

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

Aktienrechtliche Grundlagen der Cybersecurity 73

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

Relevanz von Spezialgesetzen und Soft Law 97

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

Relevanz von Cybersecurity für Vorstand und Aufsichtsrat	129
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-Grundsatz	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

Gesetzlicher Regelungsbedarf für Cybersecurity 401

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

Inhaltsübersicht	15
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
Literaturverzeichnis	432
Stichwortverzeichnis	452