

Inhaltsverzeichnis

A. Einführung	1
I. Bedeutung von Daten und ihre Verschlüsselung	1
II. Auswirkungen auf den staatlichen Schutz	2
III. Gang der Untersuchung	4
B. Die Kryptographie	7
I. Grundbegriffe: Gegenstand der Kryptographie	7
1. Terminologie	7
a) Kryptographie, Kryptoanalyse und Kryptologie	7
b) Ver- und Entschlüsselung, Klar- und Geheimtext	8
c) Abgrenzung zu steganographischen Verfahren	9
2. Zielsetzungen der Kryptographie	9
3. Rechtshistorische Einordnung	10
II. Kryptographische Verfahren	15
1. Symmetrische Verschlüsselung	15
2. Asymmetrische Verschlüsselung („public key“-Verschlüsselung)	17
3. Kombination aus symmetrischer und asymmetrischer Verschlüsselung (Hybride Verschlüsselung)	19
4. Hashfunktionen	20
III. Der Begriff der Sicherheit	21
1. Absolute und relative Sicherheit	22

Inhaltsverzeichnis

2. Ausgangsszenarien	23
3. Angriffsmethoden	24
a) „Brute-Force“-Angriff	24
b) Wörterbuchangriff	25
c) Seitenkanalangriffe	25
d) Weitere Angriffsvarianten	26
4. Ergebnis	27
IV. Rechtlicher Rahmen der Kryptographie de lege lata	27
1. Rechtlicher Rahmen in Deutschland	28
a) Ausfuhr kryptographischer Produkte	29
b) Nutzung kryptographischer Verfahren	31
c) Mitwirkung Dritter bei der Entschlüsselung	31
2. Rechtlicher Rahmen in anderen EU-Staaten	35
a) Ausfuhr kryptographischer Produkte	35
b) Nutzung kryptographischer Verfahren	35
c) Mitwirkung Dritter bei der Entschlüsselung	36
d) Zusammenfassung des rechtlichen Rahmens in anderen EU-Staaten	37
3. Rechtlicher Rahmen in anderen Nicht-EU-Staaten	38
a) Nutzung kryptographischer Verfahren in liberalen Rechtsordnungen	38
b) Nutzung kryptographischer Verfahren in restriktiven Rechtsordnungen	40
4. Ergebnis	42
C. Staatliche Regulierung kryptographischer Verfahren	43
I. Ziel und Darstellung nationaler Regulierungsvorschläge	43
1. Nationales Ziel einer Regulierung	43
2. Darstellung der potenziellen, begrenzenden, regulatorischen Maßnahmen	45
a) Festlegung maximaler Schlüssellängen	46

Inhaltsverzeichnis

b) „Backdoors“	47
c) Hinterlegung von Schlüsseln	49
d) Mitwirkungspflicht des Verschlüsselungsnutzers	52
II. Umsetzung und Durchsetzung der regulatorischen Maßnahmen	55
1. Verstoß gegen europäisches Recht	55
a) Anwendbarkeit der JI-RL	55
b) Verstoß gegen die JI-RL	58
2. Durchsetzung der rechtlichen Regulierung	60
a) Die Durchsetzungsschwierigkeiten im Ausgangspunkt	60
b) Strafrechtliche Verfolgung als Lösung der Durchsetzungsschwierigkeiten	61
c) Verstoß gegen Art. 3 Abs. 1 GG	63
III. Die betroffenen Grundrechte	64
1. Art. 10 Abs. 1 GG: Fernmeldegeheimnis	64
2. Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG: Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme	67
3. Art. 5 Abs. 1 GG: Recht der freien Meinungsäußerung	71
4. Ergebnis	73
IV. Eingriff in das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme aus Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG	74
1. Prüfungsmaßstab des Eingriffs	74
2. Eingriff durch die Festlegung maximaler Schlüssellängen	76
3. Eingriff durch „backdoors“	79
4. Eingriff durch „key escrow“	80

V. Rechtfertigung des Eingriffs in das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme aus Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG	82
1. Legitimer Zweck und Geeignetheit einer Regulierung kryptographischer Verfahren	83
2. Erforderlichkeit einer Regulierung	85
3. Verhältnismäßigkeit im engeren Sinne	88
a) Prüfungsmaßstab: Gewicht des Eingriffs	88
aa) Schwerer Eingriff	88
bb) Milderung des schweren Eingriffs durch sektorspezifische Ausnahmen?	93
b) Anlass bzw. Zweck eines Eingriffs	95
c) Anlass der Regulierung der Verschlüsselung	97
d) Maßnahme gegen den Gefahrverantwortlichen	100
e) Zugriff auf den Kernbereich	103
4. Ergebnis	106
 D. Geheimhalten der Kenntnis von Sicherheitslücken: „Zero-Day“-Schwachstellen	109
I. Definition einer „Zero-Day“-Schwachstelle	109
II. Fragestellung	113
III. Rechtmäßigkeit des Geheimhaltens von „Zero-Day“-Schwachstellen	115
1. Einfachgesetzliche Vorgaben im Umgang mit Sicherheitslücken	115
2. Vorgaben des Verfassungsrechts für „Zero-Day“-Schwachstellen	116
a) Konkrete staatliche Schutzpflicht	116

b) Ausgestaltung der konkreten staatlichen Schutzpflicht	121
aa) Staatliche Schutzpflicht und Geheimhalten einer „Zero-Day“-Schwachstelle – Vergleich mit den „Steuer-CDs“	123
bb) Zusammenfassung der Ergebnisse	126
3. Kenntnis und Geheimhalten von Sicherheitslücken durch den Staat	128
a) Nachrichtendienste des Bundes	129
b) Bundeskriminalamt	130
c) Bundesamt für Sicherheit in der Informationstechnik (BSI)	131
d) Ergebnis	133
4. Kriterien des BSI zur Risikobewertung einer Sicherheitslücke	133
5. Rechtslage de lege lata im Verhältnis zur verfassungsrechtlichen Schutzpflicht	135
a) NIS-2-Richtlinie	136
aa) Ziele der NIS-2-Richtlinie und der Schwachstellen-Meldeprozesse	137
bb) Meldepflichten nach der NIS-2-Richtlinie	139
b) JI-Richtlinie	141
aa) Verarbeitung personenbezogener Daten	141
bb) Risiko und Folge eines Verarbeitungsvorgangs	142
cc) Geplante Verarbeitungsvorgänge und geplante Abhilfemaßnahmen	143
dd) Ergebnis	144
c) Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG)	145
d) „Verbindliches Meldeverfahren zum Informationsaustausch über IT-Sicherheitsvorfälle“ vom 05.10.2017	148

Inhaltsverzeichnis

e) Allgemeine Verwaltungsvorschrift über das Meldeverfahren gemäß § 4 Abs. 6 BSIg	151
f) Die Polizeigesetze der Länder und die StPO	153
g) Struktur des BSI	155
aa) Aufgaben und Struktur des BSI	156
bb) Konkurrenz zu den IT-Sicherheitsbehörden der Länder	159
cc) Ergebnis	160
6. Ergebnis	161
IV. Rechtlicher Rahmen de lege ferenda:	
Lösungsansätze	161
1. Abwägungskriterien de lege ferenda	164
a) Wahrscheinlichkeit der Aufdeckung der Sicherheitslücke	165
b) Wahrscheinlichkeit der Schließung der Sicherheitslücke	166
c) Wahrscheinlichkeit der Entwicklung eines Patches	168
d) Sektorspezifische Begrenzung der Missbrauchsmöglichkeiten einer Sicherheitslücke	169
e) Anwendungsbereich des betroffenen Produkts	170
f) Nutzen für bestimmte Sicherheitsbehörden	171
g) Schwere der „Zero-Day“-Sicherheitslücke	172
h) Zeitliche Komponente	173
i) Ergebnis	174
2. Strukturierung des Umgangs mit „Zero-Day“-Schwachstellen	175
a) Neugestaltung der Behördenstruktur	176
aa) Unabhängiges Bundesinstitut zur technischen Bewertung	176
bb) Entfall der Aufsicht durch das BMI	177
cc) Einrichtung eines zentralen Sekretariats	180
dd) Ergebnis	182

Inhaltsverzeichnis

b) Neustrukturierung des Meldeverfahrens	182
c) Rechtliche Kontrolle des Geheimhaltens einer „Zero-Day“-Schwachstelle	185
aa) Kontrolle durch die Judikative	186
(1) Präventiver Richtervorbehalt	186
(2) Nachträgliche gerichtliche Kontrolle	189
bb) Kontrolle innerhalb der Exekutive	189
cc) Kontrolle durch das Parlament	190
(1) Frage- und Informationsrechte des Parlaments	190
(2) Parlamentarisches Kontrollgremium	193
(3) Berichtspflicht an das Parlament	196
d) Stärkere Transparenz und Information	197
e) Ergebnis	199
 E. Schlussteil	 201
I. Zusammenfassung und Ausblick	201
II. Zusammenfassung in Thesen	203
 Literaturverzeichnis	 207