

Stichwortverzeichnis

A

- Abstreitbarkeit 167
- Adblocker 96
 - Adblock Plus 96
 - Disconnect 96
 - Ghostery 96
 - Privacy Badger 96
 - uBlock 97
- Add-on
 - Browser 87, 90
 - E-Mail-Client 126
 - Enigmail *siehe* Enigmail
 - GpgOL 137
 - Mailvelope 130, 132
 - Thunderbird 139
- Adium 170
- Advanced Programming Interface (API) 90, 182
- Android
 - Android Privacy Guard (App) 156
 - K9 Mail (E-Mail-Client) 156
 - OpenKeychain (App) 156
 - PGP 156
 - R2Mail2 (E-Mail-Client) 158
 - S/MIME 156
- Anonymität 206
- AOL Instant Messenger (AIM) 164
- Apple Mail
 - PGP 145
 - S/MIME 155
- Authentifizierung 167, 169, 176, 179
 - Adium 172
 - Multifaktor- 201
 - Pidgin 169
- Authentizität 29, 54, 56

B

- Bequemlichkeit 30
- Bitcoin 110
- Blackberry 215
- Bookmarks *siehe* Favoriten
- Browser 68, 75
 - Add-on 87, 90
 - Apple Safari 77
 - Cache 88
 - Chromium 78
 - Chronik 87
 - Fingerprinting 85, 98
 - Google Chrome 77
 - HTML-Engine 80
 - Hygiene 88
 - Iceweasel 78
 - Inkognito-Modus 86
 - integrierte Suche 84
 - Internet Explorer 77
 - Konqueror 78
 - Microsoft Edge 92
 - Midori 78
 - Mosaic 68
 - Mozilla Firefox 68, 76
 - Netscape Navigator 68
 - Opera 77
 - Plug-in 87
 - Profile (Identitäten) 87
 - Synchronisation von Einstellungen 86
 - Web (Epiphany) 78
- Buffer Overflow 82
- Bugs 82
- Bundesamt für Sicherheit in der Informationstechnik (BSI) 215

C

Caesar-Chiffre 36
Certificate Authority *siehe* Zertifizierungsstelle
Chain of Trust *siehe* Web of Trust
Chaos Computer Club (CCC) 133
Chat 161
Chiffre 36
Claws 136, 220
Closed Source 61
Compiler 60
Cookies 93
– Flash-Cookies 95
– Supercookies 95
Cross-Site-Scripting (XSS) 100
– Cookie-Diebstahl 101
cryptocheck.de 142
Cryptoparty 60, 210

D

Dark Web 110
Dateisystemverschlüsselung 199
– BitLocker 199
– FileVault 199
Datenschutzgesetz 27
– Bundesdatenschutzgesetz 25
– Landesdatenschutzgesetze 25
Datensparsamkeit 27
Datenverarbeitung 27
Datenvermeidung 27
De-Mail 131
Defcon 180
Device-Mapper 199
Diffie-Hellman-Verfahren 44, 216
digitale Identität 207
digitale Signatur 53, 134
Domain Name Server (DNS)
– DNSSEC 126

E

e-Card *siehe* elektronische Gesundheitskarte (eGK)
E-Mail 117
– Client 122, 126, 128
– De-Mail 131
– E-Mail made in Germany 133

– E-Mail-Adresse 119
– Header 121
– Provider 129, 131, 139
– Server 122
Eingangsverschlüsselung 125
Electronic Frontier Foundation (EFF) 75, 96, 113, 189
– Secure Messaging Scorecard 189
elektronische Gesundheitskarte (eGK) 203
– elektronische Patientenakte (EPA) 204
– elektronisches Rezept (eRezept) 204
– Notfalldatensatz 204
elektronische Identifikationsfunktion (eID) 202
elektronischer Heilberufsausweis (HBA) 204
Ende-zu-Ende-Verschlüsselung 125, 167
– OTR 167
– Threema 182
Enigmail 138

F

Facebook 19
– Apps 19
– Cookies 95
– Datenschutz 28
– Instant Messaging 166
– Kauf von WhatsApp 181
– Like-Button 95
Favoriten 86
Festplatte 66
– löschen 66
Festplattenverschlüsselung 194
Firewall 111

G

gematik 204
Geo-Lock 214
Geolocation *siehe* Standortbestimmung
Geolokalisierung *siehe* Standortbestimmung
Gewinnspiele 21
Glättli, Balthasar 193
GnuPG (GPG) *siehe* Pretty Good Privacy (PGP)
Google 16
– Datenschutz 28
– Geschäftsmodell 18

Google Hangouts 166, 175
 GPG Suite (OS X) 145
 Greenwald, Glenn 217

H

Hardwareverschlüsselung 200
 Hashfunktion 48, 54
 – Hashabelle 50
 – Hashwert 49
 – Kollision 49
 – MD5 51
 Hippokratischer Eid 24
 Hopper, Grace 82
 Hyperlinks *siehe* Links
 Hypertext Markup Language (HTML)
 68, 71
 Hypertext Transfer Protocol (HTTP) 67
 – Extended-Validation-Zertifikate 73
 – HTTP/2 73
 – HTTPS Everywhere 75
 – Hypertext Transfer Protocol Secure
 (HTTPS) 72
 – Request 69
 – Response 70

I

ICQ 163
 – OSCAR 164
 Identitätsdiebstahl 23
 Instant Messaging (IM) 161
 – Adium *siehe* Adium
 – AIM *siehe* AOL Instant Messenger
 (AIM)
 – alternative Clients 164
 – ICQ *siehe* ICQ
 – Miranda 170
 – Pidgin *siehe* Pidgin
 – Signal *siehe* Signal
 – Skype *siehe* Skype
 – TextSecure *siehe* TextSecure
 – Threema *siehe* Threema
 – WhatsApp *siehe* WhatsApp
 – XMPP (Jabber) *siehe* XMPP (Jabber)
 – Yahoo Messenger 164
 Integrität 29, 54

Internet Exchange Point (IXP) 109
 Internet Message Access Protocol Version 4
 (IMAP4) 123
 Internet Relay Chat (IRC) 161
 iOS
 – iPGMail (App) 159
 – NetPGP 160
 – oPenGP (App) 159
 – PGP 159
 – S/MIME 159, 160
 ISO-Image 219

J

JavaScript 80, 100
 – JavaScript-Engine 80
 Jitsi 175

K

Kasper Systems *siehe* Threema
 Key Server *siehe* Schlüsselservers
 Key-Signing-Party *siehe* Cryptoparty
 Kleine-Welt-Phänomen 58
 Kleopatra 137
 kostenlos 18
 Kredit 23
 Kreditwürdigkeit 22
 Kryptografie 15, 35
 – Alice, Bob und Eve 35

L

Lesezeichen *siehe* Favoriten
 Links 68

M

Mail (Client) *siehe* Apple Mail
 Man-in-the-Middle-Attacke 52, 173, 180, 182,
 183, 187
 – IMSI-Catcher 180
 McAfee 135
 Merkel, Angela 214
 Metadaten 110, 121, 174, 191
 – MetaPhone (App) 192
 Microsoft Outlook
 – PGP 136
 – S/MIME 152

| Stichwortverzeichnis

- Mobilfunknetz
 - GSM 180
 - LTE 180
 - UMTS 180
- Mozilla Foundation 76
- Mozilla Thunderbird
 - PGP 138
 - S/MIME 154
- Multimedia-Plug-ins 105
 - Flash 105
 - Java 105
 - QuickTime Player 105
 - Shockwave 105
 - Silverlight 105
- O**
- Obama, Barack 214
- Off the record (OTR) 41, 167
- Onlinebanking 72
- Open Source 60, 138
- Open Whisper Systems 185
- OpenPGP *siehe* Pretty Good Privacy (PGP)
- OpenPGP-Assistent *siehe* Enigmail
- Outlook *siehe* Microsoft Outlook
- P**
- Partition 199
- Passwörter 32, 47, 208
 - Brute-Force-Angriff 47
 - cracken 50
 - Entropie 48
 - erraten 47
 - gute 47
 - Passphrase 45, 141
 - Passwort-Manager 48, 86, 208, 220
 - regelbasierte Attacke 51
 - Wörterbuchattacke 51
- Patch 82
- Peer-to-peer 166
- Perfect Forward Secrecy 41, 167, 185, 216
- Personalausweis
 - Geschichte 202
 - neuer Personalausweis (nPA) 201
- personenbezogene Daten 26
- PGP *siehe* Pretty Good Privacy (PGP)
- Pidgin 168
- Poitras, Laura 217
- Pop-up-Fenster 99
- Post Office Protocol Version 3 (POP3) 123
- Post Privacy 24, 31
- Posteo 126, 131
- Predictive Analytics 21
- Pretty Easy Privacy (PEP) 133, 160
- Pretty Good Privacy (PGP) 134
 - Dateiverschlüsselung 197
 - Enigmail *siehe* Enigmail
 - Gpg4win 136
 - Inline-PGP 143
 - PGP/MIME 143
 - Schlüsselverwaltung *siehe* Schlüsselverwaltung
 - Widerrufszertifikat *siehe* Widerrufszertifikat
- Primzahlen 42
- Prism Break 152, 158
- Privatsphäre 13, 24, 25, 207
- Programmcode *siehe* Quellcode
- Proxy-Server 111
- Pseudonym *siehe* Pseudonymität
- Pseudonymität 206
- Public-Key-Infrastruktur 55
- Public-Key-Kryptografie *siehe* Pretty Good Privacy (PGP), *siehe* Secure/Multi-purpose Internet Mail Extensions (S/MIME)
- Public-Key-Verfahren *siehe* Verschlüsselung
- Pufferüberlauf *siehe* Buffer Overflow
- Q**
- QR-Code 183
- Qualifizierte Elektronische Signatur (QES) 202
- Quantencomputer 43
- Quellcode 61
- quelloffen *siehe* Open Source
- R**
- Recht auf informationelle Selbstbestimmung 25
- Redphone 216
- Reverse Engineering 164

S

S/MIME *siehe* Secure/Multipurpose Internet Mail Extensions (S/MIME)

Samsung 215

Schlüsselservers 52, 135, 143, 148

- Schlüsselservers-Problem 135

Schlüsselverwaltung 138, 143, 147, 152, 155

SCHUFA 21

Schweigepflicht 24

Secure Real-Time Transport Protocol (SRTP) 216

Secure Sockets Layer *siehe* Transport Layer Security (TLS)

Secure/Multipurpose Internet Mail Extensions (S/MIME) 149

- Comodo (Zertifizierungsstelle) 151
- Schlüsselverwaltung *siehe* Schlüsselverwaltung
- X.509 151
- Zertifikate 150
- Zertifikatsverwaltung *siehe* Schlüsselverwaltung

Secusmart 215

Short Message Service (SMS) 161, 179, 185

- SMS-Daumen 161

Siedsma, Ton 193

Signal 185, 188, 217

Silk Road 110

Simple Mail Transfer Protocol (SMTP) 123

Skriptblocker

- NoScript 102
- QuickJava 102

Skype 164, 173

- Supernode 174

Smartphone 64, 214

- PGP 156
- S/MIME 156

SMS *siehe* Short Message Service (SMS)

Snowden, Edward 14, 214, 217

Social Engineering 62

- Dumpster Diving 65
- Impersonating 63
- Phishing 64, 117
- Shoulder Surfing 64, 125

Software-Updates 82

Source Code *siehe* Quellcode

Spam 117

Spitz, Malte 193

Standortbestimmung 104

- GPS 104
- IP-Adresse 104

Stasi 25

Statistik 20

Suchmaschinen

- alternative 85
- Filterbubble 84

T

T-Systems 215

Tails 128, 218

- Claws *siehe* Claws

Target 20

TextSecure 185

The Onion Routing *siehe* Tor-Netzwerk

Threema 181, 182

Thunderbird *siehe* Mozilla Thunderbird

Tor-Netzwerk 113

Tracking 95

- Do not track 98

Transport Layer Security (TLS) 72, 124, 133

Transportverschlüsselung 124, 126, 133

TrueCrypt 197

U

Überwachung 13, 25

Uniform Resource Locator (URL) 70

V

VeraCrypt 198

Verfügbarkeit 29

verschlüsselte Container 198

- TrueCrypt *siehe* TrueCrypt
- unsichtbare Container 198
- VeraCrypt *siehe* VeraCrypt

Verschlüsselung

- asymmetrisch 42
- Fingerabdruck eines öffentlichen Schlüssels 54, 144
- Geheimtext 36
- hybride 44, 134
- Klartext 36

| Stichwortverzeichnis

- Länge des Schlüssels 38
- privater Schlüssel 42, 129, 141, 147
- rot13 39
- rot26 39
- Schlüssel 36
- Schlüsselübergabe 40
- symmetrisch 36, 39
- öffentlicher Schlüssel 42, 142

Vertraulichkeit 29

Videochat

- Google Hangouts *siehe* Google Hangouts
- Jitsi *siehe* Jitsi
- Skype *siehe* Skype

Virtual Private Network (VPN) 212

- IPSec 213
- PPTP 213
- tinc 213

Voice over IP (VoIP) 216

Volkszählungsurteil (1983) 25

Vorratsdatenspeicherung (VDS) 110

W

Web of Trust 51, 53, 56, 134, 145

Webbrowser *siehe* Browser

Webseite 71

- Quellcode 71

Werbetracking *siehe* Tracking

Werbung 16

WhatsApp 181

- Verschlüsselung 181

Widerrufszertifikat 142

World Wide Web (WWW) 67

X

XKCD 32

XMPP (Jabber) 164

- Jabber-ID 165

- Jingle 166, 178

- PGP 166

- Server 165

- WhatsApp 181

Z

Z Real-time Transportation Protocol (ZRTP)
178, 216

Zertifikatsautorität *siehe* Zertifizierungsstelle

Zertifizierungsstelle 51, 53, 54, 149

- Root-CA (Wurzelzertifizierungsstelle) 55,
150

Ziele der Computersicherheit 28

- Authentizität *siehe* Authentizität

- Integrität *siehe* Integrität

- Verfügbarkeit *siehe* Verfügbarkeit

- Vertraulichkeit *siehe* Vertraulichkeit