

Inhaltsverzeichnis

Vorwort	9
1 Warum es die Öffentlichkeit nichts angeht, dass Sie nichts zu verbergen haben	13
1.1 Was Sie in diesem Buch finden werden (und was nicht)	14
1.2 Reden ist Silber – Ihre persönlichen Daten als Ware und Zahlungsmittel	15
1.3 Das Recht, Dinge für sich zu behalten	19
1.3.1 Vorhersagen durch Statistik: der Blick in die Glaskugel	20
1.3.2 Wenn die Glaskugel irrt	22
1.3.3 Ein bisschen Privatsphäre, bitte!	24
1.4 Die vier Ziele der Computersicherheit	28
1.5 Sicherheit vs. Bequemlichkeit	30
2 Grundregeln und Hintergründe der digitalen Privatsphäre	35
2.1 Grundlagen der Kryptografie	35
2.1.1 Bob trifft Alice	35
2.1.2 Symmetrische Verschlüsselung – ein Tresor für Nachrichten .	36
2.1.3 Asymmetrische Verschlüsselung – der Tresor mit Schnappschloss	42
2.1.4 Hybride Verschlüsselung	44
2.2 Gute und schlechte Passwörter – hundenname123	47
2.3 Tipps für gute Passwörter	47
2.3.1 Hashfunktionen	48
2.4 Web of Trust und Zertifizierungsstellen – Vertrauen im Netz	51
2.4.1 Digitale Signatur	53
2.4.2 Die Zertifizierungsstelle (CA)	54
2.4.3 Zertifizierung im Web of Trust (WoT)	56
2.5 Vertrauen ist gut, Open Source ist besser	60
2.5.1 Closed Source	60
2.5.2 Open Source	61
2.5.3 Vertrauen ist gut, Kontrolle ist besser	61
2.6 Sicherheit offline – Schultersurfen & Co.	62
2.6.1 Impersonating	63
2.6.2 Phishing	64

2.6.3	Shoulder Surfing	64
2.6.4	Dumpster Diving	65
3	Sicher surfen im Web	67
3.1	Das Internet in der Nussschale	67
3.1.1	Kurze Geschichte des WWW	68
3.1.2	Das Hypertext Transfer Protocol (HTTP)	69
3.1.2.1	Die Anfrage – Request	69
3.1.2.2	Die Antwort – Response	70
3.1.3	Hypertext Markup Language (HTML)	71
3.1.4	Sicheres HTTP: HTTPS	72
3.1.4.1	Verschlüsselte Verbindungen erkennen	73
3.1.4.2	HTTPS Everywhere	75
3.2	Ihr Browser und Sie	75
3.2.1	Welcher Browser für welchen Nutzer?	78
3.2.1.1	Geschwindigkeit	80
3.2.1.2	Komfort	81
3.2.1.3	Sicherheit	81
3.2.1.4	Integrierte Suche und Auswahl einer Suchmaschine	84
3.2.1.5	Synchronisation von Einstellungen über mehrere Geräte hinweg	86
3.2.1.6	Lesezeichen	86
3.2.1.7	Privates Fenster/Inkognito-Modus	86
3.2.1.8	Passwort-Manager	86
3.2.1.9	Verschiedene Browser-Profile (Identitäten)	87
3.2.1.10	Add-ons	87
3.2.2	Die Chronik – eine Einstellungssache	87
3.2.3	Der Cache – des Browsers Kurzzeitgedächtnis	88
3.2.4	Add-ons – die Zubehörpalette	90
3.2.5	Ausblick	92
3.3	Cookies – digitale Krümelmonster	93
3.4	Gefällt mir? Werbetacking, Like-Button und Browser-Fingerprints	95
3.5	Digitale Springteufel: Pop-ups	99
3.6	Freud und Leid mit JavaScript & Co.	100
3.6.1	Ein Hintertürchen für den Angreifer: JavaScript und XSS	100
3.6.2	Standortbestimmung: Wo bin ich und warum?	104
3.6.3	Plug-ins	105
3.7	Inkognito im Netz – anonym surfen	109
3.7.1	Proxy – Browsen über einen Stellvertreter	111
3.7.2	Tor – anonymes Browsen nach dem Zwiebelprinzip	112

4	Sicheres E-Mailen	117
4.1	Wie funktioniert E-Mail?	117
4.1.1	E-Mail – die Anfänge	118
4.1.2	Die E-Mail-Adresse	119
4.1.3	Der Aufbau einer E-Mail-Nachricht	119
4.1.4	E-Mails senden und empfangen	121
4.1.5	Sicher e-mailen	124
4.2	Outlook, Thunderbird, OS X Mail & Co. – der E-Mail-Client	126
4.3	GMail, GMX, WEB.DE & Co. – Vor- und Nachteile webbasierter Clients	128
4.4	De-Mail – sicher per Gesetz?	131
4.5	»Ziemlich einfache« Verschlüsselung mit PEP	133
4.6	Vertrauensbasis gemeinsame Freunde – PGP und GPG nutzen	134
4.6.1	Was sind PGP und GPG?	134
4.6.2	Gpg4win für Microsoft Outlook unter Windows	136
4.6.3	Enigmail und GnuPG für Thunderbird unter Linux oder Windows	138
4.6.4	GPG Suite für OS X	145
4.7	Vertrauensbasis neutrale Autorität – S/MIME nutzen	149
4.7.1	Was ist S/MIME?	149
4.7.2	S/MIME für Windows	152
4.7.3	S/MIME für Linux	154
4.7.4	S/MIME für OS X	155
4.8	Herausforderung sicheres E-Mailen auf dem Smartphone	156
4.8.1	PGP und S/MIME für Android	156
4.8.2	PGP und S/MIME für iOS	159
5	Sicheres Chatten, Instant Messaging und SMS	161
5.1	Quatschen digital – die Basics	161
5.2	Von Laptop zu Laptop	163
5.2.1	Grüße aus den 90ern – ICQ und AIM	163
5.2.2	XMPP/Jabber	164
5.2.3	Dieses Gespräch hat nicht stattgefunden – Off-the-Record-Messaging (OTR)	167
5.2.3.1	OTR mit Pidgin unter Linux oder Windows	168
5.2.3.2	OTR mit Adium unter OS X	170
5.2.4	Die Oma in Australien – Skype, Hangouts und sichere Alternativen	173
5.3	Problemzone Smartphone (Android, iOS)	179
5.3.1	Die gute alte SMS	179
5.3.2	WhatsApp – die Ablösung für SMS	181

| Inhaltsverzeichnis

5.3.3	Threema – kommerziell, aber sicher?	182
5.3.4	TextSecure und Signal – die Open-Source-Lösung	185
5.3.5	IM und Chat: auf dem Laufenden bleiben	189
6	Blick über den Tellerrand	191
6.1	Metadaten – Ihr Smartphone weiß, was Sie letzten Sommer getan haben	191
6.2	Der Laptop im Hofbräuhaus – kleine Übersicht über Festplattenver- schlüsselung	194
6.2.1	Dateiverschlüsselung	196
6.2.2	Verschlüsselte Container	197
6.2.3	Dateisystem- und Geräteverschlüsselung	199
6.2.4	Hardwareverschlüsselung	200
6.3	Exkurs Kryptografie im Alltag: Neuer Personalausweis und Gesund- heitskarte	201
6.4	A rose by any other name – Pseudonymität und Anonymität	206
6.5	Für Vergessliche und solche, die es werden wollen – Passwort-Manager	208
6.6	Tunnel durch Feindesland – VPNs	212
6.7	Was dem Merckelfon fehlte – verschlüsselte Telefonie	214
6.8	Das eigene Betriebssystem immer dabei – Linux on a Stick	217
6.9	Kritische Masse: Verschlüsselung setzt sich durch	222
	Glossar	225
	Stichwortverzeichnis	233