

Inhaltsverzeichnis

Einleitung	23
I. Forschungsrahmen	28
II. Gang der Untersuchung	28

1. Kapitel

Technische und organisatorische Grundlagen	33
A. Begriffsbestimmung	33
I. Definition des NIST	34
II. Definition des BSI	37
III. Zusammenfassung	37
B. Erscheinungsformen	38
I. Cloud-Betriebsmodelle	39
1. Public Cloud	39
2. Private Cloud	41
3. Community Cloud	44
4. Hybrid Cloud	45
5. Virtual Private Cloud	47
II. Cloud-Servicemodelle	48
1. Infrastructure as a Service (IaaS)	51
a) Charakteristika	51
b) IaaS in der Praxis	53
(1) Amazon Elastic Compute Cloud (Amazon EC2)	54
(2) Amazon Simple Storage Service (Amazon S3)	54
2. Platform as a Service (PaaS)	55
a) Charakteristika	55
b) PaaS in der Praxis	56
3. Software as a Service (SaaS)	57
a) Charakteristika	57
b) SaaS in der Praxis	58
4. Zusammenfassung	60

C. Referenzarchitektur	62
I. Ressourcenschicht	62
II. Virtualisierungsschicht	64
1. Virtuelle Maschinen	65
2. Virtual Machine Monitor	67
III. Serviceschicht	70
IV. Netzwerkschicht	74
V. Managementplattform	76

2. Kapitel

Insiderbedrohungen	83
A. Cybercrime-as-a-Service	84
B. Tätertypologische Betrachtung	86
I. Mitarbeiter der Cloud-Anbieter	90
II. Mitarbeiter der Subunternehmer	91
III. Nutzerseite	92
C. Tatmotive	93
D. Exemplarische Angriffsvektoren	94
I. Ressourcenschicht	97
II. Virtualisierungsschicht	99
III. Serviceschicht	110
IV. Netzwerkschicht	112
V. Managementplattform	115

3. Kapitel

Allgemeiner strafrechtlicher Schutz vor Kenntnisaufnahme und Verschaffung	119
A. Ausspähen von Daten, § 202a StGB	122
I. Geschütztes Rechtsgut	122
II. Tatobjekt	124
III. Nicht für den Täter bestimmt	129
1. Verfügungsberechtigung über die Daten	129
a) Eigentum am Datenträger	130
b) Inhaltliche Betroffenheit	131
c) Geistige Urheberschaft	132
d) Kenntnis vom Benutzerpasswort	132

e) Geheimhaltungsinteresse	133
f) Skripturakt	133
2. Bestimmung des Verfügungsberechtigten	135
a) Allgemeine Grundsätze	135
b) Spezialfälle	143
(1) Sealed Cloud	143
(2) Split Cloud	145
IV. Gegen unberechtigten Zugang besonders gesichert	146
V. Zugangsverschaffung unter Überwindung der Zugangssicherung	153
1. Erfasste Angriffsmethoden der Innentäter	157
2. Strafbare Fälle der Datenspionage	162
VI. Unbefugt	168
VII. Weitere Voraussetzungen	169
VIII. Zusammenfassung	169
B. Abfangen von Daten, § 202b StGB	170
I. Nichtöffentliche Datenübermittlung, § 202b 1. Alt. StGB	171
1. Datenübermittlung	172
2. Nichtöffentlichkeit	176
II. Seitenkanalangriffe, § 202b 2. Alt. StGB	179
III. Unbefugte Datenverschaffung unter Anwendung technischer Mittel	180
IV. Zusammenfassung	182
C. Vorbereiten des Ausspähens und Abfangens von Daten, § 202c Abs. 1 StGB	184
I. Passwörter und Sicherungscodes, § 202c Abs. 1 Nr. 1 StGB	184
II. Schadprogramme, § 202c Abs. 1 Nr. 2 StGB	189
III. Zusammenfassung	193
D. Verletzung des Fernmeldegeheimnisses, § 206 Abs. 2 Nr. 1 StGB	194
I. Tauglicher Täterkreis	196
1. Telekommunikationsunternehmen	196
2. Beschäftigte der CaaS-Anbieter	200
3. Erweiterung des Täterkreises nach § 206 Abs. 3 StGB	203
II. Verschlüsselte Sendung	203
1. Sendung	204
2. Verschlüsselung	205
III. Zusammenfassung	206

4. Kapitel

Allgemeiner strafrechtlicher Schutz vor Weitergabe und Verwertung	208
A. Datenhehlerei, § 202d StGB	209
I. Tatgegenstand	210
II. Vollendete rechtswidrige Vortat	214
III. Sonstige Voraussetzungen	217
IV. Zusammenfassung	219
B. Verletzung des Fernmeldegeheimnisses, § 206 Abs. 1 StGB	219
I. Fernmelderelevante Tatsachen	220
II. Weitergabe von E-Mails, Text- oder Sprachnachrichten	224
III. Zusammenfassung	228
C. Verletzung und Verwertung von Privatgeheimnissen, §§ 203 Abs. 4, 204 Abs. 1 StGB	229
I. Tauglicher Täterkreis	232
1. § 203 Abs. 3 Satz 1 StGB	232
2. § 203 Abs. 3 Satz 2 StGB	235
II. Fremde Geheimnisse	243
III. Tathandlung	245
1. Offenbaren	245
2. Verwerten	247
IV. Sonstige Voraussetzungen	249
V. Unterlassene Verschwiegenheitserklärung, § 203 Abs. 4 Satz 2 StGB	252
VI. Zusammenfassung	255

5. Kapitel

Nebenstrafrechtlicher Schutz der Datenvertraulichkeit	256
A. Verrat von Geschäfts- und Betriebsgeheimnissen, § 17 UWG	256
I. Geschäfts- und Betriebsgeheimnisse als Tatobjekt	257
II. Geheimnisverrat, § 17 Abs. 1 UWG	261
III. Geheimnisausspähung und -verwertung, § 17 Abs. 2 UWG	263
1. Betriebsspionage, § 17 Abs. 2 Nr. 1 UWG	264
2. Geheimnishehlerei, § 17 Abs. 2 Nr. 2 UWG	266
IV. Weitere Tatbestandsvoraussetzungen	269
V. Zusammenfassung	271
B. Strafbarkeit nach § 148 Abs. 1 Nr. 1 TKG	274
I. Verstoß gegen das Abhörverbot aus § 89 Satz 1 TKG	275
1. Tatgegenstand	275

2. Tathandlung	277
II. Verstoß gegen das Mitteilungsverbot aus § 89 Satz 2 TKG	278
III. Zusammenfassung	278
C. Bußgeldnorm nach Art. 83 DSGVO	279
I. Anwendungsbereich	280
1. Sachlicher Anwendungsbereich	280
2. Räumlicher Anwendungsbereich	282
a) Niederlassungsprinzip, Art. 3 Abs. 1 DSGVO	283
b) Marktortprinzip, Art. 3 Abs. 2 lit. a DSGVO	287
c) Résumé	289
II. Ordnungswidrigkeit nach Art. 83 Abs. 4 lit. a, Abs. 5 lit. a DSGVO	289
1. Adressat der Bußgeldtatbestände	290
2. Bußgeldbewehrte Datenschutzverstöße nach Art. 83 Abs. 4 lit. a DSGVO ..	293
3. Bußgeldbewehrte Datenschutzverstöße nach Art. 83 Abs. 5 lit. a DSGVO ..	296
4. Verschuldenserfordernis	298
5. Rechtsfolge	301
III. Zusammenfassung	303
D. Strafvorschrift gem. § 42 BDSG	305
I. Anwendungsbereich	306
II. Tatgegenstand	307
III. Tauglicher Täter	310
IV. Tathandlungen des § 42 Abs. 1 BDSG	310
V. Tathandlungen des § 42 Abs. 2 BDSG	312
VI. Sonstige Voraussetzungen	313
VII. Zusammenfassung	314

6. Kapitel

Strafrechtlicher Schutz der Datenintegrität und -verfügbarkeit	317
A. Datenveränderung, § 303a StGB	317
I. Fremde Daten	318
II. Tathandlungen	324
1. Datenlöschung	325
2. Datenunterdrückung	327
3. Unbrauchbarmachen von Daten	330
4. Datenveränderung	331
III. Rechtswidrigkeit der Tathandlung	333
IV. Zusammenfassung	337

B. Computersabotage, § 303b StGB	337
I. Cloud als Datenverarbeitung von wesentlicher Bedeutung	339
II. Tathandlungen	344
1. Datenveränderung nach § 303a Abs. 1 StGB	344
2. Eingeben oder Übermitteln von Daten	345
3. Sabotagehandlungen am Cloud-System oder an Datenträgern	348
III. Erhebliche Störung der Datenverarbeitung als Taterfolg	352
IV. Qualifikation nach § 303b Abs. 2 StGB	354
V. Besonders schwere Fälle nach § 303b Abs. 4 StGB	355
VI. Zusammenfassung	357
C. Urkundenunterdrückung, § 274 Abs. 1 Nr. 2 StGB	357
I. Tatbestandsvoraussetzungen	357
II. Zusammenfassung	361
D. Verletzung des Fernmeldegeheimnisses, § 206 Abs. 2 Nr. 2 StGB	361
I. Anvertraute Sendung	362
II. Unterdrücken	365
III. Unbefugt	366
IV. Zusammenfassung	367

7. Kapitel

Anwendbarkeit des deutschen Strafrechts 369

A. Innentäter-Angriffe aus Deutschland	372
B. Innentäter-Angriffe aus dem Ausland	373
I. Betriebs- und Geschäftsgeheimnisse, § 5 Nr. 7 StGB	374
II. Geltung für Auslandstaten in anderen Fällen, § 7 StGB	375
III. Ubiquitätsprinzip, §§ 3, 9 StGB	381
1. Erfolgsdelikte	381
2. Abstrakte Gefährdungsdelikte	383
a) Ausdehnung des Handlungsorts	383
b) Erweiterung des Erfolgsorts	384
c) Fazit	387
C. Ausländische Angriffshandlung auf eine international verteilte Cloud-Infrastruktur	388
D. Innentäter-Angriff aus dem Ausland mittels inländischer Cloud-Server	391
E. Schutzbereich der verwirklichten Straftatbestände	393
I. Schutzbereich der §§ 202a ff. StGB	395

II. Schutzbereich der §§ 203, 204 StGB; § 206 StGB und § 17 UWG	395
III. Schutzbereich des § 42 BDSG	396
IV. Ergebnis zum Schutzbereich der deutschen Straf- und Bußgeldtatbestände	396
F. Zusammenfassung	397

8. Kapitel

Strafrechtlicher Schutz de lege ferenda 398

A. Schutz der Datenvertraulichkeit	398
I. Ergänzung der Tätergruppe des § 203 Abs. 1 StGB um „IT-Dienstleister“	400
II. Schaffung eines Straftatbestands der Datenuntreue, § 202d StGB-E	401
III. Änderungsbedarf des § 202a StGB	408
IV. Änderungsbedarf des § 202b StGB	410
V. Änderungsbedarf des § 202c StGB	411
VI. Änderungsbedarf des § 202d StGB	412
VII. Änderungsbedarf des § 205 StGB	412
B. Schutz der Integrität und Verfügbarkeit der Nutzerdaten	413
I. Änderungsbedarf des § 303a StGB	414
II. Änderungsbedarf des § 303b StGB	415
C. Strafanwendungsrecht	416
D. Internationale Strafverfolgung	420
Literaturverzeichnis	424
Sachverzeichnis	471