

Inhaltsverzeichnis

Einleitung	1
A. Problemstellung	1
B. Stand von Gesetzgebung, Rechtsprechung und Forschung	5
I. Gesetzgebung	5
II. Rechtsprechung	6
1. Der Fall „Stiefeisenpresse“ des Reichsgerichts	7
2. Der Fall „Rollenwechsler“ des Oberlandesgerichts Düsseldorf	8
3. Die sog. „Geldspielautomatenfälle“	10
III. Forschung	11
C. Ziele und Gang der Untersuchung	15
1. Teil: Rechtstatsächliche Grundlagen	17
A. „Know-how“ – Definition und wirtschaftliche Bedeutung	19
I. Definition des Begriffs „Know-how“	19
1. „Know-how“ als „Wissen“	21
2. Abgrenzung des „Know-how“ zu anderen Wissensarten	24
a) Technisches Wissen	24
b) Wettbewerbsförderndes Wissen	28
c) Exklusives Wissen	29
d) Geheimes Wissen	30
e) Verkehrsfähiges Wissen	31
f) Sonderrechtlich geschütztes Wissen	32
g) Unternehmensbezogenes Wissen	35
3. Abschließender Definitionsvorschlag	36
II. Wirtschaftliche Bedeutung des „Know-how“	37
1. Marktpreisorientiertes Bewertungsverfahren	39
2. Kapitalwertorientiertes Bewertungsverfahren	40
3. Kostenorientiertes Bewertungsverfahren	41
B. Know-how-Ausspähung durch „Reverse Engineering“ . . .	43
I. Definition des Begriffs „Reverse Engineering“	43

Inhaltsverzeichnis

II. Beweggründe für „Reverse Engineering“	45
1. „Reverse Engineering“ zu Zwecken des Produktgebrauchs	45
a) Schwachstellen- und Gefährdungsanalyse	45
b) Produktreparatur	46
c) Produktcracking	46
d) Produktanpassung	47
2. „Reverse Engineering“ zu Zwecken der Produktent- wicklung	48
a) Herstellung von Konkurrenzprodukten	48
b) Herstellung interoperabler Produkte	49
c) Herstellung von Cracking-Tools	50
d) Verwendung in unabhängigen Produktzusammen- hängen	51
3. „Reverse Engineering“ zu Zwecken der Produktsabotage	51
4. „Reverse Engineering“ zum Nachweis von Rechts- verletzungen	52
5. „Reverse Engineering“ zu Forschungszwecken	52
6. Zwischenergebnis	53
III. Methoden des „Reverse Engineering“	54
1. „Hardware Reverse Engineering“	55
a) Trennung des Analyseobjekts	55
b) Bestimmung und Messung der Einzelbestandteile ..	56
c) Ergänzende Versuche zur Aufdeckung des „Know-how“	57
2. „Software Reverse Engineering“	58
a) Technische Grundlagen	59
aa) Computerhardware	60
bb) Computersoftware	62
(1) Definition der Begriffe „Computersoftware/ -programm“	62
(2) Betriebssystem und Anwenderprogramme ..	63
(3) Programmschnittstellen	64
cc) Programmiersprachen	65
(1) Maschinensprachen	65
(2) Maschinennahe Programmiersprachen	68
(3) Problemorientierte Programmiersprachen ..	70
dd) Programmablauf	74

Inhaltsverzeichnis

b) Techniken zum Schutz des Quellcodes	75
aa) Kompilierung, Assemblierung	75
bb) Obfuskatoren	76
cc) Kryptografie	77
dd) Listschutz	77
c) Techniken des „Software Reverse Engineering“	78
aa) System Monitoring	78
bb) Dekompilierung	79
cc) Disassemblierung	81
dd) Line-Tracing	82
ee) Fault Injection Tools	84
ff) Durchsicht des Begleitmaterials	84
IV. Wirtschaftliche Schäden durch „Reverse Engineering“ . . .	84
 2. Teil: Strafrechtlicher Know-how-Schutz	87
A. Betriebsspionage gem. § 17 Abs. 2 UWG	89
I. Entwicklungsgeschichtlicher Überblick	90
II. Tatbestandsmäßigkeit des „Reverse Engineering“	94
1. „Know-how“ als „Betriebs- oder Geschäftsgeheimnis“	95
a) Wissen von Tatsachen	96
b) Begrenzte Bekanntheit des Wissens	97
aa) Maximale Größe des Mitwisserkreises	98
bb) Erforderliche Geheimhaltungsmaßnahmen	102
(1) Grundsatz faktischer Beurteilung	102
(2) Qualitative Anforderungen an die Geheimhaltung	103
(3) Beurteilung des „Reverse Engineering“	105
c) Unternehmensbezogenes Wissen	112
d) Willentlich geheim gehaltenes Wissen	113
e) Geheimhaltungsinteresse des Wissensinhabers	115
f) Zwischenergebnis	117
2. „Reverse Engineering“ als Tathandlung	117
a) § 17 Abs. 2 Nr. 1 UWG	118
aa) Anwendung technischer Mittel	118
bb) Herstellung einer verkörperten Wiedergabe	119
cc) Wegnahme einer das Geheimnis verkörpernden Sache	119
dd) Geheimnisverschaffung/-sicherung	120

Inhaltsverzeichnis

b) § 17 Abs. 2 Nr. 2 UWG	121
3. „Unbefugtes“ und „sonst unbefugtes“ Handeln	122
4. Subjektiver Tatbestand	126
a) Vorsatz	126
b) Besondere Absichten	126
III. Stimmigkeitskontrolle des vorläufigen Ergebnisses	129
1. Notwendigkeit einer ergänzenden Tatbestands- eingrenzung	129
a) Meinungsstand in der Literatur	129
b) Diskussion und Kritik	132
2. Dogmatische Anbindung und inhaltliche Ausgestaltung	137
3. Beurteilung des „Reverse Engineering“	142
IV. Ergebnis zu § 17 Abs. 2 UWG	143
B. Ausspähen von Daten gemäß § 202 a StGB	145
I. Datenbegriff des § 202 a StGB	145
II. Besondere Datensicherung	145
III. Zweckbestimmung der Daten	146
C. Datenveränderung gemäß § 303 a StGB	149
3. Teil: Zivilrechtlicher Know-how-Schutz	151
A. Urheberrecht	153
I. Urheberrechtlicher Softwareschutz	153
1. Entwicklungsgeschichtlicher Überblick	153
2. Werkqualität von Software	157
a) Schöpfung	157
b) Geistiger Gehalt	158
c) Individualität	158
d) Freiheit der Ideen und Grundsätze	161
e) Zwischenergebnis	161
3. „Software Reverse Engineering“ als Eingriffshandlung	162
a) Umarbeitung gem. § 69c Nr. 2 UrhG	162
b) Vervielfältigung gem. § 69c Nr. 1 UrhG	163
aa) Programmablauf	163
(1) „Upload“ in den Arbeitsspeicher	164
(2) Sukzessives Einlesen in die Prozessorregister	165
(3) Zwischenspeicherungen in den Caches	165

Inhaltsverzeichnis

bb) Anzeigen des Programmcodes	166
cc) Disassemblierung und Dekompilierung	167
dd) Zwischenergebnis	167
4. Begrenzungen des Softwareschutzes	168
a) Herstellung von Interoperabilität gem. § 69 e UrhG	168
aa) Zweckbeschränkung	169
bb) Kreis berechtigter Personen	171
cc) Erforderlichkeit („Unerlässlichkeit“)	172
dd) Relevanz des § 69 e Abs. 3 UrhG	174
ee) Zwischenergebnis	174
b) Bestimmungsgemäße Benutzung gem. § 69 d Abs. 1 UrhG	175
aa) Berechtigung zur Programmverwendung	176
bb) Notwendige Benutzungsbefugnisse	178
(1) Privilegierte Eingriffshandlungen	179
(2) „Notwendigkeit“ des Eingriffs	184
cc) Relevanz des § 69 d Abs. 3 UrhG	185
dd) Zwischenergebnis	186
5. Rechtswidrigkeit und Verschulden	186
II. Urheberrechtlicher Schutz von Integritätsinteressen	187
1. Urheberrechtlicher Werkbegriff des § 2 UrhG	187
2. Potential des § 14 UrhG für den Schutz von „Know-how“	189
III. Schutz technischer Maßnahmen	191
IV. Ergebnis der urheberrechtlichen Betrachtung	193
B. Gewerbliche Schutzrechte	195
C. Wettbewerbsrecht: §§ 3 Abs. 1, 4 UWG	197
I. Allgemeine Voraussetzungen	197
1. „Reverse Engineering“ als geschäftliche Handlung	197
2. Eignung zur spürbaren Wettbewerbsbeeinträchtigung	199
II. Unlautere Nachahmung gem. §§ 3 Abs. 1, 4 Nr. 9 c UWG	200
1. Wettbewerbliche Eigenart des untersuchten Produkts	201
2. Nachahmungsformen	203
3. „Reverse Engineering“ als unredliche Kenntniserlangung	204
III. Gezielte Behinderung gem. §§ 3 Abs. 1, 4 Nr. 10 UWG	207
IV. Rechtsbruch gem. §§ 3 Abs. 1, 4 Nr. 11 UWG	208

Inhaltsverzeichnis

V. Unlauterkeit gem. § 3 Abs. 1 UWG	208
VI. Ergebnis der wettbewerbsrechtlichen Betrachtung	210
D. Allgemeines Deliktsrecht	211
I. Verletzung eines „sonstigen Rechts“ gem. § 823 Abs. 1 BGB	211
1. Absoluter oder rahmenrechtlicher Schutz des „Know-how“	212
a) Meinungsstand in Rechtsprechung und Literatur . . .	212
b) Diskussion und Kritik	216
aa) „Numerus Clausus der Immaterialgüterrechte“	216
bb) Verfassungsrechtlich indizierter Schutzauftrag. .	218
cc) Völkerrechtlich indizierter Schutzauftrag	226
dd) Rechtspolitische und ökonomische Betrachtung	227
2. „Know-how“ und das Recht am Gewerbebetrieb	228
a) „Know-how“ als Bestandteil des Gewerbebetriebs . .	232
b) „Reverse Engineering“ als betriebsbezogener Eingriff	232
3. Persönlichkeitsschutz für den gewerblichen Geheimbereich	234
4. Ergebnis zu § 823 Abs. 1 BGB	237
II. Schutzgesetzverletzung gem. § 823 Abs. 2 BGB	238
III. Sittenwidrige Schädigung gem. § 826 BGB	239
1. „Reverse Engineering“ als vorsätzliche Schädigung . . .	239
2. „Reverse Engineering“ als Sittenverstoß	239
E. Recht der Eingriffskondiktion	241
I. Rechtsgrundlose Vorteilserlangung in sonstiger Weise . . .	241
II. Vorteilserlangung „auf Kosten eines anderen“	242
III. Ergebnis zum Recht der Eingriffskondiktion	246
F. Recht der angemessenen Eigengeschäftsführung	247
I. Geschäftsbesorgung ohne Berechtigung	247
II. Fremdheit des angemessenen Geschäfts	248
III. Ergebnis zum Recht der angemessenen Eigengeschäftsführung	249
4. Teil: Vertraglicher Know-how-Schutz	251
A. Feststellung des vertraglichen Gestaltungsbedarfs	253

Inhaltsverzeichnis

B. Vertragliches Reverse-Engineering-Verbot	255
I. Vereinbarungsverbote aus §§ 69 g Abs. 2, 69 d Abs. 1 UrhG	256
II. Kartellrechtliche Beurteilung	258
1. Vereinbarungen zwischen Unternehmen	259
2. Wettbewerbsverhinderung, -einschränkung oder -verfälschung	259
3. Zwischenergebnis	262
III. AGB-Kontrolle	262
IV. Wirksamkeitskontrolle über § 138 BGB	265
C. Ergänzende Know-how-Schutzklauseln	267
I. Klauselweitergabepflicht	267
II. Besichtigungsrecht	267
III. Verwertungsverbot und Geheimhaltungsgebot	268
IV. Vertragsstrafeklauseln	268
D. Ergebnis zum vertraglichen Know-how-Schutz	269
Schluss teil: Gesamtergebnis und Ausblick	271
Literaturverzeichnis	275