Inhaltsverzeichnis

Abkürzungsverzeichnis XXI
Teil 1 – Einführung 1
A. Problemstellung 1
B. Gegenstand und Gang der Untersuchung 5
C. Begriff der Cyber-Risiken 8
D. Darstellung der Gefährdungslage 9
I. Angriffsarten 9
1. Schadsoftware 10
2. Phishing und Pharming 12
3. Bot-Netze und Denial-of-Service-Angriffe 12
4. Social Engineering 13
5. Advanced Persistent Threat 14
II. Ursachen auf Seiten des Angegriffenen 15
III. Urheber von Cyber-Angriffen 17
IV. Schadensarten 18
Teil 2 – Die Haftung für Cyber-Angriffe 21
A. Haftungsgrundlagen für Cyber-Angriffe 21
I. Spezialgesetzliche Haftungsgrundlagen 21
II. Vertragliche Haftung im Rahmen von § 280 Abs. 1 BGB ... 23
1. Verletzung von Hauptleistungspflichten 24
2. Schutzpflichtverletzung 24
a) Vorliegen einer Schutzpflicht hinsichtlich IT-Sicherheit 24
b) Umfang der Schutzpflicht 26
III. Deliktische Haftung 28
1. Löschung und sonstige Beeinträchtigung von Daten ... 29
a) Eigentumsverletzung 29
aa) Meinungsstand 30

(1) Keine Eigentumsverletzung 30
(2) Eigentumsverletzung am Datenträger 31
bb) Stellungnahme 32
(1) Datenlöschung 32
(2) Datenverschlüsselung und Datendiebstahl. 35
cc) Zwischenergebnis 37
b) Verletzung des Rechts am Besitz 37
c) Verletzung des Rechts am eingerichteten und ausgeübten Gewerbebetrieb 39
d) Verletzung eines Schutzgesetzes gem. § 823 Abs. 2 BGB 43
aa) Strafrechtliche Schutzvorschriften 43
bb) Datenschutzrecht, BSIG und TMG 45
e) Sittenwidrige vorsätzliche Schädigung gem. § 826 BGB 46
f) Lösungsvorschläge 47
aa) Recht am Datenbestand 47
(1) Kein sonstiges Recht i.S.v. § 823 Abs. 1 BGB 48
(2) Sonstiges Recht gem. § 823 Abs. 1 BGB 49
bb) Drittschadensliquidation 51
cc) Neues Schutzgesetz gem. § 823 Abs. 2 BGB .. 52
dd) Stellungnahme 52
(1) Recht am Datenbestand 52
(2) Schutzgesetz gem. § 823 Abs. 2 BGB 58
(3) Drittschadensliquidation 59
(4) Vorschlag de lege ferenda 60
(a) Erforderlichkeit einer eigenen Haftungsnorm 61

(b) Standort, Inhalt und Formulierungsvorschlag 62
2. Betriebsunterbrechungs-, Reputations- und Wiederherstellungsschäden 64
3. Ergebnis 67
B. Allgemeine Haftungsfragen 67
I. Anwendbares Recht und Gerichtszuständigkeit 67
1. Anwendbares Recht bei vertraglichen Schuldverhältnissen 68
2. Anwendbares Recht bei außervertraglichen Schuldverhältnissen 69
3. Gerichtszuständigkeit 73
II. Schadensfragen 75
1. Ersetzbare Schadenspositionen 75
a) Kosten für Dienstleistungsunternehmen 75
b) Abwehr und Feststellung des Schadens durch den Geschädigten 77
c) Vorsorgeaufwendungen und freiwillige Leistungen . 79
2. Schadensbemessung 81
III. Sorgfaltsmaßstab 83
1. Bestehende Normen mit IT-Sicherheitsbezug 83
2. Herleitung eines allgemeingültigen Sorgfaltsmaßstabs 85
a) Begriff der IT-Sicherheit 85
b) Gewährleistung von IT-Sicherheit 88
aa) Organisatorische und technische Vorkehrungen 88
bb) Stand der Technik 88
(1) Drei-Stufen-Theorie 89
(2) Folge für IT-Sicherheit 91
c) Umsetzung in geltendes Recht 93
IV. Verkehrssicherungspflichten 94

V. Mitverschulden 95
VI. Beweislastprobleme..... 99
1. Beweislastverteilung 99
2. Nachweisprobleme..... 102
C. Haftungsverhältnisse nach Cyber-Angriffen 103
I. Haftung des Angreifers 103
II. Haftung von Softwareherstellern 104
1. Vertragliche Haftung..... 104
a) Mängelgewährleistung 104
aa) Vertragstypologische Einordnung..... 104
bb) Vorliegen eines Mangels bei Gefahrübergang 106
cc) Schadensersatz neben der Leistung..... 109
dd) Vertretenmüssen 109
ee) Weitere Anspruchsvoraussetzungen.....111
b) Allgemeines Leistungsstörungsrecht 112
aa) Bereitstellung von Sicherheitsupdates als Hauptleistungspflicht 112
bb) Bereitstellung von Sicherheitsupdates als Nebenpflicht 113
cc) Updateverpflichtung durch Richtlinie über digitale Inhalte 117
c) Haftungsausschluss.....118
aa) Haftungsausschluss durch AGB.....118
(1) Haftungsausschlüsse.....119
(a) Ausschluss für fahrlässiges Verhalten..119
(b) Ausschluss bestimmter Schadensarten 121
(c) Begrenzung der Schadenshöhe..... 123
(d) Datensicherung und Versicherungsschutz 125

(e) Zwischenergebnis 126
(2) Haftungsprivilegierung für IT-Verträge 126
bb) Haftungsausschluss durch Individualvereinbarung 127
2. Deliktsrechtliche Haftung 128
a) Produkthaftung nach § 823 Abs. 1 BGB 128
aa) Verkehrssicherungspflichten 129
(1) Konstruktionsfehler 130
(2) Produktbeobachtungspflichten 132
(a) Meinungsstand 132
(b) Stellungnahme 134
(c) Zwischenergebnis 136
bb) Beweislastprobleme 136
b) Haftung nach § 823 Abs. 2 i.V.m. § 3 ProdSG 138
c) Haftung nach § 1 Abs. 1 ProdHaftG 139
3. Lauterkeitsrechtliche Haftung 139
4. Ergebnis 140
III. Haftung von IT-Dienstleistern 141
IV. Haftung von Geschäftsleitern für ungenügende IT-Sicherheit 142
1. Pflichtverletzung 143
a) Verletzung der Legalitätspflicht 144
b) Sorgfaltspflicht im engeren Sinne 145
c) Organisations- und Überwachungspflichten 146
aa) Allgemeine IT-Risikomanagementpflichten 147
bb) Spezialgesetzliche IT-Risiko-managementpflichten 151
d) Business Judgement Rule 152
aa) Voraussetzungen 152

bb) Anwendbarkeit bezüglich der Legalitätspflicht ... 154
2. Kausaler Schaden ... 156
3. Ergebnis ... 159
V. Haftung von Arbeitnehmern ... 159
VI. Haftung des Angegriffenen ... 161
1. Vertragliche Haftung ... 161
2. Deliktsrechtliche Haftung ... 162
a) Verkehrssicherungspflichten ... 162
aa) Einschränkungen ... 162
(1) Meinungsstand ... 162
(2) Stellungnahme ... 164
bb) Umfang ... 166
(1) Bekanntheit der Gefahr ... 166
(2) Notwendigkeit und Zumutbarkeit ... 168
(3) Konkretisierung durch technische Standards ... 170
cc) Konkrete Maßnahmen ... 171
(1) Antivirensoftware ... 171
(2) System- und Softwareupdates ... 174
(3) Dekonnektieren ... 176
(4) Unternehmensbezogene Maßnahmen ... 177
b) Kausalität ... 178
3. Ergebnis ... 179
D. Zusammenfassung ... 180
Teil 3 – Die Cyber-Versicherung ... 183
A. Überblick: Die Cyber-Versicherung ... 183
B. Grundlegende Fragestellungen ... 185
I. Versicherbarkeit von Cyber-Risiken ... 185
1. Betriebswirtschaftliche Versicherbarkeit ... 185

a) Eindeutigkeit des Risikos 186
b) Zufälligkeit des Schadensereignisses 187
c) Bewertbarkeit des Schadens 188
d) Unabhängigkeit der Risiken 189
2. Rechtliche Versicherbarkeit 192
a) Lösegeldzahlungen 193
b) Geldbußen 195
aa) Meinungsstand 196
bb) Stellungnahme 197
3. Ergebnis 199
II. Spartenabgrenzung und versicherungsvertragliche Einordnung 200
III. Auslegung von Versicherungsbedingungen 203
C. Darstellung der gegenwärtigen Versicherungsbedingungen .. 205
I. Aufbau der Versicherungsbedingungen 206
II. Allgemeine bausteinübergreifende Regelungen 207
1. Gegenstand der Versicherung 207
a) Vermögensschäden 207
b) Schadensereignis 209
aa) GDV: Informationssicherheitsverletzung 209
(1) Beeinträchtigung der Verfügbarkeit, Integrität, Vertraulichkeit von elektroni-schen Daten oder informationsverarbeitenden Systemen 210
(2) Informationssicherheitsverletzung auslösende Ereignisse 213
(a) Angriffe auf elektronische Daten oder informationsverarbeitende Systeme 213
(b) Unberechtigte Zugriffe auf elektronische Daten 215

(c) Eingriffe in informationsverarbeitende Systeme 217
(d) Verletzung von datenschutzrechtlichen Vorschriften 218
(e) Schadprogramme 220
bb) Dreiteilung: Netzwerksicherheitsverletzung, Datenschutzverletzung, Datenvertraulichkeitsverletzung 221
(1) Datenschutzverletzung 222
(2) Datenvertraulichkeitsverletzung 223
(3) Netzwerksicherheitsverletzung 225
(4) Standort 226
cc) Ausländische Versicherungsbedingungen 227
dd) Stellungnahme und Definitionsvorschlag 229
(1) Standort, Inhaltlicher Aufbau und Begrifflichkeiten 230
(2) Konkrete Ausgestaltung 232
(a) Datenschutzverletzungen 232
(b) Verletzung der Vertraulichkeit von Daten 234
(c) Daten- und IT-Systemschäden 234
(3) Definitionsvorschlag 237
2. Versicherungsfall 238
a) Eintritt des Versicherungsfalls bei Cyber-Angriffen 238
b) Versicherungsfalldefinitionen in aktuellen Bedingungswerken 240
c) Stellungnahme 240
3. Versicherter Zeitraum 246
4. Serienschaden 248
a) Ursachenklausel 249

b) Erweiterte Ursachenklausel 251
aa) Inhalt 251
bb) Wirksamkeit 253
(1) Meinungsstand zu Ziff. 6.3 AHB, Ziff. 8.3 ProdHM, Ziff. 4.2 BHV-IT 253
(2) Stellungnahme und Klauselvorschlag 255
(a) Wirksamkeit nach §§ 307 Abs. 1 S. 1, Abs. 2 Nr. 1 BGB 255
(b) Wirksamkeit nach § 307 Abs. 1 S. 2 BGB 259
(c) Klauselvorschlag 260
5. Obliegenheiten 261
a) Obliegenheiten vor Eintritt des Versicherungsfalls 261
aa) Technische und organisatorische Maßnahmen 261
(1) Gewährleistung des Stands der Technik... 262
(2) Konkrete Maßnahmen zum Schutz der IT-Systeme 266
bb) Anzeigepflicht bei Gefahrerhöhung 269
(1) Begriff der Gefahrerhöhung 270
(2) Begrenzung durch Fragebögen 273
b) Schadensabwendungs- und -minderungsobliegenheit 275
aa) Beginn 276
bb) Umfang und Rettungskostenersatz 279
c) Rechtsfolgen bei Obliegenheitsverletzungen 281
6. Einschränkungen der Leistungspflicht 284
a) Überblick 284
b) Krieg- und Terrorausschluss 287
c) Herbeiführung des Versicherungsfalls 292
III. Deckungsbausteine 294

D. Deckungsüberschneidungen mit anderen Versicherungen 297
I. Abgrenzung zu anderen Versicherungen 299
1. Allgemeine Haftpflichtversicherung 299
a) Meinungsstand zum Sachschadenbegriff 299
b) Stellungnahme 301
2. BHV-IT 304
3. Sachversicherung 307
a) Sachschaden 307
b) Feuerversicherung und Einbruchdiebstahl- und Raubversicherung 310
c) Elektronik- und Maschinenversicherung 312
d) Betriebsunterbrechungsversicherungen 315
4. Vertrauensschadenversicherung 316
a) Schäden verursacht durch Vertrauensperson 317
b) Schäden verursacht durch Dritte 320
c) Zwischenergebnis 322
5. D&O-Versicherung 322
a) Vermögensschaden 323
b) Weitere Voraussetzungen 326
6. Spezielle IT-Versicherungskonzepte 327
7. Zusammenfassung 328
a) Deckungsüberschneidungen 328
b) „Silent Cyber“ 329
II. Rechtsfolge von Deckungsüberschneidungen 331
1. Grundsätzlich: Gesamtschuldner nach § 78 VVG 331
2. Sonderfall: Geschäftsleiterhaftung und D&O-Versicherung 334
3. Abbedingung von § 78 VVG 338
a) Auslegung von Ziff. A1-12 AVB-Cyber 339

aa) Abbedingung der gesamtschuldnerischen Haftung ... 341
(1) Wortlaut ... 342
(2) Sinn und Zweck ... 343
(3) § 305c Abs. 2 BGB ... 346
bb) Abbedingung des Wahlrechts des Versicherungsnehmers ... 347
(1) Wortlaut, Sinn und Zweck ... 348
(2) § 307 Abs. 1 S. 1 BGB ... 349
(3) Fehlen einer Rechtsfolge ... 350
cc) Lösungsmöglichkeiten ... 353
b) Kollisionsmöglichkeiten ... 356
aa) Kollision von Spezialitätsklausel mit Subsidiaritätsklausel ... 356
bb) Keine Subsidiaritätsklausel ... 359
cc) Kollision von zwei Subsidiaritätsklauseln ... 359
dd) Kollision von zwei Spezialitätsklauseln ... 362
4. Ergebnis ... 362
E. Zusammenfassung ... 364
Teil 4 – Zusammenfassung und Ausblick ... 367
A. Zusammenfassung der wesentlichen Ergebnisse in Thesen ... 367
I. Die Haftung für Cyber-Angriffe ... 367
II. Die Cyber-Versicherung ... 371
B. Ausblick ... 378
Quellenverzeichnis ... 385
A. Literatur ... 385
B. Versicherungsbedingungen ... 400
C. Sonstige Quellen ... 404