Inhaltsübersicht

Vorwort	7
Inhaltsübersicht	9
Inhaltsverzeichnis	10
Abkürzungen	21
Teil 1 Thematik der Arbeit, Übersicht über den Gang der Darstellung und technischer Hintergrund	23
Teil 2 Angriff	43
Teil 3 Verteidigung	167
Glossar	285
Literaturverzeichnis	291
Zitierte Internetquellen	308

Inhaltsverzeichnis

Vorwort 7

Inhaltsübersicht 9

Inhaltsverzeichnis 10

Abkürzungen 21

Teil 1 Thematik der Arbeit, Übersicht über den Gang der Darstellung und technischer Hintergrund 23

A. Thematik der Arbeit, Übersicht über den Gang der Darstellung 23

B. Technischer Hintergrund 25

I. Die Funktionsweise des Internets 25
II. Vorbereitung von Angriffen 26
1. Sammeln von Informationen 27
a) Portscanns 27
b) Systemanalyse 29
c) Ausspionieren von Passwörtern 30
aa) Social Engineering 30
bb) Raten von Passwörtern 30
cc) Knacken von Passwörtern 30
d) Sniffing in kabelgebundenen Netzen 31
e) Sniffing in Funknetzen 32
f) Angriff auf Switches 32
g) Entführen einer Sitzung (Session-Hijacking) 33
h) Analyse der elektromagnetischen Abstrahlung 33
2. Verbergen der eigenen Identität 34
a) Fälschung von MAC-Adressen 34
b) Fälschung von IP-Adressen 35
c) Manipulation von Logdateien 36
III. Missbrauch geenterter Systeme 36
1. Einsehen von Daten 36
a) Normalfall 36
b) Ausnutzen von Programmierfehlern 37
aa) Unerwartete Daten 37
bb) Pufferüberläufe 37
c) Funknetzwerke 38
2. Einrichtung von Hintertüren 39

IV. Denial-of-Service-Angriffe 39
V. Viren, Würmer und Trojaner 40
1. Viren 40
2. Würmer 40
3. Trojaner 41

Teil 2 Angriff 43

A. Vorbereitung 43

I. Sammeln von Informationen 43
1. Portscanns, Ausspähen von Daten, § 202a StGB 44
a) Daten 44
b) Übermittlung 45
c) „Nicht für den Scannenden bestimmt" 45
d) Zugangssicherung 47
aa) Sicherung durch Firewall 48
bb) Sicherung durch Intrusion Detection System 49
cc) Besondere Scanntechniken 50
dd) Nicht standardkonforme Scanntechniken 50
e) Zusammenfassung Ausspähen von Daten 51
2. Systemanalyse 51
3. Social Engineering 52
a) Ausspähen von Daten, § 202a StGB 52
aa) Verbaler Kontakt 52
bb) E-Mail-Kontakt 52
cc) Zusammenfassung Ausspähen von Daten 53
b) Verletzung von Privatgeheimnissen, § 203 StGB 53
c) Verletzung des Dienstgeheimnisses und einer besonderen Geheimhaltungspflicht, § 353b StGB 54
d) Zusammenfassung Social Engineering 55
4. Verschaffen von Zugangsdaten (Knacken von Passwortdateien) 55
a) Manuelles Knacken 55
b) Automatisierte Passwortknacker 57
5. Sniffing in Netzwerken 58
a) Ausspähen von Daten, § 202a StGB 58
aa) Unverschlüsselte Daten 58
bb) Verschlüsselte Daten 59
cc) Zusammenfassung 61
b) Verletzung des Post- und Fernmeldegeheimnisses, § 206 StGB 61
aa) Persönlicher Anwendungsbereich 62
bb) Tathandlung 62
cc) Zusammenfassung Verletzung des Post- und Fernmeldegeheimnisses 63
c) Fernmeldegeheimnis, § 88 Abs. 3 Telekommunikationsgesetz 63

6. Angriffe auf Switches, Ausspähen von Daten, § 202a StGB 64
7. Sniffing in Funknetzen 65
a) Ausspähen von Daten, § 202a StGB 65
b) Abhörverbot, § 89 Telekommunikationsgesetz 65
aa) Nachricht, Funkanlage und Abhören 66
bb) Nicht für die Empfangsanlage bestimmt 67
8. Analyse der elektromagnetischen Abstrahlung 69
a) Ausspähen von Daten, § 202a StGB 69
b) Abhörverbot, § 89 Telekommunikationsgesetz 70
9. Weitere Straf- und Ordnungswidrigkeitenvorschriften in Spezialgesetzen 72
a) Verschaffen personenbezogener Daten, §§ 43, 44 Bundesdatenschutzgesetz 72
b) Geheimnisverrat, § 17 Gesetz gegen den unlauteren Wettbewerb 72
II. Verbergen der eigenen Identität 73
1. Fälschen der MAC-Adresse 73
a) Fälschung technischer Aufzeichnungen, § 268 StGB, durch das Senden der gefälschten MAC-Adresse 74
b) Fälschung technischer Aufzeichnungen, § 268 StGB, durch Erzeugung eines Logeintrags beim DHCP-Server 75
aa) Technische Aufzeichnung 75
(1) Darstellung von Daten 75
(2) Selbständige Bewirkung durch das Gerät 76
(a) Wortlaut 76
(b) Ratio Legis 76
(3) Erkennbarkeit des Gegenstands der Aufzeichnung 77
(4) Beweisfunktion 77
bb) Herstellen / Einwirken auf den Aufzeichnungsvorgang 78
(1) Isolierte Betrachtung der Funktion des DHCP-Servers 78
(2) Betrachtung des Netzwerkes als Gesamtsystem 79
cc) Zusammenfassung 81
c) Fälschung technischer Aufzeichnungen, § 268 StGB, durch Hinterlegung der falschen MAC-Adresse im ARP-Cache 82
aa) Darstellung von Daten 82
(1) Dauerhaftigkeit 82
(a) Wortlaut 82
(b) Systematik 83
(c) Wille des Gesetzgebers 84
(d) Ratio Legis 85
(e) Zusammenfassung 87
(2) Externe Verkörperung 87
(3) Teleologische Reduktion des Tatbestands aus kriminalpolitischen Überlegungen 88

(4) Zusammenfassung 89
bb) Sonstige Tatbestandsmerkmale einer technischen Aufzeichnung und Erfordernis der störenden Einwirkung 89
d) Zusammenfassung 89
2. Fälschen der IP-Adresse (IP-Spoofing) 89
a) Fälschung beweiserheblicher Daten im Sinne von § 269 StGB zur Anonymisierung 89
aa) Wortlaut und historischer Urkundenbegriff 91
bb) Ratio Legis 92
cc) Zusammenfassung 92
b) Fälschung beweiserheblicher Daten im Sinne von § 269 StGB zur Eroberung einer Vertrauensstellung 93
aa) Garantiefunktion 93
bb) Perpetuierung 93
cc) Zusammenfassung 95
c) Anmerkung de lege ferenda 95
d) Fälschung technischer Aufzeichnungen im Sinne von § 268 StGB 96
3. Verwenden eines geenterten Rechners 96
a) Fälschung beweiserheblicher Daten, § 269 StGB 96
b) Fälschung technischer Aufzeichnungen im Sinne von § 268 StGB 97
c) Zusammenfassung 97
4. Manuelle Manipulation von Logdateien 97
a) Fälschung technischer Aufzeichnungen, § 268 StGB 97
aa) Technische Aufzeichnung 97
bb) Verfälschung 98
cc) Täuschung im Rechtsverkehr 98
dd) Zusammenfassung Fälschung technischer Aufzeichnungen 98
b) Fälschung beweiserheblicher Daten, § 269 StGB 99
c) Urkundenunterdrückung, § 274 StGB 99

B. Missbrauch geenterter Systeme 101

I. Einsehen von Daten 101
1. Ausspähen von Daten, § 202a StGB 101
a) Zugangssicherung 101
aa) Zugangskontrollsystem 101
bb) Geschützt-ungeschützte Daten 102
cc) Sicherheitslücken (Pufferüberläufe) 104
dd) Ungesicherte Systeme 105
ee) Funknetzwerke 107
ff) Entführen einer Sitzung (Session-Hijacking) 109
gg) Zusammenfassung Zugangssicherung 109
b) Verschaffen 110
2. Exkurs Zugangskontrolldiensteschutz-Gesetz 111

II. Manipulation von Daten und Systemen 111
1. Datenveränderung, § 303a StGB 111
a) Programme als Schutzgut 112
b) Daten im Arbeitsspeicher als Schutzgut 113
c) Rechtswidrigkeit der Datenveränderung 114
d) Zusammenfassung 114
2. Computersabotage, § 303b StGB 115
a) Tatobjekt 115
b) Wesentliche Bedeutung 115
c) Tat nach § 303a Abs. 1 StGB 116
d) Einwirkung auf Hardware 116
e) Zusammenfassung Computersabotage 117
3. Computerbetrug, § 263a StGB 117
a) Bereicherungsabsicht 117
b) Unbefugte Verwendung von Daten 118
c) Verwendung unrichtiger Daten 119
d) Sonstige unbefugte Einwirkung 119
e) Unmittelbarkeit der Vermögensverschiebung 120
f) Zusammenfassung Computerbetrug 120
4. Erschleichen von Leistungen, § 265a StGB 120
a) Automat 121
b) Öffentlichen Zwecken dienendes Telekommunikationsnetz 121
5. Hinzufügen von Daten 122
a) Datenveränderung, § 303a StGB 122
b) Sachbeschädigung, § 303 StGB 123

C. Denial-of-Service-Angriffe, Computersabotage, § 303b StGB 125

D. Exkurs: Mangelnde Absicherung der eigenen Systeme 127

I. Einführung: Computer als gefährliche Werkzeuge 127
II. Zivilrechtliche Verkehrspflichten 128
1. Vermittlung der Gefahr durch Dritte 129
2. Anforderungen an die Absicherung 130
a) Möglichkeit 131
b) Grad der Gefahr und Schaden 132
aa) Gefahr, von einer Sicherheitslücke betroffen zu sein 132
bb) Gefahr, dass eine Lücke praktisch ausgenutzt wird 133
cc) Ausmaß der zu erwartenden Schädigung 134
dd) Zusammenfassung 134
3. Zumutbarkeit 134
a) Verkehrskreis der Administratoren 135
b) Verkehrskreis der Privatanwender 136
c) Zusammenfassung Zumutbarkeit 138
4. Mitverschulden des Opfers 139
5. Zusammenfassung Verkehrspflichten 140

III. Unterlassungsdelikte 140
1. Sonderverantwortlichkeit 141
2. Täterschaft und Beihilfe 143
a) Einführung 143
b) Grundsätzlich Beihilfe 143
c) Grundsätzlich Täterschaft 144
d) Differenzierte Lösung 145
3. Vorsatz 146
IV. Fahrlässigkeitsdelikte 150
V. Zulässige Verteidigung 151

E. Exkurs: Zivilrechtliche Ansprüche gegen Angreifer 152

I. Abwehransprüche 152
1. Beseitigungs- und Unterlassungsanspruch des Eigentümers, § 1004 BGB 152
a) Beeinträchtigung 152
aa) Benutzung fremden Eigentums 152
bb) Be- oder Verhinderung der Nutzung 153
cc) Zusammenfassung Beeinträchtigung 154
b) Rechtswidrigkeit 154
c) Störer 154
aa) Handlungsstörer 154
bb) Zustandsstörer 155
cc) Mehrheit von Störern 155
dd) Zusammenfassung Störer 156
d) Verschulden 156
e) Beseitigungs- und Unterlassungsanspruch 156
aa) Beseitigungsanspruch 156
bb) Unterlassungsanspruch 157
(1) Wiederholungsgefahr 157
(2) Erstbegehungsgefahr 158
cc) Zusammenfassung Beseitigungs- und Unterlassungsanspruch 158
2. Beseitigungs- und Unterlassungsanspruch des Besitzers, § 862 BGB 158
II. Schadensersatzansprüche 158
1. § 823 Abs. 1 BGB 159
a) Geschützte Rechtsgüter 159
aa) Eigentum 159
(1) Beschädigung von Daten 159
(2) Gebrauchsbeeinträchtigung 160
bb) Besitz 161
cc) Eingerichteter und ausgeübter Gewerbebetrieb 161
b) Rechtswidrigkeit 163
c) Schuld 163

2. § 823 Abs. 2 BGB 163
3. § 826 BGB 164

F. Zusammenfassung Angriff 165

Teil 3 Verteidigung 167

A. Verteidigung durch Private 167

I. Einverständnis, Einwilligung und mutmaßliche Einwilligung 167
1. Einverständnis und Einwilligung 168
2. Mutmaßliche Einwilligung bzw. mutmaßliches Einverständnis 168
II. Notwehr und Nothilfe, § 32 StGB / § 227 BGB 170
1. Notwehrlage 170
a) Angriff 170
aa) Notwehrfähige Güter 171
bb) Nothilfe zugunsten juristischer Personen 171
cc) Nothilfe zugunsten des Staates 172
(1) Fiskus 172
(2) Überindividuelle Rechtsgüter 172
(a) Wortlaut 173
(b) Ratio Legis 173
(c) Zusammenfassung 175
(3) Staatsnotstand 175
dd) Sonderproblem: aufgedrängte Nothilfe 176
(1) Einwilligung des Opfers 176
(2) Grundsätzliches Notwehrrecht gegen den Willen des Opfers 177
(3) Nothilfe, wenn das Opfer den Angriff nicht erkennt 178
ee) Angriff durch Unterlassen 178
b) Gegenwärtigkeit 179
aa) Beginn 180
bb) Dauer 182
cc) Ende 183
dd) Sonderproblem: Dauerangriffe 183
c) Rechtswidrigkeit 184
d) Sonderproblem: Rechtswidrigkeit bei fehlendem Handlungsunrecht 184
aa) Erfolgsunwert 185
bb) Handlungsunwert 185
cc) Vorsatz und Fahrlässigkeit 186
dd) Rechtswidrigkeit und Schuld 187
ee) Zusammenfassung 188

2. Notwehrhandlung 188
a) Verteidigung 188
b) Erforderlichkeit 189
aa) Geeignetheit 189
bb) Mildestes Gegenmittel 190
(1) Grundsätze 190
(2) Ausweichen 191
(3) Systemeingriffe 193
(4) Stufenweises Vorgehen 194
(5) Sonderproblem: staatliche Hilfe 195
cc) Sonderproblem: antizipierte Notwehr 195
dd) Sonderproblem: Ermittlung der Täteridentität 196
c) Gebotenheit 197
aa) („Schuldlos") Irrende 197
bb) Unerträgliches Missverhältnis der betroffenen Rechtsgüter 198
cc) Kinder und Jugendliche 199
dd) Sonderproblem: Honigtöpfe 201
d) Verteidigungswille und -absicht 203
3. Zusammenfassung Notwehr / Nothilfe 204
III. Notstand 204
1. Strafrechtlicher rechtfertigender Notstand, § 34 StGB 204
a) Notstandslage 205
aa) Geschützte Güter 205
bb) Nothilfe 205
cc) Sonderproblem: Rechtsgüter der Allgemeinheit 205
dd) Gegenwärtige Gefahr 207
(1) Gefahr 207
(2) Gegenwärtigkeit 208
(3) Szenarien 208
(a) Vorfeld eines Angriffs 208
(b) Dauergefahr 209
(c) Nach einem Angriff 210
b) Notstandshandlung 210
aa) Erforderlichkeit 211
bb) Abwägung der widerstreitenden Interessen 212
(1) Rangfolge der Rechtsgüter 212
(2) Ausmaß der Schädigung 213
(3) Gefahrengrad 213
(4) Ursprung der Gefahr 213
(5) Wesentliches Überwiegen 214
cc) Angemessenheitsklausel 214
c) Gefahrabwehrwissen / -wille 215
d) Zusammenfassung Notstand 215

2. Zivilrechtlicher Aggressivnotstand, § 904 BGB 215
3. Zivilrechtlicher Defensivnotstand, § 228 BGB 216
4. Abgrenzung § 904 BGB und § 228 BGB 217
a) Grundsituation des § 228 BGB 217
b) Grundsituation des § 904 BGB 218
c) Angreifer verwendet die Sache eines Unbeteiligten 218
d) Angreifer verwendet eine pflichtwidrig ungesicherte Sache 219
5. Beispielhafte Interessenabwägung in ausgewählten Notstandssituationen 221
a) Eingriffe in Rechtsgüter des Angreifers 221
b) Verfolgen eines Angreifers über fremde Computersysteme 222
c) Manipulieren fremder Computersysteme, die für einen Angriff missbraucht werden 223
aa) Verhindern eines Routings 223
bb) Tief greifende Systemveränderungen 224
cc) Kampf gegen Viren, Würmer und Trojaner 225
(1) Gegenvirus, -wurm oder -trojaner 226
(2) Angriff auf verseuchte oder ungesicherte Systeme 227
(a) Angriff auf ungesicherte Systeme 227
(b) Angriff auf verseuchte Systeme 228
(c) Angriffsziel verteidigt sich 228
IV. Sonderproblem: Irrtümer 229
1. Strafrecht 229
a) Notwehr 229
b) Notstand 230
c) Einwilligung 231
d) Perspektive des konkret handelnden Subjekts – Kritik an den vorgenannten Meinungen 232
e) Folgen eines Irrtums 233
aa) Erlaubnistatbestandsirrtum 233
bb) Erlaubnisirrtum und Verbotsirrtum 234
2. Zivilrecht 236
V. Exkurs: Schadensersatz trotz Rechtfertigung 236
1. Aggressivnotstand, § 904 BGB 236
a) Aktivlegitimation 237
b) Passivlegitimation 237
c) Umfang des Schadensersatzes 238
2. Defensivnotstand, § 228 BGB 239

B. Verteidigung durch den Staat 240

I. Einleitung 240
II. Anwendbarkeit allgemeiner Rechtfertigungstatbestände 240
1. Rechtfertigung eines behördlichen Verhaltens 240

a) Rechtfertigungsgründe als der gesamten Rechtsordnung immanente Prinzipien 241
b) Systematische Betrachtung 242
aa) Notstandsklauseln der Polizeigesetze 242
bb) Nothilfepflicht des Staates 243
cc) Vorschriften über den unmittelbaren Zwang und Notstandsverfassung 244
c) Anforderungen an staatliches Eingriffshandeln 245
aa) Gesetzesvorbehalt 245
bb) Bestimmtheitsgebot 247
cc) Verhältnismäßigkeitsgrundsatz 248
dd) Gesetzgebungskompetenz 249
ee) Zuständigkeit 250
ff) Zitiergebot 250
d) Zusammenfassung 251
2. Rechtfertigung des handelnden Amtsträgers 251
a) Strafrechtliche Rechtfertigung 251
b) Disziplinarrechtliche Folgen 253
aa) Gegenstand der Verfahren 254
bb) Disziplinarrechtlicher Überhang 254
(1) Ratio des § 14 Abs. 2 Bundesdisziplinargesetz 255
(2) Ne bis in idem 256
3. Zusammenfassung Anwendbarkeit allgemeiner Rechtfertigungstatbestände auf hoheitliches Handeln 256
III. Hausrecht 257
IV. Gesetzliche Ermächtigung (Polizei- und Ordnungsbehörden der Länder) 258
1. Standardmaßnahmen 258
2. Polizei- und ordnungsrechtliche Generalklauseln 260
a) Schutzgut 260
aa) Öffentliche Sicherheit 260
(1) Individualrechtsgüter 261
(2) Rechtsgüter, die dem Staat zugeordnet sind 261
(3) Zusammenfassung öffentliche Sicherheit 262
bb) Öffentliche Ordnung 262
b) Gefahr 263
c) Störer 264
aa) Verhaltensstörer 264
bb) Zustandsstörer 265
cc) Nichtstörer 266
dd) Zusammenfassung Störer 268
d) Erforderliche Maßnahmen 268
aa) Keine Grundverfügung 269
bb) Keine Androhung 270

e) Verhältnismäßigkeit 270
f) Exkurs: rechtspolitischer Ausblick 271
g) Zusammenfassung polizeiliche Generalklauseln 272
3. Zuständigkeiten 272
a) Sachliche Zuständigkeit 273
b) Örtliche Zuständigkeit 273
aa) Örtliche Zuständigkeit innerhalb eines Bundeslandes 273
bb) Örtliche Zuständigkeit innerhalb der Bundesrepublik Deutschland 275
cc) Örtliche Zuständigkeit außerhalb der Bundesrepublik Deutschland 276
dd) Zusammenfassung örtliche Zuständigkeit 276
V. Gesetzliche Ermächtigung (Bundesbehörden) 277
1. Bundespolizei 278
a) Aufgaben und Befugnisse 278
b) Räumliche Begrenzung des Aufgabenbereichs 279
2. Bundeskriminalamt 279
3. Bundesamt für Verfassungsschutz 280
4. Bundesnachrichtendienst 281
5. Bundesamt für Sicherheit in der Informationstechnik 282
6. Zusammenfassung 283

Glossar 285

Literaturverzeichnis 291

Zitierte Internetquellen 308