

# Inhaltsverzeichnis

Vorwort .....	11
Danksagungen.....	13
<b>1. Anonymität und Umgehung der Zensur .....</b>	<b>15</b>
1.1    Was bedeutet Anonymität?.....	20
1.2    Was ist Tor?.....	21
1.3    Gründe für die Verwendung von Tor.....	26
1.4    Was Tor nicht leisten kann .....	30
1.5    So funktioniert Tor .....	32
1.5.1    Bestandteile des Tor-Protokolls .....	34
1.5.2    Sichere Tunnel mit den öffentlichen Schlüsseln der Tor-Knoten aufbauen .....	36
1.5.3    Der Austrittsknoten als Vertreter des Tor-Clients .....	37
1.6    Wer verwendet Tor? .....	38
1.6.1    Normalbürger .....	39
1.6.2    Militär.....	41
1.6.3    Journalisten und ihre Leser/Zuschauer.....	41
1.6.4    Strafverfolgungsbehörden.....	42
1.6.5    Informanten und Aktivisten .....	42
1.6.6    Personen mit und ohne große Öffentlichkeitswirkung ....	42
1.6.7    Geschäftsleute und IT-Experten.....	43
1.6.8    Weitere Personen .....	43
1.6.9    Der Vorteil eines breiten Spektrums an Benutzern .....	44
1.7    Wie wird Tor verwendet? .....	46
1.7.1    Vorausplanen und Tor jetzt kennenlernen.....	47
1.7.2    TBB oder Tails? .....	48

1.7.3	Tor Browser Bundle .....	48
1.7.4	Tails .....	49
1.7.5	Vertrauen ist gut .....	49
1.8	Sichere Verwendung von Tor.....	51
1.8.1	Verwenden Sie den Tor-Browser .....	51
1.8.2	Öffnen Sie keine Dokumente .....	51
1.8.3	Installieren und aktivieren Sie keine Browser-Plug-Ins ...	52
1.8.4	Vermeiden Sie Websites ohne HTTPS .....	52
1.8.5	Verwenden Sie Bridges und suchen Sie Gesellschaft.....	52
2.	<b>Das Tor Browser Bundle .....</b>	<b>53</b>
2.1	Der Inhalt des TBB .....	53
2.1.1	Vidalia .....	54
2.1.2	Tor .....	56
2.1.3	Mozilla Firefox ESR und Torbutton .....	56
2.1.4	Weitere Inhalte .....	58
2.2	Das TBB verwenden.....	59
2.2.1	Erste Schritte.....	60
2.2.2	Das TBB starten: Windows .....	60
2.2.3	Das TBB starten: Mac OS X.....	61
2.2.4	Das TBB starten: Linux .....	61
2.2.5	Installation auf Ubuntu: GUI.....	63
2.2.6	Installation auf Ubuntu: Kommandozeile.....	63
2.2.7	Vidalia .....	66
2.2.8	Schnellzugriff .....	67
2.2.9	Logbuch.....	67
2.2.10	Tor starten/stoppen .....	68
2.2.11	Weiterleitung einrichten .....	69
2.2.12	Netzwerk betrachten .....	71
2.2.13	Eine neue Identität verwenden .....	72
2.2.14	Bandbreitengraph .....	74

2.3	Einstellungen.....	74
2.3.1	Allgemein .....	75
2.3.2	Netzwerk .....	76
2.3.3	Beteiligung.....	77
2.3.4	Dienste .....	79
2.3.5	Aussehen.....	79
2.3.6	Fortgeschritten .....	80
2.4	Den Tor-Browser verwenden .....	80
2.5	Wenn Tor keine Verbindung herstellen kann .....	81
2.5.1	Grundlegende Störungssuche .....	81
2.5.2	Brauchen Sie einen Proxy? .....	81
2.5.3	Das Logbuch einsehen.....	82
2.5.4	Tor für Firewalls einstellen .....	83
2.5.5	Wenn Tor immer noch keine Verbindung herstellen will..	83
3.	Tails .....	85
3.1	Der Umfang von Tails .....	87
3.2	Tails einrichten .....	90
3.2.1	Tails beziehen.....	90
3.2.2	Das System zum Starten von Tails einrichten.....	91
3.3	Tails verwenden .....	92
3.3.1	Tails starten.....	93
3.3.2	Tails herunterfahren .....	94
3.3.3	Tails auf einem USB-Laufwerk installieren .....	95
3.3.4	Tails manuell auf einem USB-Gerät installieren .....	97
3.3.5	Tails aktualisieren (Clone & Upgrade).....	98
3.3.6	Persistente Speicherbereiche auf dem Tails-Medium .....	99
3.3.7	Persistente Speicherbereiche einrichten .....	101
3.3.8	Whisperback.....	102
3.3.9	KeePassX .....	103

3.3.10	Metadata Anonymization Toolkit .....	103
3.3.11	Claws Mail .....	105
3.3.12	GNU Privacy Guard .....	106
4.	<b>Tor-Relays, Bridges und Ofsproxy .....</b>	107
4.1	Wenn das normale Tor nicht ausreicht .....	108
4.1.1	Wie China Tor blockiert hat .....	109
4.1.2	Ist Tor ausgefallen oder brauchen Sie eine Bridge? .....	110
4.2	Bridge-Relays .....	112
4.2.1	Bridge-Relays mithilfe der BridgeDB finden.....	114
4.2.2	Bridge-Relays per E-Mail finden.....	114
4.2.3	Andere Möglichkeiten Bridges zu finden .....	116
4.3	Tor zur Verwendung eines Bridge-Relays einrichten .....	116
4.4	Plug-In-Transportproxys und Ofsproxy .....	118
4.4.1	Plug-In-Transportproxys .....	119
4.4.2	Flash Proxy .....	120
4.4.3	Plug-In-Transportproxys verwenden .....	121
5.	<b>Tor-Ressourcen bereitstellen .....</b>	123
5.1	Einen Beitrag zum Tor-Netzwerk leisten – wie und warum?.....	123
5.2	Welche Möglichkeiten haben Sie? .....	124
5.3	Welche Risiken gehen Sie ein? .....	127
5.4	Einrichtung eines Tor-Relays .....	128
5.5	Anforderungen und Konsequenzen.....	129
5.6	Nicht-Austrittsrelay .....	130
5.7	Austrittsknoten.....	131
5.8	Bridge-Relay .....	132

6.	<b>Verborgene Tor-Dienste.....</b>	135
6.1	Gründe für die Verwendung verborgener Dienste .....	136
6.2	Funktionsweise von verborgenen Tor-Diensten.....	137
6.2.1	Das Tor-Protokoll für verborgene Dienste .....	138
6.2.2	Pseudo-URLs .....	140
6.2.3	Web-Onion-Proxys .....	142
6.2.4	Was in den Schatten lauert.....	143
6.3	Verborgene Tor-Dienste einrichten.....	144
6.3.1	Tor zum Laufen bekommen.....	145
6.3.2	Den Server installieren .....	147
6.3.3	Den verborgenen Dienst einrichten .....	148
6.3.4	Tipps, Tricks und Fallgruben .....	150
7.	<b>E-Mail-Sicherheit und Vorgehensweisen zur Förderung der Anonymität .....</b>	153
7.1	Einweg-Konten .....	155
7.1.1	10minutemail.com .....	156
7.1.2	Anonymous Email ( <a href="http://www.5ymail.com/">http://www.5ymail.com/</a> ) .....	156
7.1.3	Vermeiden Sie diese Dienste .....	157
7.2	Anonyme Remailer-Dienste .....	158
7.3	Anonyme E-Mail-Kommunikation über Tor.....	159
7.4	Anonyme E-Mail-Kommunikation als verborgener Tor-Dienst .....	161
7.5	Anonymität und Pseudonymität .....	161
7.6	Tipps für die anonyme E-Mail-Kommunikation .....	162
7.6.1	Die Anonymität bei der E-Mail-Kommunikation wahren	163
7.6.2	Verwenden Sie immer Tor .....	164
7.6.3	Verwenden Sie stets HTTPS .....	165
7.7	Schritt für Schritt: Ein anonymes E-Mail-Konto einrichten .....	165

<b>A.</b>	<b>Validierung der Tor-Software.....</b>	<b>167</b>
A.1	Tor-Software mit GNU Privacy Guard validieren .....	167
A.2	Tails-Distributionen mit GnuPG validieren .....	171
A.3	Mit welchen PGP-Schlüsseln sind welche Pakete signiert?.....	174
<b>B.</b>	<b>Wenn Tor-Downloads gesperrt werden .....</b>	<b>181</b>
B.1	Tor-Spiegel .....	182
B.2	Tor per E-Mail .....	183
B.3	Weitere Möglichkeiten.....	184
<b>C.</b>	<b>Hilfe suchen und Antworten erhalten .....</b>	<b>185</b>
C.1	Tor .....	186
C.1.1	Bug-Tracker/Wiki.....	186
C.1.2	Tor-FAQ .....	187
C.1.3	Tor-Dokumentation.....	188
C.1.4	Verbogene Tor-Server .....	188
C.2	Das Tor-Projekt .....	189
C.2.1	Kontaktinformationen.....	189
C.2.2	Menschen und Organisationen hinter dem Tor-Projekt	190
	<b>Stichwortverzeichnis.....</b>	<b>191</b>