239
(b). Ordnungsgemäße Instruktion und Einweisung des IT-sicherheitsverantwortlichen Delegationsempfängers 240
(c). Ordnungsgemäße Überwachung des IT-sicherheitsverantwortlichen Delegationsempfängers 240
(d). Hierarchische Stellung des IT-sicherheitsverantwortlichen Delegationsempfängers 241
(3). Folgepflichten eines Outsourcings 242
cc. Rechtsfolgen unterbliebener Delegation 245
d. Haftungsausschluss aufgrund der Business Judgement Rule 246
aa. Unternehmerische Entscheidung 247
bb. Handeln auf angemessener Informationsbasis 248
(1). Allgemeine Anforderungen 249
(2). Unsicherheitsfaktoren bei Cybersicherheit 250
(a). Unklare Rechtslage 252
(b). Fehlendes Fachwissen 255
cc. Handeln zum Wohle der Gesellschaft 256
dd. Freiheit von Interessenkollisionen und sachfremden Einflüssen 258
e. Widerlegung einer Pflichtverletzung 260
aa. Dokumentation des ISMS als Mindestvoraussetzung für eine Exkulpation? 260
bb. Erfüllung technischer Standards 261
(1). Meinungsspektrum 261
(2). Stellungnahme 264
cc. Regelmäßige Durchführung von IT-Sicherheitsaudits 268
3. Verschulden 269

4. Schaden der Gesellschaft 270
a. Allgemeine Grundsätze 271
b. Einzelne Schadenspositionen im Falle eingetretener Cyberangriffe 272
aa. Datenverlust 272
bb. Freiwillige Vermögensopfer der Aktiengesellschaft 274
(1). Aufwendungen zum Zwecke der Schadensbeseitigung und -minderung 275
(2). Aufwendungen zum Zwecke der Schadensaufklärung 276
(3). Aufwendungen zum Zwecke der Rechtsverfolgung 277
cc. Vermögensschaden durch Inanspruchnahme Dritter 278
(1). Vertragliche Inanspruchnahme Dritter 278
(2). Datenschutzrechtliche Inanspruchnahme Dritter 280
(3). Deliktische Inanspruchnahme Dritter 282
(4). Kapitalmarktrechtliche Inanspruchnahme Dritter 284
dd. Bußgeld 285
(1). Allgemeines 285
(2). Relevante Bußgeldtatbestände 288
(a). §§ 130, 30 OWiG 288
(b). § 120 Abs. 15 Nr. 6-11, Abs. 18 WpHG i.V.m. § 30 OWiG 290
(c). Art. 83 DSGVO 291
ee. Reputationsschaden 294
ff. Entgangener Gewinn 295
gg. Wettbewerbsnachteile 296
(1). Ausspähen von Daten 297
(2). Schlechtes Bonitätsrating 298
(3). Nachteile im Rahmen von M&A-Transaktionen 298
(4). Nachteile im Rahmen von Vergabeverfahren 299
hh. Abgeflossenes Geld 299
ii. Sonstige Schäden 301

5. Kausalität 302
a. Prozessuale Ausgangslage 303
b. Mittelbare Schadenspositionen 307
c. Vorsätzlicher Schädigungsakt eines Dritten 307
d. Rechtmäßiges Alternativverhalten 309
6. Subsidiarität der Haftung 311
a. Vorrangige Inanspruchnahme des Schädigers 311
aa. Keine Auswirkungen auf das Bestehen eines Schadens 311
bb. Haftungsbeziehung zwischen Cyberangreifer und Vorstand 312
cc. Prinzipielles Bestehen eines Gläubigerwahlrechts 314
dd. Einschränkung des Gläubigerwahlrechts 314
b. Vorrangige Inanspruchnahme eines externen IT-Security-Dienstleistungsunternehmens 316
7. Haftungsmilderung und -einschränkungen 317
II. Versicherungsrechtliche Aspekte 318
1. Eigener Versicherungsschutz der Aktiengesellschaft 318
a. Versicherbarkeit des Risikos durch die Aktiengesellschaft 318
aa. Herkömmliche Versicherungsformen 320
(1). Betriebshaftpflichtversicherung 320
(2). Sachversicherung 322
(3). Vertrauensschadenversicherung 323
bb. Cyber-Versicherung 325
(1). Allgemeines 325
(2). Relevante Ausschlusstatbestände 327
(a). Obliegenheitsverletzung 328
(b). Gefahrerhöhung 330
(c). Grob fahrlässige Herbeiführung des Versicherungsfalls 332
(d). Krieg 333
(e). Bußgeld 339
(f). Löse-/Erpressungsgelder 340
b. Entfall des Schadens aufgrund der Versicherungsleistung 340
aa. Anrechnung der Versicherungssumme nach den Grundsätzen über die Vorteilsausgleichung 340

bb. Gesetzlicher Forderungsübergang gem. § 86 Abs. 1 S. 1 VVG 342
(1). Vorstand als Dritter i.S.d. § 86 Abs. 1 S. 1 VVG 342
(2). Besonderheiten im Rahmen einer Cyber-Versicherung 344
(3). Auswirkungen auf die Grundsätze der Vorteilsausgleichung 347
c. Pflicht der Aktiengesellschaft zur Inanspruchnahme der Versicherung? 347
aa. Relevanz 348
bb. Bestehen eines Wahlrechts und dessen Einschränkungen 349
cc. Ausübung des Wahlrechts 353
2. Versicherungsschutz des Vorstands (D&O-Versicherung) 353
a. Bestehen von Versicherungsschutz dem Grunde nach 354
aa. Vorliegen eines Vermögensschadens 355
bb. Schäden im Zusammenhang mit Daten 356
b. Entfall des Versicherungsschutzes 358
c. Zusammentreffen von D&O-Versicherung und Cyber-Versicherung 359
B. Haftung gegenüber den Aktionären 360
C. Außenhaftung gegenüber Dritten 361
I. Deliktische Haftung gem. § 823 Abs. 1 BGB 362
1. Verletzung eines absoluten Rechtsguts 362
a. Insbesondere: Daten als absolutes Recht 363
b. Sonstige Rechte 365
2. Bestehen einer Garantenpflicht 368
a. Stand der Rechtsprechung 369
b. Stand der Literatur 372
c. Stellungnahme 375
II. Deliktische Haftung gem. § 823 Abs. 2 BGB 377
Teil 4: Schlussbetrachtung 379
A. Ausblick 379
B. Zusammenfassung der wesentlichen Ergebnisse 381
Literaturverzeichnis 395