HANSER

Leseprobe

Manuel Ziegler

Sicher in sozialen Netzwerken

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

ISBN (Buch): 978-3-446-44431-7

ISBN (E-Book): 978-3-446-44429-4

Weitere Informationen oder Bestellungen unter

http://www.hanser-fachbuch.de/978-3-446-44431-7

sowie im Buchhandel.

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 Synchrone 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
Deinstallation der nativen Apps ... *231*
Orbot/Orweb ... *232*
Metadaten von Bildern bereinigen ... 232
5.3.3 Freundefinder und Adressbuch-Uploads ... 233
5.3.3.1 Freundefinder ... 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 Profilfotos 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 Diensteanbieter 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

Vorwort

Liebe Leser,

vor ziemlich genau zwei Jahren hat sich der langjährige NSA-Mitarbeiter Edward Snowden mit seinen Enthüllungen darüber, in welchem Umfang und mit welchem Aufwand Geheimdienste seit einigen Jahren Menschen überall auf der Welt bespitzeln, an die Öffentlichkeit gewandt. Vermutlich zeichnen Server auf der ganzen Welt in diesem Moment Ihre Aktivitäten auf. Egal ob Sie via Whatsapp eine Nachricht an einen Freund schreiben, einen Artikel über die neue Fernsehsendung, die Sie und offenbar auch der Autor des Artikels gestern zum ersten Mal gesehen haben, auf Spiegel Online lesen, egal ob Sie gerade bei Facebook für die Geburtstagsfeier Ihrer Freundin am kommenden Samstag zugesagt oder sich telefonisch bei Ihrem Chef krank gemeldet haben, irgendwo auf der Welt ist gerade ein Computer damit beschäftigt, Ihre jüngsten Aktionen zusammen mit denen von Milliarden anderer Menschen auszuwerten.

Wenn Sie Glück haben, gehören Sie zu den über 99 % der Menschen, die dabei nicht auffallen, aber wenn nicht … Wehe wenn nicht! Was, wenn Sie in der letzten halben Stunde ein Exemplar des Kommunistischen Manifests bei Amazon bestellt haben, anschließend eine Viertelstunde mit Ihrem aufgebrachten pakistanischen Freund telefoniert haben, der bei der Einreise mal wieder von einem Flughafenbeamten tyrannisiert wurde und deshalb seinem Ärger über das Sicherheitspersonal Luft machen musste. Was, wenn Sie auf Facebook das Profil dieses muslimischen Predigers, den Sie so sehr mögen, abonniert haben und anschließend einen kritischen Artikel über die Luftangriffe des US-Militärs auf Kämpfer der Terrororganisation Islamischer Staat gelesen haben?

Nun, in diesem Fall kann Ihnen niemand garantieren, dass Sie nicht bereits auf der Beobachtungsliste der Geheimdienste stehen. Haben Sie dieses Buch online erworben? Herzlichen Glückwunsch, Sie gehören ab jetzt zu den potenziellen Terroristen, aber keine Angst, ich werde Ihnen zeigen, wie Sie erfolgreich durch die Maschen des weltweiten Überwachungsnetzwerkes schlüpfen.

Über soziale Netzwerke findet heute der wichtigste Teil Ihrer Kommunikation statt. Egal ob Facebook, Twitter, YouTube, Whatsapp oder eines der zahlreichen Dating-Netzwerke, alle sozialen Netzwerke haben eines gemein: Sie ermöglichen es Ihnen, über das Internet mit Freunden und Bekannten zu kommunizieren und neue Kontakte zu knüpfen.

Das kann eine echte Bereicherung für Ihr Leben sein. Weil die Betreiber sozialer Netzwerke jedoch dabei meist Ihre gesamte Kommunikation aufzeichnen und außerdem zahlreiche weitere Metadaten wie Positionsdaten oder Informationen darüber, welche Webseiten Sie besuchen, sammeln, bedeutet das auch, dass Sie dabei bislang unbekannten Gefahren ausgesetzt sind.

Ich bin der festen Überzeugung, dass wir in dem Moment, in dem wir unsere Privatsphäre aufgeben, auch die Kontrolle über unser eigenes Leben verlieren. Deshalb möchte ich Ihnen in diesem Buch zeigen, welche Technologien private Unternehmen und staatliche Behörden einsetzen, um Sie zu überwachen, und welche Möglichkeiten Sie haben, um sich dagegen zu verteidigen.

Im **ersten Kapitel** dieses Buches möchte ich Ihnen zeigen, welche Rolle soziale Netzwerke heute in unserem Leben spielen, welche Gründe es gibt, sie zu nutzen, und welche gesellschaftlichen Auswirkungen damit verbunden sind. Soziale Netzwerke werden von den unterschiedlichsten Interessensgruppen für ihre Ziele genutzt. Darunter sind politische Parteien, militärische Organisationen und terroristische Vereinigungen. In Anbetracht der Tatsache, dass Nutzer soziale Netzwerke oft als (primäre) Nachrichtenquelle nutzen, ist im Umgang mit sozialen Netzwerken ein sehr differenziertes Urteilsvermögen erforderlich.

Mittlerweile gibt es eine große Menge sozialer Netzwerke, die auf ganz unterschiedliche Zielgruppen abgestimmt sind. Neben dem Platzhirsch Facebook haben sich auch Google+ und Twitter zu festen Größen in der Welt sozialer Netzwerke etabliert. Frische Winde wehen aus den Bereichen mobiler Messenger (Whatsapp, Snapchat, TextSecure, Wickr) und auch YouTube hat sich als eines der einflussreichsten sozialen Netzwerke etabliert. Auch im Businessbereich sind mit XING und LinkedIn zwei soziale Netzwerke vertreten, die Sie in Ihrem professionellen Leben begleiten wollen, und natürlich darf man auch die Online-Dating-Plattformen nicht vergessen, deren Branche in den letzten Jahren stark gewachsen ist. Alternativen zu den zentralisierten sozialen Netzwerken großer Unternehmen, mit denen selbstverständlich einige Gefahren einhergehen, lernen Sie unter dem Stichwort dezentrale soziale Netzwerke im **zweiten Kapitel** des Buches kennen.

Das **dritte Kapitel** gibt Ihnen einen kurzen Überblick darüber, welche Informationen Dritte nur anhand Ihrer Profile in sozialen Netzwerken über Sie gewinnen können. Von Persönlichkeitsanalysen aufgrund von Gefällt-mir-Angaben bei Facebook bis hin zu Bewegungsprofilen und Analysen Ihrer Gewohnheiten erhalten Sie einen Einblick in die Möglichkeiten, die sich selbst außenstehenden Beobachtern sozialer Netzwerke offenbaren.

Im **vierten Kapitel** soll auf eine ganz besondere Klasse von außenstehenden Beobachtern eingegangen werden: die Geheimdienste. Seit Edward Snowdens Enthüllungen ist bekannt, welche Aufwände NSA, GCHQ und Co. betreiben, um intimste Daten über Ihr Leben zu ermitteln. Dabei beschränken sich die Möglichkeiten dieser Organisationen keineswegs nur darauf, Ihre Profile auf Facebook, Twitter oder LinkedIn zu beobachten. Geheimdienste sammeln rund um die Uhr Informationen darüber, welche Webseiten Sie besuchen, mit wem Sie über soziale Netzwerke oder per E-Mail in Verbindung treten und nach welchen Begriffen Sie bei Google oder anderen Suchmaschinen suchen. Ich

werde Ihnen die wichtigsten Programme, mit denen Geheimdienste Sie ausspionieren, vorstellen und Sie auch mit der zweiten großen Aufgabe vieler Geheimdienste, der Zensur, vertraut machen. Natürlich kommen dabei auch die politischen und demokratischen Implikationen nicht zu kurz.

Das **fünfte Kapitel** widmet sich dem Datenmissbrauch durch die Betreiber sozialer Netzwerke. Diese nutzen die Daten ihrer Nutzer, Ihre Daten also, für ihre eigenen Zwecke. Doch die Betreiber gehen noch einen Schritt weiter und ermitteln durch zahlreiche Trackingtechnologien, durch die Ermittlung Ihres Standortes und womöglich sogar mithilfe von Gesichtserkennungssoftware und Metadaten von Bildern zahlreiche weitere Informationen über Sie. Die Datenbestände der Betreiber sind in dieser Hinsicht oftmals mindestens so komplex wie die der Geheimdienste. Dabei sind die Unternehmen, die soziale Netzwerke betreiben, zunehmend unkontrollierbarer und setzen sich immer häufiger auch über geltendes Recht hinweg. Sie erfahren in diesem Kapitel, wie Sie sich gegen diese Überwachung durch die Betreiber sozialer Netzwerke wehren können.

Das **sechste Kapitel** beschäftigt sich mit sogenanntem Identitätsdiebstahl. Sie erhalten Einblicke in die Möglichkeiten eines Angreifers, Ihre Benutzerkonten zu knacken. Identitätsdiebstahl hat oft rechtliche und finanzielle Konsequenzen für die Betroffenen. Sie erfahren, worauf Sie achten müssen, um Anzeichen von Cyberbetrug zu erkennen, wie Sie Ihre Online-Konten sichern können, und nicht zuletzt, was die Betreiber sozialer Netzwerke unternehmen, um Ihre Konten vor Angriffen zu schützen.

Das **siebte Kapitel** behandelt das Thema Cybermobbing und Rufmord in sozialen Netzwerken. Anhand einiger Fälle aus der Vergangenheit werden Sie für diese Gefahren sensibilisiert.

Mit Gruppenzwang und über soziale Netzwerke entstehenden Gruppendynamiken beschäftige ich mich im **achten Kapitel**. Wir diskutieren das Phänomen und unterschiedliche Erklärungsansätze an Beispielen der jüngeren Vergangenheit.

Das **neunte Kapitel** ist mit dem Titel „Am Totenbett der Privatsphäre“ überschrieben. Tatsächlich ist Privatsphäre in unserer digitalen Gesellschaft ein nicht mehr existierendes Gut. Nicht nur Geheimdienste können jederzeit, individuell und ohne lange Vorbereitung Einzelpersonen überwachen, sondern auch einige Internetunternehmen, allen voran Google und Facebook, besitzen durchaus die Möglichkeit, intime Daten von Internetnutzern abzuschnorcheln. In diesem abschließenden Kapitel soll diskutiert werden, welche Form von Privatsphäre erstrebenswert ist, wer darüber entscheiden sollte und vor allem wie eine gewisse Privatsphäre wiederhergestellt werden kann.

Exkurse zu ausgewählten Themen sowie Anleitungen zur Installation von Software, die Ihre Privatsphäre zu schützen vermag, finden Sie schließlich im **Anhang** des Buches.

Zuletzt bleibt mir noch die angenehme Pflicht, mich bei allen an diesem Buch Beteiligten zu bedanken. Dazu gehört vor allem meine Mutter, die sich die Zeit genommen hat, ganze Textpassagen ausführlich mit mir zu diskutieren. Ebenfalls bedanken möchte ich mich bei allen weiteren Verwandten, Bekannten und Freunden, die sich während der Entstehungsphase dieses Buches – und in vielen Fällen auch bereits seit mehreren Jahren – immer wieder auf, sicherlich nicht immer einfache, Diskussionen mit mir einlas-

sen mussten und mir damit geholfen haben, eine möglichst differenzierte Sicht auf die in diesem Buch beschriebenen Sachverhalte zu entwickeln. Dank geht auch an die Leser meines ersten Buches zu diesem Thema mit dem Titel „Facebook, Twitter & Co. – Aber Sicher!“ sowie an die Zuhörer meiner Vorträge zu Themen der Privatsphäre, die mir durch ihre Anregungen und ihr Feedback dabei geholfen haben, die technischen Beschreibungen von privatwirtschaftlichem Tracking und staatlicher Überwachung möglichst anschaulich zu schildern.

Auch beim Carl Hanser Verlag und seinen Mitarbeitern, allen voran Sieglinde Schärl, möchte ich mich für die große Geduld, vor allem in der Endphase des Schreibens, bedanken. Ebenfalls bedanken möchte ich mich bei Thomas Gerhardy, der sich stets bereitwillig um die Beseitigung technischer Probleme beim Verfassen des Manuskriptes bemüht hat. Natürlich nicht zu vergessen sind Sandra Gottmann, die sich um die Beseitigung meiner Fehler im Umgang mit der deutschen Sprache kümmerte, und Irene Weilhart, die Produzentin des Buches. Vielen Dank. Natürlich gilt mein Dank auch allen anderen Mitarbeitern beim Carl Hanser Verlag, die hinter den Kullissen zum Gelingen dieses Projektes beigetragen haben. Ein ganz besonderer Dank gilt in diesem Kontext Kristin Rothe für die stets hocherfreuliche und interessante Zusammenarbeit im Umfeld des Blogs Hanser Update. Egal ob es darum geht, den Lesern meiner Bücher auch nach deren Drucklegung hilfreiche Informationen in einem Artikel zum Thema zusammenzustellen, oder ob es um ganz andere Projekte geht, Kristin hat immer neue Ideen und unterstützt mich dabei, wo sie nur kann.

Ich wünsche Ihnen trotz der ernsten Thematik dieses Buches eine angenehme Lektüre.

Manuel Ziegler

Website zum Buch

Auf der Webseite zu diesem Buch finden Sie aktuelle Informationen zum Thema Privatsphäre und Sicherheit in sozialen Netzwerken und im Internet allgemein. Weiterhin finden Sie dort einige Zusatzmaterialien zu diesem Buch, auf die ich an gegebener Stelle verweise, und zu guter Letzt finden Sie auch eine Übersicht aller in diesem Buch verwendeten Referenzen.

Sie erreichen die Webseite zum Buch unter der Domain

`network-privacy.org`

Gerne können Sie mich bei Fragen auch per E-Mail kontaktieren. Sie erreichen mich unter der Adresse

`private@manuelziegler.de`

Meinen aktuellen PGP Schlüssel können Sie auf den gängigen Schlüsselservern herunterladen, zum Beispiel unter `keys.gnupg.net`

Key-ID: `0xFC875ACB`

PGP-Fingerprint: `C3D6 ACD4 5BD2 6BDE E52D FB75 6EF4 D1CA FC87 5ACB`

Schlimm genug, dass gegen alle Nutzer von Tor, also gegen alle Menschen, die sich um ihre Privatsphäre Sorgen machen, ein Generalverdacht erhoben wird, indem deren Kommunikation herausgefiltert und abgespeichert wird. Menschen, die Tools zur sicheren und anonymen Kommunikation wie das „Amnesiac Incognito Live System" entwickeln oder verbreiten, aber auch solche, die es nutzen, gelten für die NSA als „Extremisten". Folgerichtig ist da selbstverständlich, dass diese „Extremisten" vorrangig über „extremistische Foren", wie die seit Neustem offenbar extremistische Plattform der Zeitschrift linuxjournal, eine Zeitschrift über das Betriebssystem Linux und verwandte Themen, kommunizieren.

Listing 4.4 Regeln zur Identifikation von „Extremisten" in XKEYSCORE

```
// START_DEFINITION
/* These variables define terms and websites relating to the TAILs
(The Amnesic Incognito Live System) software program, a comsec mechanism
advocated by extremists on extremist forums.
*/
$TAILS_terms=word('tails' or 'Amnesiac Incognito Live System')
and word('linux' or ' USB ' or ' CD ' or 'secure desktop' or
' IRC ' or 'truecrypt' or ' tor ');
$TAILS_websites=('tails.boum.org/') or ('linuxjournal.com/content/linux*');
// END_DEFINITION
```

Die entsprechenden, in XKEYSCORE definierten Regeln können Sie in Listing 4.4 sehen. Mit derartigen Filtern werden alle IT-Sicherheitsexperten und viele andere Menschen, die sich für sichere und anonyme Kommunikation interessieren, zu Zielpersonen. Wenn das alles Extremisten sein sollen, stellt sich die Frage, wer auf dieser Welt kein Extremist ist.

4.4 Staatliche Zensur

Neben einfacher Überwachung der Internetnutzer betreiben die meisten großen Geheimdienste autoritärer Staaten, aber auch viele Geheimdienste demokratischer Staaten, in denen die Bürger zumindest auf dem Papier Meinungs- und Pressefreiheit genießen, Programme, die dazu dienen, systematisch unerwünschte Inhalte im Internet zu zensieren. Das wohl größte Programm zur Zensur unliebsamer Inhalte im Internet wird von der chinesischen Regierung betrieben und ist unter dem Namen „Projekt Goldener Schild" (engl. The Golden Shield Project) bekannt. Man kann Projekt Goldener Schild vereinfacht wie eine Firewall betrachten, die das gesamte chinesische Internet vom Rest der Welt trennt[10]. Jegliche Seitenaufrufe von Webseiten außerhalb des abgeschotteten

[10] In Abschnitt 4.4.2 sehen Sie, dass das so nicht ganz stimmt, aber der Einfachheit halber soll uns das an dieser Stelle noch nicht interessieren.

Netzwerkes müssen zunächst das „Goldene Schild“ passieren. Handelt es sich bei den angefragten Inhalten um von der Regierungspartei als unerwünscht eingestuften Content, wird die Verbindung von dieser unterbrochen.

Doch nicht nur die autoritäre chinesische Regierung betreibt ein äußerst wirkvolles Programm zur Zensur des Internets. Unter dem Namen QUANTUMTHEORY HACKING betreiben die NSA und der britische GCHQ einige Programme (siehe Abschnitt 4.4.1), die sowohl zur Zensur als auch zur Auslieferung von eigenen Inhalten anstelle der angefragten Inhalte an individuell ausgewählte Internetnutzer geeignet sind. „Be any IP in the world“ beispielsweise ist das Ziel des QUANTUMSQIRREL-Programms. Das geht aus einer auf der Seite „The Intercept“ veröffentlichten Präsentation mit dem Titel „QUANTUMTHEORY“ von der SIGINT Development Conference 2010 hervor [24].

Doch vom Staat ausgehende Zensur ist oft gar nicht unbedingt auf derart aufwendige Programme angewiesen. In vielen Staaten kann die Zensur unliebsamer Inhalte von der autoritären Regierung selbst oder zumindest von Gerichten veranlasst und durchgesetzt werden. Für ganz bestimmte Inhalte wie beispielsweise Kinderpornografie existieren Übereinkommen zwischen vielen Staaten und auch Internet Service Providern, bestimmte Listen von Internetseiten zu zensieren. Wenngleich das grundsätzlich einem guten Zweck, nämlich dem Missbrauchsschutz von Kindern, dient, muss darauf geachtet werden, dass derartige Übereinkommen nicht missbraucht werden. So gibt es sogar demokratische Staaten, namentlich Großbritannien, in denen Internet Service Provider nach einer gesetzlichen Regelung jegliche Seiten, auf denen Pornografie angeboten wird, zensieren, und zwar so lange, bis die Internetnutzer, die diese Inhalte konsumieren wollen, einen schriftlichen Antrag dazu an ihren Internet Service Provider stellen.

4.4.1 QUANTUMTHEORY Hacking durch NSA und GCHQ

Die Bezeichnung QUANTUMTHEORY Hacking ist eine Sammelbezeichnung von NSA und GCHQ für eine Reihe von fortgeschrittenen Angriffstechnologien auf bestehende Internetprotokolle und -infrastrukturen. QUANTUMTHEORY hat dabei nichts mit Quantencomputing zu tun, sondern der Begriff beruht wohl eher auf der Protocol-Injection-Technologie, die im Rahmen des QUANTUMTHEORY Hackings genutzt wird. Dabei werden Netzwerkpakete, die über das Internet versendet werden, in Echtzeit manipuliert, sodass Protokollschwächen wie mangelnde Integritätsprüfungen oder das The-Winner-takes-it-all-Prinzip ausgenutzt werden können, um mithilfe von „Man-on-the-Side“-Angriffen Daten zu fälschen[11].

Die unter dem Namen QUANTUMTHEORY Hacking zusammengefassten Programme sind sowohl dazu geeignet, die Verbindungen einzelner Internetnutzer zu sabotieren und entweder Inhalte für diese zu zensieren, oder gar Schadsoftware auf deren Rechnern zu installieren, als auch dazu, einzelne, unliebsame Internetseiten wie beispiels-

[11] Details zur Funktionsweise solcher Techniken erfahren Sie im Laufe dieses Kapitels.

weise die von Julian Assange gegründete Enthüllungsplattform Wikileaks für längere Zeit verschwinden zu lassen. Gerade was die Zensur einer solchen Plattform betrifft, kommen auch für Geheimdienste äußerst fragwürdige Methoden, wie die unter den Programmnamen QUANTUMBOT und QUANTUMBOT2 geführten Botnets zum Einsatz [24]. Unter dem Begriff Botnet versteht man eine große Anzahl in aller Regel privater Computer, die von einem Angreifer (beispielsweise mithilfe eines Virus, unter seine Kontrolle gebracht wurden und die dazu genutzt werden können, vom Angreifer vorgegebene Operationen durchzuführen. Typischerweise werden Botnets für sogenannte Distributed Denial-of-Service-(DDoS-)Angriffe genutzt, bei denen ein Webserver durch massenhafte, zeitlich koordinierte Verbindungsanfragen absichtlich verlangsamt oder gar zum Absturz gebracht wird. Die Folge ist, dass die auf dem Webserver gehosteten Internetseiten für den Zeitraum der Attacke nicht länger erreichbar sind. Im Grunde kann so in zeitkritischen Situationen zumindest vorübergehend eine Zensur erreicht werden.

Die Enthüllungsplattform Wikileaks hatte in der Vergangenheit bereits mehrfach mit solchen Denial-of-Service-(DoS-)Angriffen zu kämpfen. Als die Plattform im Jahr 2010 die Veröffentlichung von Depeschen US-amerikanischer Botschafter ankündigte, wurde die Erreichbarkeit der Seite bereits am Vortag der angekündigten Veröffentlichung durch Denial-of-Service-Attacken gemindert und teilweise vollständig verhindert. Craig Labovitz zeigt im Arbor Networks Blog mithilfe einer Grafik, wie der Traffic des größten Wikileaks Hosting Providers um 2 bis 4 Gbps (Gigabits per second) ansteigt [25]. Das sind etwa 15 bis 30 Prozent des sonst üblichen Traffics. In einem Folgeartikel vom nächsten Tag zitiert Craig Labovitz Wikileaks, die über Twitter davon berichtet, dass die Denial-of-Service-Attacke nun einen Traffic von mehr als 10 Gbps überschreite [26]. Zum Vergleich: Der weltweit größte Internet Exchange Point De-CIX hat in einer Pressemitteilung vom 31. August 2010 unter dem Titel „Der DE-CIX knackt die 1-Terrabit-Marke“ [27] nur wenige Monate zuvor verkündet, in Spitzenzeiten einen Datendurchsatz von rund 1,2 Terrabit pro Sekunde zu leisten.

Über die Frage, wer hinter den DDoS-Attacken auf Wikileaks steckt, kann man nur mutmaßen, aber die schiere Größe der Attacke legt nahe, dass der Angreifer entweder ein enormes Botnet unter seiner Kontrolle hatte oder aber dass besonders leistungsfähige Rechner, wie sie beispielsweise in den Rechenzentren der NSA oder anderer Geheimdienste stehen, an den Angriffen beteiligt waren. Beides deutet zumindest auf die Beteiligung eines Geheimdienstes, mit derartigen Möglichkeiten, an den Angriffen hin. Man muss selbstverständlich auch überdenken, wer wohl ein Interesse daran hatte zu verhindern, dass die insgesamt 251 287 internen Berichte von US-Diplomaten, von denen etwa die Hälfte als geheim oder vertraulich eingestuft war und die zum Teil kritische Informationen über politische, militärische und geheimdienstliche Ziele und Aktivitäten der USA enthielten, an die Öffentlichkeit gelangen.

Doch was Zensur betrifft, sind Vorgehensweisen wie im Fall von Wikileaks eher die Ausnahme und zeugen eigentlich von einer Verzweiflungstat, schließlich muss klar sein, dass die Veröffentlichung von Informationen durch Wikileaks von einer Denial-

of-Service-Attacke, egal wie intensiv und umfangreich diese ausfällt, nicht aufgehalten werden kann. Früher oder später werden diese Informationen an die Öffentlichkeit gelangen. Die heute von den USA und Großbritannien etablierten Technologien zur Zensur gehen weit über den Wirkungsgrad einer Denial-of-Service-Attacke hinaus.

4.4.1.1 QUANTUMINSERT

Das QUANTUMINSERT-Programm wird in der von Edward Snowden geleakten QUANTUMTHEORY-Präsentation [24] der SIGINT Development Conference 2010 als ein Service zur HTML-Weiterleitung von Internetnutzern beschrieben, entspricht im Wesentlichen jedoch einem klassischen Man-in-the-Middle- bzw. Man-on-the-Side-Angriff.

Bei einem Man-in-the-Middle-Angriff versucht der Angreifer (in der Literatur meist als Mallory bezeichnet), sich zwischen zwei miteinander kommunizierende Partner (in der Literatur meist als Alice und Bob bezeichnet) zu drängen. Im einfachsten Fall täuscht Mallory sowohl Bob als auch Alice vor, er sei der jeweils andere, und bewirkt damit, dass beide ihre Nachrichten an ihn senden (siehe Bild 4.8). Damit hat Mallory die Kontrolle über die Kommunikation und kann Nachrichten nicht nur lesen, sondern auch darüber entscheiden, welche Nachrichten an den echten Kommunikationspartner weitergeleitet werden. Außerdem kann Mallory Nachrichten verändern oder vollständig fälschen.

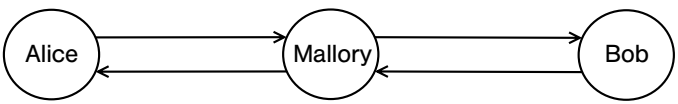


Bild 4.8 Die einfachste Form eines Man-in-the-Middle-Angriffs

Es gibt jedoch auch andere Möglichkeiten, einen Man-in-the-Middle-Angriff durchzuführen. Gerade dann, wenn man wie die NSA oder das GCHQ weite Teile des Internets überwachen und sogar kontrollieren kann, ist es möglich, die Man-in-the-Middle-Position als außenstehender, zunächst die Kommunikation nur passiv beobachtender Beteiligter zu erlangen. Dieser spezielle Man-in-the-Middle-Angriff wird auch Man-on-the-Side-Angriff genannt. Dabei kann man zum Beispiel darauf setzen, dass man selbst in der Lage ist, schneller auf eine Anfrage zu antworten als das eigentliche Ziel (siehe Bild 4.9). Die NSA ist das teilweise aufgrund ihrer Server, die sich dank Kooperationen mit großen US-amerikanischen Internet Service Providern direkt in den großen Backbones befinden und dadurch meist eine strategisch günstigere Position als die Rechenzentren der eigentlichen Zielseiten haben.

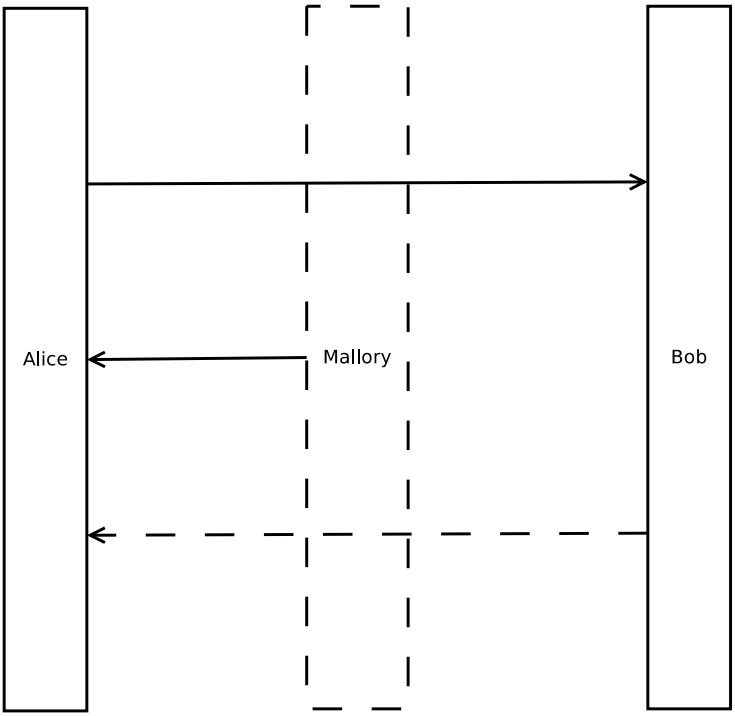


Bild 4.9 Prinzip und zeitlicher Verlauf einer Man-on-the-Side-Attacke

Wenn die Geheimdienste also aufgrund bestimmter Filter eine Anfrage einer Person identifizieren, für die eine gefälschte Seite anstelle des Originals ausgeliefert werden soll, antworten sie einfach mit einer solchen gefälschten Seite. Trifft die Antwort vor der Antwort des eigentlichen Anfrageziels beim Internetnutzer ein, wird die eigentliche korrekte Antwort verworfen[12].

Der Spiegel berichtete im November 2013 von einem mithilfe von QUANTUMINSERT gestarteten Angriff des GCHQ auf Angestellte der belgischen Telekommunikationsfirma Belgacom [28]. Der britische Geheimdienst habe demnach zunächst Angestellte des sogenannten Network Operations Center (NOC), die in den Bereichen Systemadministration oder Sicherheit tätig waren, identifiziert. Anschließend habe man ausfindig gemacht, dass diese Mitarbeiter unter anderem das soziale Netzwerk LinkedIn und die Nachrichtenplattform Slashdot.org nutzten, und habe dann das QUANTUMINSERT-Programm dazu genutzt, eine gefälschte Version von LinkedIn (oder Slashdot) an diese Mitarbeiter auszuliefern. Mit dieser gefälschten Seite wurde jedoch auch Schadsoftware

[12] Das liegt am TCP (Transmission Control Protocol). Dieses Protokoll nummeriert die einzelnen Nachrichten mit einer Sequenznummer. Trifft ein Paket mit einer bereits behandelten Sequenznummer ein, wird es verworfen, weil davon ausgegangen wird, dass dieses Paket bereits zugestellt wurde und es sich bei dem zuletzt eingetroffenen Paket um ein Duplikat handelt.

übertragen, die mithilfe eines Browser Exploits auf den Rechnern der Opfer installiert wurde. Damit erlangte das GCHQ die Kontrolle über diese im NOC privilegierten Rechner der Angestellten. Nick Kolakowski hat in seinem Artikel „GCHQ Responds to Slashdot, LinkedIn Hack“ [29] bei Dice eine entsprechende Folie des GCHQ veröffentlicht.

4.4.1.2 QUANTUMSKY/QUANTUMCOPPER

Während NSA und GCHQ mit QUANTUMINSERT zwar theoretisch in der Lage dazu sind, unerwünschte Inhalte im Internet zu zensieren, ist diese Technik für eine flächendeckende Zensur viel zu aufwendig und regional unter Umständen auch zu fehleranfällig, da die von den Geheimdiensten ausgelieferte, gefälschte Seite unter allen Umständen vor dem Original beim Opfer eintreffen muss. QUANTUMINSERT wird daher weniger zur Zensur von Inhalten als vielmehr für gezielte und individuelle Kompromittierung von Verbindungen genutzt; beispielsweise mit dem Ziel, Schadsoftware auf dem Rechner des Opfers zu installieren.

Um Personen daran zu hindern, bestimmte Webseiten aufzurufen oder Dateien auszutauschen, verwendet die NSA die Programme QUANTUMSKY und QUANTUMCOPPER [30, 31].

QUANTUMSKY ist eine seit 2004 entwickelte Software, die Internetnutzer daran hindern soll, bestimmte Webseiten aufzurufen. Dazu wird ein sogenanntes TCP-Reset-Paket von NSA-Servern, die sich als die eigentliche Zielseite ausgeben, an den Nutzer gesendet. Das TCP-Reset-Paket wird dazu verwendet, eine Verbindung zu beenden. Alle weiterhin eintreffenden Daten der Webseite werden dann ignoriert. Der Vorteil gegenüber QUANTUMINSERT liegt einerseits darin, dass keine auf den Benutzer zugeschnittenen Seiten, die womöglich erst noch dynamisch erzeugt werden müssen, versendet werden. Dadurch wird die Reaktionszeit der NSA -Server dramatisch verringert. Ein ähnliches Vorgehen verwendet auch die nationale chinesische Firewall „Projekt Goldener Schild“, die in Abschnitt 4.4.2 vorgestellt ist.

Neben QUANTUMSKY gibt es auch das seit 2008 entwickelte QUANTUMCOPPER-Programm, mit dessen Hilfe analog zur Zensur mittels QUANTUMSKY der Dateiaustausch über das Internet unterbunden werden soll. Vermutlich bedient man sich dabei einer sehr ähnlichen Technologie wie beim QUANTUMSKY-Programm und unterbindet damit Dateiuploads und Dateidownloads von ausgewählten Zielpersonen.

4.4.1.3 QUANTUMDNS

Während das Man-on-the-Side-Szenario des QUANTUMINSERT-Programms einige Nachteile mit sich bringt, erlaubt das QUANTUMDNS-Programm die Rolle des zunächst passiven, außenstehenden Beobachters in eine tatsächliche Man-in-the-Middle-Position umzuwandeln. Das verschafft der NSA gerade dann, wenn sichere, also kryptografisch abgesicherte Verbindungen genutzt werden, den notwendigen Vorteil, um weiterhin intervenieren zu können.

Das Problem bei verschlüsselten Verbindungen ist für die NSA und andere Geheimdienste nicht nur, dass sie die meisten Daten, die über die Verbindung gesendet werden, nicht lesen können, sondern auch (und vor allem), dass nach Abschluss das Handshakes, bei dem sich die beiden Parteien gegenseitig authentifizieren und einen geheimen Schlüssel für die Verschlüsselung festlegen, eine Spoofing[13]-Attacke, wie bei QUANTUMINSERT quasi unmöglich wird.

Bei einer tatsächlichen Man-in-the-Middle-Situation, bei der die Geheimdienste vor einem Eingriff in die Kommunikation nicht nur passiv beobachten, sondern zwischen den beiden Seiten vermitteln, sprich Netzwerkpakete weiterleiten, kann eine verschlüsselte TLS-(Transport-Layer-Security-)Verbindung mithilfe von gefälschten Zertifikaten kompromittiert werden.

QUANTUMDNS dient den Geheimdiensten dabei dazu, die Man-in-the-Middle-Position zu erlangen. Dazu nutzen NSA und GCHQ das DNS (Domain Name System), um ihre Opfer auf gefälschte Seiten weiterzuleiten. Das Domain Name System dient dazu, Domainnamen wie beispielsweise „facebook.com“ in tatsächlich adressierbare IP-Adressen umzuwandeln. Das ist notwendig, weil das IP-Protokoll, über das letztendlich jegliche Kommunikation im Internet abgewickelt wird, keine Domains, sondern nur IP-Adressen kennt[14].

Das Domain Name System ist ein hierarchisch aufgebautes, verteiltes System zur Namensauflösung von Domains in IP-Adressen. Die einzelnen sogenannten Nameserver sind dabei hierarchisch gegliedert. Root-Nameserver unterscheiden anhand der sogenannten Top-Level-Domain (TLD), an welchen Nameserver eine Anfrage delegiert werden soll. Eine TLD ist zum Beispiel com, de oder org. Es gibt insgesamt 13 Root-Nameserver weltweit.

Weblink

Eine Auflistung dieser Nameserver inklusive ihrer Betreiber finden Sie auf der Webseite zum Buch unter der Adresse

network-privacy.org/de/information/root-dns-server-list.

Nachdem man eine Anfrage an einen Root-Nameserver gestellt hat, bekommt man als Antwort die Adresse des zuständigen Nameservers für die entsprechende TLD. Nun sendet man die Anfrage an diesen Nameserver. Für die Top-Level-Domain „de“ ist beispielsweise die DENIC Verwaltungs- und Betriebsgesellschaft eG zuständig. Als Antwort bekommt man, immer vorausgesetzt, dass die angefragte Domain tatsächlich existiert,

[13] Bei einer Spoofing-Attacke gibt sich der Angreifer als ein anderer aus; im Falle von QUANTUMINSERT als der Zielserver einer Anfrage.

[14] Wenn Sie sich nun fragen, warum wir keine IP-Adressen anstelle von Domains nutzen, um uns mit Internetseiten zu verbinden, überlegen Sie sich einfach einmal, was besser zu merken ist: facebook.com oder 173.252.120.6.

die Adresse des Nameservers, der für die entsprechende Region zuständig ist, zurückgeliefert. In einer letzten[15] Anfrage an diesen Nameserver erhält man dann die IP-Adresse des Servers, der unter der angefragten Domain erreichbar ist. In Bild 4.10 sehen Sie ein Beispiel für eine solche hierarchische Anfrage.

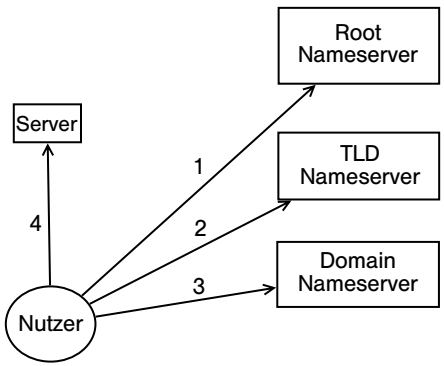


Bild 4.10
Beispiel für eine iterative Namensauflösung mithilfe von DNS

Problematisch ist bei diesem System jedoch die große Abhängigkeit von den Root-Nameservern. Da jede DNS-Anfrage zunächst an den Root-Server gerichtet werden muss, stehen diese unter besonders großer Last. Diese Last wäre so groß, dass diese Server unweigerlich unter ihr zusammenbrechen würden, obwohl diese meist ohnehin mithilfe von Anycast auf viele Hunderte physikalische Server auf der ganzen Welt verteilt ist. Deshalb gibt es zusätzlich zu den bereits vorgestellten, autoritativen Nameservern auch eine ganze Reihe von rekursiven und Caching-basierten Nameservern. Rekursiv bedeutet, dass der Nameserver den in aller Regel dreistufigen Prozess der Namensauflösung selbst durchführt und am Ende die richtige IP-Adresse der Domain zurückliefert. Caching bedeutet, dass der Nameserver die einmal ermittelte IP-Adresse zu einer Domain vorübergehend zwischenspeichert, um im Falle einer erneuten Anfrage nicht wieder den gesamten Namensauflösungsprozess durchlaufen zu müssen.

An diesem Punkt setzen viele sogenannten DNS-Spoofing-Attacken an. Sie versuchen durch sogenanntes Cache-Poisoning die temporär zwischengespeicherten Einträge eines solchen Servers zu manipulieren, denn wenn es gelingt, dort eine eigene IP-Adresse zu einer Domain, die einem selbst nicht gehört, zu platzieren, ist man in der Lage, sich für alle Nutzer dieses Nameservers als Eigentümer der Domain auszugeben. Diese Technik des Cache-Poisonings wird von NSA und GCHQ teilweise angewendet. Außerdem werden durch gefälschte Antworten von DNS-Servern teilweise auch einzelne Nutzer an falsche IP-Adressen weitergeleitet [30].

[15] Theoretisch könnten Sie auch bei dieser Anfrage noch einmal an einen weiteren Nameserver verwiesen werden.

Weblink

Wenn Sie daran interessiert sind, wie DNS-Cache-Poisoning im Detail funktioniert, können Sie dies auf der Webseite zum Buch unter der Adresse

network-privacy.org/de/information/dns-cache-poisoning

nachlesen.

QUANTUMDNS setzt NSA und GCHQ also in die Lage, sowohl eine großflächig angelegte Zensur einzelner Webseiten zu erzwingen, als auch ganz individuell Nutzer auf gefälschte Seiten zu leiten. Gerade was großflächige Zensur von Inhalten im Web angeht, hat die Strategie des DNS-Cache-Poisoning den Vorteil, dass nicht bei jeder einzelnen Anfrage der Internetnutzer intervenieren muss. Das verringert insgesamt das Risiko, dass die eingesetzte Methode einmal nicht greift.

4.4.1.4 QUANTUMSQUIRREL

Leider sind kaum technische Details über das QUANTUMSQUIRREL-Programm bekannt. In der bereits mehrfach erwähnten QUANTUMTHEORY-Präsentation [24] ist jedoch das Ziel dieses Programms aufgeführt: „Be any IP in the World“. Da es selbst für die NSA vermessen wäre, tatsächlich jeden Computer der Welt mit einem entsprechenden Virus zu infizieren, ist anzunehmen, dass damit verschiedene IP-Spoofing-Techniken gemeint sind.

Grundsätzlich ist IP-Spoofing sehr simpel: Man muss nur in das entsprechende Feld des IP-Protokolls die IP-Adresse, die man gerne annehmen möchte, einsetzen, und schon kann man Pakete im Namen dieser IP versenden. Das einzige Problem ist, dass die Antwortpakete zu dem Rechner, der diese IP tatsächlich besitzt, zurückkehren. Die NSA muss dazu also ihre Infrastruktur einsetzen, mit der sie auch QUANTUMINSERT oder gar die Überwachung des Netzwerkverkehrs realisiert, denn dann kann sie Pakete, die zu der vorgehaltenen, gefälschten IP-Adresse zurückgesendet werden, abfangen und selbst verarbeiten.

Dass diese Möglichkeit bereits offenbar weitestgehend besteht, bestätigt nur das Ausmaß der weltweiten geheimdienstlichen Überwachung.

Die Einsatzmöglichkeiten von QUANTUMSQUIRREL sind praktisch unbeschränkt, denn wann immer man sich als eine IP ausgeben kann, kann man auch alle Dienste, die unter dieser IP-Adresse betrieben werden, überwachen und manipulieren.

4.4.2 Projekt Goldener Schild in China

Das Projekt Goldener Schild[16] (engl.: Golden Shield Project oder Great Firewall of China) galt lange Zeit als das größte System zur Zensur des Internets. Diese unangefochtene Stellung muss nach den Erkenntnissen der letzten zwei Jahre zwar noch einmal grundsätzlich überdacht werden, fest steht jedoch weiterhin, dass das Projekt Goldener Schild das größte in aktivem Einsatz befindliche System zur flächendeckenden Zensur des Internets ist.

Betrieben wird das Projekt Goldener Schild vom chinesischen Ministerium für Staatssicherheit mit dem Ziel der Überwachung und Zensur des Internets.

Eigentlich ist der Begriff Firewall für das Projekt Goldener Schild nicht ganz richtig, wenngleich die Wirkungsweise ähnlich ist. Während bei einer Firewall Verbindungen tatsächlich blockiert werden, entspricht die Vorgehensweise der vom Projekt Goldener Schild eingeleiteten Zensurmaßnahmen eher dem nachträglichen Durchtrennen einer Leitung (bevor ein Antwortpaket vom Empfänger zurück zum Absender gelangt). Das liegt daran, dass der zu überwachende Netzwerkverkehr die Knotenpunkte des Projekts Goldener Schild nicht direkt passiert, sondern gesplittet und gleichzeitig zu seinem eigentlichen Empfänger gesendet wird. Auch die physikalische Position der zum Projekt Goldener Schild gehörenden Knotenpunkte ist keineswegs zentralisiert irgendwo am Rande des chinesischen Webs. Im Gegenteil, die zum Projekt Goldener Schild gehörenden Knotenpunkte sind sehr dezentral gelegen, sodass diese meistens einen lokal einigermaßen beschränkten Bereich überwachen.

Um Internetnutzer daran zu hindern, unliebsame Inhalte zu betrachten, werden verschiedene Methoden angewendet, die sich im Wesentlichen nicht besonders von den Methoden der NSA und des GCHQ unterscheiden.

Das chinesische Ministerium für Staatssicherheit filtert die Inhalte von unverschlüsselten Netzwerkpaketen nach Keywords, so wie das die NSA beispielsweise mit Google-Suchanfragen macht. Neben der Anfrage eines Benutzers wird jedoch auch der Inhalt der Serverantwort gefiltert. Kommt eine bestimmte, kritische Anzahl an Keywords in einem Paket vor, so wird die Verbindung mithilfe eines TCP-Reset-Pakets, das sowohl an den Sender als auch an den Empfänger (an diesen sogar in doppelter Ausführung) gesendet wird. Grundsätzlich gibt das Internetnutzern die Möglichkeit, Chinas „Great Firewall“ zu ignorieren, wie es Richard Clayton et al. in ihrem Artikel „Ignoring the Great Firewall of China“ [32] beschreiben. Allerdings muss dieses Verhalten sowohl vom Server als auch vom Client unterstützt werden, was den praktischen Einsatz dieses Verfahrens auf wenige Fälle einschränkt.

Wird eine Verbindung zurückgesetzt, werden für rund 20 Minuten alle weitere Verbindungsanfragen zwischen den beiden Kommunikationspartnern unterbunden.

---

[16] Daniel Anderson zitiert in seinem Artikel „Splinternet Behind the Great Firewall of China“ [41] einen Artikel aus dem Jahr 2010, der beschreibt, dass der Name Projekt Goldener Schild eigentlich für ein völlig anderes Projekt, nämlich die Implementierung eines Polizei-Intranets, steht. Da er zumindest im Deutschen, aber auch im Englischen als Synonym für das chinesische Zensursystem steht, soll er hier in diesem Kontext gebraucht werden.

Neben dem Filtern von IP-Paketen setzt das Sicherheitsministerium auch DNS Spoofing ein, um ausgewählte, unliebsame Webseiten zu blockieren. Dabei werden entweder falsche IP-Adressen oder keine Ergebnisse zurückgeliefert.

Verschlüsselt man seine Netzwerkkommunikation, beispielsweise durch die Nutzung von SSL bzw. TLS, SSH (Secure Shell) oder die Nutzung von Virtual Private Networks (VPN), um sich mit einem Rechner außerhalb von China zu verbinden, kann man zumindest verhindern, dass die Great Firewall Datenpakete auf Inhalte filtert. Trotzdem blockt das Projekt Goldener Schild Verbindungen zu bestimmten Seiten, die vom zuständigen Ministerium als unerwünscht eingestuft wurden. Außerdem berichten Menschen aus China und dort ansässige Unternehmen davon, dass verschlüsselte Verbindungen bis zur Unbenutzbarkeit verlangsamt, ja teilweise sogar vollständig unterbrochen werden. Dieses Vorgehen soll Nutzer von Verschlüsselung dazu bringen, aufgrund der damit verbundenen Unannehmlichkeiten unverschlüsselte Verbindungen zu nutzen. Eine ähnliche Idee verfolgt die NSA bei Tor-Benutzern [33].

Je nachdem wo bzw. in welchem Netzwerk sich ein Benutzer in China befindet, hat er unterschiedlich ausgeprägten Zugang zum Internet. Während Nutzer des Wissenschaftsnetzes CERNET (China Education and Research Network) zum Teil privilegierten Zugang zu bestimmten Seiten haben, wird der Rest der chinesischen Internetnutzer stark zensiert.

4.4.3 Zensur durch Gerichtsbeschlüsse, Gesetze und internationale Verträge

Um Zensur im Internet zu betreiben, bedarf es für Regierungen gar nicht immer technischer Lösungen, wie man an zahlreichen Beispielen sehen kann. Vielfach genügen Gerichtsbeschlüsse, Gesetze oder gar internationale Verträge, um unliebsame Inhalte aus dem Internet zu entfernen. Wenngleich es sich bei solchen Lösungen zumindest in Deutschland meist um die Entfernung rechtswidriger Inhalte handelt, bergen derartige Zensurmaßnahmen immerhin ein gewisses Missbrauchspotenzial. Auch das zeigen verschiedene Fälle aus der Praxis.

Egal ob im Internet oder in klassischen Medien, Zensur ist und bleibt ein sehr heikles Thema.

4.4.3.1 Zensur von Inhalten auf Twitter und YouTube in der Türkei

Im März 2014 machten die Türkei und ihr Premierpräsident Recep Tayyip Erdoğan Schlagzeilen damit, dass die Regierung die Seiten von Twitter und YouTube landesweit blockierten, nachdem über diese Plattformen Gesprächsmitschnitte aus dem türkischen Parlament verbreitet wurden [34]. Die Zensur der beiden Plattformen wurde dabei zunächst durch eine Veränderung der DNS-Einträge bei den türkischen Telekommunikationsanbietern und später durch eine Blockade der IP-Adressen erreicht [35].

Durch ein Gericht wurde diese Maßnahme nicht legitimiert. Im Gegenteil, wenige Tage später wurde diese Maßnahme der türkischen Regierung im Fall Twitter vom türkischen Verfassungsgericht für verfassungswidrig erklärt [36]. Allerdings stimmte ein anderes Gericht, das die Sperre von YouTube wenige Tage später ebenfalls als rechtswidrig einstufte, der Zensur von insgesamt 15 einzelnen Videos zu [37]. Trotz dieses Gerichtsbeschlusses ließen sich die Behörden und die Telekommunikationsanbieter mindestens 24 Stunden Zeit, das Gerichtsurteil zu ratifizieren und die Blockade der Seiten aufzuheben.

Die Tatsache, dass die Blockade einer ganzen Internetseite innerhalb eines so kurzen Zeitraums eigenmächtig von der türkischen Regierung herbeigeführt wurde, und die Tatsache, dass im Nachhinein keinerlei rechtliche Konsequenzen auf die Verantwortlichen zukamen, zeigt, wie einfach Zensur im Internet heute sein kann. Wer mittels politischer Macht Internetprovider dazu zwingen kann, Webseiten zu blockieren, der ist in der Lage dazu, Internetnutzer daran zu hindern, unliebsame Inhalte zu betrachten!

4.4.3.2 Politische Diskussionen zur Zensur des Internets in Deutschland

Auch in Deutschland werden immer wieder politische Diskussionen über Internetsperren geführt. Die Inhalte, um die es dabei geht, reichen von Kinderpornografie über „gewöhnliche“ pornografische Inhalte bis hin zu Hasspropaganda und Killerspielen. Der ein oder andere Politiker hat sich dabei durch unüberlegte Äußerungen einen neuen Spitznamen in der Netzgemeinschaft verdient.

Vor allem die Zensur von Inhalten, die gegen das Gesetz verstoßen, darunter zum Beispiel Kinderpornografie, wird häufig diskutiert. Durch die Zensur von Kinderpornografie will man beispielsweise Kinder vor Missbrauch schützen, ein grundsätzlich durchaus lobenswerter Gedanke. Doch die Kritik an Zensurprogrammen greift nicht deren Motive, sondern die Art und Weise, wie diese durchgeführt werden, an. Das verstehen viele Politiker und andere Fürsprecher derartiger Zensurmaßnahmen oft nicht. So kritisierten die Organisationen UNICEF, ECPAT, Innocence in Danger und Save the Children im Oktober 2009 die Pläne der damaligen Bundesregierung, die Sperrung von Kinderpornografieseiten auszusetzen [38]. Selbstverständlich ist es nachvollziehbar, dass zum Schutz der Kinder eine Sperrung von Seiten, die Kinderpornografie anbieten, eine naheliegende Lösung zu sein scheint, doch in Anbetracht der Tatsache, dass eine wirklich wirkungsvolle Zensur dieser Seiten eine flächendeckende Überwachung des Internets gebieten würde, und auch in Anbetracht dessen, dass eine solche Zensur das Problem ohnehin nicht lösen kann, dafür jedoch ein gewisses Missbrauchspotenzial mit sich bringt, muss man auch die Zensur von Webseiten, auf denen Inhalte veröffentlicht werden, die gegen das Gesetz verstoßen, kritisch sehen.

Die Debatte um die Zensur von Kinderpornografie im Netz, die im Jahr 2009 mit großer Leidenschaft geführt wurde, drehte sich vonseiten der Kritiker hauptsächlich um die Art und Weise, wie diese Zensur gestaltet werden sollte. Das BKA solle eine Liste mit Seiten erstellen, die von den Internetprovidern blockiert werden sollen und von denen zusätzlich direkt an das BKA berichtet werden solle, welche Nutzer versucht haben, diese Seiten aufzurufen. Das ist besonders perfide, wenn man bedenkt, dass Nutzer durchaus

versehentlich auf eine solche Seite gelangen könnten, durch die Meldung an das BKA jedoch automatisch zu Straftatverdächtigen werden.

Doch nicht nur die grundsätzliche Unschuldsvermutung der Internetnutzer wurde mit dem 2010 in Kraft getretenen und 2011 wieder aufgehobenen Gesetz zur Erschwerung des Zugangs zu kinderpornografischen Inhalten in Kommunikationsnetzen (Zugangserschwerungsgesetz – ZugErschwG)[17] unterwandert, sondern es wurde auch eine Grundlage für Zensur generell geschaffen. Auch die vom BKA geführten Listen könnten grundsätzlich dazu benutzt werden, um unliebsame Internetseiten zu sperren. Dass es durchaus Menschen mit solchen Gedanken gibt, zeigt die Aussage von Thomas Strobl, der direkt nach der Verabschiedung des Zugangserschwerungsgesetzes durch den Bundestag die Sperrung von Killerspielen ins Spiel brachte [39].

Ebenfalls einen Schritt weiter ging der CSU-Abgeordnete Norbert Geis im Sommer 2013, als er eine Sperre von Pornografie generell nach dem in Abschnitt 4.4.3.4 beschriebenen Vorbild Großbritanniens forderte. Pornografische Inhalte würden demnach von den Internetprovidern so lange blockiert werden, bis der Nutzer bei diesen die Aufhebung dieser Sperre beantrage. Das ist nicht nur aus Sicht der Privatsphäre fatal, sondern birgt auch, wie der Fall Großbritannien zeigt, ein sehr großes Missbrauchspotenzial.

4.4.3.3 Die gesetzliche Zensur von Pornografie in Großbritannien

„Is the UK Sleepwalking towards Internet Censorship?“, fragt Emma Woollacott in ihrem gleichnamigen Artikel [47] vom 27. November 2013. Ihr Fazit: Die Bestrebungen der britischen Regierung, immer mehr Inhalte im Internet zu zensieren, und vor allem das Verständnis der Bevölkerung für diese Maßnahmen lassen befürchten, dass die Bevölkerung eine zunehmend größere Akzeptanz gegenüber Zensur im Internet entwickelt. Tatsächlich scheinen die Briten die Zensurmaßnahmen ihrer Regierung, die hauptsächlich dem Kinderschutz diene, gutzuheißen, so Premierminister Cameron.

Während man durchaus noch Verständnis für die Blockade von Seiten mit kinderpornografischen Inhalten haben mag, ist die Blockade von pornografischen Inhalten generell, mit dem Ziel der Zugangserschwerung für Jugendliche, äußerst fragwürdig, doch spätestens wenn eine Regierung verkündet, aus ihrer Sicht extremistische Webseiten im Internet blockieren zu wollen, sollte man hellhörig werden! Was Regierungen zuweilen als extremistisch ansehen, haben Sie bereits im Abschnitt zu XKEYSCORE (siehe Abschnitt 4.3.5) gelesen.

Tatsächlich wird bereits durch die Filter für Zensur von Pornografie laut einem Bericht der Seite „The Independent“ fast jede fünfte Seite (19 %) der Top 100 000 Webseiten blockiert. Dabei schätzt Pam Cowburn, Sprecher der Open Rights Group, den Anteil der Seiten mit pornografischen Inhalten nur auf rund 4 Prozent. Zwar sei es abhängig vom Provider, welche Seiten tatsächlich blockiert würden, wenn man sich jedoch mithilfe der Seite *www.blocked.org.uk* die Zensurergebnisse für einige der Regierung von Groß-

[17] Der amtierende Bundespräsident Horst Köhler hatte sich zunächst geweigert, den Gesetzesbeschluss zu unterzeichnen [42].

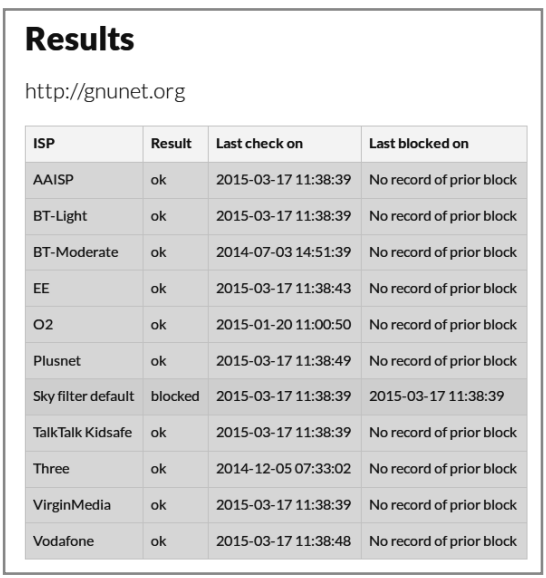
britannien sicherlich unliebsamen Webseiten ausgeben lässt, stellt man schnell fest, dass trotz allem eine ganze Reihe von Internet Service Providern Seiten, die keinesfalls pornografische Inhalte enthalten, blockieren (siehe Bild 4.11 und Bild 4.12).

Results

http://torproject.org

ISP	Result	Last check on	Last blocked on
AAISP	ok	2015-03-16 23:31:54	No record of prior block
BT-Light	ok	2015-03-16 23:31:54	2014-09-24 18:07:17
BT-Moderate	blocked	2014-07-03 16:04:53	2014-07-03 16:04:53
BT-Strict	blocked	2014-06-03 02:49:52	2014-06-03 02:49:52
EE	blocked	2015-03-16 23:32:00	2015-03-16 23:32:00
O2	blocked	2015-03-16 23:31:56	2015-03-16 23:31:56
Plusnet	ok	2015-03-16 23:32:24	No record of prior block
Sky filter default	blocked	2015-03-16 23:31:53	2015-03-16 23:31:53
TalkTalk Kidsafe	ok	2015-03-16 23:31:54	No record of prior block
TalkTalk Strict	ok	2014-07-02 20:59:29	No record of prior block
Three	blocked	2015-02-26 16:21:36	2015-02-26 16:21:36
VirginMedia	ok	2015-03-16 23:31:53	2014-11-06 22:21:13
Vodafone	ok	2015-03-17 00:04:53	2014-11-25 22:12:18

Bild 4.11
Zensur-Bericht der Seite *www.blocked.org.uk* über die Seite torproject.org vom 17. 03. 2015



Results

http://gnunet.org

ISP	Result	Last check on	Last blocked on
AAISP	ok	2015-03-17 11:38:39	No record of prior block
BT-Light	ok	2015-03-17 11:38:39	No record of prior block
BT-Moderate	ok	2014-07-03 14:51:39	No record of prior block
EE	ok	2015-03-17 11:38:43	No record of prior block
O2	ok	2015-01-20 11:00:50	No record of prior block
Plusnet	ok	2015-03-17 11:38:49	No record of prior block
Sky filter default	blocked	2015-03-17 11:38:39	2015-03-17 11:38:39
TalkTalk Kidsafe	ok	2015-03-17 11:38:39	No record of prior block
Three	ok	2014-12-05 07:33:02	No record of prior block
VirginMedia	ok	2015-03-17 11:38:39	No record of prior block
Vodafone	ok	2015-03-17 11:38:48	No record of prior block

Bild 4.12
Zensur-Bericht der Seite *www.blocked.org.uk* über die Seite gnunet.org vom 17. 03. 2015

Dass Seiten wie das Torprojekt oder die Seite von GNUnet, einer freien Peer-to-Peer-Netzwerk-Software, blockiert werden, ist äußerst dramatisch!

4.4.3.4 Regierungsanfragen zur Zensur von Inhalten durch Dienstanbieter im Internet

Die Betreiber sozialer Netzwerke und ähnlicher Plattformen erhalten nicht nur Regierungsanfragen, bei denen Nutzerdaten erfragt werden sollen, sondern teilweise auch Aufforderungen, bestimmte Inhalte zu entfernen. Während Facebook diese Anfragen leider nicht veröffentlicht, lassen sich bei Twitter und Google sehr detaillierte Auskünfte darüber, wie viele Anfragen zur Zensur von Inhalten von welchem Land eingehen, einholen. Im Grunde sprechen hier die Zahlen für sich und bedürfen keiner weiteren Interpretation (Tabelle 4.3).

Tabelle 4.3 Regierungsanfragen zur Zensur von Inhalten. Quellen: *https://www.google.com/transparencyreport/removals/government/data/?hl=en*, *https://transparency.twitter.com/removal-requests/*

		2012 HJ 1	2012 HJ 2	2013 HJ 1	2013 HJ 2	2014 HJ 1	2014 HJ 2
Türkei	Google	501	157	1673	895		
	Twitter	1	6	7	2	186	477
USA	Google	273	321	545	481		
	Twitter	0	4	2	8	31	32
Deutschland	Google	247	231	138	164		
	Twitter	0	2	4	2	2	43
Brasilien	Google	191	697	321	388		
	Twitter	0	16	10	12	8	27
Großbritannien	Google	97	103	117	132		
	Twitter	1	6	2	9	17	22

4.5 Literatur

1. *Hagger, Nicky*: Secret Power: New Zealand's Role in the International Spy Network, 1996, Craig Potton Publishing: Nelson (Neuseeland)
2. *Langenau, Lars*: Bush-Besuch: Alarmstufe eins in Mainz, Spiegel (17. Februar 2005), *http://www.spiegel.de/politik/deutschland/bush-besuch-alarmstufe-eins-in-mainz-a-342261.html*
3. *Nixon, Ron*: U.S. Postal Service Logging All Mail for Law Enforcement, The New York Times (3. Juli 2013), *http://www.nytimes.com/2013/07/04/us/monitoring-of-snail-mail.html*
4. *Gonzalez, Juan* und *Goodman, Amy*: „We Don't Live in a Free Country": Jacob Appelbaum on Being Target of Widespread Gov't Surveillance, 20. April 2012, Democracy Now, *http://www.democracynow.org/2012/4/20/we_do_not_live_in_a*
5. *Halperin, Mark* und *Heilemann, John*: Double Down – The explosive Inside Account of the 2012 Presidential Election, 7. November 2013 WH Allen
6. *Scahill, Jeremy* und *Greenwald, Glenn*: The NSA's secret role in the U.S. assassination program, 10. Februar 2014, *https://firstlook.org/theintercept/2014/02/10/the-nsas-secret-role/*
7. *Die, Bundesregierung*: Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Ulla Jelpke, Jan Korte, Dr. Petra Sitte, weiterer Abgeordneter und der Fraktion DIE LINKE: Nutzung sozialer Netzwerke zu Fahndungszwecken, 14. Juli 2011 (*http://dip21.bundestag.de/dip21/btd/17/065/1706587.pdf*)
8. *Greenwald, Glenn* und *MacAskill, Ewen*: Boundless Informant: the NSA's secret tool to track global surveillance data, 11. Juni 2013, The Guardian, *http://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining*
9. *Pitzke, Marc*: Prism-Whistleblower: „Ich erwarte nicht, mein Zuhause wiederzusehen", 10. Juni 2013, Spiegel, *http://www.spiegel.de/politik/ausland/ex-cia-mitarbeiter-outet-sich-als-prism-whistleblower-a-904676.html*
10. *Greenwald, Glenn*: No Place to hide – Edward Snowden, the NSA, and the U.S. Surveillance State, 1 (2014) Metropolitan Books: New York
11. *Greenwald, Glenn*: Die globale Überwachung: Der Fall Snowden, die amerikanischen Geheimdienste und die Folgen, 1 (2014) Droemer HC
12. *Poitras, Laura*: CITIZENFOUR, *https://citizenfourfilm.com*
13. *Greenwald, Glenn* und *MacAskill, Ewen*: NSAPrism program taps in to user data of Apple, Google and others, 07. Juni 2013, The Guardian, *http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data*
14. *CISCO*: The Zettabyte Era: Trends and Analysis (Juli 2014) *http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/VNI_Hyperconnectivity_WP.html*
15. *Neumann, Linus*: Bullshit made in Germany, 2013 (*https://www.youtube.com/watch?v=p56aVppK2W4*)
16. *http://www.alexa.com/topsites* (Stand: Dezember 2014)
17. *Gellman, Barton* und *Soltani, Ashkan*: NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say, 30. Oktober 2013, The Washington Post, *http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html?tid=pm_world_pop*

18. *Shubber*, *Kadhim*: A simple guide to GCHQ's internet surveillance programme Tempora, WIRED, 24. Juni 2013, *http://www.wired.co.uk/news/archive/2013-06/24/gchq-tempora-101*
19. Spiegel: *http://www.spiegel.de/media/media-34103.pdf*
20. *MacAskill*, *Ewen*, *Borger*, *Julian*, *Hopkins*, *Nick*, *Davies*, *Nick* und *Ball*, *James*: GCHQ taps fibre-optic cables for secret access to world's communications, the Guardian 21. Juni 2013, *http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa*
21. *MacAskill*, *Ewen*; *Borger*, *Julian*; *Hopkins*; *Nick*, *Davies*, *Nick* und *Ball*, *James*: Mastering the internet: how GCHQ set out to spy on the world wide web, the Guardian, 21. Juni 2013, *http://www.theguardian.com/uk/2013/jun/21/gchq-mastering-the-internet*
22. *Kobie*, *Nicole*: Splunk and the Squeaky Dolphin: when Big Data goes rogue, PC Pro, 28. Januar 2014*http://www.pcpro.co.uk/blogs/2014/01/28/splunk-and-the-squeaky-dolphin-when-big-data-goes-rogue*
23. *GCHQ*: Psychology – A new Kind of SIGDEV, NBC news, *http://msnbcmedia.msn.com/i/msnbc/Sections/NEWS/snowden_youtube_nbc_document.pdf*
24. Unbekannt, NSA & GCHQ, QUANTUMTHEORY, SIGINT Development Conference (2010); The Intercept – 12. März 2014, The NSA and GCHQ's QUANTUMTHEORY HACKING Tactics, *https://firstlook.org/theintercept/document/2014/03/12/nsa-gchqs-quantumtheory-hacking-tactics/*
25. *Labovitz*, *Craig*: Wikileaks Cablegate Attack, 29. November 2010, *http://www.arbornetworks.com/asert/2010/11/wikileaks-cablegate-attack/*
26. *Labovitz*, *Craig*: Round 2: DDoS Versus Wikileaks, 30. November 2010, *http://www.arbornetworks.com/asert/2010/11/round2-ddos-versus-wikileaks/*
27. *DE-CIX*: Der DE-CIX knackt die 1 Terrabit-Marke, 31. August 2010*http://presse.de-cix.net/uploads/media/PM_DE-CIX_1Terabit_final_01.pdf*
28. *Redaktion*, *Spiegel*: Quantum Spying: GCHQ Used Fake LinkedIn Pages to Target Engineers, 11. November 2013, *http://www.spiegel.de/international/world/ghcq-targets-engineers-with-fake-linkedin-pages-a-932821.html*
29. *Kolakowski*, *Nick*: GCHQ Responds to Slashdot, LinkedIn Hack, 11. November 2013, *http://news.dice.com/2013/11/11/gchq-responds-to-slashdot-linkedin-hack/*
30. *NSA*: There is More Than One Way to QUANTUM, veröffentlicht vonThe Interept, 12. März 2014*https://firstlook.org/theintercept/document/2014/03/12/one-way-quantum/*
31. *Gallagher*, *Ryan* und *Greenwald*, *Glenn*: How the NSA plans to infect ‚millions' of Computers with maleware, 12. März 2014*https://firstlook.org/theintercept/2014/03/12/nsa-plans-infect-millions-computers-malware/*
32. *Clayton*, *Richard*; *Murdoch*, *Steven J.* und *Watson*, *Robert N. M.*: Ignoring the Great Firewall of China, Proceedings of the 6th international conference in Privacy Enhancing Technologies (2006)
33. *NSA*: Tor Stinks veröffentlicht von The Guardian, *http://www.theguardian.com/world/interactive/2013/oct/04/tor-stinks-nsa-presentation-document*
34. *Gallagher*, *Sean*: Freedom-schmeedum: Turkey's government moves to „wipe out" Twitter, 21. März 2014*http://arstechnica.com/tech-policy/2014/03/freedom-shmeedum-turkeys-government-moves-to-wipe-out-twitter/*
35. *Gallagher*, *Sean*: After DNS change fails, Turkish government steps up Twitter censorship, 23. März 2014, *http://arstechnica.com/tech-policy/2014/03/after-dns-change-fails-turkish-government-steps-up-twitter-censorship/*

36. Hurriyet Daily News: Constitutional Court orders authorities to unblock Twitter, 02. April 2014, *http://www.hurriyetdailynews.com/constitutional-court-orders-authorities-to-unblock-twitter.aspx?pageID=238&nID=64481&NewsCatID=339*

37. Aljazeera: Turkey court eases YouTube restrictions, 04. April 2015, *http://www.aljazeera.com/news/europe/2014/04/turkey-court-eases-youtube-restrictions-20144492837103847.html*

38. *UNICEF*: Vorrang für Kinderschutz, 16. Oktober 2009, *http://www.unicef.de/presse/2009/vorrang-kinderschutz/36024*

39. Kölner Stadt-Anzeiger, 18. 06. 2009, *http://www.presseportal.de/pm/66749/1425454*

40. *Fischer, Sebastian*: Obamas neue Militärstrategie: Der Schattenkrieger, 01. Juni 2012, *http://www.spiegel.de/politik/ausland/obama-setzt-auf-drohnen-attacken-und-cyberwar-a-836373.html*

41. *Anderson, Daniel*: Splinternet Behind the Great Firewall of China – Once China opened its door to the world, it could not close it again, Web Security (30. November 2012) vol.10

42. Der Spiegel: Köhler verweigert Unterschrift fürs Internetsperren-Gesetz, 28. November 2009, *http://www.spiegel.de/spiegel/vorab/a-663991.html*

43. *Klein, Mark*: AT&T Whistle-Blower's Evidence, WIRED, 17. Mai 2006, *http://archive.wired.com/science/discoveries/news/2006/05/70908*

44. *Greenwald, Glenn*: No place to hide – Edward Snowden, the NSA, and the U.S. surveillance state, First Edition(2014) Metropolitan Books: New York

45. *Timberg, Craig* und *Nakashima, Ellen*: Agreements with private companies protect U.S. access to cables' data for surveillance, The Washington Post, 6. Juli 2013, *http://www.washingtonpost.com/business/technology/agreements-with-private-companies-protect-us-access-to-cables-data-for-surveillance/2013/07/06/aa5d017a-df77-11e2-b2d4-ea6d8f477a01_story.html*

46. *Applebaum, J.*; *Gibson, A.*; *Goetz, J.*; *Kabisch, V.*; *Kampf, L.* und *Ryge, L.*: NSA targets the privacy-conscious, NDR, 03. Juli 2014, *http://daserste.ndr.de/panorama/aktuell/nsa230_page-1.html*

47. *Woollacott, Emma*: Is the UK sleepwalking towards Internet Censorship?, Forbes, 27. November 2013, *http://www.forbes.com/sites/emmawoollacott/2013/11/27/is-the-uk-sleepwalking-towards-internet-censorship/*

Index

A

Adblock Plus 219
Adressbuchdiebstahl 234
Alternative für Deutschland 12, 270
Anti-Tracking-Plugins 219
Appelbaum, Jacob 152
asynchrone Kommunikation 7

B

Backbone 162
Backdoor 161
Be any IP in the World 179
Beleidigungen 262
Belgacom 175
Benutzermanipulation 8
benutzerprofilbasierte Netzwerke 2
Big Brother 277
Bildersuche 139
biometrische Verfahren 239
BLARNEY 168
Blogs 77
Bluehell Firewall 221
BOUNDLESSINFORMANT 159
browserspezifische Informationen 208
Brute-Force-Angriff 243

C

Canvas-Elemente 209
Canvas Fingerprinting 209
C-Date 95
CERNET 181
Chat 24
chatten 5
Chronik 23
Cisco Router 168
Collect it all 169
Content Delivery Network 256
Cookies 201
– Flash-Cookies 203
– löschen 282f., 285, 287
– Self-Destructing 224
Cybermobbing 264

D

Datenanalysten 170
Dating-Netzwerke 3
DE-CIX 162
De-Mail 296
Denial-of-Service-(DoS-)Angriff 173
dezentrale soziale Netzwerke 3, 76
diaspora* 76
Diskreditierung 207, 263
Domainnamen 249
Domain Name System 177
Drohnen 152
DuckDuckGo 293

E

ECHELON 149
eDarling 123
eifersüchtige Lebenspartner 140
Einbrecher 135
ElitePartner 114
E-Mail made in Germany 297
Entropie 211
ETag Tracking 204
Executive Search 47
exiftool 233

F

Facebook 19
– Einstellungen 27
– Nutzungsbedingungen 19
FAIRVIEW 168
Fingerprinting 207
Firefox 282
FiveEyes 149
Freundefinder 233
Friendica 77
FriendScout 24 128

G

GCHQ 168 f.
Gefällt-mir-Angaben 137
Geltungsdrang 269
Geolocation 227
Geotags 228
Geräteinformationen 21
geschäftliches Umfeld 47
Gesetzgeber 279
Gesichtserkennung 21, 36
gespeicherte Daten 198
Ghostery 221
Google+ 30
– Bildersuche 51
– Einstellungen 34
Google Chrome/Chromium 284
GPS-Sensoren 227
Gruppendynamiken 270
Gruppenzwang 267

H

Headhunting 47
Hintertür (siehe auch Backdoor) 161
HSTS Tracking 205
HTTPS-Everywhere 255
Hughes, Chris 19

I

Ice Bucket Challenge 268
Informations-Jamming 199
Informationskrieg 14
Informationstheorie 211
Internet
– Aufbau 162
Internet Exchange Point (IXP) 162
Internet Explorer 283
Internet Service Provider 162

J

John the Ripper 246

K

Keyserver 301
Kommunikation
– asynchrone 7
– synchrone 5
– vergängliche 66
kommunikative Netzwerke 2
kompromittierende Fotos 141

L

LinkedIn 54
Local Shared Objects 203
Lovoo 90

M

Man-in-the-Middle-Angriff 174, 254
Man-on-the-Side-Angriff 174
Matching 107
Meinungsfreiheit 151
Messenger 2
Metadaten 169, 228
Micro-Performance Benchmarks 210
Moskovitz, Dustin 19
MUSCULAR 168

N

NekNominate 267
Netzwerke
– benutzerprofilbasierte 2
– Dating-Netzwerke 3
– dezentrale soziale 3, 76
– kommunikative 2
– soziale 4
– Tier-1 165
NoScript 283
NSA 159

O

OAKSTAR 168
öffentlicher Bereich 2
Onion-Routing 289
Online-Dating 79
– Privatsphäre 140
Online-Lebenslauf 48
Open WhisperSystems 76
Orbot 292
Orbot/Orweb 232
Orweb 293
OSI-Referenzmodell 163

P

Parship 107
Passwörter 239
Passwort-Recycling 247
Peering 165
Pegida 270
persönliche Nachrichten 198
PGP 298
Phishing 248
politische Extremisten 135
politische Verfolgung 151
Pretty Good Privacy 298
PRISM 160, 168
Privatsphäre 273
Produktempfehlung 20, 192
Profil (Def.) 2
Profilbild 268
Projekt Goldener Schild 180
Protocol-Injection 172

Q

QUANTUMTHEORY HACKING 172
– QUANTUMBOT2 173
– QUANTUMCOPPER 176
– QUANTUMDNS 176
– QUANTUMINSERT 174
– QUANTUMSKY 176
– QUANTUMSQUIRREL 179

R

RedPhone 76
Regierungsanfragen 155
Room 641A 168
RSS-Feeds 78

S

Safari 286
Saverin, Eduardo 19
Schrems, Maximilian 198
Security-Token 240
Self-Destructing Cookies 224
semantische Suche 146
– Graph Search 146
Session-ID 252
Sicherheitsfrage (Facebook) 8
Skype 68
Smart-Technologie 235
S/MIME 303
Snapchat 66
Snowden, Edward 159
Social Beer Game 267
soziale Netzwerke 4
– als Kommunikationsmittel 4
Spezial-U-Boot 168
SQUEAKY DOLPHIN 170
Stalking 265
Standort-Analysen 226
Standortdienste 228
Standortinformationen 144
– Geotagging 145
STORMBREW 168
Stream 22
Suchmaschine 281
synchrone Kommunikation 5

T

TCP-Reset 180
TEMPORA 169
Terrorprävention 150
TextSecure 68
– Signal 68
Tier-1-Netzwerk 165
Tinder 84
Tor 288
Tor-Browser 226, 230, 290
traceroute 166
Tracking 201
Tracking-Unternehmen 218
transatlantische Glasfaserkabel 168

Treffpunkt18 96
Tresor 241
TrueCrypt 242
Twitter 37
– Einstellungen 41

U

Überwachung
– Briefverkehr 150
– des Netzwerkverkehrs 156
üble Nachrede 263
Umgangston 81
unverschlüsselte HTTP-Pakete 251
Upstream Collection 168, 170
User Agent 207

V

Verbrechensaufklärung 153
vergängliche Kommunikation 66
Verleumdung 263
virale Verbreitung 142
virtuelle Ermittler 154

W

Wanzen 168
Web of Trust-Browser-Plugin 249
Web-Storage 205
Whatsapp 59
Whatsapp-Kauf 62
Wickr 75
Wikileaks 173
Wireshark 156, 251
Wörterbuchattacke 245

X

XING 49
XKEYSCORE 170

Y

YouTube 45
– Kanäle 45

Z

Zahlenschloss knacken 243
Zeitaufwand für Netze 3
Zensur 8, 171
– Deutschland 182
– Großbritannien 183
– Regierungsanfragen 185
– Türkei 181
Zuckerberg, Mark 19