

Inhaltsverzeichnis

Abkürzungsverzeichnis	15
§ 1 Einleitung	17
A) Problemstellung	17
B) Ziel der Dissertation und Forschungsfragen	23
§ 2 Grundlagen	27
A) Begriffsbestimmung	27
B) Politisch-historische Grundlagen	32
I. Spannungsfeld von öffentlicher Sicherheit und IT-Sicherheit	32
II. Von Cryptowars zu „Hack-Backs“	33
C) Informationstechnische Grundlagen	40
I. IT-Sicherheitslücken und IT-Sicherheit	41
II. IT-Sicherheitslücken und behördliche Aufgabenerfüllung	47
III. Zugriffsmethoden und deren Auswirkungen auf die IT-Sicherheit	54
1. Verpflichtung zur Implementierung von Hintertüren	54
2. Staatliches Hacken der IT-Systeme selbst	59
3. Sonstige Zugriffsmethoden	67
IV. Zusammenfassung	68
§ 3 Verfassungsrechtliche Vorgaben für den Umgang mit IT-Sicherheitslücken	71
A) Grundrechtliche Vorgaben	71
I. Beschaffung	72
1. Pflicht zu Hintertüren in IT-Produkten	72
a) Nutzersicht	73
aa) Umfassender Zugriff auf IT-Systeme	73
(1) Grundrecht auf IT-Sicherheit	74
(a) Vorbemerkung: Name des Grundrechts	74

(b) Schutzbereich	77
(aa) Vertraulichkeit	79
(bb) Integrität	83
(α) Bedeutung: Schließen einer Schutzlücke	84
(β) Konflikt mit dem europäischen Datenschutzkonzept?	91
(γ) Apersonales Grundrecht?	95
(δ) Integritätsschutz über die Eigentumsfreiheit?	96
(ε) Zusammenfassung	98
(cc) Informationstechnische Systeme	100
(dd) Anwendbarkeit auf juristische Personen	105
(c) Eingriff	106
(d) Rechtfertigung	109
(aa) Verhältnismäßigkeitsprinzip	110
(α) Legitimes Ziel	110
(β) Geeignetheit	110
(γ) Erforderlichkeit	113
(δ) Angemessenheit	115
(bb) Wesensgehaltsgarantie	123
(cc) Menschenwürdekern	128
(2) Verhältnis zu explizit benannten Freiheitsrechten	131
(3) Willkürverbot	137
bb) Zugriff auf gesperrte IT-Systeme	140
(1) Grundrecht auf IT-Sicherheit	140
(a) Schutzbereich	140
(b) Eingriff	141
(c) Rechtfertigung	141
(2) Sonstige Grundrechte	143
cc) Zugriff auf laufende Kommunikation	143
(1) Telekommunikationsgeheimnis	143
(a) Schutzbereich	144
(b) Eingriff	146
(c) Rechtfertigung	146
(aa) Verhältnismäßigkeit	146

(bb) Wesensgehaltsgarantie	149
(2) Sonstige Grundrechte	150
b) Herstellersicht	151
aa) Berufsfreiheit	152
(1) Schutzbereich	152
(2) Eingriff	153
(3) Rechtfertigung	156
bb) Vereinigungsfreiheit	158
cc) Allgemeine Handlungsfreiheit	158
dd) Willkürverbot	160
c) Zusammenfassung	160
2. Ankauf von Zero-Days von Dritten	162
a) Grundrecht auf IT-Sicherheit	162
aa) Schutzbereich	162
bb) Eingriff	165
b) Sonstige Grundrechte	167
3. Suche nach Zero-Days	167
II. Verhalten nach der Kenntnisnahme von Zero-Days	167
1. Geheimhalten von Zero-Days	168
a) Schutzpflicht oder Abwehrrecht?	168
b) Schutzpflichten in der allgemeinen Grundrechtsdogmatik	169
aa) Dogmatische Herleitung grundrechtlicher Schutzpflichten	169
bb) Voraussetzungen für das Vorliegen von Schutzpflichten	170
cc) Reichweite von Schutzpflichten	172
c) Schutzpflichtdimension des Grundrechts auf IT- Sicherheit	176
aa) Herleitung der Schutzpflichtdimension	176
bb) Folgen für den Konflikt um Zero-Days	186
(1) Entscheidung des BVerfG zu IT- Sicherheitslücken	186
(2) Dogmatische Einordnung der Entscheidung	190
(a) Schutzpflichtdogmatik	190
(b) Wesentlichkeitsgedanke	195
cc) Verhältnis zu explizit benannten Freiheitsrechten	197

Inhaltsverzeichnis

dd) Zusammenfassung	203
2. Meldung von Zero-Days an Hersteller	204
3. Warnung der Öffentlichkeit vor Zero-Days	205
a) Grundrecht auf IT-Sicherheit	205
aa) Schutzbereich	205
bb) Eingriff	205
cc) Rechtfertigung	207
b) Berufsfreiheit	207
aa) Schutzbereich	207
bb) Eingriff	207
cc) Rechtfertigung	209
III. Untätigkeit	210
B) Kompetenzrechtliche Vorgaben	212
I. Vertikale Kompetenzverteilung	213
1. Entscheidung über den Umgang mit Zero-Days	214
a) Umfang der Bundeskompetenz	214
aa) Kompetenz zum Hacken	214
bb) Kompetenz aus der Natur der Sache	215
cc) Kompetenz für die Zusammenarbeit und für Zentralstellen im Sicherheitsbereich	215
dd) Kompetenz für das Recht der Wirtschaft	220
ee) Kompetenz für das Postwesen und die Telekommunikation	221
ff) Kompetenz für die Zusammenarbeit bei der IT- Infrastruktur	221
gg) Zusammenfassung	222
b) Problem der Doppelzuständigkeit	223
c) Zusammenfassung	226
2. Warnung vor Zero-Days	226
II. Horizontale Kompetenzverteilung	229
III. Zusammenfassung	231
C) Sonstige verfassungsrechtliche Vorgaben	232
I. Funktionsvorbehalt für die Ausübung hoheitlicher Befugnisse	232
II. Rechtsstaatsprinzip	234

§ 4 Regelung des Umgangs mit IT-Sicherheitslücken im einfachen Recht	237
A) Entscheidung über den Umgang mit Zero-Days	237
I. Regelungen in Gesetzen, die den Einsatz zur Quellen-TKÜ erlauben	238
II. Gesetze, die Art. 27 JI-RL umsetzen	242
III. Cybersicherheitsrechtliche Schutzvorschriften	249
IV. Meldestandard des IT-Planungsrats	253
V. Zusammenfassung	258
B) Warnung vor Zero-Days	258
§ 5 Europarechtliche Vorgaben für den Umgang mit IT-Sicherheitslücken	261
A) Primärrechtliche Vorgaben	261
I. Hintertüren	261
1. Anwendungsbereich der GRCh	262
2. Nutzersicht	265
a) Zugriff auf IT-Systeme während der Nutzung	265
aa) Recht auf Achtung des Privatlebens	265
(1) Schutzbereich: Pendant zum Grundrecht auf IT-Sicherheit?	265
(2) Einschränkung	269
(3) Rechtfertigung	270
bb) Grundrechte als allgemeine Rechtsgrundsätze	271
b) Zugriff auf gesperrte IT-Systeme	271
c) Zugriff auf laufende Kommunikation	271
d) Zusammenfassung	273
3. Herstellersicht	273
a) Unternehmerische Freiheit	273
b) Recht auf Achtung des Privatlebens	274
4. Anwendbarkeit nationaler Grundrechte	274
II. Zero-Days	276
1. Schutzpflicht aus Recht auf Achtung des Privatlebens?	276
2. Bedeutung einer Schutzpflicht für den Umgang mit Zero-Days	277
B) Sekundärrecht	281
I. NIS-2-RL	281

Inhaltsverzeichnis

II. ePrivacy-RL	284
III. DSGVO	284
IV. JI-RL	285
V. Rechtsakt zur Cybersicherheit	286
VI. Ausblick: Die Cyberresilienz-Verordnung	286
§ 6 Anpassungsvorschläge	289
A) Nationale Ebene	289
I. Verfassung	289
II. Einfache Gesetze	290
1. Abwägungskriterien	293
2. Zuständigkeit und Abwägungs- und Entscheidungsprozess	300
3. Formulierungsvorschlag	306
B) Europäische Ebene	313
§ 7 Zusammenfassung und Ausblick	315
Literaturverzeichnis	319