

Martin Hossenfelder

Pflichten von Internetnutzern zur Abwehr von Malware und Phishing in Sonderverbindungen



Nomos

Inhaltsverzeichnis

Abkürzungsverzeichnis	19
Einleitung	27
§ 1 Einführung	27
§ 2 Problemstellung	29
§ 3 Gang der Darstellung	34
Kapitel 1 Grundlagen der Schutzpflichtenlehre	37
§ 4 Schutzpflichten im Gesamtgefüge des Schuldrechts	37
I. Terminologie	37
II. Abgrenzung	38
1. Hauptleistungs- und Nebenleistungspflichten	38
2. Verkehrspflichten i. S. d. § 823 BGB	40
§ 5 Sonderverbindung, Schuldverhältnis und Schutzpflicht	41
I. Sonderverbindung	41
II. Schuldverhältnis	44
III. Die Einordnung vertragsbegleitender Schutzpflichten	45
1. Umschlagstheorie	45
2. Das einheitliche gesetzliche Schutzpflichtverhältnis	46
3. Deliktsrechtliche Einordnung von Schutzpflichten	47
4. Stellungnahme	47
§ 6 Normative Grundlagen	48
I. § 241 Abs. 2 BGB	49
1. Der Inhalt des Schuldverhältnisses	49
2. Die Bedeutung des Merkmals »kann«	50
3. Adressat der Schutzpflichten	50
4. Rechte, Rechtsgüter und Interessen	50
5. Zusammenfassung	51
II. § 242 BGB	51
1. Anwendbarkeit auf Schutzpflichten	51
a. Vor der Schuldrechtsreform	51
b. Nach der Schuldrechtsreform	51

c.	Stellungnahme	52
2.	Voraussetzungen	54
a.	Sonderverbindung	54
b.	Treu und Glauben mit Rücksicht auf die Verkehrssitte	55
c.	Interessenabwägung	55
aa.	Risikoordnung	56
bb.	Subjektive Elemente und Öffentliche Interessen	57
cc.	Der Einfluss der Grundrechte	57
3.	Zusammenfassung	58
§ 7	Zwischenergebnis	58
Kapitel 2 Kriterien zur Beurteilung von Schutzpflichten		61
§ 8	Vermeidbarkeit	62
I.	Faktische Möglichkeit der Schadensverhinderung	62
1.	Maßstab	62
2.	Verfügbarkeit	63
II.	Rechtliche Möglichkeit der Schadensverhinderung	63
III.	Abgrenzung	63
§ 9	Zumutbarkeit	64
I.	Dogmatische Grundlagen	65
1.	Zumutbarkeit als umfassender Rechtsgrundsatz	65
2.	Zumutbarkeit als regulatorisches Rechtsprinzip	66
3.	Zumutbarkeit als Interessenabwägung	67
4.	Zumutbarkeit und § 242 BGB	67
II.	Zumutbarkeit als Kriterium zur Schutzpflichtbestimmung	68
III.	Kriterien zur Ausfüllung des Begriffs der Zumutbarkeit	69
1.	Ausmaß der Gefahr	69
a.	Prüfungsgegenstand	69
b.	Gefahrneigung	70
aa.	Einwirkungsmöglichkeiten Dritter	71
bb.	Dauer der Sonderverbindung bzw. der Gefahr	72
2.	Wahrscheinlichkeit eines Schadenseintritts	72
a.	Wahrscheinlichkeit als Rechtsbegriff	72
aa.	Umgangssprachlicher und subjektiver Wahrscheinlichkeitsbegriff	73
bb.	Objektiver Wahrscheinlichkeitsbegriff	74
b.	Wahrscheinlichkeit bei fehlendem statistischen Datenmaterial	75
c.	Erfolgswahrscheinlichkeit von Schutzmaßnahmen	75

2.	Lösung bei beidseitigem Vertrauen auf verkehrsgerechtes Verhalten der anderen Seite	103
III.	Zumutbarkeit des Selbstschutzes	104
IV.	Zusammenfassung	105
§ 11	Einzelfallabhängige Kriterien	106
I.	Höherrangiges Recht	106
1.	Grundrechte	106
2.	Europarecht	107
II.	Mittelbare Wirkung von Sicherheitsregelungen	107
1.	Technische Regeln und öffentlich-rechtliche Sicherheitsvorgaben	107
a.	Verbindlichkeit solcher Regelungen	108
b.	Unverbindlichkeit solcher Regelungen	108
c.	Stellungnahme	109
2.	Empfehlungen	110
III.	Weitere Aspekte	110
§ 12	Zusammenfassung	111
Kapitel 3	Technik	113
§ 13	Bedrohungen	113
I.	Malware	113
1.	Klassifikation	114
a.	Viren	114
b.	Würmer	116
c.	Trojanische Pferde	116
d.	Mischformen	118
2.	Übertragungswege	118
II.	Potenziell gefährliche bzw. unerwünschte Programme	120
1.	Rootkits	120
2.	Dialer	120
3.	Spam	121
4.	Adware	121
III.	Besondere Formen des Identitätsdiebstahls und Identitätsmissbrauchs	122
1.	Phishing	122
2.	Pharming	123
3.	Man-in-the-middle-Angriffe durch DNS-Spoofing	124
§ 14	Schutzmöglichkeiten	125

I.	Malwareschutzprogramme	125
1.	Arten	125
2.	Erkennungsverfahren	126
3.	Updates	127
4.	Kosten	127
II.	Firewalls	128
1.	Arten	128
2.	Schutzumfang	129
III.	Sichere Einstellung und Aktualisierung der verwendeten Software	130
1.	Konfiguration von Browser und E-Mail-Programm	130
2.	Aktualisierung von Browser und Betriebssystem	131
IV.	Vorsichtiger Umgang mit E-Mails, Internet und fremder IT-Infrastruktur	131
V.	Ergebnis	132
Kapitel 4 Schutzpflichten zur Abwehr von Malware und Phishing		133
§ 15	Meinungsstand	134
I.	Rechtsprechung	134
1.	BGH, Urt. v. 24.04.2012, Az: XI ZR 96/11	134
2.	BGH, Urt. v. 04.03.2004, Az: III ZR 96/03	135
3.	BGH, Urt. v. 16.03.2006, Az: III ZR 152/05	136
4.	LG Köln, Urt. v. 21.07.1999, Az: 20 S 5/99	137
5.	LG Hamburg, Urt. v. 18.07.2001, Az: 401 O 63/00	137
6.	LG Stralsund, Urt. v. 22.02.2006, Az: 1 S 237/05	138
7.	LG Berlin, Urt. v. 11.08.2009, Az: 37 O 4/09; KG, Urt. v. 29.11.2010, Az: 26 U 159/09	138
8.	LG Berlin, Urt. v. 08.11.2011, Az: 21 O 80/11	140
9.	LG Landshut, Urt. v. 14.07.2011, Az: 24 O 1129/11	140
10.	LG Köln, Urt. v. 05.12.2007, Az: 9 S 195/07	141
11.	LG Nürnberg-Fürth, Urt. v. 28.04.2008, Az: 10 O 11391/07	141
12.	AG Wiesloch, Urt. v. 20.06.2008, Az: 4 C 57/08	143
13.	Störerhaftung bei W-LAN	143
a.	Pflicht zur Sicherung	143
b.	Übertragbarkeit auf die Malwareproblematik	144
14.	Zusammenfassung	145
II.	Literatur	146
1.	Sonderverbindungsspezifische Merkmale	146
2.	Malwareschutzmaßnahmen	147
a.	Malwareschutzprogramme	147

aa. Sorgfaltspflicht	147
bb. Updates	149
b. Firewalls	149
c. Weitere Maßnahmen	150
3. Verhalten bei Phishing	151
4. Zusammenfassung	152
§ 16 Malware- und Phishingschäden als Teil des allgemeinen Lebensrisikos	153
§ 17 Schutzpflichten innerhalb von Vertragsbeziehungen	154
I. Die unbeabsichtigte Weiterleitung von Schadprogrammen zwischen den Vertragsparteien	155
1. Abgrenzung	156
2. Typische Gefährdungen	157
3. Schutzpflichten	157
a. Vermeidbarkeit	157
aa. Die Reaktionsmöglichkeiten der Hersteller von Schutzsoftware	158
bb. Abschalten des Systems als Sonderfall	158
b. Zumutbarkeit	159
aa. Ausmaß der Gefahr	159
bb. Wahrscheinlichkeit eines Schadenseintritts	160
cc. Größe des Vermeidungsaufwands	161
(1) Malwareschutzprogramme und Firewalls	161
(2) Gefahrvermeidungsgefälle	162
(3) Interessenprinzip	162
(4) Zusammenfassung	164
dd. Bekanntheit der Gefahr	164
ee. Abwägung	165
c. Schutzwürdigkeit	166
aa. Schutzsoftware	166
(1) Vertrauensvorsprung zu Gunsten des Gefährdeten	167
(2) Unterschiede im Haftungsregime zwischen Unternehmern und Privaten	168
(a) Gesellschaftsrecht	169
(b) Datenschutzrecht	170
(c) Banken- und Wertpapierrecht	171
(d) Berufsrecht	172
(e) BSI-Grundschutzkataloge und ISO 27001	173
(f) Zusammenfassende Bewertung	174
(3) Mitverschulden und Tatbestandsausschluss	174
bb. Vorsichtiger Umgang mit E-Mails	176
cc. Datensicherung	177

d.	Einzelfallabhängige Kriterien	178
aa.	IT-Grundrecht und privatrechtliche Verträge	178
bb.	IT-Grundrecht und öffentlich-rechtliche Verträge	179
4.	Ergebnis	180
5.	Exkurs: Disclaimer in E-Mails	181
II.	Onlinebanking	182
1.	Typische Gefährdungen	183
2.	Risikoverteilung und Haftungsstruktur bei Zahlungsdiensten	183
a.	Risikoverteilung bei nicht autorisierten Zahlungen, § 675u BGB	184
b.	Schadensersatzansprüche der Bank, § 675v BGB	186
aa.	Begriffserklärung	186
(1)	Zahlungsauthentifizierungsinstrument	186
(2)	Personalisierte Sicherheitsmerkmale	187
bb.	Dreistufiges Haftungskonzept	187
cc.	Missbrauch beim Onlinebanking	188
c.	Zumutbarkeit des Schutzes vor unbefugtem Zugriff, § 675l BGB	189
3.	Schutzpflichten	190
a.	Vermeidbarkeit	190
b.	Zumutbarkeit	191
aa.	Ausmaß der Gefahr	191
bb.	Wahrscheinlichkeit eines Schadenseintritts	192
(1)	Malwarebasierte Angriffe	192
(2)	Phishing	193
cc.	Größe des Vermeidungsaufwands	194
(1)	Schutzsoftware	194
(a)	Kostenlose Schutzsoftware	194
(b)	Kostenpflichtige Schutzsoftware	194
(2)	Onlinebanking-Software	195
(3)	Aktualisierung des Browsers	196
(4)	Aktualisierung des Betriebssystems	196
(5)	Erkennung von Phishing	196
(6)	Nutzung sicherer Infrastruktur	197
(7)	Mitteilungspflichten	197
(8)	Gefahrvermeidungsgefälle	198
(9)	Interessenprinzip	199
dd.	Bekanntheit der Gefahr	199
ee.	Abwägung und Einteilung nach Fahrlässigkeitsgraden	200
(1)	Abgrenzung von einfacher und grober Fahrlässigkeit	200

(a)	Einfache Fahrlässigkeit	200
(b)	Grobe Fahrlässigkeit	201
(2)	Bewertung einzelner Schutzmaßnahmen	202
(a)	Schutzsoftware	202
(b)	Aktualisierung von Browser und Betriebssystem, Nutzung sicherer Infrastruktur und Mitteilungspflichten	204
(c)	Erkennung von Betrugsversuchen	204
c.	Schutzwürdigkeit	206
aa.	Unsichere Authentifizierungsverfahren	206
bb.	Mängel bei der Aufklärung des Kunden	208
cc.	Verwirrung des Kunden	209
dd.	Abwägung nach Verschuldensgraden	209
d.	Allgemeine Geschäftsbedingungen	210
aa.	Verstoß gegen zwingendes Recht	211
bb.	Spezifische Schutzpflichten	213
cc.	Geheimhaltungsklauseln	214
4.	Ergebnis	216
III.	Onlinezahlungsdienste	217
1.	Klassifizierung	218
a.	Pre-Paid- und Pay-Now-Systeme	218
b.	Pay-Later-Systeme	219
2.	Typische Gefährdungen	219
3.	Vertragliche Einordnung	220
a.	Anwendbarkeit deutschen Rechts	220
b.	Zahlungsdiensterecht, §§ 675c ff. BGB	220
aa.	Zahlungsdienste	220
bb.	Die Haftungsverteilung bei Missbrauchsfällen	221
(1)	Grundsatz: Verschuldensabhängige Haftung	222
(2)	Ausnahme: Verschuldensunabhängige Haftung	222
(3)	Ausnahmen für elektronisches Geld und Kleinbetragsinstrumente, § 675i BGB	223
(a)	§ 675i Abs. 3 BGB	223
(b)	§ 675i Abs. 2 Nr. 3 BGB	226
(c)	Zwischenergebnis	227
4.	Schutzpflichten	228
a.	Vermeidbarkeit	228
b.	Zumutbarkeit	228
aa.	Ausmaß der Gefahr	228
bb.	Wahrscheinlichkeit eines Schadenseintritts	229
cc.	Größe des Vermeidungsaufwands	230

dd.	Bekanntheit der Gefahr	231
ee.	Abwägung und Einteilung nach Fahrlässigkeitsgraden	231
(1)	Schutzsoftware	231
(2)	Aktualisierung von Browser und Betriebssystem und Nutzung sicherer Infrastruktur	232
(3)	Erkennung von Betrugsversuchen und Mitteilungspflichten	232
c.	Schutzwürdigkeit	233
aa.	Unsichere Authentifizierungsverfahren	233
bb.	Mängel bei der Aufklärung des Kunden	233
d.	Allgemeine Geschäftsbedingungen	234
aa.	Verstoß gegen zwingendes Recht	234
bb.	Geheimhaltungsklauseln	235
cc.	Exkurs: Verstoß gegen Onlinebanking- Sonderbedingungen durch Weiterleitung personalisierter Sicherheitsmerkmale	236
5.	Ergebnis	237
IV.	Onlinehandel	237
1.	Abgrenzung	238
2.	Typische Gefährdungen	238
3.	Rechtliche Einordnung der Beziehung zwischen Onlinehändler und Accountinhaber	238
4.	Schutzpflichten	240
a.	Vermeidbarkeit	240
b.	Zumutbarkeit	240
aa.	Ausmaß der Gefahr	240
bb.	Wahrscheinlichkeit eines Schadenseintritts	241
cc.	Größe des Vermeidungsaufwands	241
dd.	Bekanntheit der Gefahr	242
ee.	Abwägung	242
c.	Schutzwürdigkeit	242
aa.	Unsichere Authentifizierungsverfahren	242
bb.	Mängel bei der Aufklärung des Kunden	243
5.	Ergebnis	244
V.	Internetdienste mit Kommunikationsinhalten	244
1.	Typische Gefährdungen	244
2.	Vertragliche Einordnung	245
a.	Bereitstellung eines E-Mail-Accounts	245
b.	Soziale Netzwerke	246
3.	Schutzpflichten	247
a.	Vermeidbarkeit	247

b.	Zumutbarkeit	247
aa.	Ausmaß der Gefahr	247
bb.	Wahrscheinlichkeit eines Schadenseintritts	247
cc.	Größe des Vermeidungsaufwands	248
dd.	Bekanntheit der Gefahr	249
ee.	Abwägung	249
c.	Schutzwürdigkeit	250
aa.	Unsichere Authentifizierungsverfahren	250
bb.	Mängel bei der Aufklärung des Kunden	250
d.	Allgemeine Geschäftsbedingungen	250
4.	Ergebnis	251
VI.	Vergleich des Regelungssystems der §§ 675c ff. BGB mit der allgemeinen Haftungsordnung bei Identitätsmissbräuchen	252
1.	Unterschiede	252
a.	Verschuldensabhängige Haftung	252
b.	Verschuldensunabhängige Haftung	253
2.	Analoge Anwendung des § 675v BGB auf weitere Fälle des Identitätsmissbrauchs im Internet	254
a.	Planwidrige Regelungslücke	254
b.	Vergleichbare Interessenlage	255
VII.	Exkurs: Die Haftung des Arbeitnehmers für Malware- und Phishingschäden	256
1.	Betrieblich veranlasste Tätigkeit	256
a.	Betrieblich veranlasste Internet- und E-Mail-Nutzung	257
b.	Private Internet- und E-Mail-Nutzung	258
2.	Einteilung nach Fahrlässigkeitsgraden	259
3.	Schutzwürdigkeit des Arbeitgebers	259
VIII.	Zusammenfassung	260
§ 18	Schutzpflichten innerhalb vorvertraglicher Schuldverhältnisse	261
I.	Aufrufen von Internetseiten mit Vertragsabschlussmöglichkeit	261
1.	Typische Gefährdungen	261
2.	Websitebesuch als Fall des § 311 Abs. 2 Nr. 2 BGB	262
3.	Schutzpflichten	263
a.	Vermeidbarkeit	263
b.	Zumutbarkeit	263
aa.	Ausmaß der Gefahr	263
bb.	Wahrscheinlichkeit eines Schadenseintritts	264
cc.	Größe des Vermeidungsaufwands	264
dd.	Bekanntheit der Gefahr	264
ee.	Abwägung	265
c.	Schutzwürdigkeit	265

II. Zusammenfassung	266
§ 19 Schutzpflichten innerhalb von Gefälligkeitsverhältnissen	267
I. Abgrenzung	267
II. Einteilung nach alltäglichen Gefälligkeiten und Gefälligkeitsverhältnissen	268
III. Sorgfaltsmaßstab und Haftungsprivilegierung	269
IV. Ergebnis	270
Kapitel 5 Durchsetzbarkeit und Rechtsfolgen	273
§ 20 Schadensersatz und Rücktritt	273
I. Schadensersatz	273
1. Anspruchsgrundlagen	273
2. Schadensberechnung und Schadensumfang	274
3. Rechtmäßiges Alternativverhalten	276
II. Rücktritt	277
§ 21 Anspruch auf Erfüllung von Schutzpflichten	278
I. Abgrenzung	278
II. Voraussetzungen	280
III. Übertragbarkeit auf Malware- und Phishingfälle	281
§ 22 Anwendbarkeit der §§ 320, 273 BGB	282
I. Verweigerung einer Leistungspflicht bei Vernachlässigung von Schutzpflichten	282
II. Verweigerung einer Schutzpflicht bei Vernachlässigung von Leistungspflichten	283
III. Verweigerung einer Schutzpflicht bei Vernachlässigung von Schutzpflichten	284
Kapitel 6 Zusammenfassung der Ergebnisse	285
§ 23 Ergebnisse zur Prüfung von Schutzpflichten	285
§ 24 Ergebnisse zu Schutzpflichten im Umgang mit Malware und Phishing	286
Literaturverzeichnis	289
Stichwortverzeichnis	313