

Manuel Ziegler

Sicher in sozialen Netzwerken

Vom Cybermobbing bis zur
staatlichen Überwachung –
Tipps & Anleitungen zum Schutz
persönlicher Daten

HANSER

Inhalt

Vorwort	XIII
1 Die Bedeutung sozialer Netzwerke im Alltagsleben	1
1.1 Zielgruppen	1
1.1.1 Mitgliederstruktur	3
1.2 Soziale Netzwerke als Kommunikationsmittel	4
1.2.1 Synchroner Kommunikation via Kurznachrichten	5
1.2.1.1 Mobile Messenger und ständige Erreichbarkeit	5
1.2.1.2 Kommunikation im Wandel	6
1.2.1.3 Gesellschaftliche Auswirkungen	6
1.2.2 Asynchrone Kommunikation	7
1.2.2.1 Soziale Netzwerke als Informations- und Nachrichtenquelle	7
1.2.2.2 Soziale Netzwerke als Diskussionsplattform	9
1.2.2.3 Soziale Netzwerke als Werbemedium	10
... für Privatpersonen	11
... für Unternehmen	11
... für politische, religiöse und gesellschaftliche Gruppierungen	11
1.3 Literatur	15
2 Bedeutende soziale Netzwerke	17
2.1 Klassische, kommerzielle soziale Netzwerke	18
2.1.1 Facebook	19
2.1.1.1 Ein Überblick über die Nutzungsbedingungen	19
2.1.1.2 Die Benutzeroberfläche	21
Der Stream	22
Die Chronik	23
Der Chat	24
Veranstaltungen	25
Apps	26
Gruppen	27
2.1.1.3 Einstellungen	27

2.1.2	Google+	30
2.1.2.1	Ein Überblick über die Nutzungsbedingungen	30
2.1.2.2	Die Benutzeroberfläche	31
2.1.2.3	Einstellungen	34
2.1.3	Twitter	37
2.1.3.1	Ein Überblick über die Nutzungsbedingungen	37
2.1.3.2	Die Benutzeroberfläche	37
2.1.3.3	Einstellungen	41
2.1.4	YouTube	45
2.1.4.1	Ein Überblick über die Nutzungsbedingungen	45
2.1.4.2	Die Benutzeroberfläche	45
2.2	Soziale Netzwerke im Businessbereich	47
2.2.1	Headhunter in sozialen Netzwerken	47
2.2.2	Online-Lebenslauf	48
2.2.3	XING	49
2.2.3.1	Ein Überblick über die Nutzungsbedingungen	49
2.2.3.2	Die Benutzeroberfläche	49
2.2.3.3	Einstellungen	52
2.2.4	LinkedIn	54
2.2.4.1	Die Benutzeroberfläche	55
2.2.4.2	Einstellungen	57
2.3	Mobile soziale Netzwerke	59
2.3.1	Whatsapp	59
2.3.1.1	Die Benutzeroberfläche	60
2.3.1.2	Einstellungen	61
2.3.1.3	Facebooks Whatsapp-Kauf	62
2.3.2	Instagram	63
2.3.2.1	Die Benutzeroberfläche	63
2.3.2.2	Einstellungen	65
2.3.3	Snapchat	66
2.3.3.1	Die Idee und Umsetzung vergänglicher Kommunikation	66
2.3.4	Skype	68
2.3.5	TextSecure	68
2.3.5.1	Verschlüsselungsverfahren	69
2.3.5.2	Die Benutzeroberfläche	69
2.3.5.3	Einstellungen	72
2.3.6	Wickr	75
2.3.7	RedPhone	76
2.4	Dezentrale soziale Netzwerke und ähnliche Kommunikationsmedien	76
2.4.1	Die Idee eines dezentralen sozialen Netzwerkes	76
2.4.2	diaspora*	76
2.4.3	Friendica	77

2.4.4	Blogs als dezentrales soziales Netzwerk	77
2.4.4.1	RSS-Feeds	78
2.5	Online-Dating-Plattformen	79
2.5.1	Der Markt von Singlebörsen und Flirt-Apps	80
2.5.1.1	Marketing in der Online-Liebesbranche	81
2.5.2	Der Umgangston auf Flirtplattformen	81
2.5.3	Durch Online-Dating veränderter Flirtkontakt	83
2.5.4	Flirtplattformen	84
2.5.4.1	Tinder	84
	Der Prozess der Partnersuche	84
	Nutzungsbedingungen	85
	Benutzeroberfläche	86
	Einstellungen	88
2.5.4.2	Lovoo	90
	Der Prozess der Partnersuche	90
	Benutzeroberfläche	90
	Einstellungen	93
2.5.5	Erotikplattformen	95
2.5.5.1	C-Date	95
	Der Prozess der Partnersuche	95
	Nutzungsbedingungen	95
2.5.5.2	Treffpunkt18	96
	Der Prozess der Partnersuche	96
	Nutzungsbedingungen	96
	Benutzeroberfläche	99
	Einstellungen	101
2.5.6	Online-Partnerbörsen	107
2.5.6.1	Parship	107
	Der Prozess der Partnersuche	107
	Benutzeroberfläche	108
	Einstellungen	112
2.5.6.2	ElitePartner	114
	Der Prozess der Partnersuche	114
	Benutzeroberfläche	116
	Einstellungen	121
2.5.6.3	eDarling	123
	Der Prozess der Partnersuche	123
	Benutzeroberfläche	124
	Einstellungen	125
2.5.6.4	FriendScout 24	127
	Der Prozess der Partnersuche	128
2.6	Literatur	130

3 Spionage durch Dritte	131
3.1 Motivationen	131
3.1.1 Journalisten	132
3.1.2 Privatpersonen	133
3.1.3 Unternehmen und andere Organisationen	134
3.1.4 Kriminelle	134
3.1.4.1 Cyber-Kriminelle	134
3.1.4.2 Einbrecher	135
3.1.4.3 Politische Extremisten	135
3.1.5 Staaten	136
3.2 Gefällt-mir-Angaben und ähnliche Sympathiebekundungen	137
3.2.1 Was sagen Interessen über einen Nutzer aus?	137
3.2.2 Der Zugriff auf Gefällt-mir-Angaben	137
3.3 Spionage auf Dating-Plattformen	138
3.4 Kompromittierende Fotos	141
3.4.1 Virale Verbreitung	142
3.4.2 Verlinkung auf Bildern	143
3.5 Verratener Aufenthaltsort	144
3.5.1 Explizite Ortsangaben	144
3.5.2 Implizite Ortsangaben	144
3.6 Graph Search und ähnlich mächtige Suchmaschinen für soziale Netzwerke ..	146
3.6.1 Funktionsweise	147
3.6.2 Problematik	147
3.7 Literatur	148
4 Spionage und Zensur durch staatliche Behörden	149
4.1 Motivationen	149
4.1.1 Terrorprävention	150
4.1.2 Politische Verfolgungen	151
4.1.3 Verbrechensaufklärung	153
4.2 Wege zu Benutzerinformationen	154
4.2.1 Manuelle Analyse von (öffentlichen) Benutzerprofilen	154
4.2.2 Automatisiertes Crawling von Benutzerinformationen	154
4.2.3 Zugriffe auf die Datenbestände der Betreiber	155
4.2.3.1 ... mit richterlichem Beschluss	155
4.2.3.2 ... uneingeschränkt	156
4.2.4 Überwachung des Netzwerkverkehrs	156
4.3 Bekannte Überwachungsprogramme	159
4.3.1 Die Bedeutung von Edward Snowdens Enthüllungen	159
4.3.2 Das PRISM-Programm der NSA	160

4.3.3	Überwachung der Internet-Kommunikation	162
4.3.3.1	Aufbau des Internets	162
4.3.3.2	Programme zum Datenzugriff	168
	FAIRVIEW, BLARNEY, OAKSTAR, STORMBREW	168
	TEMPORA	169
4.3.4	SQUEAKY DOLPHIN	170
4.3.5	XKEYSCORE	170
4.4	Staatliche Zensur	171
4.4.1	QUANTUMTHEORY Hacking durch NSA und GCHQ	172
4.4.1.1	QUANTUMINSERT	174
4.4.1.2	QUANTUMSKY/QUANTUMCOPPER	176
4.4.1.3	QUANTUMDNS	176
4.4.1.4	QUANTUMSQUIRREL	179
4.4.2	Projekt Goldener Schild in China	180
4.4.3	Zensur durch Gerichtsbeschlüsse, Gesetze und internationale Verträge	181
4.4.3.1	Zensur von Inhalten auf Twitter und YouTube in der Türkei	181
4.4.3.2	Politische Diskussionen zur Zensur des Internets in Deutschland	182
4.4.3.3	Die gesetzliche Zensur von Pornografie in Großbritannien	183
4.4.3.4	Regierungsanfragen zur Zensur von Inhalten durch Dienstanbieter im Internet	185
4.5	Literatur	186
5	Datenmissbrauch durch Netzbetreiber	189
5.1	Der finanzielle Wert von Benutzerdaten	189
5.2	Missbrauch freiwillig veröffentlichter Daten	190
5.2.1	Gefällt-mir-Angaben	190
5.2.2	Soziale Netzwerke	192
5.2.3	Beiträge und andere Textinhalte	197
5.2.4	Datenspeicherung verhindern	198
5.2.4.1	Informations-Jamming	199
5.2.4.2	Gezielte Täuschung	200
5.3	Ermittlung zusätzlicher Daten	200
5.3.1	Tracking-Technologien	201
5.3.1.1	Cookies und andere Tracking-Technologien auf Basis einer clientseitig gespeicherten ID	201
	Klassische Cookies	201
	Flash-Cookies	203
	ETag Tracking	204
	Tracking mithilfe des Web-Storage	205
	HSTS Tracking	205

5.3.1.2	Fingerprinting	207
	... anhand des HTTP-Headers	207
	... mithilfe von JavaScript	208
	Browserspezifische Informationen	208
	Canvas Fingerprinting	209
	Micro-Performance Benchmarks	210
5.3.1.3	Ab wann ist ein Internetnutzer eindeutig identifizierbar?	210
5.3.1.4	Fortgeschrittene Tracking-Möglichkeiten	212
	IP-Adressen, Bandbreite und Hops	213
	Login-basiertes Tracking	214
	Backend Tracking	215
	Tracking des One-Step-Clickpath durch Weiterleitungen	215
	Tracking auf Basis von Browserverhalten	216
5.3.1.5	Einsatz der Tracking-Methoden	216
	Facebook	217
	Google	217
	Tracking-Unternehmen	218
5.3.1.6	Gegenmaßnahmen	218
	Adblock Plus	219
	Bluehell Firewall	221
	Ghostery	221
	PrivacyBadger	223
	BetterPrivacy	223
	Self-Destructing Cookies	224
	NoScript	225
	Tor-Browser inklusive Tor-Button	226
5.3.2	Standort-Analysen	226
5.3.2.1	... auf Basis der IP-Adresse	227
5.3.2.2	... mithilfe von Sensoren in Smartphones	227
5.3.2.3	... durch Metadaten in Bildern	228
5.3.2.4	Gegenmaßnahmen	230
	Tor-Browser	230
	Smartphones	230
	<i>Deinstallation der nativen Apps</i>	231
	<i>Orbot/Orweb</i>	232
	Metadaten von Bildern bereinigen	232
5.3.3	Freundfinder und Adressbuch-Uploads	233
5.3.3.1	Freundfinder	233
5.3.3.2	Adressbuchdiebstahl	234
5.3.3.3	Gegenmaßnahmen	234
5.4	Die grenzenlosen Überwachungsmöglichkeiten durch „Smart“-Technologie	235
5.5	Die Macht der Technologiekonzerne	236
5.6	Literatur	237

6	Identitäts- und Datendiebstahl	239
6.1	Passwörter und Brute-Force-Attacken	239
6.1.1	Der richtige Aufbewahrungsort für Passwörter	241
6.1.2	Aufwand zum Brechen eines Passwortes	242
6.1.3	Sichere Passwörter generieren	246
6.1.4	Passwort-Recycling	247
6.2	Phishing	248
6.2.1	Eingabe von Login-Informationen auf Betrugsseiten	249
6.2.2	Das Web of Trust-Browser-Plugin	249
6.3	Ungesicherte Verbindungen	251
6.3.1	Abhören von Passwörtern	251
6.3.2	Abhören von Session-IDs	252
6.3.3	Man-in-the-Middle-Angriffe	254
6.3.4	HTTPS-Everywhere	255
6.4	Datensicherheit	255
6.4.1	Die Sicherheit Ihrer Bilder bei Facebook und Co. oder „Security through Obscurity“	256
6.4.2	Wann ist Kommunikation sicher?	258
6.5	Literatur	259
7	Rufmord und Cybermobbing	261
7.1	Erscheinungsformen	261
7.1.1	Beleidigungen	262
7.1.2	Diskreditierung	263
	Üble Nachrede	263
	Verleumdung	263
7.1.3	Mobbing	264
7.2	Gegenmaßnahmen	264
7.3	Stalking	265
8	Gruppenzwang und Gruppendynamik	267
8.1	Beispiele für Gruppenzwang in sozialen Netzwerken	267
8.1.1	NekNominate	267
8.1.2	Riskante Profildfotos und Videos	268
	8.1.2.1 Fotos im Gleisbett	268
8.1.3	Cold Water Challenge und Ice Bucket Challenge	268
8.1.4	Bin ich hässlich oder schön?	269
8.2	Gruppendynamiken	270
8.3	Literatur	272

9 Am Totenbett der Privatsphäre	273
9.1 Privatsphäre trotz Social Networking	274
9.2 Big Brother	277
9.3 Literatur	280
10 Anhang	281
10.1 Browser sichern	281
10.1.1 Firefox	282
10.1.1.1 Standardsuchmaschine ändern	282
10.1.1.2 Cookies löschen	282
10.1.1.3 NoScript	283
10.1.2 Internet Explorer	283
10.1.2.1 Chronik und Cookies löschen	283
10.1.4 Google Chrome/Chromium	284
10.1.4.1 Standardsuchmaschine ändern	284
10.1.4.2 Cookies löschen	285
10.1.4.3 JavaScript deaktivieren	285
10.1.5 Safari	286
10.1.5.1 Standardsuchmaschine ändern	286
10.1.5.2 Cookies löschen	287
10.1.5.3 JavaScript deaktivieren	288
10.2 Das Tor-Netzwerk und der Tor-Browser	288
10.2.1 Aufbau und Funktionsweise des Netzwerkes	289
10.2.2 Verwendung	290
10.2.2.1 Der Tor-Browser	290
10.2.2.2 Orbot und kompatible Smartphone-Apps	292
Orweb	293
DuckDuckGo	293
ChatSecure	295
Proxy-Konfiguration am Beispiel der Twitter-App	295
10.3 E-Mail-Verschlüsselung	296
10.3.1 Warum ist die De-Mail nicht verschlüsselt?	296
10.3.1.1 Weitergabe von Sozialdaten an die akkreditierten Dienstanbieter der De-Mail	297
10.3.2 Ist „E-Mail made in Germany“ eine Lügenkampagne?	297
10.3.3 Wirklich sichere E-Mail-Verschlüsselung	298
10.3.3.1 PGP	298
10.3.3.2 S/MIME	303
10.4 Literatur	304
Index	305